How to prevent a Stuxnet like attack on India's Power Infrasturcture

Adarsh Palaskar

June 22, 2022

1 Abstract

Internet connectivity across the world has made it smaller place. IoT (Internet of Things) has revolutionized how the masses communicate and consume media, as well as how countries interface with each other and transformed the business process. Enormous amount of data is now flowing or being stored, at this very moment. We are increasingly dependent on the internet and all the digitization to function. All this huge information infrastructure is completely dependent on electricity, which has had its importance for a while now in the modern era. The power sector, given its continuous, ever-increasing demand and being the core of digitization, does an excellent job of managing its operations. However, the issue of cyber security remains opaque and difficult to manage and counter. It is critical that this space be analysed. This paper covers how the current state of cyber security in the power sector in India can be improved and led closer to cyber deterrence, and how can a Stuxnet like attack be prevented on the nation's soil.

2 Methodology and Assumption

The focus of this paper is to make a cyber security plan for the power grids and the corresponding architecture against a potential cyber warfare scenario, also considering protecting the future architecture of smart grids, which would involve a lot of IoT devices, leaving more vulnerabilities in the infrastructure. Introduction of a smart

grid brings with it certain security risks and concerns, particularly to a nation's cyber security. Increased interconnection and integration may render the grids vulnerable to cyber threats, putting stored data and computers at great risk.

Ministry of Power has in October 2021 released the guideline for the Cyber Security in Power Sector, a critical information infrastructure (CII). They can be found in the references at the bottom.

A key point that has been factored in the guidelines while identifying Critical Information Infrastructure (CII) is the inter-dependencies that they have, to determine which are the 'most critical'. Using this matrix, NCIIPC settled on the Power Sector as the most critical followed by the Energy Sector. The guidelines mainly define various key terms, Critical Assets, Critical System and Cyber Assets, Protected System and Vulnerability in relation to the cyber security. It lays down the Cardinal Principles to be followed while framing the cyber security policy by the Responsible entity. It also mandates its annual review. The guidelines also prompt to test and audit the systems regularly and take necessary actions if new vulnerabilities are found. The guidelines mandate ICT-based procurement from identified "Trusted Sources" and identified "Trusted Products". In case the procurement is not from a trusted source, the product needs to be tested for Malware/Hardware Trojan before deployment for use in power supply systems.

According to the National Cyber security Index (NCSI), India is ranked 46th in the National security index and a lowly 134th in the ICT development index in 2020, which shows how the country is heavily compromised due to outdated and potentially compromised hardware. Also India scores highly in the cyber security policy development but a zero in its implementation, which shows exactly where the nation lacks in the cyberspace.

Figure 1: Policy Development and implementation scores of India

3 Cyber Deterrence challenges

A cyber deterrence strategy depends whether a state or nation can restrain an opponent by threats, incentive or enforcement. It is controversial whether cyber threats can actually be deterred and whether a strategy which used in nuclear warfare can be used in an entirely different domain.

1. **Attribution:** Identifying the intruders correctly is the greatest challenge during any cyber attack. Hackers can launch attacks from any geographical location, hide their identities and even employ false clues in their attack to misguide the target state. And even if the intruders are identified to be from a particular region or nation, it is further very difficult to prove if the attack was state sponsored, private entity sponsored or planned and executed by a single person. This makes it difficult for the victims to counter attack or openly reveal the attacker as it may impact their crebility and ultimately their deterrence.

2. **Uncertainity of effect:** In case of nuclear weapons, the potential damage is already known to everyone which plays the major role in nuclear deterrence. Whereas, consequences due to cyber attacks are unknown and uncertain, and may also go out of control of the intruders themselves. It was found that Stuxnet, which was a joint attack by US-Israel on the Natanz nuclear facilily of iran, used limited potential and slowly destroyed a fraction of their centrifuges, whereas it was capable to destroy the entire facility at once, and if something would have went slightly wrong, it would have had devastating consequences

3. **Unintended Co-lateral damage:** During the Stuxnet attack, the worm also spread not only outside the nuclear facility in Iran, but in a lot of nations worldwide, even though it was designed to limit its spread. It is estimated that Stuxnet infected around 200,000 computer all around the world. NotPetya, which is considered to be one of the most devastating cyberweapon also spread beyond its intended target, Ukraine, and it disrupted business chains worldwide causing approximately 10 billion dollars in damage.

