

SECTOR COMMENT

8 November 2019

 Rate this Research

Contacts

Lesley Ritter +1.212.553.1607  
Vice President – Senior Analyst  
lesley.ritter@moodys.com

Abhishek Tyagi +65.6398.8309  
VP-Senior Analyst  
abhishek.tyagi@moodys.com

Toby Shea +1.212.553.1779  
VP-Sr Credit Officer  
toby.shea@moodys.com

Leroy Terrelonge 1.212.553.2816  
AVP-Cyber Risk Analyst  
leroy.terrelonge@moodys.com

Jim Hempstead +1.212.553.4318  
MD-Utilities  
james.hempstead@moodys.com

CLIENT SERVICES

Americas 1-212-553-1653  
Asia Pacific 852-3551-3077  
Japan 81-3-5408-4100  
EMEA 44-20-7772-5454

# Infrastructure & Project Finance – Global Cyberattack on Indian nuclear plant shows vulnerabilities of critical infrastructure

On 30 October, the Nuclear Power Corporation of India Limited (NPCIL) announced that a cybersecurity breach had occurred at its Kudankulam nuclear power plant, the largest nuclear power facility in India. The breach affected the plant's information technology (IT) network but there is no indication that the attackers successfully compromised the operational technology (OT) network, which monitors and operates the plant's physical operation. Nuclear reactors are typically heavily defended because of the potential consequences of an attack on these assets. Therefore, the disclosure of a cyber breach on this facility is a stark reminder that nuclear generation assets remain front of mind for sophisticated attackers.

From a credit perspective, the attackers' ability to remotely hack into the internet-connected IT network of the plant is negative regardless of the intent of the attack. The motive is not known, but likely motives include operational disruption or degradation, or intellectual property theft. Additionally, the fact that attackers were able to compromise a computer in a location purported to be among the most secure in India calls into question the effectiveness of the company's corporate governance oversight. NPCIL is not a public company; therefore, its disclosures are limited.

To date, there have been only a handful of well-publicized examples of malicious cyberattacks on critical infrastructure physical assets globally (see Exhibit 1). However, the risks are rising as state actors grow more interested in hacking into these critical infrastructure assets, according to the US Department of National Intelligence's [2019 Worldwide Threat Assessment Report](#).

Exhibit 1

Examples of prior attacks on critical infrastructure assets, classified by motive

	Survey & Reconnaissance	Theft & Monetization	Disrupt & Destroy
<b>Purpose</b>	- Gather industrial control system (ICS) related information - Establish points of access in ICS network	- Gather trade secrets or economically valuable information - Leverage ICS criticality for extortion or ransom	- Deny, degrade or destroy ICS operations - Cause process disruption or physical destruction
<b>Example</b>	- ALLANITE - DYMALLOY - Dragonfly	- NorskHydro 2019 - Rheinmetal Group 2019	- Nuclear enrichment plant, Iran 2010 - Electric distribution, Ukraine 2015 - Electric distribution, Ukraine 2016 - Oil & gas refinery, Saudi Arabia 2017

Sources: Dragos and Moody's Investors Service

Although the technology that operates the plant and its reactor reportedly run on a different network than the one breached, we still view an infection of the IT network as a material risk. That is because the breach could conceivably allow the attackers to view or modify content

on the compromised computer by uploading and exfiltrating files, including additional malware, and spreading them laterally through the network. This could infect further systems. Maintaining a strategic foothold in a nuclear plant's IT network could also make it easier for a motivated, well-funded attacker to pivot into the critical OT environment later on and carry out a disruptive or destructive attack in the future.

OT networks are gaining attention for their vulnerabilities to cyberattacks. These networks have newer cybersecurity practices that trail those of IT networks. The physical assets operating in the OT environment began to adopt digital technology in a meaningful way only recently. Furthermore, these assets were not designed with cybersecurity in mind. They were set up to operate on a standalone basis, in a siloed environment and over multiple decades, with the primary goal of achieving the highest levels of availability and reliability. As a result, the inherent nature of OT networks does not lend itself particularly well to good cybersecurity practices such as patching for new vulnerabilities, which requires assets to be brought offline. According to cyber experts cited in an October 2015 [report](#) from The Center for Strategic and International Studies, the defenses around OT are a full decade behind the current levels of defenses for information technology.

OT and IT environments are converging. The OT environment is changing as industrial asset owners rapidly add digital technologies to engineering equipment to realize the operational efficiencies and financial savings from adoption of these new tools. This move toward digitization and increased interconnectivity among networks is introducing new vulnerabilities to these critical sectors, and hackers are taking advantage of these attack vectors.

