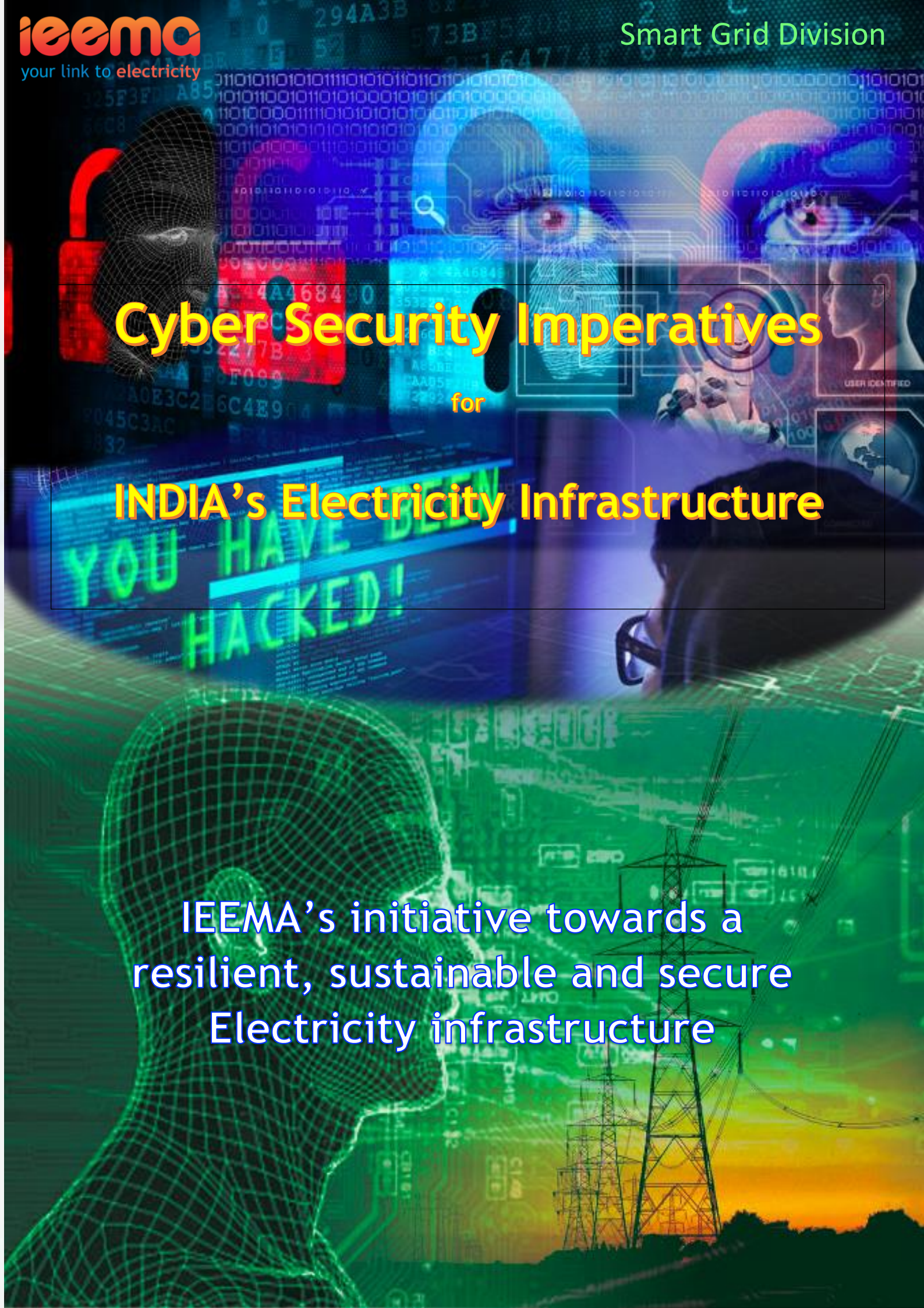
ieema
your link to electricity

Smart Grid Division



Cyber Security Imperatives

for

INDIA's Electricity Infrastructure

IEEMA's initiative towards a resilient, sustainable and secure Electricity infrastructure

About IEEMA:

Indian Electrical & Electronics Manufacturers' Association (IEEMA) is an Apex Industry Association of the Indian electrical equipment, industrial electronics and allied equipment manufacturers – representing a combined turnover of $42 Billion. First ISO certified industry association in India, represents businesses encompassing the complete value chain in generation, transmission & distribution equipment. IEEMA has more than 900 members who have contributed to more than 90% of the power equipment installed in India. A platform for constructive interactions between Industry, Utilities and Policy Makers.

Acknowledgements:

IEEMA places on record its sincere thanks to, Mr. Deepak Pandey, Vice Chairman, IEEMA Smart Grid Division and Director, Business Operations GE-Digital India and Mr. N. Kishor Narang, Mentor & Principal Design Architect, Narnix Technolabs Pvt. Ltd. for developing and editing this White Paper and accompanying comprehensive Study Report. We also recognize the active support and contributions by Mr. Mayank Sharma, Schneider Electric, Mr. Rohit Sharma, Siemens Ltd, Mr. Amit Golhani, L&T Ltd, Mr. Anil Mehta, Secure Meters Ltd and the coordinating officer from IEEMA Mr. Akeel Khan for their contributions for the White Paper.

IEEMA further place on record the guidance and supervision of Mr. Sunil Singhvi, Chairman IEEMA Smart Grid Division and CEO, Secure Meters Ltd and Mr. Vikram Gandotra, Past Chairman IEEMA Smart Grid Division and General Manager Siemens Ltd for his inputs.

