Case Study

Critical Infrastructure : Power and Energy Sector

Case : Mumbai Blackout

Chinese Cyber Exploitation in India's Power Grid

Introduction

During 2020 summer, Chinese and Indian troops clashed in a surprise border battle in the remote Galwan Valley, bashing each other to death with rocks and clubs .

Four months later On October 13, Mumbai faced a power outage which lasted for two hours starting from 10 am until the power situation was resolved by noon. Sources in the Maharashtra cyber department have revealed that in their initial investigation they have traced the infusion of malware at the Padgha-based state load dispatch center .The state load dispatch monitors power transmission and manages load dispatch to various areas across the Mumbai Metropolitan Region (MMR) covering the Mumbai City, Thane district, including areas across Navi Mumbai. The load dispatch center works on an automated system where data is monitored and could have been attacked

Some areas in suburban central Mumbai suffered outages for almost 10 to 12 hours till the power services resumed . Hospitals had to switch to emergency generators to keep ventilators running amid a coronavirus outbreak that was among India's worst. Government hospitals only had ICUs running on minimal back-up while Covid centers also ran on back-ups. Private generators were called in for supply at various hospitals and offices till the power services were back .The primary cause of the power outage was said to be due to tripping at the Padgha-based load dispatch center in Thane district which distributes power for Mumbai, Thane and Navi Mumbai areas.

During the stand-off between India and China at the Galwan valley, sources from Maharashtra Cyber through a report said that China-based hackers had started attacking the Indian cyberspace. The Chinese Information Warfare cell with the Chinese Army was suspected to be behind the growing number of attacks in the country.

The Maharashtra cyber department suspects that a malware attack could be responsible for Mumbai's power outage of October 2020. The Maharashtra cyber department has been roped in by the state government to conduct a probe in the matter.

The Maharashtra cyber department submitted a provisional report to the Maharashtra government on the massive grid failure which hit Mumbai and surrounding areas on October 12 2020. The 100-page report confirms a malware attack was behind the blackout and said that about 14 Trojan Horses and 8 GB of unaccounted data was found in the system, which according to the investigation was installed in the Maharashtra State Electricity Board (MSEB) system by unverified sources.

The Maharashtra Cyber department had said after thorough analysis and investigation it was found that all these attacks generated from China and were targeted at some of the most crucial sectors. Chinese malware was flowing into the control systems that manage electric supply across India, along with a high-voltage transmission substation and a coal-fired power plant.

The flow of malware was pieced together by Recorded Future, a Somerville, Mass., company that studies the use of the internet by state actors. It found that most of the malware was never activated. And because Recorded Future could not get inside India's power systems, it could not examine the details of the code itself, which was placed in strategic power-distribution systems across the country. While it has notified Indian authorities, so far they are not reporting what they have found.

Authorities began a formal investigation. Since then, Indian officials have gone silent about the Chinese code, whether it set off the Mumbai blackout and the evidence provided to them by Recorded Future that many elements of the nation's electric grid were the target of a sophisticated Chinese hacking effort.

It was possible that Indians were still searching for the code. But acknowledging its insertion, one former Indian diplomat noted, could complicate the diplomacy in recent days between China's foreign minister, Wang Yi, and his Indian counterpart, Subrahmanyam Jaishankar, in an effort to ease the border tensions.

The investigators who wrote The Recorded Future Group, said that "the alleged link between the outage and the discovery of the unspecified malware" in the system "remains unsubstantiated." But they noted that "additional evidence suggested the coordinated targeting of the Indian load dispatch centers," which balance the electrical demands across regions of the country. "I think the signaling is being done" by China to indicate "that we can and we have the capability to do this in times of a crisis," said retired Lt. Gen. D.S. Hooda, a cyberexpert who oversaw India's borders with Pakistan and China. "It's like sending a warning to India that this capability exists with us."

