VIF Paper | December 2019

Cyber Attack on Kudankulam Nuclear Power Plant

A Wake Up Call

Maj Gen P K Mallick, VSM (Retd)

Vivekananda
International
Foundation

Published in December 2019 by
Vivekananda International Foundation
3, San Martin Marg | Chanakyapuri | New Delhi - 110021
Tel: 011-24121764 | Fax: 011-66173415
E-mail: info@vifindia.org
Website: www.vifindia.org

Follow us on

Twitter | @vifindia
Facebook | /vifindia

ISBN : 978-81-943795-2-2

The paper is the author's individual scholastic articulation. The author certifies that the article/paper is original in content, unpublished and it has not been submitted for publication/web upload elsewhere, and that the facts and figures quoted are duly referenced, as needed, and are believed to be correct.

One of the foremost experts on electronics and communication, **Maj Gen PK Mallick, VSM (Retd)** is a graduate of Defence Services Staff College and M Tech from IIT, Kharagpur. He has wide experience in command, staff and instructional appointments in Indian Army. He has also been a Senior Directing Staff (SDS) at National Defence College, New Delhi. Presently, he is a Consultant with the Vivekananda International Foundation, New Delhi.

Cyber Attack on Kudankulam Nuclear Power Plant – A Wake Up Call

Introduction

The media is agog with the report of a cyber attack in India's largest civil nuclear facility - the Kudankulam Nuclear Power Plant (KNPP) in Tamil Nadu. Cyberspace provides a new opportunity for determined adversaries to wreak havoc at nuclear facilities possibly without ever setting foot inside the nuclear plant. If the network that runs the machines and software controlling the nuclear reactor are compromised, cyber attacks on nuclear power plants could have physical effects. This can be used to facilitate sabotage, theft of nuclear materials and sensitive information, or at its worst, a reactor meltdown. In a densely populated country like India, any radiation release from a nuclear facility would be a major disaster.

Threats may be posed by nation states, terrorists, extremists, criminals including organized groups, outsiders such as suppliers or insiders acting intentionally or negligently. There is no such thing as a perfectly secure system. Systems are going to be breached - even one that may be disconnected from the Internet. Those looking to attack critical infrastructure can wait for years for a single mistake to be made. This is cyber warfare and vulnerabilities are going to be found. There have been over 20 known cyber incidents at nuclear facilities since 1990 all over the world which shows that the nuclear sector is not immune to cyber related threats. As the digitalization of nuclear reactor instrumentation and control systems increases, potential for malicious and accidental cyber incidents also increases. Authorities responsible for cyber security of nuclear installations have to be constantly on the vigil.

The cyber attack on KNPP is not a surprise. Attacks may happen to other nuclear installations also in future. Today's defenses are no longer adequate and a fresh look at how to protect nuclear facilities from cyber attack is needed. There is a need to have a holistic view of how the attack took place, what are the shortcomings in the existing system and mitigating measures to be taken. The threat is too great and the potential consequences are too high to remain comfortable with the status quo.

The Kudankulam Nuclear Power Plant (KNPP)

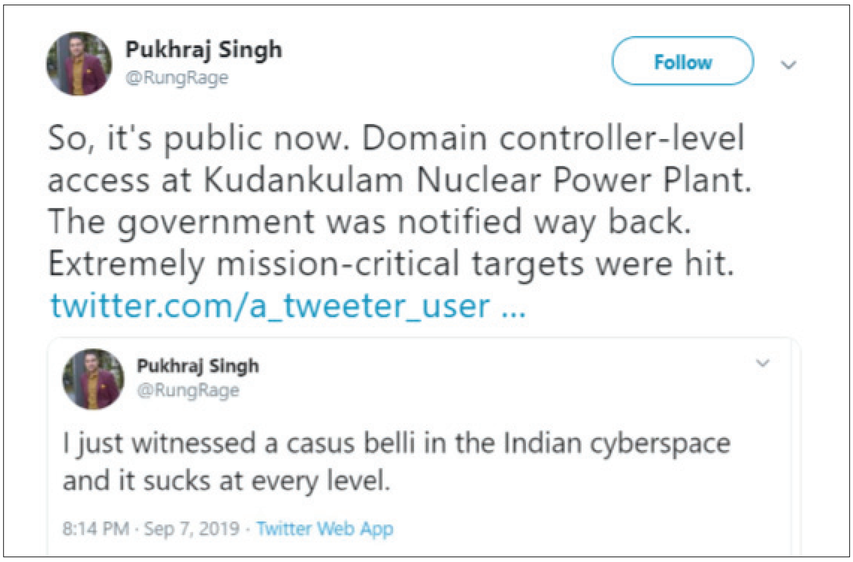
Kudankulam is India's biggest nuclear power plant, "equipped with two Russian-designed and supplied Water-Water Energy Reactor (i.e. Water-Cooled Water-Moderated Energy Reactor pressurized water reactors with a capacity of 1,000 megawatts each. Both reactor units feed India's southern power grid. The plant is adding four more reactor units of the same capacity, making the KNPP one of the largest collaborations between India and Russia." The nuclear plant will produce over 47.4 billion kWhs per year.[1]

There have been over 70 shutdowns since the reactors went active in 2013. According to KNPP officials on October 19, the plant's second reactor was shut down due to a fault in the reactor's steam generation. The shutdown was not related to the malware attack.[2]

Image Source : https://www.zdnet.com/article/confirmed-north-korean-malware-found-on-indian-nuclear-plants-network/

What Happened

Pukhraj Singh, a former researcher at India's National Technical Research Organization (NTRO) and an independent Indian cyber security professional was the first to alert the authorities on September 4. He states, "I notified the National Cyber Security Coordinator about network intrusions into the KNPP and Indian Space Research Organization (ISRO), after being tipped off by a third-party. It was right around the time of Chandrayaan-2's final descent. I made a responsible disclosure on social media on October 28, after the technical indicators of the attack started trickling into the cyber security community at-large. It seemed that the infection was still prevalent, nearly two months after the notification. I did, however, post a cryptic tweet on September 7, which hinted at a *casus belli* – an act of war – in Indian cyberspace."[3]



Pukhraj Singh
@RungRage

So, it's public now. Domain controller-level access at Kudankulam Nuclear Power Plant. The government was notified way back. Extremely mission-critical targets were hit. twitter.com/a_tweeter_user ...

Pukhraj Singh
@RungRage

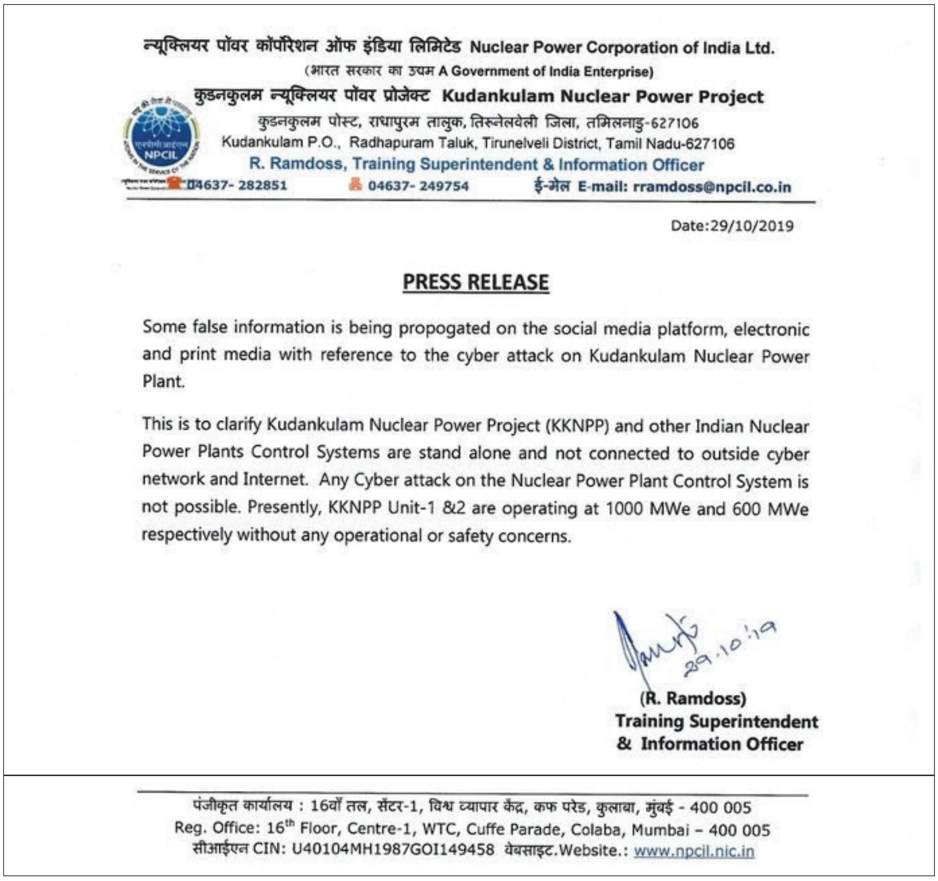
I just witnessed a casus belli in the Indian cyberspace and it sucks at every level.

8:14 PM · Sep 7, 2019 · Twitter Web App

Pukhraj Singh's tweet and revelation caught on the media like wild fire. According to a report in *The Indian Express*, a U.S.-based cyber security company had, on September 3, made the National Cyber Coordination Centre – a set up under a classified project "to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing" - aware of a 'threat actor' breaching master 'domain controllers' at the Kudankulam plant and at ISRO with a malware, later identified as a "Dtrack." Sources said both Nuclear Power Corporation of India Limited (NPCIL) and ISRO were alerted on September 4.

Reaction of Government Agencies Responsible for Security

Initially, KNPP officials denied that they've suffered any malware infection, issuing a statement to describe the tweets as "false information", and that a cyber-attack on the power plant was "not possible." However, within 24 hours, the KNPP's parent company NPCIL admitted to the security breach in a separate statement. It stated, "Identification of malware in NPCIL system is correct. The matter was conveyed by Computer Emergency Response Team-India (CERT-In) when it was noticed by them on September 4, 2019. The matter was immediately investigated by the Department of Atomic Energy (DAE) specialists. The investigation revealed that the infected Personal Computer (PC) belonged to a user who was connected in the internet connected network for administrative purposes. "This is isolated from the critical internal network," it said, adding that the networks were being monitored continuously.



न्यूक्लियर पॉवर कॉर्पोरेशन ऑफ इंडिया लिमिटेड Nuclear Power Corporation of India Ltd.
(भारत सरकार का उद्यम A Government of India Enterprise)
कुडनकुलम न्यूक्लियर पॉवर प्रोजेक्ट Kudankulam Nuclear Power Project
कुडनकुलम पोस्ट, राधापुरम तालुक, तिरूनेलवेली जिला, तमिलनाडु-627106
Kudankulam P.O., Radhapuram Taluk, Tirunelveli District, Tamil Nadu-627106
R. Ramdoss, Training Superintendent & Information Officer
☎ 04637- 282851 04637- 249754 ई-मेल E-mail: rramdoss@npcil.co.in

Date:29/10/2019

PRESS RELEASE

Some false information is being propogated on the social media platform, electronic and print media with reference to the cyber attack on Kudankulam Nuclear Power Plant.