Notwithstanding these challenges, the absence of a cyber deterrence policy can cause hostile nations to attack India fearlessly. According to the Indian government, nearly 1.15 million cases of cyber attackes were reported

in 2020, which is almost 3 times from 2019 and 20 times from 2016. This trend is likely to continue and India would have to face even more cyber attacks in the future.

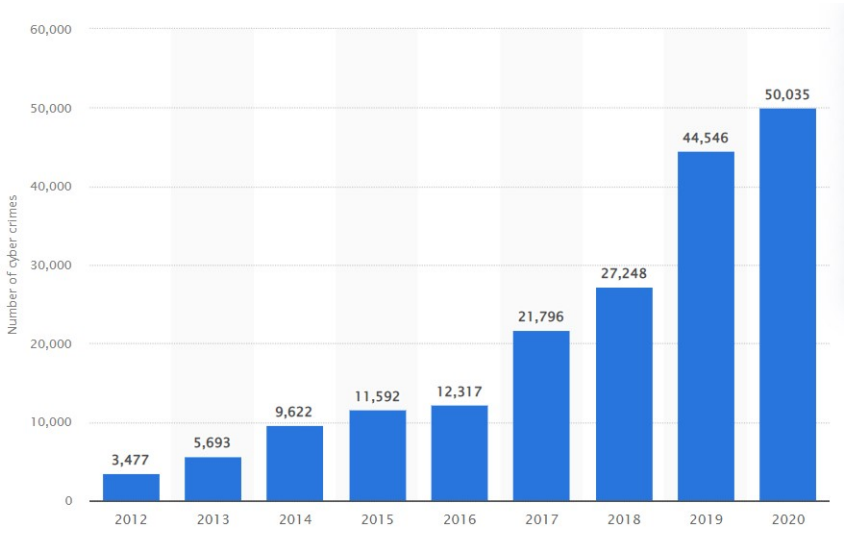

Figure 2: Increasing cyber crimes in India

The potential developments in India cyber deterrence strategy are mention in the solution architecture section of the paper.

4 Legal Treaty and assumptions:

India has signed various MLATs, MoUs, Joint statements and Cyber Frameworks. An MLAT is an agreement between two or more countries, drafted for the purpose of gathering and exchanging information in an effort to enforce public or criminal laws. A MoU (Memorandum of Understanding) is a non-binding agreement between two or more states outlining the terms and details of an understanding, including each party's requirements and responsibility, it is often the first stage in the formation of a formal contract.

5 Solution Architecture:

To establish a strong security against cyber warfare, we must analyse significant attacks that were performed in the history, to protect those exploits and obtain the perspective of an attacker.

Key points obtained after analysing Stuxnet worm:

1. Stuxnet was created by the US-Israeli force to silently sabotage the nuclear facility in Natanz, Iran. Its key highlight was that the worm used four zero-day vulnerabilities in the Microsoft operating system, and was thus able to penetrate in any version of the OS, right rom Windows 95 to Windows 7.

2. Two vulnerabilities were used to spread Stuxnet, the LNK vulnerability and the printer spooler vulnerability. The worm was also coded in a way that a infected device can only infect three other devices, which was expected to limit the spread, which eventually failed since Stuxnet spread across the world.

3. To elevate privileges on an infected system, Win32.sys key board layout vulnerability and Task Scheduler vulnerability were used. Although all of them are patched by the vendor after the detection of Stuxnet, new vulnerabilities keep cropping up and finding and patching requires a significant amount to time, enough for attackers to exploit them after detection.