The conspicuous placement of malware in an adversary's electric grid or other critical infrastructure has become the newest form of both aggression and deterrence against the Enemy nations.Both India and China maintain medium-size nuclear arsenals, which have traditionally been seen as the ultimate deterrent. But neither side believes that the other would risk a nuclear exchange in response to bloody disputes over the Line of Actual Control, an ill-defined border demarcation where long-running disputes have escalated into deadly conflicts by increasingly nationalistic governments.Cyberattacks give them another option ,less devastating than a nuclear attack, but capable of giving a country a strategic and psychological edge. Russia was a pioneer in using this technique

The Chinese government, which did not respond to questions about the code in the Indian grid, could argue that India started the cyberaggression. In India, a patchwork of state-backed hackers were caught using coronavirus-themed phishing emails to target Chinese organizations in Wuhan during February 2020. A Chinese security company, 360 Security Technology, accused state-backed Indian hackers of targeting hospitals and medical research organizations with phishing emails, in an espionage campaign.

Four months later, as tensions rose between the two countries on the border, Chinese hackers unleashed a swarm of 40,300 hacking attempts on India's technology and banking infrastructure in just five days. Some of the incursions were so-called denial-of-service attacks that knocked these

systems offline; others were phishing attacks, according to the police in the Indian state of Maharashtra, home to Mumbai.

By December, security experts at the Cyber Peace Foundation, an Indian nonprofit that follows hacking efforts, reported a new wave of Chinese attacks, in which hackers sent phishing emails to Indians related to the Indian holidays in October and November. Researchers tied the attacks to domains registered in China's Guangdong and Henan Provinces, to an organization called Fang Xiao Qing. The aim, the foundation said, was to obtain a beachhead in Indians' devices, possibly for future attacks."One of the intentions seems to be power projection," said Vineet Kumar, the president of the Cyber Peace Foundation.

The foundation has also documented a surge of malware directed at India's power sector, from petroleum refineries to a nuclear power plant, since year 2019. Because it is impossible for the foundation or Recorded Future to examine the code, it is unclear whether they are looking at the same attacks, but the timing is the same.

Yet except for the Mumbai blackout, the attacks have not disrupted the provision of energy

On Feb. 28, 2021 The New York Times (NYT), based on analysis by a U.S. based private intelligence firm Recorded Future, reported that a Chinese entity penetrated India's power grid at multiple load dispatch points. Chinese malware intruded into the control systems that manage electric supply across India, along with a high-voltage transmission substation and a coal-fired power plant.

The NYT gives the impression that the alleged activity against critical Indian infrastructure installations was as much meant to act as a deterrent against any Indian military thrust along the Line of Actual Control as it was to support future operations to cripple India's power generation and distribution systems in event of war. It was founded that most of the malwares were never activated . The cyber security company had sent its findings to the Indian Computer Emergency Response Team (CERT-In) within the Ministry of Electronics and Information Technology of the Government of India. It informs that the government has acknowledged the receipt twice, though there has been no confirmation that the code infected in the power grid may have any links with China-based hackers.

Stuart Solomon, Recorded Future's chief operating officer, said that the Chinese state-sponsored group, which the firm named Red Echo, "has been seen to systematically utilize advanced cyber intrusion techniques to quietly gain a foothold in nearly a dozen critical nodes across the Indian power generation and transmission infrastructure." There have been recent reports of Chinese hacking activities in Indian cyberspace. According to the reports and above information it is concluded that this attack took place due to on going military deterrence challenge

Details of the report of Recorded Future

Since early 2020, Recorded Future's Insikt Group observed a large increase in suspected targeted intrusion activity against Indian organisations from Chinese state-sponsored hacker groups. In this report, details of a campaign conducted by a China-linked threat activity group, RedEcho,

targeting the Indian power sector has been analysed. The activity was identified through a combination of large-scale automated network traffic analytics and expert analysis. Data sources include the Recorded Future Platform, SecurityTrails, Spur, Farsight and common open-source tools and techniques.

Recorded Future's midpoint collection, from mid-2020 onwards, revealed a steep rise in the use of infrastructure tracked as AXIOMATICASYMPTOTE, which encompasses ShadowPad command and control (C2) servers, to target a large part of India's power sector. Using a combination of proactive adversary infrastructure detections, domain analysis and Recorded Future Network Traffic Analysis, it was found that a subset of these AXIOMATICASYMPTOTE servers share some common infrastructure tactics, techniques, and procedures (TTPs) with several previously reported Chinese state-sponsored groups, including APT41 and Tonto Team. According to cyber security firm FireEye, the targeting makes use of a modular backdoor called ShadowPad that was originally connected to state-sponsored groups like APT41 or Barium.