The Kudankulam plant, which has 2 gigawatts (GWs) of generating capacity, became operational only recently. Unlike the other 4.5 GW of nuclear plants operating in India that rely on domestically developed Pressurized Heavy Water Reactor (PHWR) technology, the Kudankulam plant relies on Russian Water-Water Energetic reactor technology (VVER) (see Exhibit 2). The plant also has another 2 GW under construction that will also use VVER reactor technology and is scheduled to go into operation in 2023.

Exhibit 2

**Operational nuclear power plants in India**

Power Station	Operator	State	Type	Units (MW)	Total capacity (MW)
Kaiga	NPCIL	Karnataka	PHWR	220 x 4	880
Kakrapar	NPCIL	Gujarat	PHWR	220 x 4	440
Kudankulam	NPCIL	Tamil Nadu	VVER-1000	1000 x 2	2,000
Madras (Kalpakkam)	NPCIL	Tamil Nadu	PHWR	220 x 2	440
Narora	NPCIL	Uttar Pradesh	PHWR	220 x 2	440
Rajasthan	NPCIL	Rajasthan	PHWR	100 x 1 200 x 1 220 x 1	1,180
Tarapur	NPCIL	Maharashtra	BWR PHRW	160 x 2 540 x 2	1,400
<b>Total</b>					<b>6,780</b>

Source: Nuclear Power Corporation of India Limited

Nuclear power plants are within the electric utilities sector, which we view as highly vulnerable to cyberattacks. (See [Credit implications of cyber risk will hinge on business disruptions, reputational effects](#), February 2019.) The sector's foundational role in supporting most aspects of a country's broader economy and way of life amplifies the risk of a successful cyberattack and, consequently, makes it a prized target for attackers interested in causing widespread harm and disruption. Select segments of the industry also use cutting-edge technology, which makes these companies particularly exposed to intellectual property theft as well as operational risks.

This publication does not announce a credit rating action. For any credit ratings referenced in this publication, please see the ratings tab on the issuer/entity page on [www.moody's.com](http://www.moody's.com) for the most updated credit rating action information and rating history.

### Plant's forensics indicate targeted malware did not infect its OT systems

NPCIL notified the Indian Computer Emergency Response Team on 4 September that it had fallen victim to a successful targeted malware attack that infected a computer connected to its IT network. Forensics of the attack by Dragos, an industrial control system cybersecurity firm, identified computer code samples that appear to allow the attacker to establish a Remote Access Tool (RAT) in the victim's IT network. A RAT can be used to steal data as well as enable control over infected systems.

Cyber forensic experts think the analyzed samples could align with the RAT malware known as DTrack. Researchers first disclosed DTrack in late September 2019 and identified the tool as targeting Indian financial institutions and research centers. DTrack has no industrial control systems specific component that would interact with any control systems that monitor or operate the plant.

The number of victims affected by the DTrack RAT is still very low, and cybersecurity experts have not been able to identify a precise security hole that the attackers might have used to deliver the threatening program.

## Moody's related publications

### Sector In-Depth

- » [Regulated utilities and power companies - North America: Grid modernization heightens vulnerability of utilities to cyberattacks, November 2019](#)
- » [Cyber Risk – Global: Cyber disclosures reveal varying levels of transparency across high-risk sectors, October 2019](#)
- » [Electric and gas – US: Pipeline cybersecurity standards help plug security loophole in utility supply chain, July 2019](#)
- » [Cross-Sector - Global: Credit implications of cyber risk will hinge on business disruptions, reputational effects, February 2019](#)
- » [Regulated electric and gas utilities - US: Cyber risk is on the rise, but the likelihood of government relief is high, September 2018](#)
- » [Public power electric utilities - US: Growing grid interconnectivity increases cybersecurity risks, June 2017](#)

### Sector Comments

- » [Norsk Hydro ASA, Severe cyberattack forces operations into partial manual mode, a credit negative, March 2019](#)
- » [Utilities and power companies – US: GAO's call for improved electric grid cybersecurity oversight is credit positive, but highlights vulnerability risk, October 2019](#)
- » [Utilities remain vulnerable and attractive target of cyber attacks, a credit negative, January 2017](#)

### Topic Page

- » [Cyber Risk](#)

To access any of these reports, click on the entry above. Note that these references are current as of the date of publication of this report and that more recent reports may be available. All research may not be available to all clients.

© 2019 Moody's Corporation, Moody's Investors Service, Inc., Moody's Analytics, Inc. and/or their licensors and affiliates (collectively, "MOODY'S"). All rights reserved.