This is to clarify Kudankulam Nuclear Power Project (KKNPP) and other Indian Nuclear Power Plants Control Systems are stand alone and not connected to outside cyber network and Internet. Any Cyber attack on the Nuclear Power Plant Control System is not possible. Presently, KKNPP Unit-1 &2 are operating at 1000 MWe and 600 MWe respectively without any operational or safety concerns.

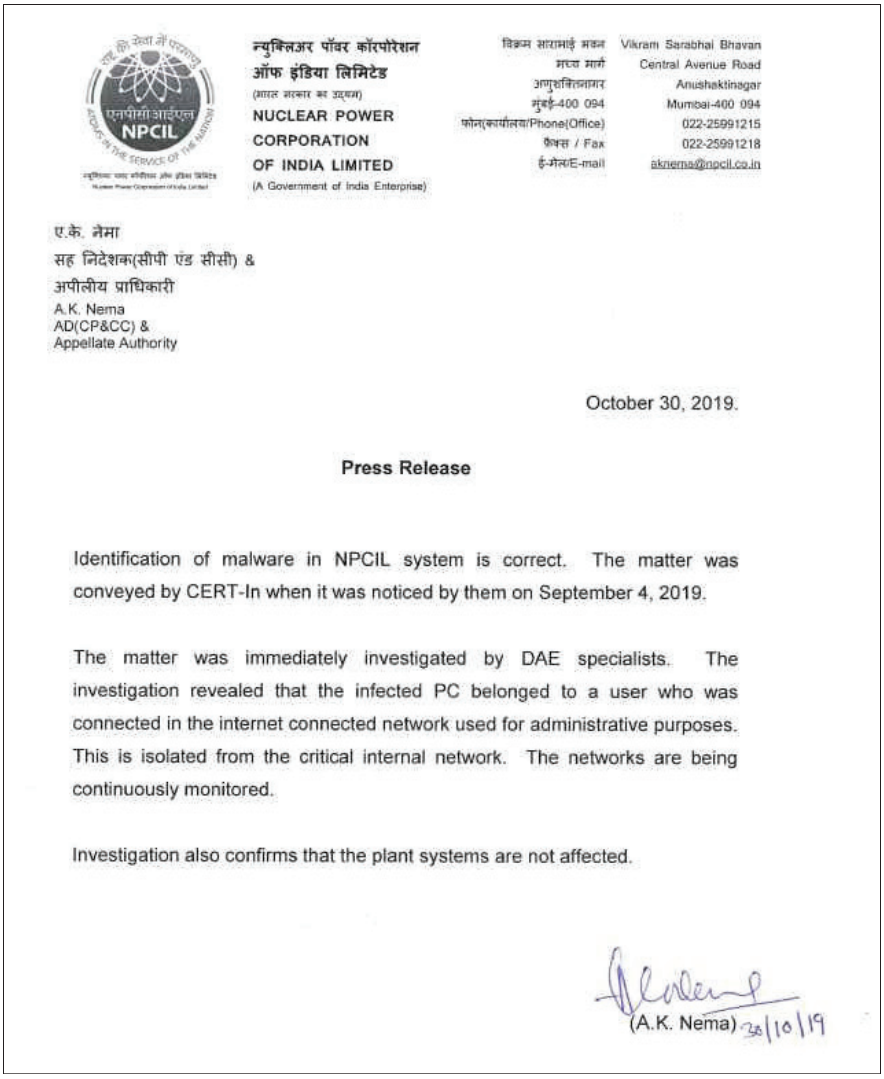
29.10.19

(R. Ramdoss)
Training Superintendent
& Information Officer

पंजीकृत कार्यालय : 16वाँ तल, सेंटर-1, विश्व व्यापार केंद्र, कफ परेड, कुलाबा, मुंबई - 400 005
Reg. Office: 16th Floor, Centre-1, WTC, Cuffe Parade, Colaba, Mumbai – 400 005
सीआईएन CIN: U40104MH1987GOI149458 वेबसाइट.Website.: www.npcil.nic.in

Source: https://www.timesnownews.com/india/article/kudankulam-nuclear-power-plant-hit-by-cyber-attack-knpp-denies-says-both-units-generating-power/509108

The KNPP in Tamil Nadu is a joint venture between India and Russia. Indian authorities have apprised Russia that necessary steps have been taken to prevent similar incidents in future. Deputy Chief of the Russian Embassy Roman Babushkin said, "The Russian authorities are working with Indian agencies to stop any further attacks."[4] An official in a cyber security division of the government, asking not to be named, said that a tip-off was received from "a friendly country" and a team of experts was rushed to the facility located in Tirunelveli in Tamil Nadu in early September. "The foreign government's help allowed for a quick response," this person added.



न्युक्लिअर पॉवर कॉरपोरेशन
ऑफ इंडिया लिमिटेड
(भारत सरकार का उद्यम)
NUCLEAR POWER
CORPORATION
OF INDIA LIMITED
(A Government of India Enterprise)

विक्रम साराभाई भवन
मध्य मार्ग
अणुशक्तिनगर
मुंबई-400 094
फोन(कार्यालय/Phone(Office)
फैक्स / Fax
ई-मेल/E-mail

Vikram Sarabhai Bhavan
Central Avenue Road
Anushaktinagar
Mumbai-400 094
022-25991215
022-25991218
aknema@npcil.co.in

ए.के. नेमा
सह निदेशक(सीपी एंड सीसी) &
अपीलीय प्राधिकारी
A.K. Nema
AD(CP&CC) &
Appellate Authority

October 30, 2019.

Press Release

Identification of malware in NPCIL system is correct. The matter was conveyed by CERT-In when it was noticed by them on September 4, 2019.

The matter was immediately investigated by DAE specialists. The investigation revealed that the infected PC belonged to a user who was connected in the internet connected network used for administrative purposes. This is isolated from the critical internal network. The networks are being continuously monitored.

Investigation also confirms that the plant systems are not affected.

(A.K. Nema) 30/10/19

Source : https://www.scribd.com/document/432687853/NPCIL-statement

Analysis of the Cyber Incidence

The incidence has been analysed by various cyber security professionals from different agencies. Some of the reports are listed below.

Kaspersky

A Russian cyber security company, Kaspersky Labs, had said on September 23 that "banks and research centres in India" were targeted by *Dtrack* "in the beginning of September 2019". Dtrack is usually used for reconnaissance purposes and as a dropper for other malware payloads. Previous Dtrack samples have been usually spotted in politically-motivated cyber espionage operations and in attacks on banks. It is considered as a 'new type' of malware, which was deliberately created for data theft and spying.[5] A custom version of Dtrack, named AMTDtrack also being discovered last month. This Trojan includes features for:-

- Keylogging.
- Retrieving browser history.
- Gathering host IP addresses, information about available networks and active connections.
- Listing all running processes.
- Listing all files on all available disk volumes.

Kaspersky's detailed analysis indicated that it had similarities to another related virus called 'ATM DTrack'. This was used to steal financial information from bank ATMs and has been found in many financial institutions and research centers. In October 2016, a major breach was detected at an Indian private bank's ATM network that quickly spread through the entire banking system. In a few months the government had to recall an estimated 2.9 to 3.2 million credit and debit cards that had been compromised by the ATM DTrack virus.[6]

The North Korean Link

According to Kaspersky, the malware was the work of Lazarus, "an umbrella name that typically describes hacking activity which advances Pyongyang's interests". While there is no hard intelligence on who the 'Lazarus Group' works for, there have been indications that it has done some work for North Korea. Also within the code were other clues that link the cyber attack to a much bigger operation that runs out of North Korea or through hackers who are linked to the regime.

Issue Makers Lab

Established in 2008, the South Korea based Issue Makers Labs is a group of experts of malware analysts working in the cyber security field. It operates as a non-profit intelligence organization.[7] Its members have won commendations from South Korea's Defense Ministry and taken part in conferences and events hosted by the South Korea Information and Security Agency. Much of the group's research deals with North Korean capabilities.

Simon Choi leads the group as a founder and principal researcher of Issue Maker Labs. He has explained the incidents with some startling facts. These are:- [8,9,10]

- The hack on the Indian nuclear power plant originated in North Korea. Public attribution of the attack led to the North Korean threat actor Lazarus and its intrusion tool-kit DTrack. It has a persistent presence in Indian networks. It was also linked to the 2016 breach of a debit card database.

- In the case of KNPP, Lazarus seemed to be after cutting edge nuclear technology. DTrack also undertook a destructive attack on a South Korean nuclear installation.

- The North Korean hackers have now been tasked with either disrupting atomic plants or stealing atomic technologies. This is a major upgrade of North Korea's cyber attack capabilities, which used to be deployed against civilian targets. India has nuclear weapons.

- The key entry point targeted for attack was Anil Kakodkar, former chairman of the Atomic Energy Commission of India (AEC) as well as the director of the Bhabha Atomic Research Centre (BARC). Currently holding a chair of excellence to continue his research work, Kakodkar and his colleague S A Bharadwaj still use official email addresses given by BARC. Kakodkar specializes in Thorium based reactors, since India has very limited quantities of uranium.

- The North Koreans sent a malware link to Kakodkar and Bharadwaj's official and personal email accounts. Once Kakodkar and Bharadwaj clicked on the link while still using the Kudankulam plant's domain, the malware spread quickly through the IT networks.

- North Korean hackers knew the IP network of the Indian plant. They penetrated inside the plant, but did not send destructive code. Nuclear Power Plant technology-related data has been taken.

- Issue Makers Lab had not been able to identify the individuals or the hackers' actual group. While the North Korean attackers had the capability of causing major damage, the aim of the Kundakulam raid was data retrieval and not destruction.

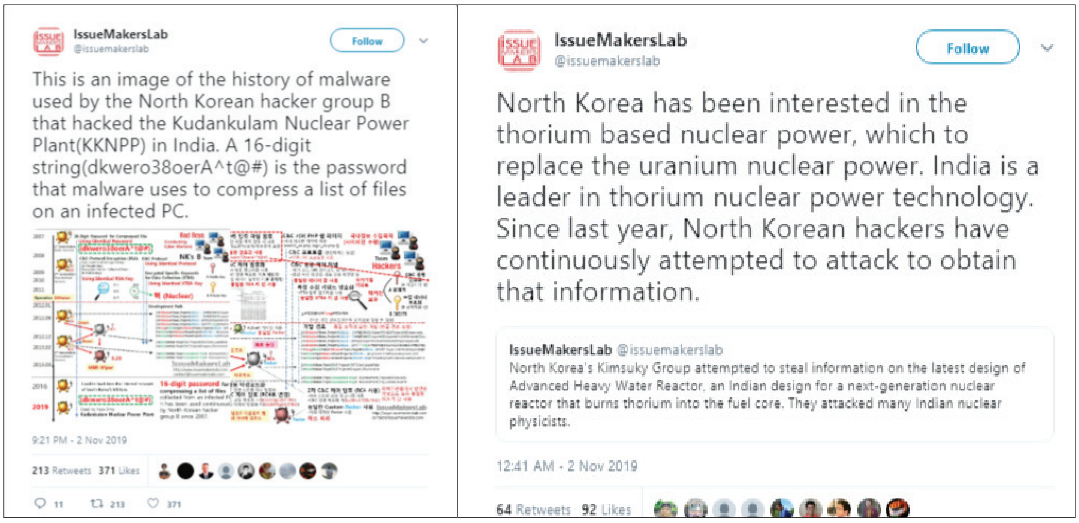
- The computer used as the launch pad for the hack was a model that is produced in, and only used in North Korea. This helped them get the MAC address of the machine, as well as details of the IP address. Both bear North Korean signatures. Their investigation also found that the Korean language was used in the malware code.