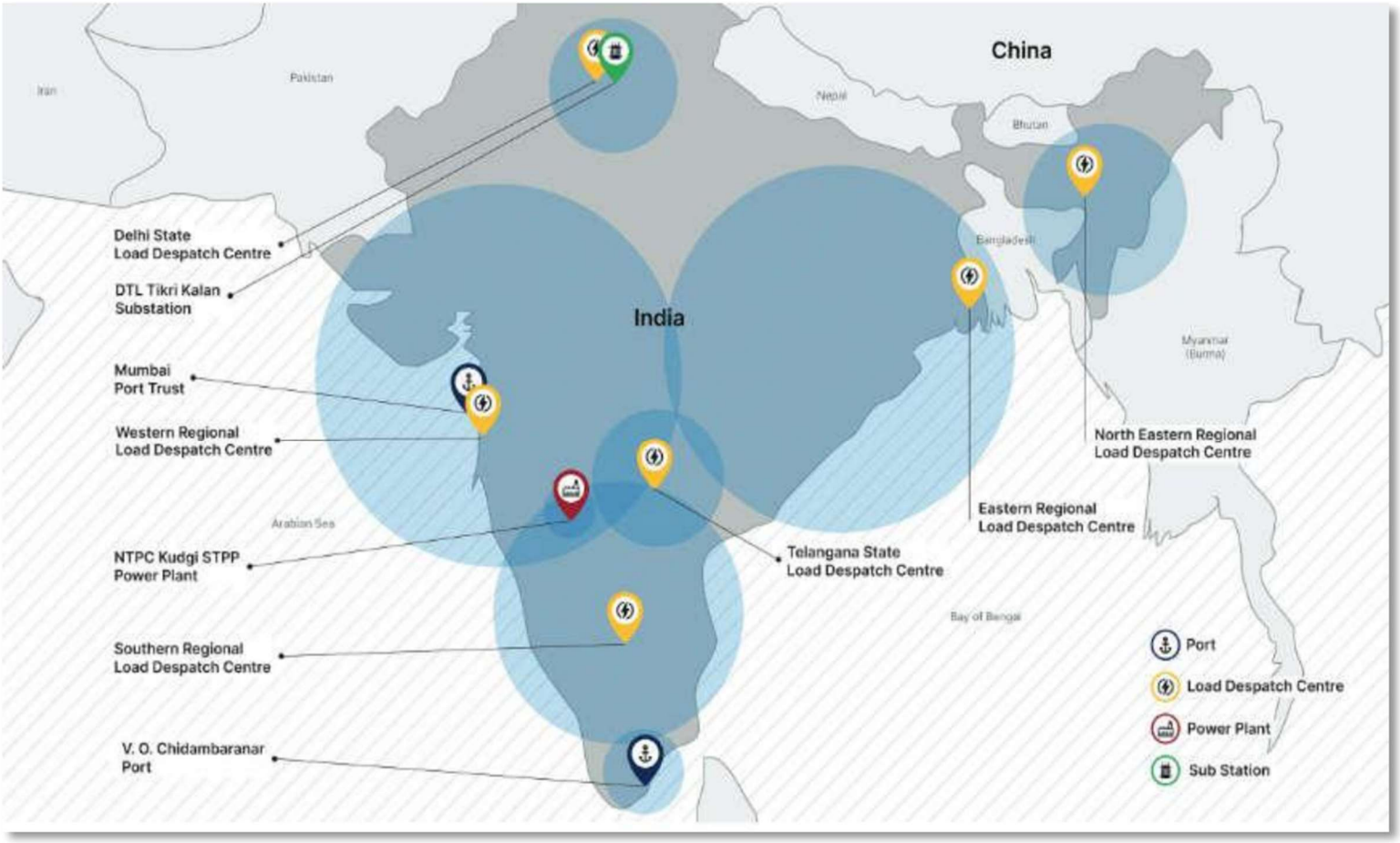
Over the last couple of years, at least five Chinese threat activity groups have used ShadowPad, including Tonto Team, KeyBoy, and Tick, suggesting that it is one of the latest capabilities being shared across Chinese state-sponsored groups for network intrusion campaigns since 2017. The report stated, "We assess that the sharing of ShadowPad is prevalent across groups affiliated with both Chinese Ministry of State Security (MSS) and groups affiliated with the People's Liberation Army (PLA), and is likely linked to the presence of a centralized ShadowPad developer quartermaster responsible for maintaining and updating the tool."

