ORF ISSUE BRIEF
OCTOBER 2020
ISSUE NO. 412

Ensuring Cyber Security in India's Nuclear Systems

Pulkit Mohan

ABSTRACT Cyber security should take centrestage in nuclear-policymaking. This brief evaluates the current state of cyber security in India's civilian and military nuclear systems, as gleaned from both incidents of breach on-ground and analyses in the public discourse. It outlines the level of threats faced in this domain, and makes a case for the development of policy measures for an integrated cyber-nuclear security strategy.

Attribution: Pulkit Mohan, "Cyber Security in India's Nuclear Systems," *ORF Issue Brief No. 412, October 2020*, Observer Research Foundation.

INTRODUCTION

Cyber security is a pillar of nuclear security.[1] Various incidents in different parts of the world have demonstrated the vulnerability of nuclear facilities to cyber threats. (See Table 1)

In India, there has historically been little attention to cyber risks pertaining to civilian and military nuclear facilities. Overall, India's cyber security policy has remained inadequate amidst the changing and emerging threats of cyber warfare and attacks, especially in critical sectors such as nuclear energy. In late 2019, the Indian Space Research Organisation (ISRO) headquarters in Bengaluru and the Kudankulam nuclear power plant in Tamil Nadu both suffered breaches in their security.[6]

To begin with, defining 'nuclear security' will be helpful in understanding the systems in place for the protection of nuclear establishments. As defined by the International Atomic Energy Agency (IAEA), nuclear security is "the prevention of, detection of, and response to, criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities, or associated activities."[7] The sensitive nature of nuclear command, control and communications (NC3) systems, and of nuclear facilities, calls for a powerful security architecture that accounts for consequences emerging from physical

Table 1: Incidents of cyber-attacks on nuclear systems

COUNTRY & ATTACK SITE	YEAR	TYPE OF CYBER-ATTACK	COMPONENTS AFFECTED
United States [2] **Davis-Besse Nuclear Power Plant**	2003	Slammer computer worm	Compromised the safety control system for over four hours
Iran [3] **Natanz uranium enrichment plant**	2010	Stuxnet computer worm	Plant's computer software and nuclear centrifuges were infected and damaged
United States [4] **Hanford nuclear site**	2015	Hacking	Two Chinese hackers were indicted in 2020; believed to have targeted the site to gain information about individuals involved in the development of the atomic bomb during the Cold War
Germany [5] **Gundremmingen nuclear power plant**	2016	W32.Ramnit and Conficker viruses	Viruses infected the computer systems and USB drives; did not pose a direct threat to plant's operating systems.

and cyber threats and attacks. Similarly, understanding the concept of 'cyber security' can guide policymakers in determining its connection with nuclear security measures. Although there is no single definition of 'cyber security', a useful definition in this context is the following: "the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security."[8] The term 'cyber threats', meanwhile, encompasses a range of threats including cyber terrorism,[a] cyber espionage,[b] malware attacks,[c] and distributed denial of service (DDoS).[d]

As cyber technologies have become more seamlessly integrated in the infrastructure and architecture of nuclear systems, the risks of their hacking, disruptions, and sabotage have also heightened. Vulnerable cyber security mechanisms and outdated cyber security technologies and practices increase the risks associated with the functioning of nuclear facilities. The intersection of cyber security and nuclear security, therefore, is an immediate concern.