- When lab personnel dissected the malignant code that had been deployed at the Indian nuclear power plant, they discovered that the code was already known to them. It had previously been used by North Korea in cyber attacks on South Korean banks and broadcasters in 2013 and on Seoul's Ministry of National Defense in 2016.

- There is evidence that the hackers of North Korea were disguised as employees of the Atomic Energy Regulatory Board (AERB)and BARC of India and sent hacking mails. The KNPP attack was not intended to cause destruction but to extort the confidential data and reconnaissance.

- No one from the Indian Government has reached out to him, let alone worked with him to research the cyber attack and gather more details.

An image of the history of malware used by the North Korean hacker group B that hacked the KNPP in India is given here. A 16-digit string (dkwero38oerA^t@#) is the password that malware uses to compress a list of files on an infected PC. They have used the same password for multiple attacks since 2007.



IssueMakersLab
@issuemakerslab

This is an image of the history of malware used by the North Korean hacker group B that hacked the Kudankulam Nuclear Power Plant(KKNPP) in India. A 16-digit string(dkwero38oerA^t@#) is the password that malware uses to compress a list of files on an infected PC.

9:21 PM - 2 Nov 2019

213 Retweets 371 Likes

IssueMakersLab
@issuemakerslab

North Korea has been interested in the thorium based nuclear power, which to replace the uranium nuclear power. India is a leader in thorium nuclear power technology. Since last year, North Korean hackers have continuously attempted to attack to obtain that information.

IssueMakersLab @issuemakerslab
North Korea's Kimsuky Group attempted to steal information on the latest design of Advanced Heavy Water Reactor, an Indian design for a next-generation nuclear reactor that burns thorium into the fuel core. They attacked many Indian nuclear physicists.

12:41 AM - 2 Nov 2019

64 Retweets 92 Likes

Who Was Behind the Attack?

As per Issue Makers Lab:- [11]

- Two separate groups who worked together on this on this attack. While the attack had been attributed to the Lazarus group, technically the perpetrators are a separate group. There are approximately seven hacker groups in North Korea. The group which had attacked South Korea's government website in 2009 and Sony Pictures in 2014 is termed as 'Group A', which is more commonly referred to as 'Lazarus Group'.

- There is 'Group B' which generally attacks the Korean Army and have attacked Korean banks and networks in 2013. This is the group that attacked KKNPP. This group is normally known as 'Dark Seoul' or 'Operation Troy'. These two groups are controlled by North Korean government and they can be considered as one.

- There is also a 'Group C' which attacked Korea Hydro and Nuclear Power Co. Ltd. in 2014. This Group C started attacking India's nuclear power plant related persons from last year.

How was the Attack Carried Out?

The evidence gathered suggests the attack on KNPP was carried out by Group B and C's association. While Group C was involved in reconnaissance over the last one year and sending malware to senior nuclear scientists, Group B was the one to deploy the malware on the plant's IT systems. When Group C gets authority by reconnaissance done on people associated with the nuclear power plant, they hand over this data collected to Group B. The hackers of North Korea disguised as employees of the AERB and the BARC and sent the hacking mail to their chairmen and other senior experts. Then

Group B extorts the confidential documents from the nuclear power plant system. So the malware found in the nuclear power plant system is Group B's malware.

Why did they Attack Kudankulam?

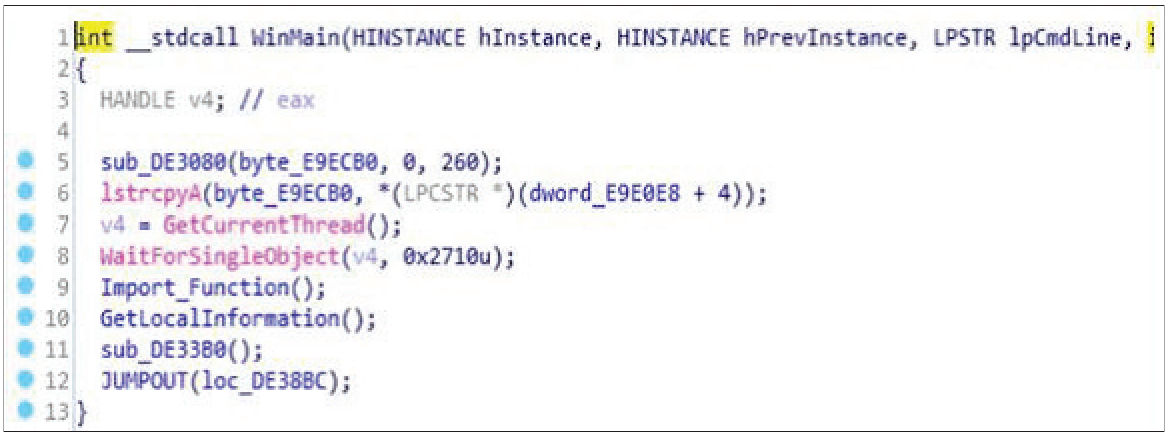
It may be assumed that the motive of the attack could be theft of information on thorium based nuclear power. The KNPP attack was not intended to cause destruction. It was to extort the confidential data and reconnaissance. But if they intend to cause destruction, they would have done it by sending another malware.

Sensecy (a Verint Company) Report on Cyber Threat Intelligence Alert of Indian Nuclear Power Plant

Dtrack malware is a backdoor Trojan designed specifically to steal data from the compromised device. It was created by the known North Korean state sponsored group, Lazarus (aka APT38.) The malware was found to contain credentials for the internal network of the power plant, indicating the attack was intentional. Some even suggested that a shutdown at one of the reactors at the plant was connected to this incident. However, this claim was rejected.

Initially, it was classified as a banking Trojan implemented on ATMs to steal customer credit card data, especially in India. The malware that was first called ATMDtrack was eventually found to have been modified to also compromise corporate and private computers, but this version was called Dtrack. This malware had different capabilities, such as keylogging, listing the files and processes running on the computer, uploading and downloading files from the victim's computer and more.

A link for downloading a sample of the malware was posted on Twitter on October 28, 2019, by an unknown user dubbed '@a_tweeter_user.3'. Following this, some security researchers analyzed it to ascertain its capabilities and objectives. After the malware is installed, it attempts to identify the Windows API address and then starts to collect information about the target, which is its main objective. This information includes IP address, information on routing and interfaces and task listing, which is then saved in a temporary file in '%APPDATA%/Temp/temp/'.



```
int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, i
{
  HANDLE v4; // eax

  sub_DE3080(byte_E9ECB0, 0, 260);
  lstrcpyA(byte_E9ECB0, *(LPCSTR *)(dword_E9E0E8 + 4));
  v4 = GetCurrentThread();
  WaitForSingleObject(v4, 0x2710u);
  Import_Function();
  GetLocalInformation();
  sub_DE3380();
  JUMPOUT(loc_DE38BC);
}
```

Main Functions of the Malware

In addition, the sample looks for specific information in two specific drives, C and E, which indicates the threat actors had previous knowledge of the systems' structure. There, it looks for different software of interest to them. It searches for browser information, such as URLs, by loading an SQLite driver. All of the gathered information is saved in an organized manner and can be easily read by the threat actor. The name given to the folder is the system's IP address.

After all the information is collected, it compresses the aforementioned folder in 'PPDATA%/Temp/~77FDD3EAMT.tmp' as a zip file, using one of two passwords – 'dkwero38oerA^t@#' or 'abcd@123', before sending to server '10.38.1[.]35'. This seems to be the server controlled by the attacker, because in every case, it sends the information there. The '~77FDD3EAMT.tmp' file is eventually deleted, however, not before it after it copies it to a better hidden directory, such as Windows\Temp\MpLogs. It was found that different capabilities, such as command and control, can be added to the sample to weaponize it. However, these behaviours were not found.

The attribution to Lazarus was because of similarities found in different strings of the code in the current sample and the previous report of September 2019. This attack corresponds with previous knowledge about the modus operandi of the Lazarus group, particularly their emphasis on reconnaissance and information gathering.

Even though it was announced that the malware did not access the Supervisory Control and Data Acquisition (SCADA) network of the plant, we know from previous attacks against SCADA systems that threat actors first attack the IT network in order to the infiltrate the Information and Communication (ICS) networks and then cause the damage. However, as the main function of Dtrack is information gathering, there is a good chance it was used for reconnaissance purposes, for future attacks. It could also indicate a new type of attack target for the Lazarus group, in addition to their known targets like government agencies and financial institutions.[12]

Virus Total, a Virus Scanning Website owned by Alphabet (Google's Parent)

The Washington Post has quoted Virus Total, a virus scanning website owned by 'Alphabet' (Google's parent), saying a large amount of data was stolen during the breach. Virus Total, which in turn contacted 46 virus scanning engines that classified it as a part of the DTrack Malware family. This data could be used to plan the next attack more efficiently. Subsequent attacks could have serious repercussions for more critical systems; cyber attacks can be used to facilitate sabotage, theft of nuclear materials, or in the worst case scenario a reactor meltdown which could be a major disaster.[13]

Role of North Korea

The syndicate Lazarus is believed to have been behind the audacious 2016 Bangladesh bank heist, which led to a loss of over $81 million. Its hackers were able to find loopholes in the 'SWIFT' international money transfer system. This allowed them to use bank employee credentials to send money to the Philippines-based Rizal Commercial Banking Corporation. (Notably, North Korea has immerged as significant cyber power of the world. The author of this paper has written on North

Korea's cyber capabilities in his blogsite available at: https://strategicstudyindia. blogspot.com/2017/11/north-korea-david-of-cyber-world.html and https:// strategicstudyindia. blogspot.com/2017/11/north-korea-david-of-cyber-world_4.html. The same is also available as Notrh Korea, David of the Cyber World at : https:// drive.google.com/file/d/1W1j-IpQEHiodB0RsUl3wy_VPnkDOLnO3/view).

Tom Plant, an expert at the Royal United Services Institute (RUSI), a think tank in London, points out that there are several plausible reasons why North Korea might take an interest in Kudankulam in particular. One, its own nuclear aspirations may be a reason. North Korea has been building an experimental light water nuclear reactor, which may be similar to India's and may be approaching start up.

North Korea has no known experience with this type of reactor. UN sanctions mean it cannot legally gather information about such technology. Mr. Plant is of the view that it would make sense for North Korea to acquire data wherever it can, if its design is based on the type of Russian designed reactor used in Kudankulam, something that is unknown. Adam Meyers of Crowdstrike, a cyber security firm, agrees that the aim of the hack was probably intelligence collection, with the purpose of furthering the energy plank of North Korea's national economic development strategy.