Recorded Future's chief operating officer, Stuart Solomon, told The New York Times that Red Echo "has been seen to systematically utilise advanced cyber intrusion techniques to quietly gain a foothold in nearly a dozen critical nodes across the Indian power generation and transmission infrastructure". The report states that the targeting of Indian critical infrastructure offers limited economic espionage opportunities. It causes significant concerns over potential pre-positioning of network access to support Chinese strategic objectives later. It can be used:

- To send a robust signaling message as a "show of force."
- To enable influence operations to sway public opinion during a diplomatic confrontation.
- To support potential future disruptive cyber operations against critical infrastructure.

Researchers of Recorded Future did not find enough evidence to attribute the activity to an existing group such as APT41 or Tonto Team. They are tracking it as a closely related but distinct group named RedEcho4. Within India's power sector, RedEcho conducted suspected network intrusions targeting at least four out of the country's five Regional Load Despatch Centres (RLDCs), alongside two State Load Despatch Centres (SLDCs). RLDCs and SLDCs are responsible for ensuring realtime integrated operation of India's power grid through balancing electricity supply and demand to maintain a stable grid frequency. The 12 organisations targeted by Red Echo included Power System Operation Corporation Limited, NTPC Limited, NTPC's Kudgi power plant, Western Regional Load Dispatch Centre, Southern Regional Load Dispatch Centre, North Eastern Regional Load Dispatch

Centre, Eastern Regional Load Dispatch Centre, Telangana State Load Dispatch Centre, Delhi State Load Dispatch Centre, the DTL Tikri Kalan (Mundka) sub-station of Delhi Transco Ltd, VO Chidambaranar Port and Mumbai Port Trust.



Suspected Indian power sector victims of RedEcho targeted intrusionsRecorded Future, Google Maps

Historical hosting overlaps also exist between RedEcho DDNS domain railway.sytes net and the previously reported APT41/Barium cluster. However, it is important to note that several DDNS domains attributed to Barium by Microsoft were also previously linked to Tonto Team threat activity in public reporting from Trend Micro. In their report, Trend Micro also noted that Tonto Team targeted India's Oil and Gas and Energy industries. The Recorded Future study investigators said that "the alleged link between the outage and the discovery of the unspecified malware in the system remains unsubstantiated." But they noted that "additional evidence suggested the coordinated targeting of the Indian load dispatch centres, which balance the electrical demands across regions of the country."

There have been indications of Chinese cyber-espionage activities in India earlier. In February 2021, Hindustan Times reported that the number of Indian government officials, including those from the sensitive ministries of defence and external affairs, had been subjected to a phishing campaign on February 10 that involved compromised government domain email addresses. While the news report

does not identify Chinese state-supported entities as being behind it, in the past, the Indian government had directly 8 identified China as being attempts to hack computers belonging to officials in the national security establishment5. Red Flag. On October 13, 2020 Mumbai faced a power outage that lasted for two hours, starting from 10 am until the power situation was resolved by noon. This had led to the cancellation of train services, stop work at the stock exchange and all the other offices and commercial establishments across Mumbai, Thane and Navi Mumbai areas. Government hospitals only had ICUs running on minimal back-up while Covid centres also ran on backups. Some areas in suburban central Mumbai suffered outages for almost 10 to 12 hours till the power services resumed. The power outage's primary cause was said to be due to tripping at the Padgha-based load dispatch centre in Thane district, which distributes power for Mumbai, Thane and Navi Mumbai areas. India Today reported that he Maharashtra cyber department suspects that a malware attack could be responsible for Mumbai's power outage. In their initial investigation, sources in the Maharashtra cyber department revealed that they had traced the infusion of malware at the Padgha-based state load dispatch centre. The Maharashtra Cyber department had said after thorough analysis and investigation, it has been found that all these attacks generated from China and were targeted at some of the most crucial sectors.