4. Stuxnet contained components digitally signed with potentially stolen certificates, making signature detection useless and taking advantage of a default password in Siemens WinCC software's database server, it reprogrammed the PLCs, thus effectively changing the readings provided by the sensors and feeding false data, making it undetectable for the operators at Natanz as they were only able to see the tampered output.

5. In this way the worm controlled the centrifuges in the facility, but the operators were fed with false information conveying everything was under control and functioning as desired.

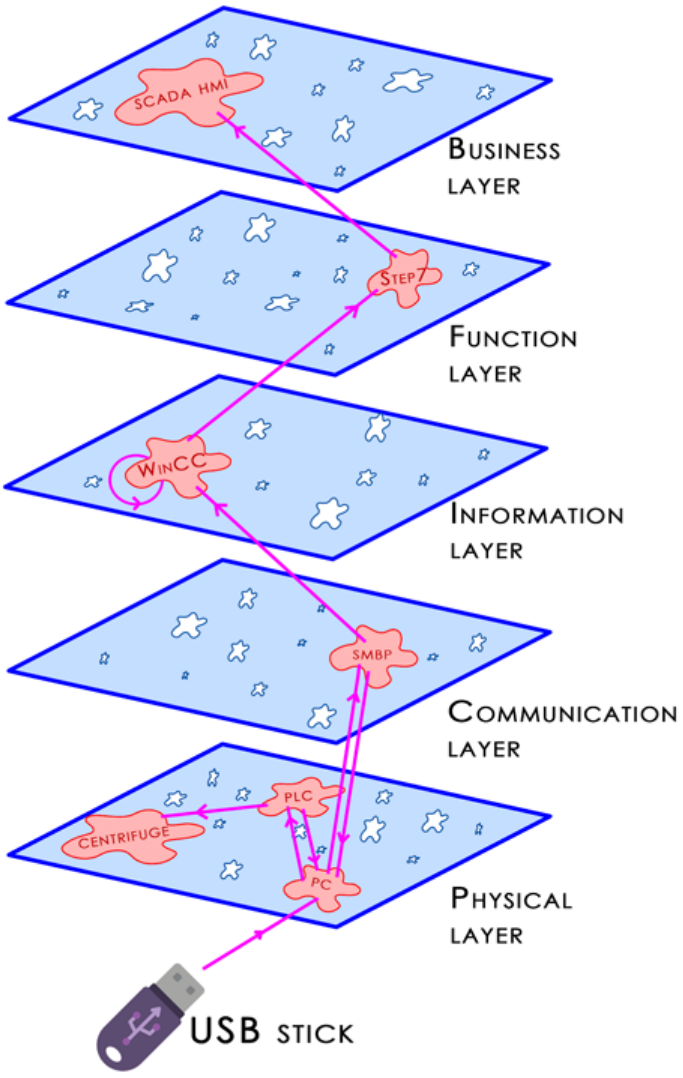

Figure 3: Stuxnet routing simulation

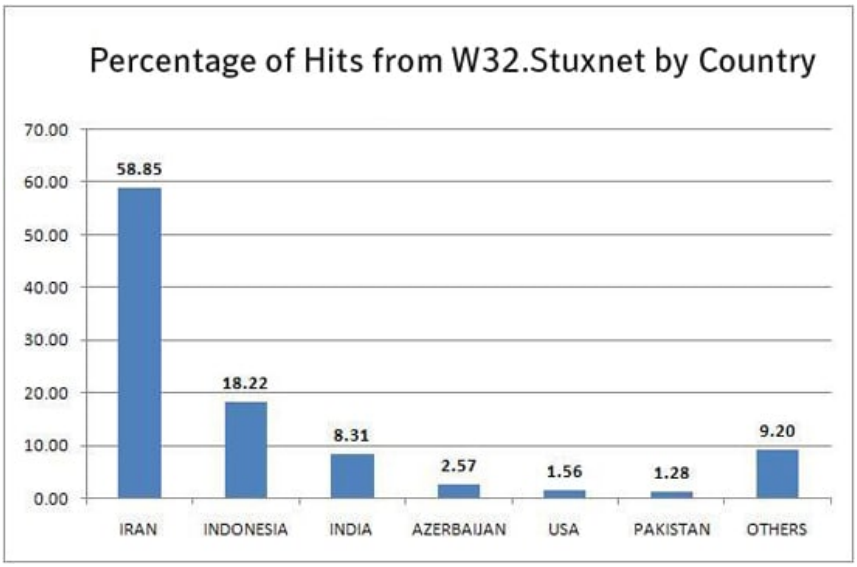

Figure 4: Worldwide infections of Stuxnet

Electricity grids and the corresponding power infrastructure is now about 50 years old and thus the concept of smart grids helps revolutionize power transmission even further, However the current architecture has cyber security flaws and smart grids can potentially introduce new and increased vulnerabilities, even if the present ones are rectified while introducing the smart infrastructure. Therefore, we will focus on the vulnerabilities and possible solutions in the current as well as the smart grid architecture.