NUCLEAR SYSTEMS AND FACILITIES: KEY RISKS

Nuclear establishments and NC3 systems predate the cyber risks and threats to their security that have emerged in the recent years. To reduce the cyber risks at nuclear facilities, the threats that exist must first be identified, to begin with. Vulnerabilities in the operation of nuclear systems include, but are not limited to the following: [9]

- communications between command and control centres;
- communications from command stations to missile platforms (e.g. submarines) and missiles;
- telemetry data from missiles to ground- and space-based command and control assets;

a Cyber terrorism refers to the intersection of unlawful terrorist activities with cyberspace through attacks on computer networks and associated information and technologies. See https://www.usip.org/sites/default/files/sr119.pdf

b Cyber espionage refers to the use of computer systems to illegally gain access to confidential information of organisations such as governments. See https://law.emory.edu/elj/content/volume-66/issue-3/articles/cyber-espionage-electronic-surveillance-media-coverage.html

c Malware attacks are those attacks on computer systems and networks through the introduction of malicious software such as viruses, works, spyware etc. See https://digitalguardian.com/blog/what-malware-definition-tips-malware-prevention

d DDoS attacks are designed to disrupt or suspend normal services of a targeted network by overwhelming the server which compromises the effectiveness of the system. See https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack/

- analytical centres for gathering and interpreting long-term and real-time intelligence;
- cyber technologies in transport;
- cyber technologies in laboratories and assembly facilities;
- pre-launch targeting information for upload;
- real-time targeting information from space-based systems including positional, navigational, and timing data from global navigational systems;
- real-time weather information from space-, air-, and ground-based sensors;
- positioning data for launch platforms (e.g. submarines);
- real-time targeting information from ground stations;
- communications between allied command centres; and
- robotic autonomous systems within the strategic infrastructure.

The risks are multi-dimensional: from hardware and software vulnerabilities of operating systems, to faulty defences and network vulnerabilities. A cyber-nuclear security nexus also demands an assessment of the origins of the threats (i.e. actor-specific threats). Threats can emerge from state actors,[10] non-state actors (such as terrorist organisations, hackers, lone-actors),[11] and insiders.[e] Cyber threats present a unique challenge and therefore require addressing both the role of adversaries and the uncertainty that comes from cyber vulnerabilities. Given the sensitivity around nuclear weapons systems and their management, creating a more aware and well-incorporated cyber-nuclear security infrastructure will be instrumental in countering the increasing vulnerabilities.

Consequences of Cyber Attacks and their Implications on Nuclear Security

The severity of a cyber-attack can be determined by the level of access gained through such an attack. In the context of military nuclear systems, for example, an adversary's ability to gain access into the NC3 systems holds specific and multi-level implications. If an adversary gains access to the command and control infrastructure of a nuclear weapons system, they would have the ability to defeat the security of the weapons and possibly conduct an unauthorised launch or use of nuclear warheads or missiles.[12] Cyber breaches

e "Insider threat' is "a security risk to an organization that comes from within the business itself. It may originate with current or former employees, contractors or any other business associates that have – or have had – access to an organization's data and computer systems." https://awakesecurity.com/glossary/insider-threat/

increase the likelihood of vulnerabilities in nuclear systems. Infiltration of malware or viruses into the systems can occur at a number of stages in the production and supply chain.[13] This could occur through embedded codes in conventional and nuclear weapons[14] which may be used to compromise the weapons in the case of a conflict or their ability to act as deterrents.

Disruptive cyber-attacks also provide adversaries with the opportunity to undermine communications systems between individuals responsible for nuclear weapons systems and the system itself, thus preventing the flow of information, obtaining confidential information, disrupting dual-use communications, overloading key communication networks, and preventing the use of communication channels to de-escalate a crisis situation.[15]

Cyber-attacks have economic, operational and reputational costs[16] to the country. Given the dynamics involved in possessing and maintaining nuclear systems, it is important to acknowledge the consequences of a breach. More importantly, a cyber-attack on a specific component exposes vulnerabilities in the entire system; this should call for a rehaul of the security practices and infrastructure at every level. Any breach of safety gives rise to distrust of the systems and may negatively impact relations with allies and adversaries alike, and call into question the reliability of a country possessing nuclear weapons.[17]

The human factor in determining cyber threats to nuclear systems cannot be ignored. Nuclear systems and their security is predicated upon human judgement and is "therefore vulnerable to human fallibility".[18] There is the possibility of false information from warning systems as a result of human error, which could be an accident or a deliberate act.[19]

