INSTITUTE FOR DEFENCE
STUDIES & ANALYSES
रक्षा अध्ययन एवं विश्लेषण संस्थान

IDSA
Issue Brief

Kudankulam:
One Incident, Many Facets

Cherian Samuel & Munish Sharma

December 17, 2019

Summary

This issue brief examines the breach of the administrative network of the Kudankulam Nuclear Power Plant in an attempt to achieve greater clarity on the incident, its fallout, and the larger questions it raises about the security of critical information infrastructure.

A malware infection in the IT network of the Kudankulam Nuclear Power Plant (KKNPP) located in Tamil Nadu was first reported in social media on October 28.[1] The coincidental shutdown of one of the plants in the preceding week led to speculations that the two were connected. An initial official response from the plant authorities refuted these reports.[2] Subsequently, officials from other agencies including office of the National Cyber Security Coordinator (NCSC) confirmed these reports, and the Nuclear Power Corporation of India Limited (NPCIL) – the parent body responsible for running the nuclear power plants in the country – came out with an official press release giving some details of the incident. In its October 30 press release, the NPCIL clarified that the infected personal computer was in use for administrative purposes only, and the control systems of the plant and critical functions were unaffected by the breach.[3] These details were later confirmed by the Union Minister of State for the Department of Atomic Energy in the Parliament on November 20.[4]

The breach of a critical information infrastructure, particularly in the nuclear domain, cannot be taken lightly. It also affords an opportunity to review existing security practices and address the lacunae, where found. Now that much of the dust has settled down, this issue brief seeks to examine the incident and address the larger questions it raises about the security of critical information infrastructure.

Security of the Control Systems: A Backgrounder

Nuclear power is considered to be pivotal to the energy security of developed and developing countries alike. At present, around 10 per cent of the global electricity need is met by 450 nuclear power reactors in 30 countries, with a total installed capacity of around 394 GWe.[5] Given the vulnerability of nuclear installations to accidental, adversarial, and environmental events – Chernobyl in 1986, Stuxnet in 2010, and Fukushima disaster in 2011 – they have been subject to tight safety regulations. Nuclear programmes and research facilities themselves are of great strategic vlue, and they are closely guarded – physically as well as otherwise.

Not surprisingly, they are often found to be a prime target of espionage operations. Cyberspace has just added a whole new dimension to the debates on nuclear safety and security. Information technology (IT) and operational technology (OT), for

[1] "Kudankulam nuclear power plant denies being victim of cyber spy attack," *India Today*, October 29, 2019 (Accessed December 12, 2019).

[2] Ibid.

[3] NPCIL Press Release, *Nuclear Power Corporation of India Limited*, October 30, 2019 (Accessed December 02, 2019).

[4] "Cyber Attack on KKNPP," Unstarred Question No. 659, *Lok Sabha, Parliament of India*, November 20, 2019 (Accessed December 12, 2019).

[5] "World Nuclear Performance Report 2018," *World Nuclear Association*, August 2018 (Accessed November 14, 2019).

business needs and safety and control systems respectively, has become a new front for clandestine operations and has opened vast opportunities for both espionage and sabotage. In the OT space, Industrial Control Systems (ICS)[6] remain the prime target as they control the core functions and physical processes in industrial plants. Their unavailability, incapacitation, degradation or destruction could have physical consequences. In the case of nuclear installations, at the extreme, it could be the release of radioactive material in the environment.

In a nuclear power plant, ICS perform a host of monitoring, supervision and control functions, such as reactor protection systems, safety features actuation systems (emergency core cooling), safe shutdown systems, emergency power supply and diesel generator control systems, reactor control systems and access control systems. Digital ICS were inducted for enhanced reliability, improved performance and efficiency, regulatory compliance, and safety requisites. ICS could also be termed as the nervous system of a nuclear power plant as they are not just the interface with physical parameters of the plant operations (monitoring the vital parameters such as neutron flux, temperature, pressure and flow), but they also monitor abnormalities through plant health diagnostic systems and adjust the physical processes through control and safety systems.[7] Sensors and actuators are placed in every nook and corner of a nuclear power plant to ensure that temperatures, pressures and flow rates, etc. remain well within the design limits. To prevent untoward incidents, of the likes of core meltdown, reactor protection systems monitor operational variables and initiate a shut down if pre-defined thresholds are passed.