Details

Security experts of an Indian nonprofit organisation, the Cyber Peace Foundation, that follows hacking efforts reported a new wave of Chinese attacks, in which hackers sent phishing emails to Indians in October and November. Researchers tied the attacks to domains registered in China's Guangdong and Henan Provinces to an organisation called Fang Xiao Qing. The aim was to obtain an entry into Indians' devices, possibly for future 9 attacks.

Sources said that the ministry received an email from the Indian Computer Emergency Response Team (CERT-In) on November 19, 2020 on the threat of malware called Shadow Pad at some control centres of POSOCO. Accordingly, the action was taken to address these threats.

After the ministry came to know about the threats, all IPs and domains listed in the NCIIPC mail were blocked in the firewall at all control centres . Due to the on going conditions between china and India were not in the favour of India so government decided to remain silent instead of taking any legal actions over the nation

The ministry had noted, "Observations from all RLDCs & NLDC shows that there is no communication and data transfer taking place to the IPs mentioned. There is no impact on any of the functionalities carried out by POSOCO due to the referred threat. No data breach/data loss has been detected due to these incidents. Prompt action is being taken by 10 the chief information security officers at all these control centres under operation by POSOCO for any incident or advisory received from various agencies like CERT-in, NCIIPC, CERT-Trans and others

Cybersecurity is important because **it protects all categories of data from theft and damage**. This includes sensitive data, personally identifiable information (PII), protected health information

(PHI), personal information, intellectual property, data, and governmental and industry information systems.

In the current Indian scenario though many cyber security directives and guidelines exists, but none of them are power sector specific. Ministry of Power has directed CEA to prepare Regulation on Cyber Security in Power Sector. And as an interim measures CEA has been directed to issue Guideline on Cyber Security in Power Sector, under the provision of Regulation 10 on Cyber Security in the "Central Electricity Authority (Technical Standards for Connectivity to the Grid) (Amendment) Regulations, 2019"

"The requester and the user shall comply with cyber security guidelines issued by the Central Government, from time to time, and the technical standards for communication system in Power Sector laid down by the Authority."

Experts said cyber attacks can be acts of war if they **cause physical destruction**. A Department of Defense law of war manual states that some cyber operations should be subject to the same rules as physical, or "kinetic" attacks.

Cyber security in power sector is key to **protecting national critical infrastructure**. Poor cyber security planning would impact the power sector in India. A laissez-faire approach to cyber security in power sector may not yield results. There is a need for power sector specific cyber security regulations.

When malicious attackers gain access to an industrial control system they are able to sabotage control and safety processes, leading to costly outages, damaged turbines, threats to personnel safety and even environmental disasters.

The most important element in power plant cybersecurity is protecting the industrial network perimeter from harmful traffic from less trusted external networks . Unidirectional Gateways enable safe IT/OT integration, continuous real-time monitoring and disciplined control for energy sites while preventing all remote cyber security attacks on plant equipment.

Critical infrastructure industries and government agencies should work together to inventory and monitor critical assets. If we can't see the critical assets, we can't defend them. The Department of Energy (DOE) launched a 100-day action plan to increase real-time information-sharing, visibility, detection, and response capabilities of operational technology in the electricity sector. The CEO-led Electricity Subsector Coordinating Council of electricity companies liaised with the DOE and deployed a technology tool that could provide visibility into electric systems. The initiative, known as Neighborhood Keeper, improved the visibility and monitoring of US electrical systems from 5% to 70%, while keeping the data anonymous and protecting companies' privacy. Information about threats and vulnerabilities is shared real time with each participant and E-ISAC (Electricity-Information Sharing and Analysis Center) for the collective defense of a critical infrastructure sector.

Solution

India needs to take resolute action against cyber attacks. Data on almost everything now including power transmission and distribution systems are controlled in cyberspace. If the control does not work the way it is supposed to or is hijacked by criminals, it will lead to chaos. The need is to go beyond adherence to ISO standards, and have in place systems to guard against large scale disruption. Action should include mandating all companies to report such attacks and create a specialised government agency to track the patterns and take remedial measures.