Attribution

It can be reasonably assumed from the analysis available in the open domain that the cyber attack was originated from North Korea. Attribution by civilian experts from other countries cannot be taken up with North Korean Government or international agencies as official proof by the Government of India. Attributing cyber attacks is hard but not impossible. In recent years, America and its allies have fingered Russia, China and North Korea for conducting cyber attacks. They have produced large amounts of evidence including forensic analysis of code as well as intelligence gathered by human and technical means. Attribution is more complicated in 'false-flag' attacks, when hackers deliberately pass themselves off as those of other countries. Starting in 2016, Lazarus itself adopted a Russian garb when attacking Polish banks. Britain and America claimed that Russian hackers had hijacked the command-and-control systems of Iranian ones to deploy malware in at least 35 countries. Malware developed by one country can be deployed by another. But doing so consistently and persuasively is very hard. There is no indication of a false flag in the Indian power plant hack. There exists the possibility that North Korea did it for someone else for money.

The questions that can be asked are:- [14]

- Does the Government of India have the capability to attribute to the perpetrators of this action and nail them comprehensively?

- Does India have the capability to take offensive action as a measure of deterrence? North Korea has been active in cyber crime related activities in India.

- What are the options for diplomatic action available to India?

Air Gapped Network

An air gap is the concept of physically isolating critical computers or networks from unsecure networks such as the public Internet. In theory, devices on either side of this gap are unable to communicate, making an air gap an attractive option for securing the most important networks including the industrial control systems present in many nuclear facilities. Though air gaps offer a high level of security, they are not failsafe. A March 2019 report from the Fissile Materials Working Group observed, "Although many asset owners feel their systems are protected because there is no physical or logical connectivity into critical network enclaves, the networks are very rarely and ever truly isolated." Undesirable consequences can be caused by accessibility to vital networks through both authorized and unauthorized methods. This includes contractor access, removable media or the compromise of vital networks due to mis-configuration of security counter-measures. Approved access points often exist for maintenance activities, including for third party updates and monitoring, that could potentially be compromised.

Air gaps provide some level of protection, but they create a sense of complacency. Air gapped nuclear facilities can be attacked. It is insufficient to meet the threat of a targeted attack perpetrated by a determined, well-resourced adversary. Air gaps can be effective against unsophisticated and untargeted cyber threats but not against targeted attacks. Such attacks are constructed on the basis of extensive research of targeted systems and go beyond network connections - generally by leveraging witting or unwitting humans or a long and difficult-to-defend supply chain to deliver the attack. The most commonly described compromises of air-gapped systems are through the use of removable media (e.g., USB drives). This has been demonstrated in high profile cases, most notably in the Stuxnet malware that destroyed centrifuges inside an air-gapped uranium enrichment facility in Iran.[15]

Standard design of a nuclear power plant typically requires two distinct networks that are critical to its operations as described below.

Industrial Control System (ICS) or Operational Technology (OT). This controls the actual running of the machines in the plant, controlling the input and output of data to ensure power is generated through a controlled nuclear reaction.

Information Technology (IT) systems. All other functions of the plant are based on IT systems that contain vast amounts of data. This data is essential for functions such as managing personnel, access controls, materials control and accounting, safety standards, safe and secure operation of the facility, maintenance schedules and quality monitoring among a host of other functions. By its nature this is connected to the internet.

Laser/optical data diodes can physically ensure a one way flow of information. These are widely used in nuclear facilities as a way to help ensure security between networked zones. These devices facilitate the one way egress of operational data from vital networks to non vital areas while preventing the ingress of data into vital networks from non vital networks. However, a data diode does not make an air-gapped network. Organizations must transfer data into and out of their operational networks for a variety of reasons and in many cases augment their architecture to meet data transfer needs. Some of the risks are:-[16]

- Use of traditional network firewalls/switches for network segmentation. These devices can be reconfigured to compromise the segmentation and create a bypass around security measures.

- Allowing USB keys to enter and exit their OT network. A data diode, firewall or switch has no capability to stop removable media from being physically brought into a facility networking environment.

- Allowing hardware to enter and exit their OT network as part of facility and operations of vendor maintenance.

- Use of laser data diode in one direction may still have a need for data to go the other direction. The requirement for bi-directional data exchange results in some cases in the use of one data diode for inbound and one for outbound. This effectively means there is no air gap. Without allowing data to enter the OT network, an operator may not be able to update software, hardware, etc.

Air gaps have failed at the Davis-Besse nuclear power plant in Ohio in 2003 and even classified U.S. military systems in 2008. A report from Chatham House found ample sector-wide evidence of employee behaviour that would circumvent air gaps, like charging personal phones via reactor control room, USB slots and installing remote access tools for contractors.[17] Software patching is a sequence of defensive reactions to protect vulnerabilities discovered in software. There are conflicting priorities and cultural divides between operational technology engineers and their IT counterparts. Even when compromises between nuclear facility personnel are achieved, patching at nuclear plants presents unique challenges.

Nuclear plants are using SCADA systems for better integration. It incorporates 'off the shelf' hardware and software, such as Windows or Linux, from a limited number of vendors. This practice provides plant operators with greater cost savings and efficiency. The eternal 'L1' (lowest bidder) syndrome and audit requirements do not help. But it comes at the expense of facilitating the rise of 'insecure by design' nuclear facilities, as programmable code can be altered by hackers to change the function of a device. In conjunction with the constant evolution of viruses and worms, the protracted upgrade cycle of cyber security at nuclear facilities is incompatible with the critical need for expeditious software upgrades to close security gaps. The legacy products are vulnerable to discontinued manufacturer support due to obsolescence and might also be incompatible with newer software updates. Thus, operators need to adopt best practices and ensure defense in depth, including plans for emergency response/resilience planning.

Cause for Concern. The vulnerabilities of air gap network is known to all. The myth was busted in 2010 by Stuxnet. Initial reaction of KNPP officials stating their confidence in air gap network is surprising.[18]

Role of Regulators

Governments and particularly nuclear regulators, play a key role in setting requirements for security at nuclear facilities. In an effort to better reflect these priorities governments and regulators Have to:-

- Work to develop and implement regulatory frameworks.
- Promote the development of active defense strategies and capabilities.
- Support—with financial, personnel and research resources.
- Undertake or fund transformative research.

Regulators play a key role in the national cyber security effort. With the constantly changing Information and Communication Technology (ICT) environment and the dynamics of cyber security, the role of the regulator in this area has to evolve and adapt. Regulators must remain relevant in this dynamic environment. A strong regulatory framework is needed to address cyber security specially for nuclear domain. They must draw talented people into the cyber-nuclear field. Organizations that comply with cyber regulations may still be vulnerable to attack as regulations only serve as a baseline based on historic attack patterns. It has been shown that compliance does not necessarily equate to security. Organizations fully compliant with regulatory requirements have been compromised.

The majority of cyber security regulations for nuclear facilities are high level performance guidance. The challenge is how the regulations are implemented and evaluated. Best practices may not be incorporated into regulations, but they can be a part of regulatory guidance development, which is well needed.

Questions must be raised about core competencies and resources of the regulator. There are a number of cross competencies that regulators should demonstrate before taking an active role in any aspect of cyber security. These comprise of:- [19,20]

- **Institutional Maturity**. Regulators must look closely at the range of cyber security roles and responsibilities undertaken by other regulators and to decide which options and approaches are best suited to their critical information infrastructure. They should appraise realistically what they can and cannot do and what needs to be left to others to manage and lead.
- **Engagement of the Private Sector.** How should the expertise available in the private sector be tapped?
- **Technical and Industry Expertise**. Regulator must have requisite technical and industry experience and expertise.
- **Mandate and Jurisdiction.** Must be clearly spelt out. Regulators require a clearer mandate with regard to their cyber security role.

- **Appropriate Resourcing**. In order to carry out its roles and responsibilities effectively, a regulator has to have the appropriate financial and manpower resources.

- **Engagement in International Cooperation**. Must maintain close cooperation with international agencies dealing with cyber security of nuclear plants.

- **Policy Making**. Normally ICT policy is made typically by the ministry. Regulators often play a key supporting role in policy making:-

  - By virtue of their familiarity with the sector that they regulate.

  - Resources available to them.

  - Processes and mechanisms that have been put in place to engage in consultations with industry stakeholders.

- **Incident Management and Cyber Security Readiness Assessment.** Regulators may undertake the following roles:-

  - Preparing and implementing periodic cyber security risk assessments, audits and reviews.

  - Conduct cyber security exercises to test readiness and responsiveness.

Questions. The following questions are relevant regarding cyber security regulators:-

- How are the regulators appointed.

- How are their competencies assessed.

- Do regulators have a proficient process? Do they possess the technical know-how.

- Do they have the practical experience to relate to challenges faced by the nuclear sector.

- What is the process of appointment and evaluation of regulators.

- Are the regulators consulting vertically and horizontally with other regulators of critical information infrastructure? Who organizes these interactions.

- What control does National Cyber Security Coordinator has on the regulators.

Who is Responsible for India's Nuclear Sector

'National Critical Information Infrastructure Protection Centre' (NCIIPC) is the nodal agency under Section 70A(1) of the Information Technology (Amendment) Act 2008 for taking all measures including associated Research and Development for the protection of Critical Information

Infrastructures (CIIs) in India. Energy, transport, banking, telecommunication, nuclear and space fields are some of the fields mandated to be protected by NCIIPC.[21]

The NCIIPC started off with several sectors, but has now truncated them into five broad areas that cover the 'critical sectors'. These are:-

- Power and Energy.
- Banking, Financial Institutions and Insurance.
- Information and Communication Technology.
- Transportation.
- E-governance and Strategic Public Enterprises.

Balance of the sectors are now the responsibility of CERT-In. As per the Indian Express, the CERT-In received a tip from an anti-virus company that observed 'malicious activity' in the external network of KNPP in early September. A computer used by an employee in the finance department had been compromised. The malware got domain controller access to the system. Domain controller is the device that will verify the authenticity of all the other devices on the network. If that's compromised, it can approve any device as authentic, including those of foreign agents'.

Subsequently, an inter-agency team, consisting of CERT and NCIIPC, was sent for clean-up in mid-September. Since it is a nuclear power plant, NCIIPC was sent.[22]

Operating System

It has been reported in the media that NPCIL issued tenders for Windows systems and subsequently bought them. This shows that there were several Windows enabled computers operational within the KNPP air gap. What was the Operating System (OS) used on the operations side? The only alternative explanation could be that the operations of the plant were run on an OS developed in India like the 'BOSS' and the other developed by BARC exclusively for use by India.

The question is what is this OS based on and how long did it take to integrate the said system with Russian equipment which would add a whole new layer of complexity and vulnerability in addition to malfunction to an already complex system. It is important to note that the virus in question 'DTRACK' is programmed to attack Windows operating systems.

Two leading scientific organizations in the country, the BARC and ISRO, have developed world class indigenous security solutions as they had to undergo international restrictions and strict security requirements. BARC has developed an excellent network security solution called Secure Network Access System (SNAS). Electronic Corporation of India Limited (ECIL) has been made the designated agency for servicing and maintenance. When there is so much of emphasis on Make in

India, in the classified networks of armed forces or in the critical information infrastructures OS like SANS is expected to be utilized.