Smart grid Architecture:

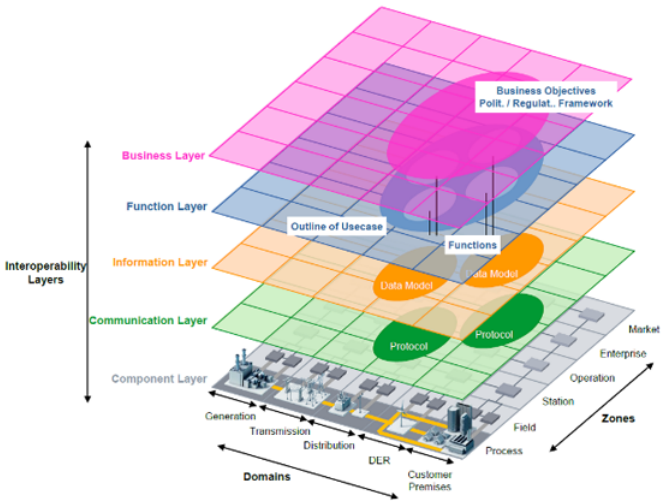

Figure 5: Smart grid Architecture

Potential threats and entry points for attackers:

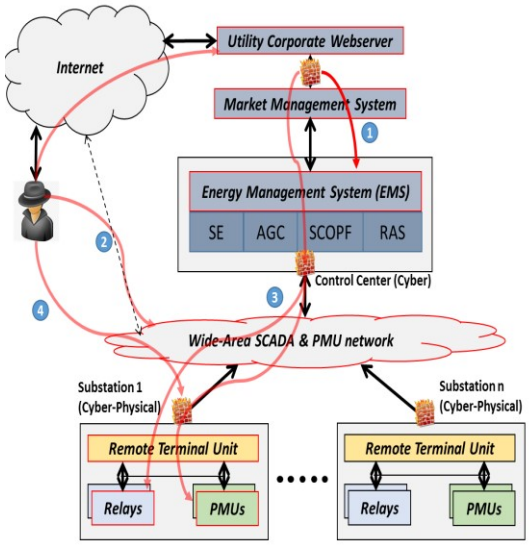

Figure 6: Attack surfaces on the Infrastructure

The security strategy should provide protection against the required security criteria according to the NCIIPC guidelines stated as: "Security Architecture: shall mean a framework and guidance to implement and operate a system using the appropriate security controls with the goal to maintain the system's quality attributes like confidentiality, integrity, availability, accountability and assurance."

1. **Confidentiality:** Preserving authorized restrictions on information access and disclosure.
2. **Availability:** Ensuring timely and reliable access to and use of information.
3. **Integrity:** Protecting against improper modification of the information.
4. **Accountability:** Ensuring tractability of the system.