ICS are, therefore, responsible for critical safety functions such as quick boron injection, containment spray, and high pressure safety injection. In a nuclear power plant, systems and networks associated with safety, security, emergency preparedness, and their support systems are termed as Critical Systems. They are designed to withstand seismic and environmental events and built with heightened defences against cyber-attacks so that they can safely shut down the reactor and prevent any radioactive release in the environment.

These are the same control systems which the October 29 KKNPP press release stated to be "not connected to outside cyber network and Internet"[8], or in other terms, air gapped. That notwithstanding, ICS are increasingly being connected to the corporate

[6] These systems include Distributed Control Systems (DCS), Supervisory Control and Data Acquisition (SCADA) systems, Programmable Logic Controllerers (PLC), Remote Telemetry Units (RTU), etc. SCADA is generally used to control dispersed assets using centralised data acquisition and supervisory control. DCS is generally used to control production systems within a local area such as a factory using supervisory and regulatory control. PLC is generally used for discrete control for specific applications and generally provide regulatory control.

[7] "Instrumentation and Control (I&C) Systems in Nuclear Power Plants: A Time of Transition," *International Atomic Energy Agency*, p. 4.

[8] no.1.

business systems, built with remote access capabilities, and are being designed using industry standard computers, operating systems and network protocols. To prevent any inadvertent exposure of the ICS, they are isolated from the corporate or the IT network of the facility. Though air gaps can provide some basic level of protection to the critical systems from untargeted cyber threats, they are inadequate in the face of threats arising from determined and well-resourced adversaries to the nuclear industry. ICS remain vulnerable to risks such as unauthorised changes to instructions, commands, or alarm thresholds, inaccurate information sent to system operators, initiation of inappropriate actions, modifications to software or configuration settings, and interference with the operation of equipment protection systems or of safety systems,[9] especially since many of the software systems used for plant operations are sourced from different companies.

Therefore, stringent controls and security practices are put in place to reduce the risks to ICS and the control network of nuclear power plants from cyber-attacks. Beyond air gapping, these practices vary from the basics such as restricting use of media, personal computers, laptops, etc. to heightening defences using data flow restriction, deep package inspection, deployment of firewalls (packet filtering, stateful inspection, and application-proxy gateway) and intrusion detection systems (network-based and host-based), authentication and authorisation controls, implementing intermediate demilitarised zone (DMZ) network, and consistent monitoring, logging, and auditing.

Nuclear facilities have been a prime target of both espionage and sabotage operations in the past. The Nuclear Threat Initiative (NTI) enlists around 23 cyber incidents at nuclear facilities over the last three decades — owing to a multitude of threat actors and vectors such as software error, espionage, data theft, employee attempted sabotage, network intrusion, spear-phishing, and so forth.[10] Stuxnet remains one of the most discussed and referenced cyber incidents, where PLCs were commandeered to sabotage the centrifuges at Iran's Natanz uranium enrichment plant. The cyber incident at KKNPP is going to be a new addition to this list, and it is worthwhile to look at the various motivational factors behind this incident.

One Incident: Many Inferences

The October 29 press release made it quite clear that the control systems at KKNPP are air gapped and the cyber-attack is not possible. However, air gapping alone cannot fully warrant security from cyber-attacks. Heightened defences make it hard for the adversary to access gapped systems, but certainly not an impossible task.

[9] Keith Stouffer et al., "Guide to Industrial Control Systems (ICS) Security," NIST Special Publication 800-82, *National Institute of Standards and Technology, US Department of Commerce*, May 2015, p. 2.

[10] "References for Cyber Incidents at Nuclear Facilities," *Nuclear Threat Initiative* (Accessed December 01, 2019).