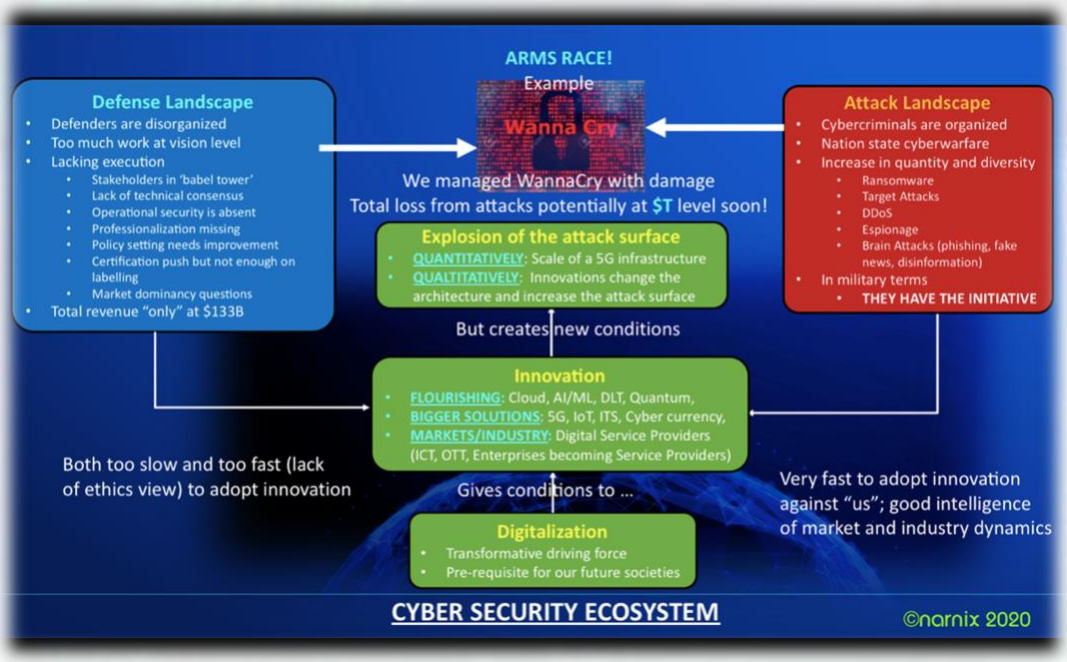
Disclaimer:

This report is the compilation of study, findings and views of the members of the Cybersecurity focused group in IEEMA Smart Grid Division. This paper has been prepared as a Study by the Members and to be considered as a guiding document only. The views/analysis expressed in this report/document do not necessarily reflect the official view of IEEMA. Efforts have been taken to ensure the accuracy and authenticity of the information presented in the report; however, IEEMA does not guarantee the accuracy of any data included in this publication, nor does it accept any responsibility for the consequences of its use.

Challenges that all economies are facing today in safeguarding the security and privacy of its ecosystem including citizen are - Transnational Nature of Cyber Crime, 'Cultural' Vulnerabilities, Internet Resilience and Threat Landscape.

The new paradigm of Smart Grid, Smart Home, Smart Building, Smart Manufacturing, Smart City already complicated by the 'Internet of Things' & Internet of 'Everything' made further complex by the Artificial Intelligence, Machine Learning, Blockchain & Quantum Computing, make it truly complex to develop and embed comprehensive Security, Privacy and Trustworthiness attributes in the products, systems and solutions for any use case or application - be it consumer, commercial, industrial, automotive or strategic domains like critical infrastructure, defense and aerospace.

The recent evolution of disruptive technologies and digitalization compounded by the Covid 19, changing geopolitical situations and increasing cyber-attacks from not-so-friendly nations; bring a whole new set of challenges for the Security and Security Evaluation Methodologies for complex nature & architectures of Critical Infrastructures of the nation leveraging the IT & Communication Networks evolving to meet these rising needs of the Society.



On one hand, we have the highly protected Networks for the 'Critical Information Infrastructures'; on the other hand, these very 'highly protected networks' need to give access to the consumers and citizens for Consumer/Citizen Engagement and Participation in these Smart (Digital) Infrastructures to meet the true drivers of setting them up. These large Smart Networks are actually highly complex 'Systems of Systems' and "Networks of Networks', and thus create fresh challenges in the Security Paradigm and development of Protection Profiles.

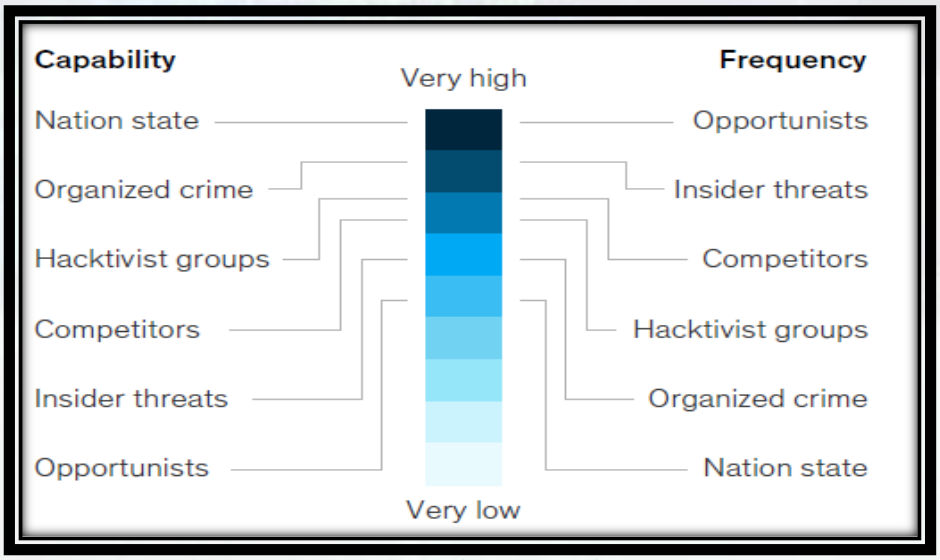
India is among the top 10 countries facing cyber-attacks.