The different attacks compromising one or more security characteristics are as follows:

1. **Reconnaissance:** Attacker gathers and collects information about the target.
2. **Scanning:** Attacker tries to identify the system's vulnerabilities.
3. **Exploitation:** Attacker tries to compromise the target and get full control of it.
4. **Maintain Access:** Attacker installs a stealthy and undetectable program for future access.

As there are a whole lot of possible exploits and possible breaches, and more of them are discovered every day, cyber security cannot be achieved through one specific solution. Instead, several techniques should be incorporated to establish a global strategy, which should go through regular revisions and should be updated so that it can protect against the newly discovered exploits and malpractices.

Architecture of the Security Strategy:

The defence can be broken into three parts according to the stage the at which the attack is discovered. Since prevention is the best cure, implementing ample of solutions covering all vulnerabilities would be our key goal and thus most of the security solutions are covered in the Pre-Attack stage.

1. **Pre Attack:** The major aspects in this stage is to make sure that all the layers in the architecture are secure and cannot be penetrated by attackers. This would mainly include Network Security, Data Security and Device Security.
   The various methods by which this can be obtained are as follows:

   (a) **Incorporating use of Effective Firewalls:** Firewalls control flows of network traffic between networks or hosts based on security policies. To further improve their security and effectiveness, firewall policies should be created in such a way that they specify how firewalls should handle inbound and outbound network traffic. All requirements of a network should be identified before determining what firewall technologies should be implemented at different places. The various technologies are Packet Filtering, Stateful Inspection, Application Firewalls, Application-Proxy Gateways, Dedicated Proxy Servers, Virtual Private Networking, Network Access Control, Unified Threat Management, Web Application Firewalls, Firewalls for Virtual Infrastructures.

   (b) **Using Intrusion detection and intrusion protection systems (IDS and IPS):** Intrusion detection is the process of monitoring the events occurring in a computer system or network and analysing them for signs of possible incidents. Intrusion prevention is the process for performing intrusion detection and attempting to stop detected possible incidents. They make use of Signature-based detection, Anomaly-based detection and stateful protocol Analysis. The types of Intrusion detection and prevention systems are:

      i. **Network-Based:** monitors network traffic for suspicious activity.

      ii. **Wireless:** monitors wireless network traffic for suspicious activity.

iii. **Network Behaviour Analysis:**examines traffic to identify threats that generate unusual traffic flows, e.g., DDoS attacks, malware, policy violations.

iv. **Host-Based:** monitors characteristic of a single host and events occurring for suspicious activity.

For a Stuxnet like infection a host-based intrusion prevention system would watch for suspicious behaviour taking place on the actual industrial control system and force the lockdown of the system when called for, so new malware cannot be injected. Many industrial control system developers are reluctant to load third-party software that they will have to validate and support, but Stuxnet demonstrated the game has changed and greater cooperation is warranted.

(c) **Use of SIEM solutions:** Security Information and Event Management (SIEM) offers real-time monitoring and analysis of events as well as tracking and logging of security data for compliance or auditing purposes. It isa security solution that helps organizations recognize potential security threats and vulnerabilities before they have a chance to disrupt business operations. It surfaces user behaviour anomalies and uses artificial intelligence to automate many of the manual processes associated with threat detection and incident response and has become a staple in modern-day security operation centers (SOCs) for security and compliance management use cases. Thus, the system can detect internal threats and modern-day security breaches like Phishing attacks, SQL Injections, DDoS (Distributed-Denial-of-Service) Attacks, Data exfiltration etc.

(d) **Upgrading to improved and advanced encryption techniques:**

In 2018, NIST (National Institute of Standards and Technology), USA retired the old DES(Data Encryption Standard) based encryption technique, namely (3DES/TDEA) known as triple DES which used the DES encryption 3 times. Instead AES encryption is the new standard and is a more mathematically efficient and elegant cryptographic algorithm. Its main strength rests in the option for various key lengths. AES allows you to choose a 128-bit, 192-bit or 256-bit key, making it exponentially stronger than

the 56-bit key of DES. AES uses permutation-substitution, which involves a series of substitution and permutation steps to create the encrypted block. The original DES designers made a great contribution to data security, but one could say that the aggregate effort of cryptographers for the AES algorithm has been far greater.