Stuxnet remains a prime example of how air gapped systems could be breached. A politically motivated adversary or a well-funded state proxy can have the requisite resources, technical know-how and wherewithal to target IT and control networks. Such attacks need meticulous planning and precise information about the instruments deployed at the facility, its design and process flow documentation. Since business sensitive and classified information traverses over IT networks, and are stored and processed over IT systems, they are an obvious and a soft target to gather sensitive information. It could further be used in perpetrating malicious and hostile acts which could disable, destroy or compromise the computer resource critical to the security or safety of the facility.[11]

The October 30 NPCIL press release conceded that a personal computer connected to the IT network at KKNPP was found infected with the malware.[12] However, the press release explicitly clarified that the plant systems were not affected, and the infected computer was meant for administrative purpose only. Since the infected machine was a personal computer deployed for administrative functions, it could have either carried personal information of the employees, their addresses, email communications, browsing history or information related to procurement, tenders, finance and other aspect of day-to-day administration of the plant. This information might seem irrelevant at the face value, but it could very well be used for precise phishing attacks on the employees, contractors or vendors possibly for a much more serious intrusion. The Indian Computer Emergency Response Team (CERT-In) is currently investigating the malware incursion along with specialists from the Department of Atomic Energy and other agencies.

There is no denying that the infected computer could possibly have been used to gather information (classified or otherwise) or to harvest login credentials of the users or the administrator to perpetrate an attack. CERT-In had notified the authorities in early September,[13] but it is quite likely that the malware was residing on the network before it was detected. The possibility of a much more widespread infection cannot be ruled out either since cleaning operations are still underway. Malware for espionage operations are designed to spread through the network and can still remain undetected. The identified computer might have been the one interfacing the external command and control server, or in other words, could be just the tip of the iceberg. The true extent of the malware infection is hard to assess and it would never be disclosed. However, the incident has given rise to many speculations.

[11] "Computer Security at Nuclear Facilities," Technical Guidance/Reference Manual, Nuclear Security Series No. 17, *International Atomic Energy Agency*, 2011, p. 2.

[12] no. 3. As an operational imperative, any industrial plant needs an IT network for business needs such as reporting, office automation, email communication, etc. beyond the operations of the plant.

[13] Ibid.

Security researchers analysing the available evidence were of the opinion that the Lazarus group of hackers were behind this malware, that it was custom made to gain access to the IT network of KKNPP, and that those controlling the malware probably had access to the entire IT network.[14] Lazarus is a North Korea-based hacker group, held responsible for the 2013 cyber-attacks in South Korea and WannaCry ransomware attacks in the United Kingdom (UK) in 2017. The Seoul-based group of malware analysts, Issue Makers Lab, which has vast expertise in analysing malware of North Korean origin, also produced evidence supporting this argument.[15]

Prima facie, this seems to have been an espionage operation which means that the attackers were either looking for information specific to KKNPP or about the nuclear programme. Again, information related to the Indian nuclear programme has two aspects – the weapons programme and the three-stage nuclear energy programme. Since the reactors at KKNPP are placed under the International Atomic Energy Agency (IAEA) safeguards,[16] the fuel (1.6-4.1 per cent enriched uranium) and spent fuel is accounted for at each and every step even though India can reprocess the spent fuel and retain the plutonium, but strictly for civil use.[17] Moreover, Russia is supplying the fuel for KKNPP. These facts make KKNPP an inappropriate target to seek information either on India's uranium enrichment programme, or details on the nuclear weapons programme.

The fact that KKNPP houses two units of Russian made VVER-1000 (AES-92) pressurised water reactors (PWRs) also weakens the argument that the attackers were looking for information related to India's indigenous three-stage nuclear power programme which is based on a thorium fuel cycle. The three-stage programme utilises pressurised heavy water reactors (PHWRs) in Stage I, fast breeder reactors in Stage II, and thorium based breeder reactors in Stage III.[18] NPCIL operates two boiling water reactors, 18 PHWRs and two PWRs which are installed at KKNPP. The PWR technology is neither developed indigenously by India nor does it have any pertinent role in India's three-stage nuclear power programme. India's competency lies in PHWR technology. Therefore, KKNPP in itself holds little value as a target of espionage seeking information regarding India's nuclear programme, either civil or

[14] Debak Das, "An Indian nuclear power plant suffered a cyberattack. Here's what you need to know," *The Washington Post*, November 04, 2019; Sean Gallagher, "Indian nuclear power plant's network was hacked, officials confirm," *Ars Technica*, October 30, 2019; and Catalin Cimpanu, "Confirmed: North Korean malware found on Indian nuclear plant's network," *ZDNet*, October 30, 2019 (Accessed December 12, 2019).