CYBERTHREAT LANDSCAPE

Those of us who have worked in cybersecurity for many years often start to think we've "seen it all". We haven't. Recent years have ushered in a host of new adversaries, new attack methods and new challenges for those of us in the cybersecurity industry.

Ransom demands have been growing larger with time. Tactics are becoming more cutthroat. Established criminal organizations are busy expanding their respective operations, and affiliates of the Ransomware-as-a-Service (RaaS) malware developers are adopting BGH (Big Game Hunting) attacks.

Malware-as-a-Service (MaaS) developers have introduced ransomware modules. Banking trojans are continuing to be repurposed for Download-as-a-Service (DaaS) operations — a trend started to distribute malware families associated with BGH. Even targeted eCrime appears to be in a state of change, apparent by the recent activities of adversaries, notable for their high-volume spam campaigns and limited use of ransomware.



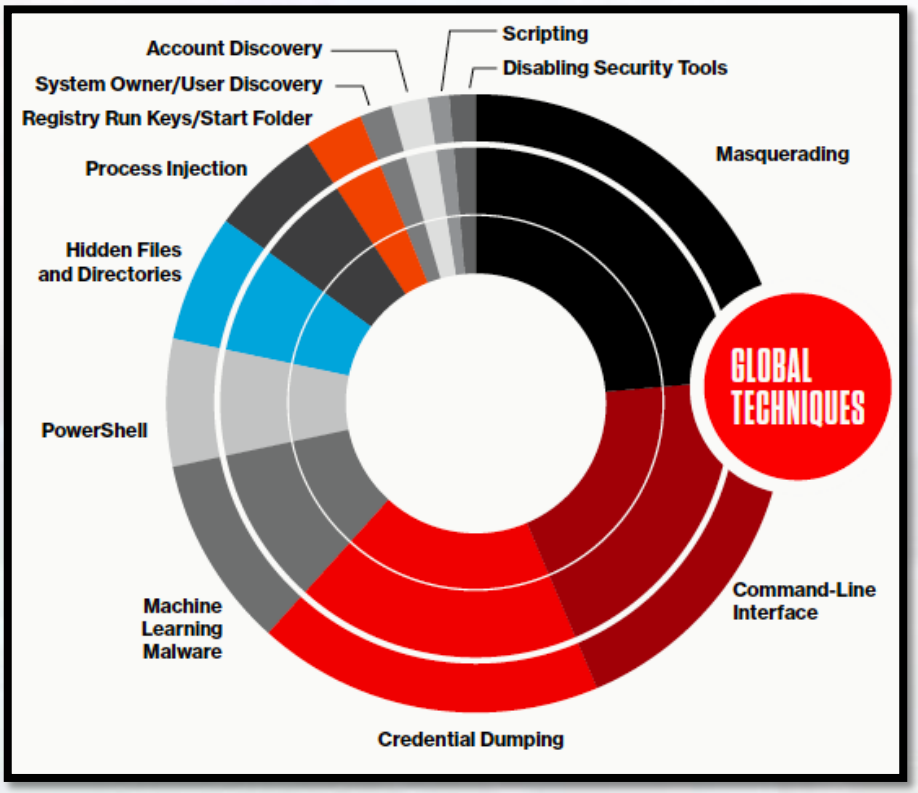
McKinsey on Risk, November 2019

The trend toward Malware-Free Attacks is accelerating with these types of attacks surpassing the volume of Malware Attacks.

BREAKOUT TIME:

Security teams are encouraged to strive to meet the metrics of the 1-10-60 rule: detecting threats within the first minute, understanding threats within 10 minutes, and responding within 60 minutes. However, the average breakout time for all observed intrusions rose from an average of 4 hours 37 minutes in 2018 to 9 hours in 2019.

The MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) framework is an ambitious initiative that is working to bring clarity to how the industry talks about cyberattacks. It breaks intrusions into a series of 12 tactics that adversaries may employ, each with a number of different techniques that have been observed to be in use.



TTPs (Tactics, Techniques & Procedures) used by attackers in 2019 (www.crowdstrike.com)

There was an almost 56% rise in malicious traffic on internet during the COVID-19 lockdown period also on account of the culture of work from home. This might be just the beginning, which suggests even more increased interest in exploiting cyber breaches.

About 38% of Advance Persistent Threat Vectors like APT40, APT3, APT10 and APT17 have been reported to be developed and deployed by China for espionage, stealing of data and IP. Some APTs are general purpose tools but others are customized for specific countries and purposes. The techniques and tools like APT1, APT3, APT10, APT15, APT17, APT26 etc. have been deployed against India too. The rogue nations are in the process of developing technology to penetrate the internet through satellite channels. Under the influence by rogue nations, our bordering country too has deployed APT 36 targeting Indian entities. The role of hacker group called LAZARUS is well known in carrying out attacks on financial targets in India, Bangladesh and other South Asian countries.

"The current situation is very tricky. We do not have the facts to decide on actions. This paralysis puts our critical infrastructure at risk."