Media reports suggest that the NPCIL has procured Windows operating system through a tendering process.[23] It is relevant here to examine the following questions:-

- What is the system of pushing software updates of windows operating system in the nuclear plant's IT network?

- All the critical networks in the country have their own system of upgrading their operating systems through a complicated process of sandboxing and other technique. This is not cent percent full proof but degree of difficulty to breach the network would be extremely high. Did the authorities responsible for cyber security interacted with other officials responsible for critical information infrastructure?

- What is the system followed in BARC and ISRO? Were they consulted?

- Who is coordinating these inter agency interactions? Is it the office of the National Cyber Security Coordinator or NCIIPC?

- Who has the authority to make people responsible for cyber security of respective national critical infrastructure to implement suggested measures?

International Best Practices

There is no internationally recognized 'gold standard' on how nuclear cyber security should be organized. As per International Atomic Energy Agency (IAEA) security is a national responsibility. For the civil nuclear sector, the IAEA publishes nuclear security recommendations that reflect internationally accepted best practice, but there are no recognized international regulations as such. However, some guidance exist like:-

- Non-governmental organizations such as the World Institute for Nuclear Security (WINS) have issued high-level guidance documents on how national infrastructure for cyber security might be prepared.

- The National Institute of Standards and Technology (NIST), a non-regulatory agency of the U.S. Department of Commerce, has developed guidance specifically to assist nuclear facilities in complying with multi-faceted regulations to verify that the computers, digital communications and systems in Critical National Infrastructure (CNI) are protected from cyber attacks.

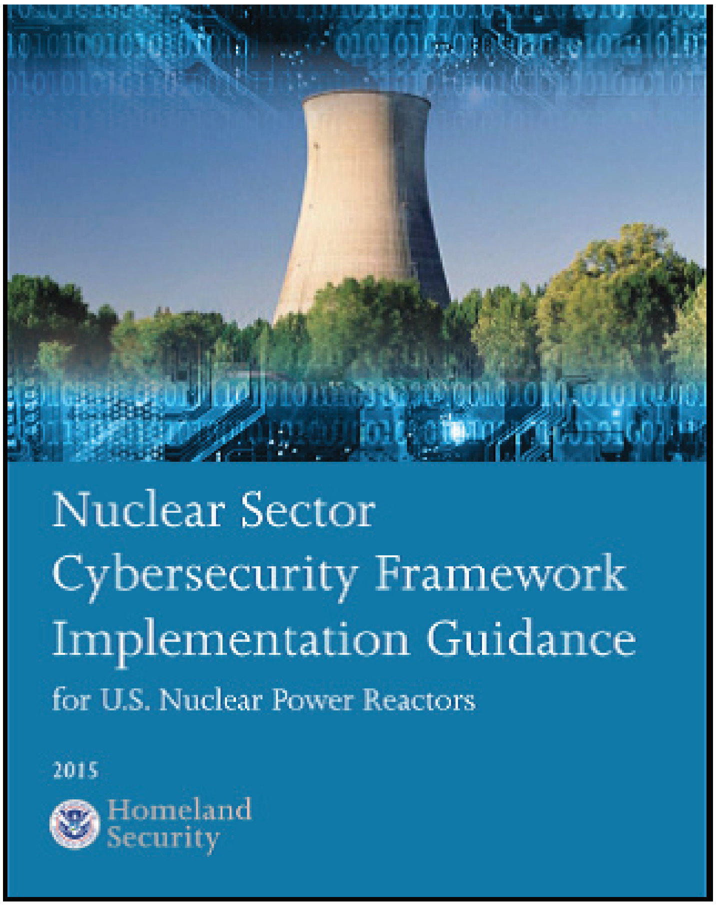
- Guidance for greater cyber security at nuclear facilities has been issued through regional advisory bodies, such as the European Union's Energy Expert Cyber Security Platform (EECSP). A cross–sectoral EECSP report from February 2017 identified vulnerable cyber security gaps in EU member states' energy sectors, and recommended various initiatives for the European Commission to develop a European strategic framework and auxiliary legislative acts to promote greater cyber security in the nuclear sector.

- At the international level, successive UN Groups of Governmental Experts (GGE) delivered reports in 2010, 2013, 2015 and 2018 on cyber developments in the context of international security.

The operators and their security teams in the cyber space must utilise the dynamic open-source toolkit that leverages past experience and successes from the global community. This toolkit would incorporate materials already proven effective and could be adapted from existing International Atomic Energy Agency (IAEA) guidance, international standards and industry good practices and insight/ lessons provided by nuclear regulatory agencies, cyber security experts, or experienced sector personnel. This model is tried and tested.[24]

U.S. Example

The Nuclear Regulatory Commission (NRC) has issued guidance for U.S. operators on improving workforce development and performance assessment for cyber security at nuclear power plants. National Nuclear Security Administration includes cyber security in their security assessments at U.S. and international facilities, along with technical exchanges and training programs. It also developed a course on cyber security for nuclear power plant operators in partnership with the International Atomic Energy Agency which has published its own technical guidelines on computer security. It recently held its first cyber security course for nuclear power plant operators.[25]



Nuclear Sector Cybersecurity Framework Implementation Guidance

for U.S. Nuclear Power Reactors

2015

Homeland Security

Each U.S. nuclear power plant is equipped with extensive security measures to protect the facility from intruders and to protect the public from the possibility of exposure to radioactive releases caused by acts of sabotage. The U.S. NRC calls nuclear power plants "among the best-protected private sector facilities in the nation."

In November 2005, Nuclear Energy Institute (NEI) released NEI 04-04, "Cyber Security Program for Power Reactors," Revision 1. NEI provides guidance on establishing and maintaining a cyber security program, and incorporates assessment methodology. The NEI program provides for the cyber security protection of all systems in the plant including those necessary for reliable electrical generation. The guidance provides a risk-informed approach, where consequences to plant functions are considered and provides guidance on establishing a cyber security defensive strategy incorporating multiple defensive layers with increasing levels of security protection. NEI also provides guidance on incorporating cyber security considerations into the procurement process. The NEI program includes the following steps:- [26]

- Define current cyber security program.
- Identify Critical Digital Assets (CDAs).
- Validate configuration.
- Assess susceptibility.
- Assess consequences.
- Determine risk.
- Refine defensive strategy.
- Continue program management

In May 2010 the NRC endorsed NEI 08-09, 'Cyber Security Plan for Nuclear Power Reactors'. It provides a template for cyber security plans and a catalog of technical, operational and management of cyber security controls. The template for the implementation schedule provides eight milestones—seven interim milestones and an eighth milestone for full implementation. The first seven milestones are designed to address the most prominent threats to the plant's most important systems. These milestones include the establishment of a cyber security assessment team, hardware-based isolation of key networks and assets, tightening controls over portable media and equipment, enhancing existing insider threat mitigation, instituting protective measures for digital equipment that could impact key safety systems and establishing ongoing monitoring and assessment activities for implemented cyber security measures. By December 31, 2012, each plant completed the initial seven milestones.

Post-2012 activities (the eighth milestone) include the completion of policy and procedural revisions that enhance existing capabilities, the completion of any remaining design related modifications necessary to implement the cyber security plan and institution of protective measures for lower consequence assets. In January 2013, the NRC began inspecting power plant cyber security program implementation of the initial seven milestones and completed inspections at each power plant at the end of 2015.

U.K. Example

The Office for Nuclear Regulation (ONR) is the UK regulator for safety and security in the civil nuclear industry and is responsible for ensuring that operators comply with current UK regulatory requirements. In 2007, the ONR announced a Generic Design Assessment (GDA) process to scrutinize candidate designs for new build nuclear power plants in the UK, with the express purpose of verifying that such designs could be safely and securely constructed and operated within the UK.[27]

At the international level, important efforts have been undertaken by the IAEA and the World Institute for Nuclear Security (WINS). The IAEA, for instance, provides hands on training in cyber security at nuclear facilities to member states. Moreover, it has worked to develop and publish guidance for developing and implementing cyber security plans at nuclear facilities.[28]

To try to get ahead of the threat, the non-partisan, non-profit organization Nuclear Threat Initiative (NTI) identified four overarching priorities, as well as specific actions, that if implemented would dramatically reduce the risk of damaging cyber attacks on nuclear facilities. They include:-

- Institutionalize cyber security.
- Mount an active defense.
- Reduce complexity.
- Pursue transformation.

It is worth perusing their report for the details of these priorities. It is critical that these priorities be implemented by coordinated actions among government, industry and regulators.[29]

Issues to Consider

A study of the above documents will indicate that comprehensive instructions exist for cyber security of nuclear plants globally. Similar strict instructions and standard operating procedures would also be available with Germany, Japan, France, Russia and other countries having nuclear power plants. Training for personnel responsible for cyber security is also organized. Have the people/ organization responsible for the cyber security of our nuclear installations studied all these instructions available in open domain, interacted with foreign peers and issued comprehensive cyber security instructions tweaking these to our specific requirements. Have there been some high end training from these organizations? Who would issue these instructors : the regulators or NCIIPC?

Collaboration with National and International Agencies

Interoperability and interdependency requirements that an asset owner shares with its service provider and supply chain create new attack vectors for the adversary. Regulators, suppliers/vendors, auditors, advisors and other contractors are all vulnerable to cyber attacks and are potential vectors for compromising operators/transporters. Relationships with them need to be well managed as attackers will often target these entities as a pathway to the organization due to their often vulnerable security posture. All organizations are expected to include cyber security as part of their general risk assessment and promote cyber awareness among their leadership, staff and any other employed entities. There is a requirement of stronger cyber security requirements for operational partners that operators and stakeholders rely on specifically for third parties, contractors and suppliers involved with the nuclear sector.

There has been discussions with European Union (EU), the U.S. work on the National Institute of Standards and Technology (NIST) Cyber security Framework and the U.S.-Canadian electric sector to arrive at possible models that could be used alongside some countries' minimum regulatory requirements. As advanced persistent threat cannot be prevented, defense-in-depth and resilience are critical for nuclear installations. Countries need not depend solely on international organizations or other governments for this expertise. Public-private partnerships like the World Institute for Nuclear Security and World Association of Nuclear Operators also share information about best practices and can serve as a knowledge conduit for states where nuclear power implicates national security concerns. India has established the Global Centre for Nuclear Energy Partnership as a forum for bilateral and multilateral cooperation in nuclear security that could be widened to include cyber security. This could be an opportunity for India to become a leader in nuclear cyber security.

Audit

Regular cyber security audits of these extremely sensitive nuclear installations are done by designated organizations. Normally auditors see whether standard instructions are complied with. Some standards like ISO 27001 are used as benchmarks. IEC 62645, a new standard by the International Electro-technical Commission (IEC) focused on the issue of requirements for computer security programmes and system development processes to prevent and/or minimize the impact of cyber attacks against computer-based Instrumentation and control (I&C) systems.

Developed since 2009 and published end of 2014, the standard is intended to be used for changing or establishing new security programmes for I&C systems of operating and new nuclear power plants. The IEC 62645 standard has been developed by the Subcommittee 45A (SC45A) of the IEC, addressing I&C of nuclear facilities. SC45A has issued many worldwide respected standards on different areas of I&C systems and more particularly for safety related I&C. It works in close coordination with the IAEA on Safety related issues for decades and more recently on cyber security issues.