[15] Issue Makers Lab, Twitter Post, November 02, 2019, 9:21 PM (Accessed December 12, 2019).

[16] Y. K. Pandey and Ashok Chauhan, "Fuel Management of VVER-1000 Reactors of Kudankulam Nuclear Power Plant, India," *Nuclear Power of Corporation of India Limited*, p. 2.

[17] "Nuclear Power in India," *World Nuclear Association*, Updated February 2019 (Accessed November 14, 2019).

[18] "Thorium fuel cycle in India: Three-stage Indian Nuclear Power Programme," *Bhabha Atomic Research Centre, Department of Atomic Energy, Government of India* (Accessed November 14, 2019).

weapons. That could also mean that the whole operation ran much deeper or wider; KKNPP being just one of the points where it was detected.

Beyond the circumstantial evidence, as produced by the Issue Makers Lab, the sole motive for North Korea to perpetrate this incident rests on the fact that it has been working on its light water reactor[19] for a long time now and is desperately looking for the associated technology. North Korea was assured of the Soviet assistance with light water reactor technology when it joined the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) in 1985.[20] It desired to withdraw from the Treaty to pursue military nuclear ambitions, but an Agreed Framework in 1994, which even promised America-led assistance for the replacement of its graphite-moderated reactors with light water reactor power plants of approximately 2000 MW throughput, was designed to put pressure on it to desist from pulling out of the Treaty.[21] However, this never fructified and North Korea finally withdrew from the NPT in 2003.

North Korea has since followed an aggressive nuclear weapons programme. In 2010, it even announced its intention to build an indigenous light water reactor. An experimental light water reactor at the Yongbyon Atomic Energy Research Centre is part of this endeavour. The attack could possibly be a North Korean attempt to gather as much as information available on LWR technology. India is one of the few countries with whom North Korea enjoys good diplomatic relations. India is also the second largest trade partner of North Korea after China. Hacking a nuclear power plant network – either IT or OT – would have serious ramifications, even risking diplomatic and trade ties. These considerations reduce the likelihood of this incident being a state-authorised attack.

Another facet of this attack points to the possibility that KKNPP was merely a means to an end. Russia has supplied the same VVER-1000 reactors to another five countries including China and Iran. The model V-466 is installed at Bushehr facility in Iran.[22] The Iranian nuclear programme remains a prime target of espionage and sabotage operations. The possibility that KKNPP was used to gather information on the VVER-1000 reactor which could be used for a sabotage operation at an Iranian facility cannot be ruled out outright. It also leads to another possibility of the Lazarus group acting at the behest of another state to either pass on harvested information or simply to ring an alarm among the populace about insecure nuclear power plants, most sensitive amongst the critical infrastructure. Else, the attackers were just

[19] Boiling Water Reactor and Pressurised Water Reactor are the two types of Light Water Reactor.

[20] "North Korea," *Nuclear Threat Initiative*, Last Updated October 2018 (Accessed November 26, 2019).

[21] "Agreed Framework of 21 October 1994 Between the United States of America and the Democratic People's Republic of Korea," INFCIRC/457, *International Atomic Energy Agency*, November 02, 1994, p. 1.

[22] "The VVER Today: Evolution, Design, Safety," *ROSATOM*, p. 13 (Accessed December 11, 2019).

imitating the modus operandi of the Lazarus group to direct the needle of suspicion at them, something that has happened earlier.

Post-Incident Response

The fear of accidents and radiation creates a lot of apprehension among the wider populace in the case of nuclear power plants. Thus, the official response must be prompt and factual. In the current incident, there was quite a bit of unnecessary confusion and obfuscation in the initial response which led to much social media frenzy. Media reports were often contradictory, with attribution to various unnamed government officials in the absence of a single point of contact for information. As a case in point, at last count, newspaper reports have credited no less than three different government agencies with discovery of the intrusion, along with sundry other private companies, and even friendly foreign governments.[23] By way of comparison, the entire public communication in the case of WannaCry Ransomware incident in the UK was handled by a single entity – the National Cyber Security Centre. Therefore, in the face of cyber-attacks with nationwide significance, designating a lead investigating agency is not just reassuring but also helps in reducing the scope for misinterpretation and disinformation.