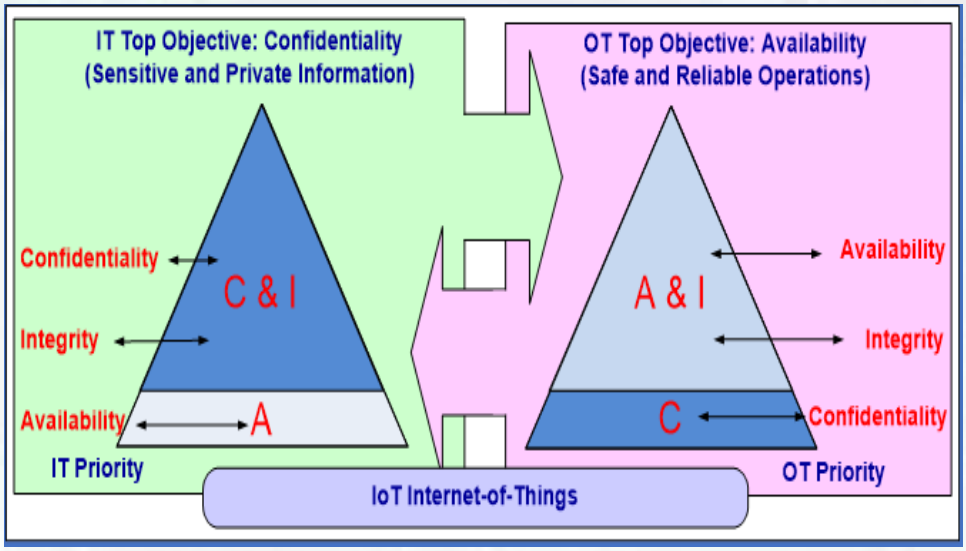
CYBERTHREAT for GRID

The Indian Electricity Infrastructure is also going through a paradigm shift in the wake of Global Initiatives in the fields of Energy Security, Renewable Energies, Smart Grids, Energy Efficiency, Electric Mobility etc. in order to make our planet Earth Green and Sustainable. Electric utilities now find themselves making three classes of transformations:

- ⇨ Improvement of Infrastructure, also called the **Strong Grid**;
- ⇨ Addition of the digital layer, which is the essence of the **Smart Grid**;
- ⇨ Business process transformation, necessary to capitalize on the investments in smart technology.

It must take into consideration the implications of other concurrent infrastructures and/or services running for the consumers/stakeholders to optimize the Life Cycle (Total) cost of all the infrastructures for a given geographical territory. To ensure a comprehensive and structured deployment of nationwide smart grid infrastructure, it's Imperative to address the current challenges like 'energy security', 'Electricity for all', and 'financial health of distribution utilities' along with 'Modernization of the Grid' in a holistic and sustainable manner.

The Smart Grid being the convergence of IT, Communication & Power Technologies, designed to cater to a nation's Integrated Energy Infrastructure requirements comprehensively, is a mission critical deployment needing the highest possible grade of security.



The Contrast - It is easy to see why IT security and industrial control security are facing challenges when it comes to integration. These two Titans clash because at the lowest level the security considerations their entire design structures are based on, are at odds.

Blurring line between Cyber and Physical Attacks

This targeting of Industrial Control System (ICS), which has developed over a decade, is blurring the lines between cyber and physical attacks, prompting national security concerns in many countries. ICS attacks have evolved in scope and purpose across the globe.

Risks with AI and Machine Learning

AI is a tool that can be used for offensive as well as defensive cybersecurity applications. Just as organizations can use artificial intelligence to enhance their security posture, cybercriminals may begin to use it to build smarter malware.

The next generation of situation-aware malware will use AI to behave like a human attacker: performing reconnaissance, identifying targets, choosing methods of attack, and intelligently evading detection. Adversaries may discover how to use AI to stage future attacks on the grid, designed to disguise the intrusion and then overwhelm defenses.

Purchase, Upgrades & Patches:

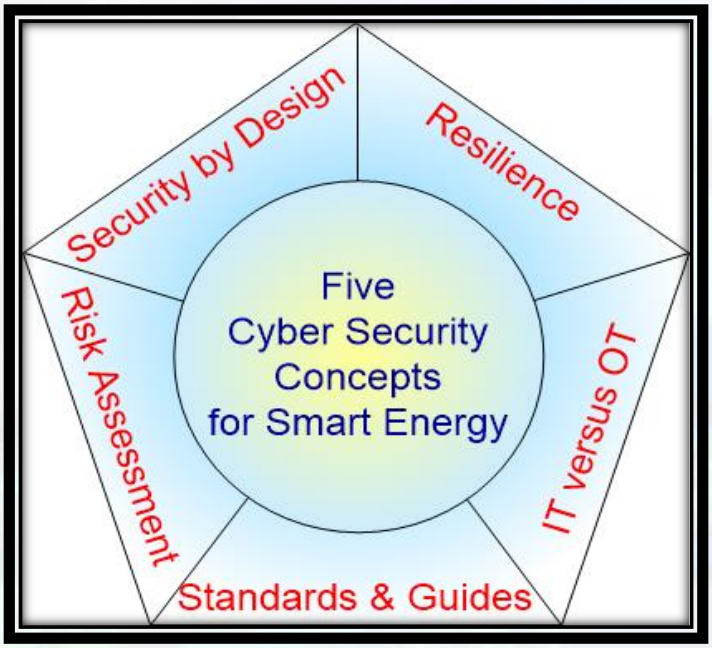
Utilities purchase information, hardware, software, services, and more from third parties across the globe. And threat actors can introduce compromised components into a system or network, unintentionally or by design, at any point in the system's life cycle. This may be through software updates or "patches," which are downloaded frequently, or through firmware that can be manipulated to include malicious codes for exploitation at a later date. Adversaries may also compromise the hardware that utilities install in their operating systems.

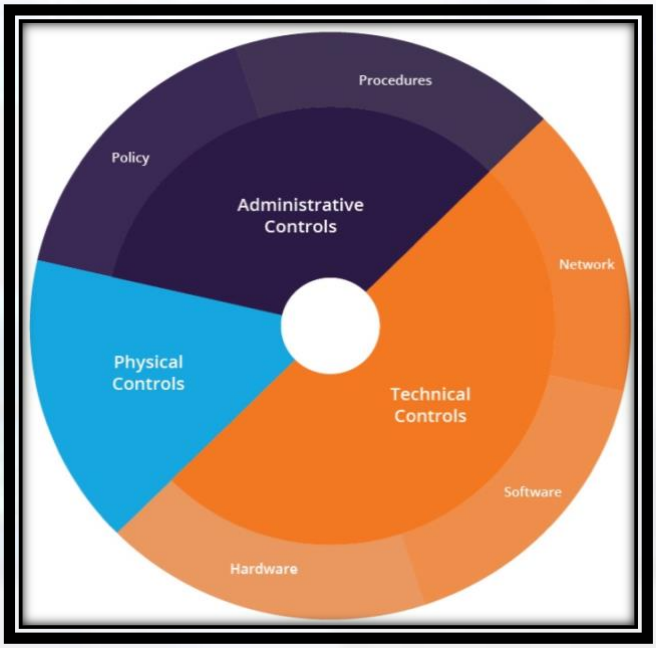
Human Factor in Cybersecurity

Many cybersecurity breaches are caused by individuals falling prey to phishing or similar attacks which are used to gain credentials to access utility systems. The human factor is thus considered by many to be the weakest link in cybersecurity. Development and deployment of better tools to secure the human interface could potentially reduce cybersecurity threats via email systems, in particular. In the meantime, targeted phishing attacks are reported to be increasing.