Standards such as ISO/IEC 27001 and ISO/IEC 27002 are not directly applicable to Cyber security of digital I&C systems in nuclear power plants, due to their specificities including regulatory and safety requirements. The IEC 62645 standard for computer security brings a new set of guidance from IEC, in conjunction with IAEA and country specific standards, to the international community with regards to computer security for nuclear facilities. This is the first standard in a new series of IEC nuclear standards to address computer security and respond to the ever growing and expanding threat from electronic means to challenge the protection, control and information systems supporting nuclear plants around the world.

The following logical process highlights how a nuclear facility can develop, implement, maintain and improve computer security:-

- Follow national legal and regulatory requirements.
- Examine relevant IAEA and other international guidance.
- Ensure senior management support and adequate resources.
- Define a computer security perimeter.
- Identify the interactions between computer security and facility operation, nuclear safety and other aspects of site security.
- Create a computer security policy.
- Perform risk assessment.
- Select, design and implement protective computer security measures.
- Integrate computer security within the facility's management system.
- Regularly audit, review and improve the system.

An organization should plan, establish, implement and maintain an audit program, including the frequency, methods, responsibilities, regulatory guidance, reporting and technical requirements. The audit programs should consider the importance of the processes concerned and the results of previous audits. The organization should also ensure that the results of the audits are reported to the relevant management and retain documented information as an evidence of the audit program and audit results. The security audits should gradually cover multiple parts of a nuclear power plant over multiple audit sessions in subsequent years. As a good practice, typically security aware utilities are performing internal audits followed by external security audits. During the independent external security audits typically the internal audit results will be considered a part of the guidance for selecting security audit topics.

Audit Considerations

The following questions arise in the context of Audit:-

- Which audit standard was followed by both internal and external auditors? Was it latest version of IEC 62645 standard?
- Who are the internal auditors of nucler power plants, how are they selected?
- In the last audit was the cyber attack detected?

- Auditors check certain following of instructions. Were they capable of detecting the sophisticated attack, if it was not reported from outside?

Role of Private Sector

New skill combinations will also be essential. Cyber security specialists and teams responsible for critical infrastructure will need to consult with each other and expand their skill sets to develop a complete, accurate picture of vulnerabilities, issue severity and possible impacts. For example, to accurately reflect risk exposure and protect the power grid from cyber attack, states will need combined expertise in cyber and the cascading impacts of destabilizing the physical power stations. It is also important to consider that preventive measures are not always foolproof. Improving awareness of how new threats present themselves and being able to detect abnormal conditions and expedite responses are essential to reducing harm to the public when attackers are successful.

Challenges to addressing the cyber threat are aggravated by a shortage of technical expertise in the cyber-nuclear space. Finding experts with specific knowledge of digital control systems in a nuclear environment is difficult.

Threat to ISRO

The *Indian Express* reported that on September 4 that both the NPCIL and the ISRO were alerted about a possible cyber security breach in their systems by a suspected malware. The warning came from a U.S.-based cyber security company, which said a 'threat actor' had breached master 'domain controllers'. ISRO has not commented on this issue or issued any public statement. However, sources reportedly confirmed to the newspaper that with the proposed lunar landing of Chandrayaan 2 due in about 100 hours (it subsequently failed) and the safety of a nuclear power plant at stake, a multi-agency team swung into action soon after the threat was received.[30]

In the past, North Korean cyber activity has targeted the ISRO's National Remote Sensing Center and the Indian National Metallurgical Laboratory and conducted network reconnaissance on laboratories and research centers. The use of humans, rather than network connections, to bypass an air gap in Indian critical infrastructure by North Koreans or their associates, cannot be totally ruled out. The malware that attacked the KNPP system was reportedly custom-built for the nuclear power plant's IT systems. That suggests that such a breach to the nuclear power plant could have happened already.[31] The concerned agencies like ISRO must have looked into such issues and prepared in case of any future incidence.

Leaving no Coincidences Uninvestigated

One of the KNPP's power units stopped power generation on October 19 due to low Steam Generator level. The two power units had some problem on the "feed water side, with a valve which feeds water to the steel generator". The temporary shutdown rectified the problem and the two power units are now operating at 100 percent (1000 MW) and 60 percent (600 MW) capacity, respectively. The second unit is not operating at full capacity because there is a 'vibration problem'. As per manufacturer's instructions, the operations have been restricted. As per authorities these were mechanical issues, not ones arising out of any hack or cyber security compromise.

The fact that the plant has suffered multiple shut downs suggests a serious and persistent equipment problem. If this is not malware related, this points to a possibly more serious design problem.[32] Some of the issues to examine are:- [33]

- To what extent external network at KNPP could have been compromised?
- What kind of data the Dtrack could be mining from the external network?
- What might have caused the valve in the second power plant to stop functioning?
- Will it be in order for India to have a disclosure policy when it comes to cyber attacks on national infrastructure?

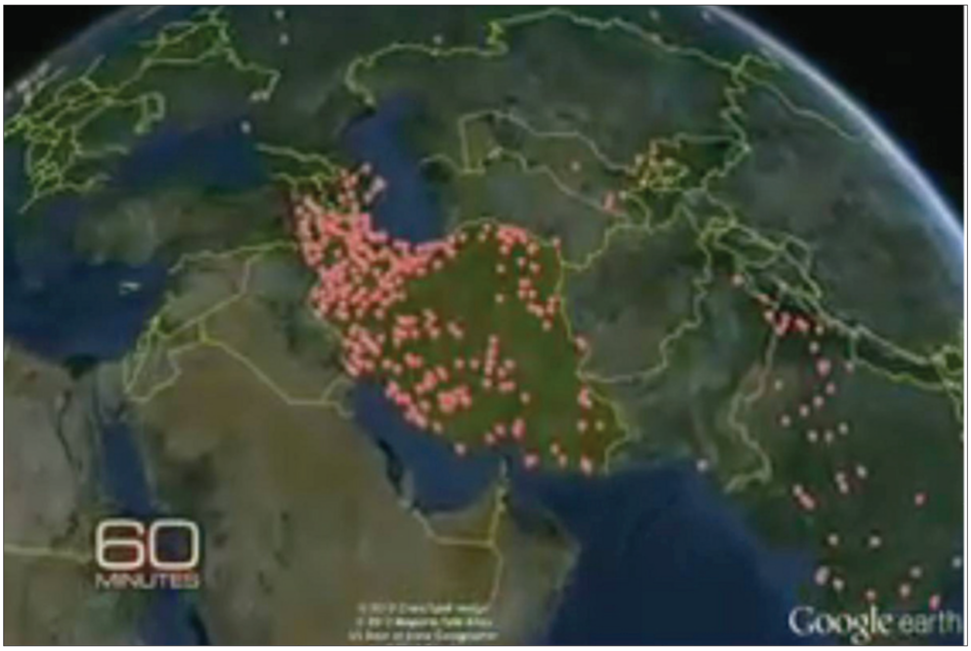
GSLV-F2 Launch Failure

India's Geosynchronous Satellite Launch Vehicle (GSLV-F02), with INSAT-4C on board, was launched from Satish Dhawan Space Centre, Sriharihota Range (SHAR) on July 10, 2006. However, GSLV-F02 could not complete the mission. ISRO in an official statement said, "The detailed analysis of the data received from the vehicle is being analysed to pinpoint the exact reasons."[34]

However, unsubstantiated reports said that failure of the ISROs launch during that time was due to infection of Siemens Programmable Logic Controller (PLC) which ISRO also used. An U.S. based security researcher, Jeffrey Carr, author of the book 'Inside Cyber Warfare', has drawn a link between the failure of INSAT 4B and Stuxnet; the Siemens-targeting Stuxnet worm was created by U.S. and Israel. While Stuxnet had made its way to the Iran's first nuclear power plant, Carr stated that the ISRO, which utilized the flawed Siemens devices, had also fallen prey to the Stuxnet worm. Around half of the transponders on the Indian satellite INSAT-4B closed down suddenly because of a solar panel failure on 9 July 2010. Carr suggested that China was behind the attack. In Forbes' The Firewall Blog, Carr wrote that ISRO "is a Siemens customer". According to the resumes of two former engineers who worked at the ISRO's Liquid Propulsion Systems Centre, the Siemens software in use is Siemens S7-400 PLC and SIMATIC WinCC, both of which will activate the Stuxnet worm."

A report in September from Symantec pointed out that while 58 per cent of infections were in Iran, about 18 per cent was in Indonesia and nearly 10 per cent in India.[35] The ISRO officials countered that it doesn't seem to have been the Stuxnet which did INSAT 4B in but it was a power supply anomaly in one of the solar panel that brought the transponders down. ISRO officials, requesting anonymity, said that the worm only strikes a satellite's programme logic controller (PLC). "We can confirm that Insat-4 B doesn't have a PLC. So the chances of the Stuxnet worm attacking it appear remote. In PLC's place, Insat-4 B had its own indigenously-designed software which controlled the logic of the spacecraft".[36] On 9 July, half the transponders on India's three-year old INSAT-4B satellite shut down unexpectedly due to a solar panel failure. While there is no reason to counter the government agencies, the coincidences leave reasons to raise eye brows. Lack of official statements does not help.

A photo of Siemens PLC affected by Stuxnet is given below; a large number of affected PLCs were in India.



Implications on Cyber Warfare

In all probability, the present case could be a Computer Network Exploitation Operation. The intruders seemed to be focusing on gathering of sensitive information and technology theft. Access could have been gained over extended periods of time. Any data on yields or fissile material would have proved invaluable to the hackers. The hackers could be looking for fissile material yields as part of a larger operation to determine India's current civilian and military nuclear programs. India's nuclear secrets on yields could help them build a picture of the country's strategic weapons force posture, as well as civilian command and control of its nuclear power generation facilities. It is suspected that the North Koreans were a front for the Chinese and the Pakistanis, both being India's traditional rivals. However, the linkages cannot be established.

To shift from computer network exploitation operations to computer network attacks or offensive cyber operations is not very difficult. An ongoing espionage operation like the one which affected KNPP could easily be weaponised into a destructive attack if the intruder was already inside the system, and the malware could be made to do offensive operations if the intent is changed. It was not destructive because the actor decided against it.

India is a recognized nuclear weapons power and its nuclear program, both civil and military, are joined at the hip. The DAE reports directly to the Prime Minister, as does the Nuclear Command Authority. Being extremely sensitive in nature, any cyber attacks on nuclear weapons systems, command and control etc. cannot be discussed in the open domain. However, it is certain that implications of KNPP cyber intrusion are analysed and discussed threadbare and remedial action, if any, is required taken.

Hacking into a nuclear weapon would undoubtedly be very hard, but no nuclear system or its support systems are invulnerable. An example of a nuclear submarine may be taken. While it would be extremely difficult to hack the submarine while on patrol somewhere at the bottom of the Indian Ocean, but the submarine and its weapons systems rely on coding written by humans for all aspects of its operations. These are regularly patched and updated when in port. Both activities provide potential access points for attackers wishing to deploy malware that might be used or triggered at a later date. Likewise, an adversary might attack early warning systems or command and control infrastructure as an aggressive, coercive or even pre-attack action. The 2007 Israeli bombing of a suspected Syrian nuclear facility in Operation Orchard, where hackers purportedly neutralised Syrian air defence radar, is a good example of this.