CREDIT RATINGS ISSUED BY MOODY'S INVESTORS SERVICE, INC. AND ITS RATINGS AFFILIATES ("MIS") ARE MOODY'S CURRENT OPINIONS OF THE RELATIVE FUTURE CREDIT RISK OF ENTITIES, CREDIT COMMITMENTS, OR DEBT OR DEBT-LIKE SECURITIES, AND MOODY'S PUBLICATIONS MAY INCLUDE MOODY'S CURRENT OPINIONS OF THE RELATIVE FUTURE CREDIT RISK OF ENTITIES, CREDIT COMMITMENTS, OR DEBT OR DEBT-LIKE SECURITIES. MOODY'S DEFINES CREDIT RISK AS THE RISK THAT AN ENTITY MAY NOT MEET ITS CONTRACTUAL FINANCIAL OBLIGATIONS AS THEY COME DUE AND ANY ESTIMATED FINANCIAL LOSS IN THE EVENT OF DEFAULT OR IMPAIRMENT. SEE MOODY'S RATING SYMBOLS AND DEFINITIONS PUBLICATION FOR INFORMATION ON THE TYPES OF CONTRACTUAL FINANCIAL OBLIGATIONS ADDRESSED BY MOODY'S RATINGS. CREDIT RATINGS DO NOT ADDRESS ANY OTHER RISK, INCLUDING BUT NOT LIMITED TO: LIQUIDITY RISK, MARKET VALUE RISK, OR PRICE VOLATILITY. CREDIT RATINGS AND MOODY'S OPINIONS INCLUDED IN MOODY'S PUBLICATIONS ARE NOT STATEMENTS OF CURRENT OR HISTORICAL FACT. MOODY'S PUBLICATIONS MAY ALSO INCLUDE QUANTITATIVE MODEL-BASED ESTIMATES OF CREDIT RISK AND RELATED OPINIONS OR COMMENTARY PUBLISHED BY MOODY'S ANALYTICS, INC. CREDIT RATINGS AND MOODY'S PUBLICATIONS DO NOT CONSTITUTE OR PROVIDE INVESTMENT OR FINANCIAL ADVICE, AND CREDIT RATINGS AND MOODY'S PUBLICATIONS ARE NOT AND DO NOT PROVIDE RECOMMENDATIONS TO PURCHASE, SELL, OR HOLD PARTICULAR SECURITIES. NEITHER CREDIT RATINGS NOR MOODY'S PUBLICATIONS COMMENT ON THE SUITABILITY OF AN INVESTMENT FOR ANY PARTICULAR INVESTOR. MOODY'S ISSUES ITS CREDIT RATINGS AND PUBLISHES MOODY'S PUBLICATIONS WITH THE EXPECTATION AND UNDERSTANDING THAT EACH INVESTOR WILL, WITH DUE CARE, MAKE ITS OWN STUDY AND EVALUATION OF EACH SECURITY THAT IS UNDER CONSIDERATION FOR PURCHASE, HOLDING, OR SALE.

MOODY'S CREDIT RATINGS AND MOODY'S PUBLICATIONS ARE NOT INTENDED FOR USE BY RETAIL INVESTORS AND IT WOULD BE RECKLESS AND INAPPROPRIATE FOR RETAIL INVESTORS TO USE MOODY'S CREDIT RATINGS OR MOODY'S PUBLICATIONS WHEN MAKING AN INVESTMENT DECISION. IF IN DOUBT YOU SHOULD CONTACT YOUR FINANCIAL OR OTHER PROFESSIONAL ADVISER. ALL INFORMATION CONTAINED HEREIN IS PROTECTED BY LAW, INCLUDING BUT NOT LIMITED TO, COPYRIGHT LAW, AND NONE OF SUCH INFORMATION MAY BE COPIED OR OTHERWISE REPRODUCED, REPACKAGED, FURTHER TRANSMITTED, TRANSFERRED, DISSEMINATED, REDISTRIBUTED OR RESOLD, OR STORED FOR SUBSEQUENT USE FOR ANY SUCH PURPOSE, IN WHOLE OR IN PART, IN ANY FORM OR MANNER OR BY ANY MEANS WHATSOEVER, BY ANY PERSON WITHOUT MOODY'S PRIOR WRITTEN CONSENT.

CREDIT RATINGS AND MOODY'S PUBLICATIONS ARE NOT INTENDED FOR USE BY ANY PERSON AS A BENCHMARK AS THAT TERM IS DEFINED FOR REGULATORY PURPOSES AND MUST NOT BE USED IN ANY WAY THAT COULD RESULT IN THEM BEING CONSIDERED A BENCHMARK.

All information contained herein is obtained by MOODY'S from sources believed by it to be accurate and reliable. Because of the possibility of human or mechanical error as well as other factors, however, all information contained herein is provided "AS IS" without warranty of any kind. MOODY'S adopts all necessary measures so that the information it uses in assigning a credit rating is of sufficient quality and from sources MOODY'S considers to be reliable including, when appropriate, independent third-party sources. However, MOODY'S is not an auditor and cannot in every instance independently verify or validate information received in the rating process or in preparing the Moody's publications.