THE FIRST LINE OF DEFENSE IS THE EMPLOYEES THEMSELVES

CYBER SECURITY CONCEPTS FOR SMART GRID





Key Cybersecurity Concepts applicable to Electric Power Operations

- ⇨ Resilience: Ensuring business continuity (Safety, security, and reliability of the processes and services).
- ⇨ Security by Design: Cost-effective approach to systems and operations from the beginning
- ⇨ IT & OT interplay: They are similar but different with many differing security constraints and requirements
- ⇨ Risk Assessment, Risk Mitigation & continuous update of Processes - human safety, physical, functional, environmental, financial, societal, reputational.
- ⇨ Cyber Security Standards & Best Practices Guidelines for energy OT environments for risk management process and establish security programs and policies: at the right time.

Security Requirements for Utility Operation: Security Processes

- ⇨ Security Policy,
- ⇨ Security Assessment,
- ⇨ Security Deployment,
- ⇨ Security Training and
- ⇨ Security Audit (Monitoring).

7 Layers of Security

- ⇨ Information Security Policies. These policies are the foundation of the security and well-being of our resources;
- ⇨ Physical Security;
- ⇨ Secure Networks and Systems;
- ⇨ Vulnerability Programs;
- ⇨ Strong Access Control Measures;
- ⇨ Protect and Backup Data;
- ⇨ Monitor and Test Your Systems.

Security Defense-in-Depth Concept

Since, it is believed that Security will ALWAYS be breached at some time – there is no perfect security solution. Security Defense-in-Depth is an information assurance strategy that provides multiple, redundant defensive measures in case a security control fails, or a vulnerability is quite effective.

Data Analytics

Using data analytic techniques, big data can be turned into useful information. High-performance computing can take advantage of fast processing to examine data sets collected from smart grid systems into operational information, providing insights into customer behaviour. It can also be used to recognize (or potentially predict) patterns or trends in data of new physical or cybersecurity threats to the grid.

Artificial Intelligence for Cybersecurity

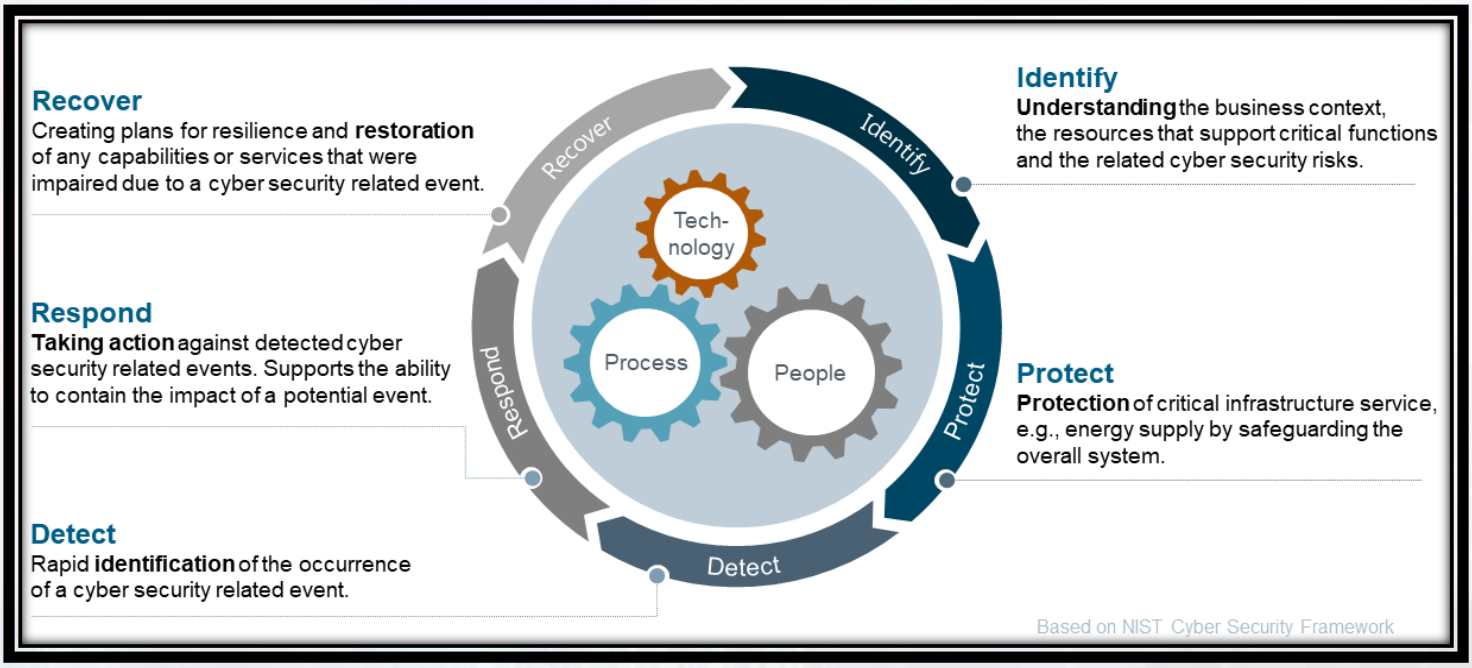
The speed of processing of AI systems is currently seen as providing protection for ICS and other networks that human operators may not be able to match, especially as cyber-attackers are employing increasingly sophisticated methodologies. AI can potentially respond to a cyberattack scenario far more quickly than a human decisionmaker.