There is also the risk of insider threat. After all, nuclear systems are managed and operated by individuals with different security clearances, which also exposes the structure to cyber infiltrations from within. In this context, insider threat could manifest in ways such as creating and exploiting software vulnerabilities, introducing viruses, and sharing critical information with adversaries.[20] In the context of nuclear security, the insider threat has been often articulated but requires measures in the cyber domain as well. Nuclear systems are susceptible to cyber risks across the supply chain, and therefore there is a need to tackle this at the level of both technology and personnel.

THE INDIAN CONTEXT

The importance of cyber security of the nuclear architecture is not any different for India. In 2018, according to an internet security threat report issued by security software company Symantec, India was amongst the top five nations in the world that are facing cyber threats and targeted attacks.[21] In 2013, the Department of Electronics and Information Technology released a policy framework—the first of its kind—to articulate a national cyber security

policy. The policy document sets out guidelines and objectives for the protection of the country against cyber-attacks. This policy was created in the aftermath of the Snowden leaks,[f] which suggested that the US National Security Agency (NSA) was spying on Indian citizens—made possible by the absence of appropriate cyber safeguards in India.[22] With the unveiling of the policy, the government articulated the importance of addressing the risks and vulnerabilities that came with cyberspace,[g] which has already become a pillar of public and private infrastructure.[23] The government also announced the setting up of a 'Defence Cyber Agency' that will create mechanisms within the security infrastructure to battle cyberwarfare and cyber infiltration in India's defence networks.[24] India also has a National Technical Research Organisation (NTRO) tasked with the country's "cyber intelligence and cyber counter intelligence";[25] the body is independent of the technical wings of other government agencies.

The 2013 policy identifies a number of strategies that must be adopted to create a secure cyber ecosystem in terms of best practices, establishing standards and mechanisms for information, identifying and classifying risk perceptions, periodic verification, and testing of the effectiveness of cyber security measures.[26] However, the policy has been implemented in a rather lackadaisical manner, and there is little discussion, if at all, around how the policy should be executed across India.

Indeed, although the 2013 policy is comprehensive, it is not exhaustive. It has also not been updated in the past seven years to articulate a more effective approach to cyber threats, given the exponential progress in cyber technology that has occurred over this time period. In addition to the policy, a national-level 'Computer Emergency Response Team (CERT-In), created in 2004, works to coordinate all efforts undertaken for "cyber security emergency response and crisis management."[27] CERT-In remains one of India's key efforts to address issues of cyber security and has been extensively involved in international collaborations in creating a more robust cyber security system in India.[h]

---

f Edward Snowden is an American whistleblower and a former contractor for the Central Intelligence Agency (CIA). He was responsible for leaking classified information from the US' National Security Agency (NSA) pertaining to numerous surveillance programs conducted by American intelligence agencies across the world. The news about the Snowden leaks broke out in June 2013 and included surveillance programs for countries like China, Germany, France, India and several others. See https://www.bbc.com/news/world-us-canada-23123964

g The Indian government describes the cyberspace as "a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks." https://nciipc.gov.in/documents/National_Cyber_Security_Policy-2013.pdf

h CERT-In releases annual reports which highlight its major activities such as incident reports, international collaboration, events and initiatives. The annual reports are useful in looking at the broader cyber security infrastructure as well as the level of threats and vulnerabilities in India. They can be accessed here: https://www.cert-in.org.in/s2cMainServlet?pageid=PUBANULREPRT

The 2013 policy is lacking in any explicit mention of the correlation between cyber and nuclear security. The document is more general in its security objectives and strategies pertaining to the cyber security of government infrastructure. There is a need to respond to the possible challenges and failures of standard operating procedures in this context at an inter-agency level through enhanced coordination and continued collaboration in building a strong cyber security culture.