India has had some debacles in its naval fleet while at port/dock in spite of all possible security measures; possible human follies, intended or unintended may not be overlooked.

Recommendations

A large number of questions have been raised in this paper. It is quite probable that many of these questions had been addressed earlier. The incident at KNPP needs to be analysed in great details. Suitable lessons must be learned. Necessary remedial actions, wherever applicable, should be put into place. The following issues could be deliberated upon:-

Government Response in the Media. Though the media reported that the malware also attacked ISRO, there has been no official response. In absence of official statements there is a scope of rumour mongering and kite flying. Two contradictory statements by NPCIL have been construed by the media as lack of openness (the attack happened almost two months earlier); there should be an institutional mechanism to address the media after any such report.[37]

Attribution. The Government of India should develop the capability to attribute to the perpetrators of this action and nail them comprehensively. India must have capacity to take offensive action as a measure of deterrence.

Role of Regulators. There is a requirement of re visiting the following issues:-

- Core competencies and resources of the regulator and as to how are their competencies to be assessed.
- The process of appointment and evaluation of regulators.
- The process of consulting vertically and horizontally with other regulators of CII.
- DEsignating the regulators.

Operating System. A decision needs to be taken as to which operating system should be used in the IT network of all CII. If the network is air gapped then do we require patching and software upgradation? Best practices from our own agencies should be followed for patch management. It is recommended that security solution called Secure Network Access System (SNAS) developed by BARC and maintained by Electronic Corporation of India Limited (ECIL) be considered for use.

International Best Practices. The people/organization responsible for the cyber security of our nuclear installations have to be abreast with latest practices followed by nuclear power plants all over the world, regularly interact with foreign peers and issue comprehensive cyber security instructions tweaking these to our specific requirement. They should attend some high end training from globally recognized bodies.

Audit. For cyber audit of nuclear power plants, the globally accepted standard is the latest version of IEC 62645. This should be used in our nuclear power plants.

Role of Private Sector. Lot of competencies in this niche field reside in the private sector. How can these expertise be incorporated into the government organizations need to be examined.

Conclusion

Determined adversaries use targeted, adaptive strategies and customized cyber tools and may even consider compromising the supply chain meaning equipment could be infected before it is even installed at a nuclear facility. Targeted attacks have proved effective in compromising conventional cyber security defenses. It is clear that well resourced, persistent adversaries can defeat even technologically advanced security solutions. The examples of the Stuxnet attacks on the Natanz uranium enrichment facility in Iran, hack of Korea Hydro and Nuclear Power in South Korea, malware found on systems at a German nuclear power plant etc. demonstrate that the current approach to cyber security at nuclear facilities is not equal to the challenge.

The table given at the Appendix lists 23 publicly disclosed cyber incidents that have occurred at nuclear facilities around the world since 1990. It is possible that more incidents have occurred that have not been publicly disclosed or for which the details are classified or otherwise unavailable.

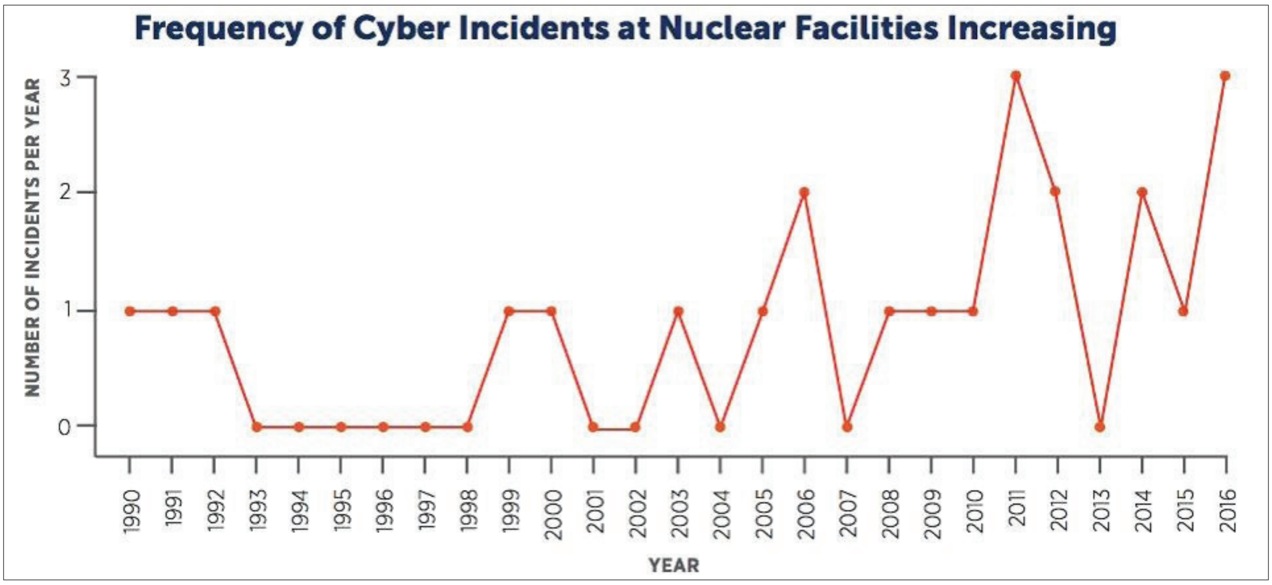


Image Source : https://www.forbes.com/sites/jamesconca/2019/11/08/how-well-is-the-nuclear-industry -protected-from-cyber-threats/#496e7a753497

Protecting nuclear facilities from damaging cyber attacks is made more difficult by their complexity. A typical facility might include a huge number of digital components, including legacy systems with no built-in security. Older facilities are transitioning to digital systems that often bring greater reliability and safety, but also increase vulnerability to cyber attacks.

The problem of cyber security is not new to the nuclear power industry. It does not require solutions radically different from those already in place in other critical information infrastructure. The nuclear industry's history of safety and security culture and the body of research on sector specific cyber security recommendations, globally together, can offer a path toward a nuclear power industry that better defends itself against cyber threats. The avenues for fostering cooperation and sharing best practices have been established, as has the need for workforce development.

Crafting a strategy that protects facilities from dynamic, evolving cyber threats requires fresh, unconstrained examination of the overarching framework that guides cyber security. Organizations must manage residual risk. One way to manage risk is to enhance resilience, which enables the organization to absorb the adverse impact of the security incident and re-establish itself quickly.

According to cyber security major 'Symantec', India is among the top three countries in the world after the U.S. and China when it comes to phishing and malware attacks. As per Subex, an Indian telecommunications firm which produces regular reports on cyber security, in the first half of this year, no country endured more cyber attacks on its Internet of Things - the web of internet connected devices and infrastructure - than India did. Between April and June alone, it recorded cyber attacks jumped by 22 percent, with 2,550 unique samples of malware discovered.[38]

While governments can't control every aspect of cyber security, they can certainly help shape the future of cyber security based on lessons learned from other nations, threats and technologies. Cyber security is vital to a proper functioning and prosperous economy and it is important for citizens to realise the importance of government to the evolution of cyber security in both the public and private sectors.[39] Today's defenses are no longer adequate, and a fresh look at how to best protect nuclear facilities from cyber attack is needed. The threat is too great and the potential consequences are too high. As an energy provider, the nuclear industry is just one element of critical infrastructure, albeit a special one given potential consequences. The work to make critical infrastructure as a whole 'cyber-secure' should therefore be considered.

In view of the incident at the KNPP, all stakeholders have to their heads together, identify the vulnerabilities in the critical information infrastructure and take remedial measures in a time bound manner. The questions raised in this paper come to the mind of an independent observer who is not a part of the system. Many of the issues highlighted may have therefore been addressed already. Yet, the nation must be assured that these extremely critical infrastructures are in safe from anti-national machinations.

Appendix

Cyber Incidents at Nuclear Facilities

Ser	Month /Year	Name	Country	Description	Category
1	Jan 1990	Bruce Nuclear Generating Station	Canada	Software error leading to release of radioactive water	Accidental
2	Sep 1991	Sellafield reprocessing plant	United Kingdom	Software bug leading to unauthorized opening of doors; widespread software errors	Accidental
3	Feb 1992	Ignalina Nuclear Power Plant	Lithuania	Employee attempted sabotage	Intentional
4	Jun 1999	Bradwell Nuclear Power Plant	United Kingdom	Employee altered/destroyed data	Intentional
5	Jan 2000*	Kurchatov Institute	Russian Federation	Bug in nuclear materials accounting software	Accidental
6	Jan 2003	Davis-Besse Nuclear Power Station	United States	Virus blocked operator access to reactor core information	Accidental
7	Jun 2005*	Japanese Nuclear Power Plants	Japan	Data release	Unknown
8	Aug 2006	Browns Ferry Nuclear Plant	United States	Technical failure	Accidental
9	Dec 2006	Syrian Nuclear Program	Syria	Espionage	Intentional
10	Mar 2008	Edwin I. Hatch Nuclear Power Plant	United States	Shutdown caused by software update	Accidental
11	Mar 2009	Energy Future Holdings	United States	Employee attempted sabotage	Intentional
12	Jun 2010*	Natanz Nuclear Facility	Iran	Stuxnet virus used to destroy centrifuges	Intentional
13	Apr 2011	Oak Ridge National Laboratory	United States	Data theft via spear-phishing	Intentional
14	Sep 2011	Areva	France	Network intrusions	Unknown
15	Oct 2011*	Natanz Nuclear Facility	Iran	Duqu virus used to conduct espionage	Intentional
16	May 2012*	Natanz Nuclear Facility	Iran	Flame virus used to conduct espionage	Intentional
17	Nov 2012	Susquehanna Nuclear Power Plant	United States	Technical failure	Accidental
18	Jan 2014	Monju Nuclear Power Plant	Japan	Data release	Unknown
19	Dec 2014	Korea Hydro and Nuclear Power Company	South Korea	Data theft and release	Intentional
20	Feb 2015	Japanese nuclear material control center	Japan	Nuclear facility used as relay point in cyber attack	Unknown
21	Feb 2016*	Nuclear Regulatory Commission/U.S. Department of Energy	United States	Employee attempted to infect government computers with viruses distributed via spear-phishing emails	Intentional
22	Apr 2016	Gundremmingen Nuclear Power Plant	Germany	Two viruses entered plant's fuel rod monitoring system	Unknown
23	Jun 2016*	University of Toyama, Hydrogen Isotope Research Center	Japan	Data theft via spear-phishing	Intentional

Endnotes

1. Debak Das, An Indian nuclear power plant suffered a cyberattack. Here's what you need to know, 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/

2. Sean Gallagher, Indian nuke plant's network reportedly hit by malware tied to N. Korea, October 29, 2019, https://fortunascorner.com/2019/10/30/indian-nuke-plants-network-reportedly-hit-by-malware-tied-to-n-korea/

3. Pukhraj Singh, What the cyber attacks on Kudankulam and Isro show, https://www.hindustantimes.com/analysis/what-the-cyber-attacks-on-kudankulam-and-isro-show-analysis/story-OVlR5MO18yk7jQFrnRvTpM.html