Smart Meters

Networked embedded equipment, like Smart Energy Meters and Controllers found throughout the Smart Energy Grid need to be protected from a variety of security threats to avoid the possibility of significant financial losses due. Side-Channel Analysis is one of the most sophisticated forms of attack on cryptographic systems that uses information that leaks, unintentionally, from the real-world implementations of cryptographic hardware. For example, an attack might examine the characteristics of a cryptographic device when a variety of security keys are presented. Measurements and analysis of the power use (called Differential Power Analysis, or DPA), timing responses or electromagnetic radiation given off could provide clues as to the nature of the protected keys used within the hardware. Possible solutions - Tamper Resistant secure MCU, Secure element, Secure library (Crypto Library + Secure Storage).

Cybersecurity Requirements for Communication Protocols

- ⇨ Authentication
- ⇨ Authorization
- ⇨ Data Integrity
- ⇨ Accountability/ Non-repudiation
- ⇨ Confidentiality
- ⇨ Availability.



security management cycle for an organization

CHAIN IS AS STRONG AS THE WEAKEST LINK

Risk-Based Cyber Security

To ensure a secure environment, a strategy to protect the organization's cyber space is required for managing risks and boosting resilience. Organizations must build and implement a risk based cyber security policy with clear priorities, minimum ICT security baseline with threat and vulnerability information, build incident response capabilities and create awareness, educating and training opportunities.

We don't need to reinvent the wheel. We need a Cyber Risk Management Information System that has a user-friendly interface. It should integrate the best, most recent data from our own sources. It has to be a lean machine. At the same time, it should give us more transparency than we have today. Step by step, we can make the cyber risk MIS our own. The whole process takes less than half a year, and yet the finished product really feels like something that was made for us, not like an off-the shelf solution.

"Step by step, we can make the cyber risk MIS our own. The whole process takes less than half a year, and yet the finished product really feels like something that was made for us, not like an off-the shelf solution."

STANDARDIZATION IMPERATIVES

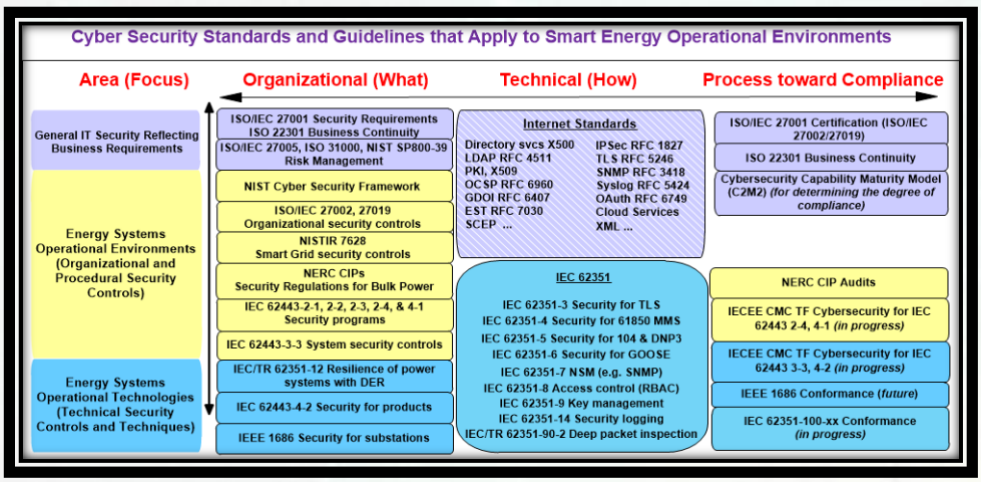
> "The beauty of standards is that there are so many to choose from!"
>
> Andrew S. Tanenbaum (1990)

In an ideal world, we would have exactly one standard for each task or interface. In reality, there are often overlapping or rivalling standards, driven by different vendor "camps", in case of Cyber Security, Standards by different Global, regional & National SDOs.

One of the most challenging Imperatives for "Standard Development Organizations" is Harmonization of Standards. "Standards & even SDOs are not at the forefront of Critical Infrastructure planners', utilities' or users' minds". There are misconceptions on what standards are for, and, the case for use of standards has not been made. Liberalization and Markets have a lot of great virtues, but they cannot create their own conditions of existences: they must be designed!

The multiplicity of technologies and their convergence in many new and emerging markets, however, particularly those involving large-scale infrastructure demand a top-down approach to standardization starting at the system or system-architecture rather than at the product level. Therefore, the systemic approach in standardization work can define and strengthen the systems approach throughout the technical community to ensure that highly complex market sectors can be properly addressed and supported. It promotes an increased co-operation with many other standards-developing organizations and relevant non-standards bodies needed on an international level. India needs to define and develop its own globally harmonized framework and architecture for the Electricity Infrastructure keeping in mind the new paradigm of Integrated Critical Infrastructure, where Smart Grid shall be one of the key (but not the only) component to meet the imperative of a 'smart, green and secure community'.

The key IEC, ISO, IEEE, NIST, and IETF cyber security standards and best practices are shown in the diagram below, organized by type (What, How, Process towards Compliance) and by level (High general level, High energy-specific level, Detailed technical level).