In September 2019, the cyber-attack on India's Kudankulam Nuclear Power Plant[28] highlighted the importance of strengthening the country's cyber-nuclear security infrastructure. The government confirmed the malware attack on the administrative system, while assuring the public that no plant control or instrumentation had been affected.[29] Cyber security researchers suggested that the attack was caused by a DTRACK virus[i] developed by a group linked to North Korea; these reports, however, were not corroborated by the Indian government.[30] ISRO also confirmed that it was alerted to a breach attempt by the same virus that targeted Kudankulam.[31] While it is important to note the government's acknowledgement that the attack was limited to the administrative systems, it still exposed the serious vulnerabilities in the security of the country's nuclear facilities. It has been noted in previous instances of cyber-attacks that air-gaps provide limited protection on their own and are often under-maintained.[32] A large amount of data had been taken from the administrative network, implying the possibility of future attacks on more critical systems at the plant.[33] It is important to strengthen systems against cyber threats using preventive access tools such as "firewalls, anti-virus programs, air gaps and unidirectional gateways."[34]

A new Cyber Security Policy is expected to be released in 2020. Any new policy must fill the inadequacies in the current one, to ensure that India can address the evolving challenges to cyber security in the nuclear domain.

A FRAMEWORK FOR INDIA'S CYBER-NUCLEAR SECURITY POLICY

The nuclear security architecture in India is shrouded in secrecy[35] and the effectiveness of the country's cyber security infrastructure leaves much to be desired. It is important to advocate for a robust and well-articulated approach to mitigate the potential consequences of cyber-attacks. The Kudankulam breach highlighted the outdated nature of India's approach to cyber defence mechanisms; while there exists a cyber-security policy, it largely fails to inspire confidence.[36]

To begin with, there is no mechanism in place where the public can be informed

i DTRACK is a malware developed by a North Korean hacker group called Lazarus which allows hackers to gain remote access and control to a device and extract data remotely. See https://www.indiatoday.in/india/story/kudankulam-nuclear-power-plant-dtrack-north-korea-atms-1614200-2019-10-30

of any breach of the country's cyber and nuclear infrastructure. The information on the Kudankulam incident, for instance, is ambiguous and does little to address the larger discussions around cyber security at nuclear facilities. This leads one to argue that threats to India's cyber-nuclear security architecture, as discussed in the larger context, remain largely "unresolved, undeveloped and, to some extent, unrecognised."[37]

Going forward, it is important to build an adaptive, reliable and robust system of cyber threat analysis, to identify actionable channels in the entire nuclear security establishment. A few possible additional measures may serve as the first important steps towards a more robust and resilient system in countering the cyber-nuclear security threat.

India would do well to draw lessons from the experiences of other countries in strengthening the cyber protection of their nuclear infrastructure. Countries like the United States (US), United Kingdom (UK) and Japan, for example, have managed to nurture advanced cyber-security systems and mechanisms to protect their nuclear infrastructure. (See Table 2)

Indian policymakers must also engage in multilateral dialogues to help develop appropriate international regulatory frameworks, norms and institutions for cyber and nuclear security. In bilateral terms, India could work with partners and allies like Japan and Australia to facilitate cooperation and promote sharing of best practices in this domain.[50]

As mentioned in CERT-In annual reports,[51] India is involved in international collaborations in the context of cyber security in general. These can be extended to cyber-nuclear security, specifically in the case of civilian nuclear facilities. There is immense potential, in this regard, for India to engage with experts to develop its own cyber-nuclear security infrastructure and extend it to other parts of its nuclear establishment without fear of oversharing sensitive information or technologies.