4. Days after cyberattack, India tells partner Russia that Kudankulam nuclear plant safe, November 13, 2019, Available at : https://www.indiatoday.in/india/story/days-after-cyberattack-india-tells-partner-russia-that-kudankulam-nuclear-plant-safe-1618307-2019-11-13

5. Kaspersky Press Release on DTrack: previously unknown spy-tool by Lazarus hits financial institutions and research centers, September 23, 2019, available at : https://usa.kaspersky.com/about/press-releases/2019_dtrack-previously-unknown-spy-tool-hits-financial-institutions-and-research-centers

6. Konstantin Zykov, Hello! My name is Dtrack, September 23, 2019, available at : https://securelist.com/my-name-is-dtrack/93338/

7. Sushovan Sircar, N Korea Stole Data From Kudankulam Attack, Says Expert, The Quint, November 07, 2019, available at : https://www.thequint.com/news/india/kudankulam-nuclear-power-plant-cyber-attack-malware-north-korea-stole-information-data

8. Saikat Datta and Anand Venkatanarayanan, Cyberattack scare dogs India's nuclear plants, Asia Times, October 30, 2019, Available at : https://www.asiatimes.com/2019/10/article/cyberattack-scare-dogs-indias-nuclear-plants/

9. Saikat Datta and Andrew Salmon, North Koreans behind Indian nuclear plant hack, Asia Times, November 12, 2019, available at : https://www.asiatimes.com/2019/11/article/north-koreans-behind-indian-nuclear-plant-hack/

10. Sushovan Sircar, N Korea Stole Data From Kudankulam Attack, Says Expert, The Quint, November 07, 2019, available at : https://www.thequint.com/news/india/kudankulam-nuclear-power-plant-cyber-attack-malware-north-korea-stole-information-data

11. Kudankulam cyber attack: North Korean hackers stole technology data, analysts tell The Quint, November 07, 2019, available at : https://scroll.in/latest/942940/kudankulam-cyber-attack-north-korean-hackers-stole-technology-data-analysts-tell-the-quint

12. Sensecy, A Verint Company Report, Cyber Threat Intelligence Alert, Indian Nuclear Power Plant Attacked with Dtrack Malware, November 2019.

13. Along With Kudankulam, ISRO Also Warned About Cyber Security Breach: Report, The Wire, November 06, 2019, available at : https://thewire.in/tech/isro-kudankulam-cyber-security

14. A cyber-attack on an Indian nuclear plant raises worrying questions, The Economist, November 07, 2019, available at : https://www.economist.com/asia/2019/11/01/a-cyber-attack-on-an-indian-nuclear-plant-raises-worrying-questions

15. Alexandra Van Dine, Michael Assante, Page Stoutland, Ph.D. Outpacing Cyber Threats, Priorities for Cybersecurity at Nuclear Facilities, Nuclear Threat Initiative, 2016, available at : https://media.nti.org/documents/NTI_CyberThreats__FINAL.pdf

16. Kevin Poulsen, "Slammer worm crashed Ohio nuke plant network," Security Focus, August 19, 2003, available at : https://www.securityfocus.com/news/6767 . Debra Decker, Kathryn Rauhut, "Cyber Risks Go Nuclear," Nuclear Intelligence Weekly, August 10, 2018, available at : https://www.stimson.org/content/cyber-risks-go-nuclear . ICS-CERT Recommended Practices, available at : https://ics-cert.us-cert.gov/Recommended-Practices

17. Debra Decker, Kathryn Rauhut, Sara Z. Kutchesfahani and Erin Connolly, Nuclear Cybersecurity Risks And Remedies, Fissile Materials Working Group, Stimson, March 2019, available at : https://armscontrolcenter.org/wp-content/uploads/2019/03/FMWG_CyberReport_webready.pdf

18. Ankit Panda , Indian Nuclear Power Facility Denies Unverified Reports of a Cyber Attack, October 29, 2019, available at : https://thediplomat.com/2019/10/indian-nuclear-power-facility-denies-unverified-reports-of-a-cyber-attack/

19. Draft Background Paper Cybersecurity: The Role and Responsibilities of an Effective Regulator, 9th ITU Global Symposium for Regulators Beirut, Lebanon, November 2009.

20. The background paper on Cybersecurity: The Role and Responsibilities of an Effective Regulator, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/papers.html

21. Maj Gen PK Mallick, VSM (Retd), Cyber Security in India Present Status, Vivekananda International Foundation, October 2017, available at : https://www.vifindia.org/issuebrief/2017/octobe/30/cyber-security-in-india-present-status

22. Aditi Agrawal, What we know about the alleged cyber attack on the Kudankulam Nuclear Power Plant (and what we don't know), October 30, 2019, available at: https://www.medianama.com/2019/10/223-kundankulam-nuclear-power-plant-cyber-attack/

23. Saikat Datta and A. Venkatanarayanan, Cyberattack scare dogs India's nuclear plants, October 30, 2019, available at : https://www.asiatimes.com/2019/10/article/cyberattack-scare-dogs-indias-nuclear-plants/

24. For a chart of IAEA safety and security reviews, available at : https://gnssn.iaea.org/Pages/PeerReviewsandAdvisoryServicesByAudienceAndTheme.asp . Physical security reviews are part of IAEA International Physical Protection Advisory Service (IPPAS) missions. See IPPAS Computer Security Review Guidelines starting on p. 214, available at : https://www-pub.iaea.org/MTCD/Publications/PDF/SVS29_web.pdf. For a broader understanding of nuclear industry performance assessments, available at : https://www.stimson.org/content/nuclear-energy-securingfuture-case-voluntary-consensus-standards.

25. United States Nuclear Regulatory Commission, Audit of NRC's Cyber Security Inspections at Nuclear Power Plants, June 4, 2019 available at : https://www.nrc.gov/docs/ML1915/ML19155A317.pdf

26. Nuclear Sector Cybersecurity Framework Implementation Guidance for U.S. Nuclear Power Reactors, Homeland Security, 2015, available at : https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/nuclear-framework-implementation-guide-2015-508.pdf

27. Roger Brunt, Beyza Unal, Cybersecurity by Design in Civil Nuclear Power Plants, International Security Department, July 2019, available at : https://www.chathamhouse.org/sites/default/files/2019-08-15-CybersecurityNuclearPowerPlants.pdf

28. The IAEA has published several relevant documents and is continuing to work to assemble guidance on this issue. The documents are International Atomic Energy Agency, Technical Guidance Reference Manual: Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No.17 (Vienna: IAEA, 2011), available at : www.pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf ; International Atomic Energy Agency, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Specific Safety Guide No. SSG-39 (Vienna: IAEA, 2016), available at : www.pub.iaea.org/MTCD/publications/PDF/Pub1694_web.pdf ; International Atomic Energy Agency, Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants, IAEA Nuclear Energy Series No. NP-T-3.12 (Vienna: IAEA, 2011), available at : www.pub.iaea.org/MTCD/Publications/PDF/Pub1495_web.pdf ; International Atomic Energy Agency, Conducting Computer Security Assessments at Nuclear Facilities (Vienna: IAEA, 2016), available at : www.pub.iaea.org/MTCD/Publications/PDF/TDL006web.pdf ; and International Atomic Energy Agency, Computer Security Incident Response Planning at Nuclear Facilities (Vienna: IAEA, 2016), available at : www.pub.iaea.org/MTCD/Publications/PDF/TDL005web.pdf

29. James Conca, How Well Is The Nuclear Industry Protected From Cyber Threats? November 8, 2019, available at : https://www.forbes.com/sites/jamesconca/2019/11/08/how-well-is-the-nuclear-industry-protected-from-cyber-threats/#19e118213497

30. Sam Spencer, Was Hack on Indian Nuclear Plant Used to Test Cyber Intrusion Abilities? Available at : https://www.ccn.com/was-hack-on-indian-nuclear-plant-used-to-test-cyber-intrusion-abilities/

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

32. Aditi Agrawal, What we know about the alleged cyber attack on the Kudankulam Nuclear Power Plant (and what we don't know), October 30, 2019, available at: https://www.medianama.com/2019/10/223-kundankulam-nuclear-power-plant-cyber-attack/

33. Abhijit Iyer-Mitra, Questions the alleged cyber-incident at Kudankulam Nuclear Plant raises, Moneycontrol.com , October 30, 2019, available at: https://www.moneycontrol.com/news/india/security-questions-the-alleged-cyber-incident-at-kudankulam-nuclear-plant-raises-4585321.html

34. https://www.isro.gov.in/update/10-jul-2006/gslv-f2-launch-failure

35. Anirudh Bhattacharyya, Stuxnet hits India the most, Hindustan Times, October 04, 2010, available at: https://www.hindustantimes.com/world/stuxnet-hits-india-the-most/story-KMX3bWo7kNG5Az6IXK3NKM.html

36. Srinivas Laxman, Cyber threat: Isro rules out Stuxnet attack on Insat-4 B, October 12, 2010,The Economic Times, available at : https://economictimes.indiatimes.com/tech/internet/cyber-threat-isro-rules-out-stuxnet-attack-on-insat-4-b/articleshow/6733370.cms

37. Jay Mazoomdaar, Not only Kudankulam, ISRO, too, was alerted of cyber security breach, November 6, 2019, available at : https://indianexpress.com/article/india/not-only-kudankulam-isro-too-was-alerted-of-cyber-security-breach-6105184/

38. N Madhavan, 2019Is India cyber security ready? November 07, available at : https://www.thehindubusinessline.com/opinion/columns/is-india-cyber-security-ready/article29911679.ece

39. Evolving Role Of Government In Cyber Security, White Paper, Fire Eye, 2018, available at : https://www.fireeye.com/content/dam/fireeye-www/solutions/pdfs/wp-evolving-role-gov.pdf

About the VIVEKANANDA INTERNATIONAL FOUNDATION

The Vivekananda International Foundation is an independent non-partisan institution that conducts research and analysis on domestic and international issues, and offers a platform for dialogue and conflict resolution. Some of India's leading practitioners from the fields of security, military, diplomacy, government, academia and media have come together to generate ideas and stimulate action on national security issues.

The defining feature of VIF lies in its provision of core institutional support which enables the organisation to be flexible in its approach and proactive in changing circumstances, with a long-term focus on India's strategic, developmental and civilisational interests. The VIF aims to channelise fresh insights and decades of experience harnessed from its faculty into fostering actionable ideas for the nation's stakeholders.

Since its inception, VIF has pursued quality research and scholarship and made efforts to highlight issues in governance, and strengthen national security. This is being actualised through numerous activities like seminars, round tables, interactive dialogues, Vimarsh (public discourse), conferences and briefings. The publications of VIF form lasting deliverables of VIF's aspiration to impact on the prevailing discourse on issues concerning India's national interest.

VIVEKANANDA INTERNATIONAL FOUNDATION
3, San Martin Marg, Chanakyapuri, New Delhi – 110021
Phone: +91-11-24121764, 24106698
Email: info@vifindia.org,
Website: https://www.vifindia.org
Follow us on twitter@vifindia

ISBN 978-81-943795-2-2
9 788194 379522