CYBER SECURITY REGULATIONS & POLICIES LANDSCAPE

Initiatives in India:

- Information Technology Act,2000 (17.10.2000)
- National Cyber Security Policy notified in 2013
- National Critical Information Infrastructure Protection centre (NCIIPC) 10.01.2014:
  - Guidelines for protection of critical Infrastructure (CII)
  - Framework for evaluation of Cyber Security
- Computer Emergency response Teams (CERT-In)
- Mandatory Reporting as per Rule 12(1) (a) of IT Rules 2013
- ISO: 27001 under the Information Technology Act, 2000

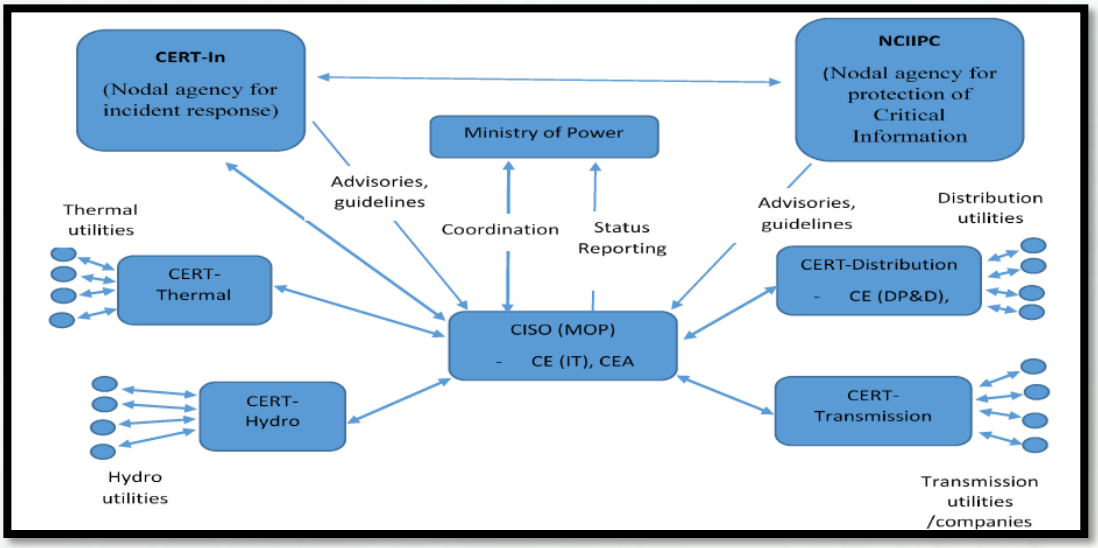
In Power Sector:

Indian Electricity Grid code Clause 4.6.5; IS-16335 :2015 Power Control Systems-Security; CERC (Communication System for inter-State transmission of Electricity) Regulations, 2016.

CEA is formulating a comprehensive strategy to address the cyber security issues that Power Sector faces. A National policy doctrine to address cyber security for national critical infrastructure and a regulatory framework that provides guidance to the industry players across generation, transmission and distribution - To review preparedness with respect to advisories on Cyber Security Framework and to vet self-assessment of gaps vis-à- vis baseline security & resilience requirement; To prepare the requirement for setting up of C-SIRT (eligibility criteria, scope of work etc.); To design and develop Cyber Security Policy (CSP) & Procedures along with CCMP; Security Policy and Management; Security Organization; Security Mandates for the Corporate IT Systems; Domain Specific security standards for Control Systems; Business Continuity Planning and Disaster Recovery; Customer Data Protection; Physical Security Requirements; Periodic Assessments and Reporting; Data Sharing and Collaboration…

Organization structure for Cyber Security in Power system

Courtesy CEA dated presentation (2017)



It is evident that Cyber Security is a very complex paradigm, and with evolving new technologies, requirements and ever-increasing Attack Surface the vulnerabilities are rising many folds with time. In such a dynamic scenario, how do we develop a Cyber Security Strategy to make our Critical Infrastructure comprehensively Safe, Secure, Resilient and Trustworthy?

It is evident that Cyber Security is a very complex paradigm, and with evolving new technologies, requirements and ever-increasing Attack Surface the vulnerabilities are rising many folds with time. In such a dynamic scenario, how do we develop a Cyber Security Strategy to make our Critical Infrastructure comprehensively Safe, Secure, Resilient and Trustworthy?

Though government of India has put measures in place to check for any mal-intentioned bug or subcomponent in these equipment / systems, but these are not providing....

Lack of high level of assurance from intentional built in mechanism meant to compromise security of system due to following reasons/constraints: Sheer volume of equipment and their subcomponents; Gaps of Standards; Gaps in Capacity Skill set in Utilities/DISCOMs and budget provisions... Experience confirms that when the entire organization shares a common way of thinking about vulnerabilities, security can be significantly enhanced.

National Cyber Security Strategy 2020 (NCSS 2020)

The Indian Government under the aegis of National Security Council Secretariat through a well-represented Task Force is in the process of formulating the National Cyber Security Strategy 2020 (NCSS 2020) to cater for a time horizon of five years (2020-25).

Pillars of Strategy - various facets of cyber security are under examination under the following pillars:

- ⇨ **Secure** (The National Cyberspace)
- ⇨ **Strengthen** (Structures, People, Processes, Capabilities)
- ⇨ **Synergize** (Resources including Cooperation and Collaboration)

Proposed vision is to ensure **a safe, secure, trusted, resilient** and **vibrant cyber space** for our **Nation's prosperity.**

GAPS & CHALLENGES

IF YOU THINK TECHNOLOGY CAN SOLVE YOUR SECURITY PROBLEMS, THEN YOU DON'T UNDERSTAND THE PROBLEMS AND YOU DON'T UNDERSTAND THE TECHNOLOGY.

The power sector cyberthreat landscape is rapidly evolving and expanding, with more frequent attacks, more numerous and varied threat actors, and increasingly sophisticated malware and tools that are more widely available and sometimes indiscriminately deployed. Power companies are among the most frequently attacked targets, increasingly by nation-state actors aiming for disruption and even destruction through Industrial Control System (ICS).