Inorder to protect this can be a proper solution to Keep the infrastructure off the internet. You have a separate network for the energy network. It isn't perfect but the only way it can then be attacked is from USB sticks. It means you need two computers for a lot of locations. One online for paperwork and one offline dedicated for the energy infrastructure which has limited connections (USB ports) and it isn't connected to the other network. This isn't exactly new. It has been know for over 30 years but … it costs more.

Protecting against malware isn’t easy because malware can enter your system through so many avenues. A cybercriminal devoted to undermining a network, potentially even equipped with resources from a foreign government, is a significant threat.

Make security a top priority thoughout your organization. Implement, at the very least, basic cyber hygiene practices such as firewalls, strong passwords, and antivirus/malware software.

To be truly effective though, critical infrastructure providers must fold cybersecurity into the fabric of their organization. Read on to learn more about preventing critical infrastructure cyberattacks.

The main solution functionalities:

• Application whitelisting (Application startup control) – blocks all applications from launching except those that are explicitly allowed. The protection component provides test mode to support easy setup and debugging at deployment stage

• Device control – allows administrators to define and specify which devices can be connected to protected industrial hosts. The technology provides opportunities to protect industrial systems from unauthorized device connections. The technology supports masks for easy administration and bulk device operation

• Wi-Fi network control – enables the monitoring of any attempt to connect to unauthorized Wi-Fi networks

• Malicious software detection (including ransomware) – combines signature and heuristic protection methods to protect Windows workstations against known, unknown and advanced threats. Special Anti-Cryptor technology allows to prevent ransomware attacks

• Host-based firewall – provides abilities to limit network connections to industrial hosts

• PLC integrity check – enables additional control over controller configuration via periodical checks of any changes in projects

• Centralized management and security policy control – feature allows configuration of security settings for both individual devices and groups

• Centralized update of antivirus databases on protected network nodes (even if the technological network is not connected to the Internet) – that helps to support a high security level due to the update of security agents from a single control server within the technological network. Updates can be downloaded to the control server directly from the Internet from a retransmission node (installed on the IT network or DMZ), or transferred to the control server by an administrator via USB devices

• Testing of new updates before distribution – allows updates to be checked for compatibility with industrial software prior to distribution on industrial hosts

• Role-based model for separate policy management and actions with the security agent – eliminates the possibility of unauthorized security policy changes on the control server, as well as preventing protection disabling or endpoint solution setting changes

• Centralized collection of endpoint security events data of enables comprehensive information security data analysis based on registered events, while identifying the exact causes of incidents and facilitating mitigation planning

Network integrity monitoring:

• Self-training mode that allows detection and registration of all available LAN nodes and communications between them – this data can be used as a reference point and for change tracking

• IP and MAC address-based detection and registration of new network devices connected to the controlled segments of the technological network

• Detection and registration of new network communications between nodes based on the following attributes: sender node address, recipient node address, network protocol, port, number of allowed connections, etc.

2. Deep packet inspection:

• Review, analysis and registration of important messages of technological protocols according to configuration: - Detection of device management commands (for example, switching On/Off) via industrial network protocols (IEC 61850, IEC 60870-5-104) - Detection of commands to change protection and control system operation parameters (for example, set-point group switch) via industrial network protocols (IEC 61850, IEC 60870-5-104) - Detection of IED control and parameterization attempts with service software via controlled network segment

• General telemetering message monitoring 3. Events storage:

• KICS for Networks system provides storage of detected events in an internal secure database

• The information is limited by storage period and the limit of archive size. An example of the solution shown in illustrates one potential deployment scenario for KICS for Networks and KICS for Nodes deployment scenarios

A secured protection and control system includes two LAN segments of ring topology. The first segment of the electrical power substation is the station bus (according to IEC 61850), which provides communications between IEDs. In addition, substation bus, substation controllers and telemetering gateways are used for informational interaction with higher levels of dispatching control. The LAN segment provides access to the protection and control system equipment by means of engineering software. Service access can be provided both locally and remotely. Local service access is provided using a notebook connected directly to IEDs or to the station bus LAN. Service access can also be performed from a remote workstation. Prompt communications between network nodes during stable operation are conducted according to protocol IEC 61850 MMS.