To the extent permitted by law, MOODY'S and its directors, officers, employees, agents, representatives, licensors and suppliers disclaim liability to any person or entity for any indirect, special, consequential, or incidental losses or damages whatsoever arising from or in connection with the information contained herein or the use of or inability to use any such information, even if MOODY'S or any of its directors, officers, employees, agents, representatives, licensors or suppliers is advised in advance of the possibility of such losses or damages, including but not limited to: (a) any loss of present or prospective profits or (b) any loss or damage arising where the relevant financial instrument is not the subject of a particular credit rating assigned by MOODY'S.

To the extent permitted by law, MOODY'S and its directors, officers, employees, agents, representatives, licensors and suppliers disclaim liability for any direct or compensatory losses or damages caused to any person or entity, including but not limited to by any negligence (but excluding fraud, willful misconduct or any other type of liability that, for the avoidance of doubt, by law cannot be excluded) on the part of, or any contingency within or beyond the control of, MOODY'S or any of its directors, officers, employees, agents, representatives, licensors or suppliers, arising from or in connection with the information contained herein or the use of or inability to use any such information.

NO WARRANTY, EXPRESS OR IMPLIED, AS TO THE ACCURACY, TIMELINESS, COMPLETENESS, MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OF ANY CREDIT RATING OR OTHER OPINION OR INFORMATION IS GIVEN OR MADE BY MOODY'S IN ANY FORM OR MANNER WHATSOEVER.

Moody's Investors Service, Inc., a wholly-owned credit rating agency subsidiary of Moody's Corporation ("MCO"), hereby discloses that most issuers of debt securities (including corporate and municipal bonds, debentures, notes and commercial paper) and preferred stock rated by Moody's Investors Service, Inc. have, prior to assignment of any rating, agreed to pay to Moody's Investors Service, Inc. for ratings opinions and services rendered by it fees ranging from \$1,000 to approximately \$2,700,000. MCO and MIS also maintain policies and procedures to address the independence of MIS's ratings and rating processes. Information regarding certain affiliations that may exist between directors of MCO and rated entities, and between entities who hold ratings from MIS and have also publicly reported to the SEC an ownership interest in MCO of more than 5%, is posted annually at [www.moody.com](http://www.moody.com) under the heading "Investor Relations — Corporate Governance — Director and Shareholder Affiliation Policy."

Additional terms for Australia only: Any publication into Australia of this document is pursuant to the Australian Financial Services License of MOODY'S affiliate, Moody's Investors Service Pty Limited ABN 61 003 399 657 AFSL 336969 and/or Moody's Analytics Australia Pty Ltd ABN 94 105 136 972 AFSL 383569 (as applicable). This document is intended to be provided only to "wholesale clients" within the meaning of section 761G of the Corporations Act 2001. By continuing to access this document from within Australia, you represent to MOODY'S that you are, or are accessing the document as a representative of, a "wholesale client" and that neither you nor the entity you represent will directly or indirectly disseminate this document or its contents to "retail clients" within the meaning of section 761G of the Corporations Act 2001. MOODY'S credit rating is an opinion as to the creditworthiness of a debt obligation of the issuer, not on the equity securities of the issuer or any form of security that is available to retail investors.

Additional terms for Japan only: Moody's Japan K.K. ("MJKK") is a wholly-owned credit rating agency subsidiary of Moody's Group Japan G.K., which is wholly-owned by Moody's Overseas Holdings Inc., a wholly-owned subsidiary of MCO. Moody's SF Japan K.K. ("MSFJ") is a wholly-owned credit rating agency subsidiary of MJKK. MSFJ is not a Nationally Recognized Statistical Rating Organization ("NRSRO"). Therefore, credit ratings assigned by MSFJ are Non-NRSRO Credit Ratings. Non-NRSRO Credit Ratings are assigned by an entity that is not a NRSRO and, consequently, the rated obligation will not qualify for certain types of treatment under U.S. laws. MJKK and MSFJ are credit rating agencies registered with the Japan Financial Services Agency and their registration numbers are FSA Commissioner (Ratings) No. 2 and 3 respectively.

MJKK or MSFJ (as applicable) hereby disclose that most issuers of debt securities (including corporate and municipal bonds, debentures, notes and commercial paper) and preferred stock rated by MJKK or MSFJ (as applicable) have, prior to assignment of any rating, agreed to pay to MJKK or MSFJ (as applicable) for ratings opinions and services rendered by it fees ranging from JPY125,000 to approximately JPY250,000,000.

MJKK and MSFJ also maintain policies and procedures to address Japanese regulatory requirements.

REPORT NUMBER 1201930

## CLIENT SERVICES

Americas	1-212-553-1653
Asia Pacific	852-3551-3077
Japan	81-3-5408-4100
EMEA	44-20-7772-5454