(e) **Leverage reputation-based detection techniques:** Traditional protections, such as signature-based antivirus, are the most common method of defending against the initial infection stage. Unfortunately, many modern pieces of targeted malware rely on mutated code that is altered before each new attack and tested against antivirus solutions to ensure it will evade detection. Some malware even utilizes self-mutating code that makes it all but invisible to traditional signature-based protection. In addition, signature-based detection is ineffective at identifying brand new, never-before-seen malware. Such was the case with many of the initial Stuxnet infections. Look for a reputation-based detection system that leverages massive databases containing demographic information on virtually all good and bad files in existence to single out unknown and likely malicious software applications.

(f) **Implementation and enforcement of Device control policies:** A feature of advanced endpoint protection solutions, device control provides administrators with the ability to monitor and control the behaviour of devices by creating and enforcing related policies. Because industrial control systems are often disconnected from the Internet and overall corporate networks for security reasons, thumb drives are frequently used to transfer data to and from such systems and also to implement patch updates. Stuxnet authors knew this and the spread of the threat relied on this fact. In fact, infected thumb drives carried into organizations by unwary contractors was likely one of the initial propagation methods used to spread the threat. Device control policies can control what files and applications are allowed to run off thumb drives and, if properly set, will prevent malicious executable files, like those used by Stuxnet, from running on targeted systems.

(g) **Ensuring tempo of software certificate revocation updates:** In order to further evade detection and bury itself deeper into tar-

geted systems, Stuxnet used two stolen digital certificates, one from JMicron and another from Realtek, to try and make itself appear as a legitimate program. Both of these certificates were revoked, but if a system were not kept up-to-date in terms of certificate revocations, the stolen certificates used by Stuxnet would have still serve as an effective deception. There is no reason to think that future threats will not also attempt to exploit compromised certificates.

(h) **Secure by design:** The PLCs and SCADA systems used in the Natanz Nuclear power plant had major design flaws, since security was not considered major concern during their manufacturing. For example, the input data in the Siemens PLCs was read and write by default, which must be read only. Thus the data could be easily rewritten without the system detecting any security breach. Such faults should be checked for by proper penetration testing before installing any new piece of hardware from a trusted vendor. A long term, effective but costly and delayed solution could be to encourage the manufacture of these hardware equipment in India itself, by which we can mitigate all the design issues through proper research and also be independent in our operations, which would not only improve the security of our systems, but also ultimately contribute to high cyber deterrence.

(i) **Use of endpoint management software to ensure adequate patching procedures:** As previously mentioned, Stuxnet, like many targeted and non-targeted attacks, used previously unknown software vulnerabilities to gain access to susceptible systems. Security updates were issued to fix the vulnerabilities exploited by Stuxnet, but unless the patches were actually applied, systems were as vulnerable as ever. Endpoint management solutions can help manage patch updates and ensure they are applied properly. This is especially important when it comes to patches issued out-of-band, as these updates can often be overlooked because they fall outside the routine patch schedule.

(j) **Employing automated compliance monitoring to root out default password use:** Some industrial control system manufacturers insist that their systems – no matter where they are deployed – use default password setups. This may be for legit-

imate reasons, but Stuxnet highlighted the obvious weakness in such a strategy. Because Stuxnet targeted a specific industrial control system, one in which the default passwords were public knowledge and easily attained. In environments where default password use is not necessary, a situation that will hopefully increase, automated compliance monitoring can assert detection and control over default password setups, ensuring default passwords are not used. It also identifies failed password guess attempts.