In the context of the global supply chain, a number of tools and instruments involved in India's infrastructure are imported and not indigenously produced. Infiltration of malware can happen at any stage during the supply chain. It can lay dormant for an extended period of time within any component and result in a lax approach towards the equipment or system. Therefore, the resilience of said supply chain to cyber risks must be examined. Strong policies should be adopted in terms of "sourcing, vendor management, supply chain continuity and quality, transportation security."[52] There also needs to be an effort to educate and create awareness of cyber vulnerabilities within the nuclear establishment.[53] It is essential to normalise the practice of and commitment to managing cyber threats and promote its importance across all personnel. This in turn will strengthen measures in addressing insider threats.

Table 2. Cyber security policies of Japan, the United Kingdom, and United States

	Japan	US	UK
Key governing body/act	Basic Act on Cyber security (Act No. 104 of November 12, 2014.[38]	United States Cyber Command[39]	National Cyber Security Centre[40]
Mission	Free, fair and secure cyberspace, protection from cyber-attacks and disruption of social systems.[41]	Cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners	Practical guidance of cyber security, response to cyber incidents, collaboration with industry experts, reduction of risks by securing public and private networks
Identification	Actors involved in critical information for national security need to keep in mind that critical information could become a possible target of global cyber attackers[42]	Virtual private networks and hidden supply chain connections, privilege escalation, roaming notebooks, wireless access points, embedded exploits in software and hardware, or maintenance entry points[43]	Cyber security is identified as a Tier 1 threat in the National Security Strategy (alongside terrorism, war and natural disasters)[44]
Measures & counter-measures	Relevant actors will work to increase awareness of cybersecurity for all people involved in advanced technology, and take necessary measures, including: enhancing monitoring of and response capabilities against cyber-attacks from abroad; tightening the examination and verification of goods and services obtained externally; strengthening collaboration between the public and private sectors for information sharing and others **Nuclear:** Calls for strong public-private partnerships to protect critical information infrastructure (CII) Consider information-sharing arrangements for the protection of nuclear materials[45]	Improve supply chain management, risk management, information technology activities, strengthen, security of sensitive government information, improve transportation cyber security[46] **Nuclear:** Modernising its integrated communications system to have efficient and integrated nuclear systems[47]	Close coordination with the National Crime Agency. Develop cyber skills, provide threat intelligence and expert advice with government and industry professionals Work closely with individuals and agencies involved in owning and operating critical national infrastructure to ensure essential services.[48] **Nuclear:** Protect civilian nuclear sector against cyber-attacks. Build resilience to detect, mitigate and contain cyber-attacks.[49]

Cyber threats in India's security establishment are exacerbated by the lack of inter-agency coordination in developing countermeasures as well as a gap in information-sharing. This needs to be upgraded. Furthermore, in the context of cyber-nuclear security, India would benefit from clear demarcations of roles in the

case of preparation, accountability and examination. It is important to advocate for creating a resilient and accountable framework that rewards policies, behaviours and measures that promote cyber-security in the nuclear domain.

CONCLUSION

Given the rapid nature of technological advancements, cyber security should be a key consideration while modernising nuclear systems and facilities.[54] Government agencies should be at the forefront of technological advancements and develop measures to prepare for consequences across procedures and scenarios, even as the participation of the private sector is encouraged.

Indeed, threats are constantly evolving and the risks to critical infrastructure cannot be ignored. The onus to mitigate these risks lies with a country's ability to develop robust cyber security measures that account for existing threats and allow for necessary changes for those others that may not exist yet. Faced with challenges associated with the modernisation of nuclear systems, and the concomitant emerging threats from state and non-state actors, the discussion around cyber security should be a continuous one and involve more stakeholders. ORF

ABOUT THE AUTHOR

Pulkit Mohan is a Junior Fellow at ORF.