Questions have also been raised as to why such attacks on critical infrastructure cannot be deterred or prevented by government agencies. Prevention was successful to the extent that attackers were only able to access the administrative network, as per the official notifications. According to Kaspersky, the most effective measures against the DTrack malware that was used to infiltrate the Kudankulam network includes strong network security and password policies, and constant monitoring of the network for any abnormal activities.[24] However, that may not be enough to deter a determined adversary. A more proactive approach would require measures such as monitoring the dark web as well as taking cognisance of the new threat vectors, such as vulnerabilities in third-party vendors since most functions are increasingly being outsourced. Most of the recent high-profile attacks have been through third-party vendors, which range from cloud providers to security intelligence companies. Efforts to reduce the threat surface by mandating measures such as certifying third-party

[23] Binayak Dasgupta and Sudhi Ranjan Sen, "Admin computer network of Kudankulam nuclear plant breached by hackers based abroad," *The Print*, October 30, 2019; Karishma Mehrotra, "Kudankulam nuclear plant denies hacking of its control system, officials say audit found breach," *The Indian Express*, October 30, 2019; and "Nuclear Power Corporation Confirms Presence of Malware in System at Kudankulam Plant," *The Indian Express*, October 30, 2019 (Accessed December 11, 2019).

[24] Konstantin Zykov, "Hello! My Name Is Dtrack," *Securelist*, *Kaspersky*, September 23, 2019 (Accessed December 12, 2019).

vendors for critical infrastructure notwithstanding, the attack surface is only set to increase as dependency on such third party vendors increases.

Technical and forensic attribution has to be coupled with a broader approach that takes into account the means, motives and methods of the perpetrators in order to have a better visibility and awareness of where the next attack might come from. This will help authorities to be better prepared to recognise such attacks and have measures in place to respond and shut them down. There have been calls to take punitive actions against the perpetrators, to serve as a warning and to deter others from undertaking such actions. The fear of a strong response to an attack and the scale or severity of the retaliation strengthens deterrence by punishment. Failure to punish the guilty weakens the deterrence posture. However, this requires precise attribution, which is difficult in a space where false flag operations, designed to place the blame on a third party are a norm rather than the exception.

None of the major cyber incidents in India have ever been officially attributed, whether to a foreign entity, government or any other threat actor. It must be understood that attribution with high probability is to the core the practice of deterrence by punishment.[25] The existing approach to cyber security is heavily tilted towards practising deterrence by denial, essentially by building defences. Be that as it may, countries like the United States that have the capacity and wherewithal to define the "redlines" of acceptable and unacceptable behaviour in cyberspace, essential to practice deterrence by punishment, have not had much success in deterring attacks on their cyber-infrastructure. Evidently, the concept of deterrence needs further tweaking to make it workable in cyberspace.

International co-operation in cyber-security has been more of a rhetoric, limited to delivering aspirational statements at various fora with very little progress in practical terms. The 2015 UN Group of Governmental Experts (UN GGE) had declared that "A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public."[26] This was one of the 11 norms to be followed by states in cyberspace. The UN GGE report was accepted by the UN General Assembly in 2016 but several follow-up reports and proposals expanding on this norm remain only on paper. In the meantime, attacks on critical infrastructure continue to emerge as the new normal in cyberspace.

[25] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies*, 38 (1-2), 2015, p. 4.

[26] "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," Seventieth Session, *United Nations General Assembly*, July 22, 2015 (Accessed December 10, 2019).

About the Authors

Cherian Samuel is a Research Fellow (Cyber Security Project) at the Institute for Defence Studies & Analyses, New Delhi.

Munish Sharma is a Associate Fellow (Cyber Security Project) at the Institute for Defence Studies & Analyses, New Delhi.

The Institute for Defence Studies and Analyses (IDSA) is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Disclaimer: Views expressed in IDSA's publications and on its website are those of the authors and do not necessarily reflect the views of the IDSA or the Government of India.

Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
contact.idsa@nic.in www.idsa.in
Twitter @IDSAIndia
www.facebook.com/InstituteforDefenceStudiesAnalyses