(k) **Using effective data loss and access solutions:** Data loss prevention technology specializes in finding and preventing internal data spill events. It is not yet widely understood, but many data breach events are the result of internal data spills left unintentionally by well-meaning insiders. Not using data loss prevention technology to identify these spill events, clean them up and encrypt the content, simply makes the job of an attacker that much easier. In the case of Stuxnet, to target specific organizations the attackers needed sensitive data describing the systems the targeted organizations were running and their configurations. By preventing attackers from acquiring this detail, a similar attack in the future is much less likely to be successful. Also in case of the Ukraine power grid sabotage in 2015, the attackers also wiped out a huge amount of important data of the systems, and thus not having an effective backup can also affect future operations for a long time.

(l) **Reducing the attack surface:** There are 3 main types of attack surfaces:

   i. **Physical attack surface:** This includes organizational assets that a hacker can get if they have physical access to your premises.

   ii. **2. Digital attack surface:** These are assets that are accessible through the internet and live outside a firewall. Digital attack surfaces include known assets such as your corporate servers/ operating system, unknown assets such as a forgotten website, and rogue assets such as apps that impersonate your company.

   iii. **Social engineering attack surface:** This is one of the most critical yet often overlooked attack surfaces. In this case, the

hackers exploit human psychology and manipulate your employees into divulging sensitive information. This mainly includes phishing attacks.

2. **Under-Attack:** When under attack is extremely important to detect the attack and find out the affected entities as quickly as possible, so that attack mitigation measures can be implemented as soon as possible.

   (a) **Using Intrusion Detection system (IDS):** As mentioned in the previous step, using IDS solutions can help to find the type of intrusion as well as affected entities so that appropriate action can be taken.

   (b) **Pushback and Reconfiguration methods:**
   There are two types of responses:

      i. Preventive or proactive, where the architecture of the system and its controller are improved offline.

      ii. Reactive response, which corresponds to the type of response where the control input (or a set of control inputs) is modified online in such a way that the impact of the attack is mitigated.

   (c) **FHSS, DHSS:** Frequency Hopped Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) can be used to pushback the entire system devices with different IP addresses, or different ports.

3. **Post-Attack:**

   Post attack analysis involves forensics-based methods to find out the intruder and also check which vulnerabilities in the system were exploited so that they can be patched as soon as possible to protect the system from future attacks.

   (a) **Forensic Analysis:** A deep investigation must be initiated to find the intruders to potentially launch a counter attack, or exposing them thus regaining ground in the nation's cyber deterrence.

   (b) **Restoring and updating the critical infrastructure:** Using the forensic reports, IDS signatures, anti-virus database and security policies must be updated for protection against the newly discovered threats.

6 Benchmarks for success

Success while preventing cyber attacks can be measured by evaluating the nation's performance against other nations through indexes like the NCSI (National Cyber Security Index). Performance can also be evaluated by predicting the number of cyber attacks in the future using appropriate Machine Learning models and time series forecasting on the basis of past data, and then comparing the predictions with real data to find out the quantitative improvements using the current strategy. Success during a cyber attack can be evaluated by comparing the damage prevented using the current cyber security strategy and the estimated damage that an older strategy could have prevented. Similarly, during an offensive, success can be evaluated on the basis of how much damage was done to the enemy compared to the proposed damage in the offensive plan.

7 References

- NCSI Website
- Central Electricity Authority, Ministry of Power; Executive Summary of Power Sector, Ministry Of Power. New Delhi: Central Electricity Authority, 2016. Print. December 2016
- Dileep G (2020) A survey on smart grid technologies and applications. Renew Energ 146: 2589–2625.
- Gunduz MZ, Das R (2020) Cyber-security on smart grid: Threats and potential solutions. Comput Netw 169: 107094.
- Cyber Physical Security of Power grid
- Dewa Z, Maglaras LA (2016) Data mining and intrusion detection systems. International Journal of Advanced Computer Science and Applications 7: 62–71.
- Guidelines for the Cyber Security in Power Sector, a critical information infrastructure (CII).