ENDNOTES

1 Vesselin Giaurov, "The Cyber-Nuclear Security Threat: Managing the Risks," *Vienna Center for Disarmament and Non-Proliferation*, (January 2017), 1, http://large.stanford.edu/courses/2017/ph241/bunner2/docs/giaurov_2017.pdf

2 Brent Kesler, "The Vulnerabilities of Nuclear Facilities to Cyber Attack," *Stanford Strategic Insights,* (Spring 2011), 20

3 David Kushner, "The Real Story of Stuxnet," *IEEE Spectrum,* February 26, 2013, https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

4 Kip Hill, "Chinese nationals indicted in Eastern Washington on charges of hacking Hanford," *The Spokesman Review*, July 21, 2020, https://www.spokesman.com/stories/2020/jul/21/chinese-nationals-indicted-in-eastern-washington-o/

5 Christoph Steitz and Eric Auchard," German nuclear plant infected with computer viruses, operator says," *Reuters,* April 27, 2016, https://www.reuters.com/article/us-nuclearpower-cyber-germany-idUSKCN0XN2OS

6 Jay Mazoomdar, "Not only Kudankulam, ISRO, too, was alerted of cyber security breach," *The Indian Express*, November 6, 2019, https://indianexpress.com/article/india/not-only-kudankulam-isro-too-was-alerted-of-cyber-security-breach-6105184/

7 "Nuclear Security Series Glossary," *International Atomic Energy Agency*, Version 1.3, (November 2015), https://www.iaea.org/sites/default/files/18/08/nuclear-security-series-glossary-v1-3.pdf

8 Juliana De Groot, "What is Cyber Security? Definition, Best Practices & More," *Data Insider: Digital Guardian's Blog*, https://digitalguardian.com/blog/what-cyber-security

9 Patricia Lewis and Beyza Unal, "Cyber Threats and Nuclear Weapons Systems," in *Understanding Nuclear Weapon Risks* ed. John Borrie, Tim Caughley and Wilfred Wan (UNIDIR, 2017), 61, https://www.unidir.org/files/publications/pdfs/understanding-nuclear-weapon-risks-en-676.pdf

10 Patricia Lewis and Beyza Unal, "Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences," *Chatham House*, https://www.chathamhouse.org/sites/default/files/publications/research/2018-01-11-cybersecurity-nuclear-weapons-unal-lewis-final.pdf

11 Lewis and Unal, "Cyber Threats"

12 Page O. Stoutland and Samantha Pitts-Kiefer, "Nuclear Weapons in the New Cyber Age," *Nuclear Threat Initiative,* (September 2018), 12, https://media.nti.org/documents/Cyber_report_finalsmall.pdf

13 Lewis and Unal, "Cyber Threats," 12

14 Stoutland and Pitts-Kiefer, "Nuclear Weapons," 18

15 Stoutland and Pitts-Kiefer, "Nuclear Weapons," 16

16 Lewis and Unal, "Cyber Threats," 19

17 Lewis and Unal, "Cyber Threats," 19

18 Lewis and Unal, "Cyber Threats," 8

19 Stoutland and Pitts-Kiefer, "Nuclear Weapons," 12

20 Stoutland and Pitts-Kiefer, "Nuclear Weapons," 9

21 "India ranks 3rd among nations facing most cyber threats: Symantec," *Economic Times,* April 4, 2018, https://economictimes.indiatimes.com/tech/internet/india-ranks-3rd-among-nations-facing-most-cyber-threats-symantec/articleshow/63616106.cms?from=mdr

22 Glenn Greenwald and Shobhan Saxena, "India among top targets of spying by NSA," *The Hindu,* September 23, 2013, https://www.thehindu.com/news/national/india-among-top-targets-of-spying-by-nsa/article5157526.ece

23 "National Cyber Security Policy 2013," Ministry of Communications and Information Technology (India), 3-4, https://nciipc.gov.in/documents/National_Cyber_Security_Policy-2013.pdf

24 National Cyber Security Policy 2013, 3-4

25 R.S. Bedi, "NTRO: India's Technical Intelligence Agency," *Indian Defence Review,* April 23, 2015, http://www.indiandefencereview.com/spotlights/ntro-indias-technical-intelligence-agency/