Service communications regarding the parameterization of protection and control system devices are provided under the internal application protocols of the equipment manufacturer. The physical LAN segment of the bus is a ring network, formed by two connected switches. All devices are connected to the switches as double attached nodes (DAN). Therefore, there is no single point of failure on the segment that provides a higher level of network reliability. The IEDs are equipped with built-in switches and combined in chains. The ends of chains are connected to the ring network switches; therefore, traffic between the devices of one chain is not transmitted via ring network switches. Ring topology network control is executed using the RSTP. The network switch is included to provide remote service access to the industrial network through a VPN. The second segment – operator network segment – is also represented by a ring network topology designed for operator workstations and process control system server's interaction. Interaction with Network Control Center and System Operator is provided directly through a substation controller connected to the automation system. Exchange is performed through protocol IEC 60870-5-104

All control network communications are encrypted. In the event of control network failure, KICS for Networks and KICS for Nodes components will continue their operation in standalone mode. Collected data will be transmitted to Kaspersky Security Center when the network segment operation is restored. KICS supports integration with SIEM systems. Kaspersky Security Center organizes an encrypted channel with the SIEM system and transfers configured events into the SIEM (HP ArcSite, IBM QRadar and others through Syslog format). Notifications can also be sent using email and SMS

Officially, critical infrastructure can be any of 16 sectors ranging from the expected, such as nuclear and chemical, to the perhaps more unexpected, such as agriculture and rail car manufacture. But the proper functioning of these sectors doesn't stop at just the companies involved—there are many critical functions that require the support of a wide range of stakeholders, from software companies to internet and web-hosting service providers to regulators. The success of security strategies such as defense in depth or layered defense depends on all of these stakeholders working toward a common goal. But importantly, each of these stakeholders has a different set of incentives pushing and pulling on their behavior. Even adversaries are incentivized by different trends to increase or decrease their attacks. The challenge is that in such a complex environment as critical

infrastructure, the incentives of one player may combine with the incentives of other players in unexpected ways, often leading to actions that look individually rational but have irrational effects at the industry level.

Securing critical infrastructure from cyberattacks takes more than defending critical infrastructure assets; it requires an understanding of the incentives of all those stakeholders and then shaping them. If we can harness the positive incentives toward collaboration and social connection, then, just like the children in the experiment, we can enjoy the reward , perhaps not a marshmallow, but more resilient critical infrastructure that is available when citizens need it most.

The complex mix of incentives across all stakeholders is a massive challenge, but it can also offer the path to a solution. If incentives stand in the way of the adoption of better security procedures or more effective information-sharing, then reshaping those incentives can be an effective way to make progress toward more security.

There are many ways to reshape incentives for individuals, organizations, and even adversaries. Economists, philosophers, and legal theorists have argued over them for centuries. One useful categorization is to think that incentives can be shaped by enforcement, market, reputational, and moral pressures Our mapping of the tangled web of incentives across the various cyber stakeholders can help show not only where those pressures can be exerted, but also who has the ability to exert them.

Cyber attacks cannot be stopped but they can be prevented by spreading awareness among employees and the team with proper training .

Electrical power sector can be protected by using the powerful protection tool / program which can protect the system at any condition by performing some specific actions . Such as proper code/program which will make sure that before any data enters in the system it should check a hidden code attached with the file . Which simply means you have to assign some secret code to the data that sector requires and than the required data will be fetched by the program and check whether it is safe or not if secret code is not present in the system then that data should be sent into the queue where the professional analyzer will check the data and if data is not found to be malicious then the analyzer will externally add the secret code in the data file and pass it over the program then program will pass the data to the particular power sector.
In order to carry out this task all we need is proper program which will detect the malicious activites and the man power to analyze whether the detected activities are actual malicious or not.

Conclusion

No cyber defence can be full-proof. Attacks will come, defences would be breached. Points to be considered are: when do we realise that breach has happened, does it have the capacity to damage the system, what is the resilience of the system, how much time it takes to plug the gap etc. and make a proper way out with experienced team.