26 National Cyber Security Policy 2013, 7-9

27 National Cyber Security Policy 2013, 10

28 Binayak Dasgupta and Sudhi Ranjan Sen, "Cyber attack at Kudankulam; critical system safe," *Hindustan Times*, October 30, 2019, https://www.hindustantimes.com/india-news/cyber-attack-on-kudankulam-plant-network-not-possible/story-4b5QiRVGuTtTi4MlOexadL.html

29 Utpal Bhaskar, "India confirms malware attack at Kudankulam nuclear power plant," *Live Mint*, November 20, 2019, https://www.livemint.com/news/india/india-confirms-malware-attack-at-kudankulam-nuclear-power-plant-11574262777163.html

30 Debak Das, "An Indian nuclear power plant suffered a cyberattack. Here's what you need to know," *The Washington Post*, November 4, 2019, https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/

31 "ISRO confirms it was alerted about DTRACK malware during Chandrayaan 2, says it had no impact," *First Post*, November 10, 2019, https://www.firstpost.com/tech/science/isro-confirms-it-was-alerted-about-dtrack-malware-during-chandrayaan-2-says-it-had-no-impact-7626131.html

32 Éireann Leverett, "Cyber Insurance for Civil Nuclear Facilities: Risks and Opportunities," *Chatham House*, May 8, 2019, 4-5

33 Das, "An Indian nuclear power plant suffered a cyberattack"

34 Alexander Van Dine, Michael Assante and Page Stoutland, "Outpacing Cyber Threats: Priorities for Cybersecurity at Nuclear Facilities," *Nuclear Threat Initiative*, (2016), 15, https://media.nti.org/documents/NTI_CyberThreats__FINAL.pdf

35 Sitakanta Mishra, "'Secrecy as Security Strategy' in India's Nuclear Governance," *Kalinga Institute of Indo-Pacific Studies,* October 27, 2019, http://www.kiips.in/research/secrecy-as-security-strategy-in-indias-nuclear-governance/

36 Das, "An Indian nuclear power plant suffered a cyberattack"

37 Giaurov, "The Cyber-Nuclear Security Threat," 1

38 "Cybersecurity Strategy," *Government of Japan*, September 4, 2015, 5, https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf

39 "Mission and Vision," *United States Cyber Command*, https://www.cybercom.mil/About/Mission-and-Vision/

40 "National Cyber Security Centre," *Government of United Kingdo*, https://www.ncsc.gov.uk

41 "Cybersecurity Strategy" Japan

42 "Cybersecurity Strategy, Japan", 26

43 John Borrie, Tim Caughley and Wilfred Wan, "Understanding Nuclear Weapon Risks," *UNIDIR*, April 10, 2017, 64-65, https://www.unidir.org/files/publications/pdfs/understanding-nuclear-weapon-risks-en-676.pdf

44 "The Cyber Threat," *GCHQ*, https://www.gchq.gov.uk/information/cyber-threat

45 "Cybersecurity Strategy" Japan

46 "National Cyber Strategy," *Government of United States of America*, September 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

47 Borrie, Caughley and Wan, "Understanding Nuclear Weapons Risks"

48 "The Cyber Threat," *GCHQ*

49 "Civil Nuclear Cyber Security Strategy," *Department for Business, Energy and Industrial Strategy*, February 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/591619/170213_-_Civil_Nuclear_Cyber_Security_Strategy.pdf

50 Stoutland and Pitts-Kiefer, "Nuclear Weapons," 28

51 "Annual Report," Indian Computer Emergency Response Team, *Ministry of Electronics and Information Technology*, https://www.cert-in.org.in/s2cMainServlet?pageid=PUBANULREPRT

52 Giaurov, "The Cyber-Nuclear Security Threat," 15

53 Giaurov, "The Cyber-Nuclear Security Threat," 12

54 Stoutland and Pitts-Kiefer, "Nuclear Weapons," 25

OBSERVER RESEARCH FOUNDATION
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