One of the most challenging vulnerabilities to address is cyber supply chain risk, given the increasingly far-flung and complex nature of the supply chain. Cyber supply chain accountability and ownership are not well-defined within companies, most CISOs have no control over their enterprises' supply chain, and they may have little access to supply chain cyber risk intelligence or visibility into suppliers' risk management processes. Add to that a lack of manpower and the sheer number of suppliers and transactions, and you begin to appreciate the scope of the challenge. Most companies are just beginning to make suppliers more aware and accountable, and to demand supplier integrity.

- ⇨ Volume of equipment and Sub-Components:
- ⇨ Lack of Testing Infrastructure
- ⇨ Gaps in Standards: Simplification and Relevance
- ⇨ Skill set in DISCOM - Approach to handle Contractually rather Technically
- ⇨ Budget Constraints
- ⇨ Protecting CII (Critical Information Infrastructure)
- ⇨ Digital Infrastructure Security

The problem is not the lack of standards, but lack of understanding on relevance and usage of the right standard for Indian ecosystem. Internationally there are too many standards available and very often having duplicities, hence, these required to be simplified and modelled for Indian Utilities. Utilities shall spec-in such standards which are drafted by national organization.

ONLY AMATEUEURS ATTACK MACHINES, PROFESSIONALS TARGET PEOPLE

Experience confirms that when the entire organization shares a common way of thinking about vulnerabilities, security can be significantly enhanced.

SOLUTIONS FOR INDIA

Secure Cyberspace Assurance –

Promise of a trustworthy Cyber-ecosystem

Internet Resilience of India - It is of utmost importance to ensure the security and resilience of the INTERNET within the country to enhance cyber security capabilities to better protect Indians and defend critical government and private sector systems.

THE WAY FORWARD for INDIA is to develop Internet Resilience for the nation. It is of utmost importance to ensure the security and resilience of the INTERNET within the country to enhance cyber security capabilities to better protect Indians and defend critical government and private sector systems. National Electricity Infrastructure - There is a need to develop Resilient, Secure and Trustworthy Grid which to a large extent is immune to cyber-attacks. Cyber Security - as the world is increasingly interconnected, everyone shares the responsibility of securing cyberspace.

PROCESS

- Cyber Laws: refined as per utility needs.
- Trusted Vendor List: Develop "National Charter of TRUST" under NSA, publish trusted vendors for Critical infrastructure.
- Policy Level actions: Inspiration from bold steps by USA, Australia & New Zealand to protect power systems.
- Blocking unreliable vendors:
  - Those debarred by international agencies due to fraudulent practices
  - Belonging to countries having restrictive clause for mission critical applications.
- Physical Security processes: Stringent process for Document Control, Access control, User authentication and password protection.
- Security education and training programs on sharing security vulnerabilities, threats, and solution information.
- Utilities form a cyber division of experts & take ownership of complete security.

COMMERCIAL

- ⇨ Limit participation of neighbouring countries having national boundary conflict
- ⇨ Global companies which have registered offices for engineering, design, integration, testing, equipment inspection in India should only participate.
- ⇨ RACI Matrix on Cyber security as part of bid document.
- ⇨ Equipment Support for 10 Years.
- ⇨ Service support team within India
- ⇨ Equipment compliant to standards BIS, IEC, IEEE & ITU etc.
- ⇨ Bidder has >80% Indian Employee in organization
- ⇨ Mandatory annual security audit /penetration testing for systems.
- ⇨ QCBS basis for bid evaluation.

TECHNICAL

- ⇨ Follow CERT-In guideline and push for IEC 62443 and ISO 27019 to meet OT/IT cybersecurity requirement.
- ⇨ Products certified by Cyber security test facility in India e.g. CPRI, STQC (under MeitY), TEC (under DOT) or designated global test agencies.
- ⇨ Hardware shall be CE or equivalent.
- ⇨ Configuration of products / application in English language.
- ⇨ Origin of Source code of application must be declared
- ⇨ Firmware shall be readily available on support sites.
- ⇨ Data Centre should comply to minimum Tier-3 level security along with comprehensive SOC capability
- ⇨ Reference Architecture of Smart Grid application as published by IEC/IEEE / BIS / IEEMA should be used

One of the proposed solutions could be that all utilities form a cyber division of experts & take ownership of complete security instead of relying on different vendors for their respective deliveries. Some of the issues that are critical for securing the Smart Infrastructure are: Best Security Practices for Protecting Big Data; Approach to Address Security of data in Cloud and Standards for Emerging Technologies, Data Management - Minimum security assurance in Devices & systems; Mandatory certification of Devices before bringing it in market; Increase in numbers of testing labs; India specific protection profile of new devices coming up in emerging technologies…

AS THE WORLD IS INCREASINGLY INTERCONNECTED, EVERYONE SHARES THE RESPONSIBILITY OF SECURING CYBERSPACE.

CONCLUSION & RECOMMENDATIONS

Power systems are among the most complex and critical infrastructures of a modern digital society, serving as the backbone for its economic activities and security. It is therefore in the interest of every country to secure their operation against cyber risks and threats.

It is imperative to delve into the security, privacy & trustworthiness aspects and implications of the new paradigm of "Critical Information Infrastructure" and "Internet of Things" that the pervasive computing has enabled, thus raising new challenges for the 'IT & Communication Security' Development & Evaluation Eco-system. Hence, needing a new rigorous and vigorous effort in developing a "Comprehensive Cyber Security, Resilience & Trustworthiness" Strategy Framework encompassing all the critical domains and Stakeholders classifications and their respective imperatives from Cyber Security, Resilience & Trustworthiness Perspective.

Considering the current and future evolving Cyberthreat Landscape, it would be absolutely critical to have Two National Documents:

1. A concise yet comprehensive **'National Cyber Security Strategy'** that sets clear, top-down directions to enhance the cyber resilience for the ecosystem that includes government, public and private sectors, the citizenry, and also addresses international cyber issues.
2. A separate **'National Cyber Security Policy'** based on principles laid down in the 'Strategy'. It must be outcome-based, practical and globally relevant, as well as based on risk assessment and understanding of cyberthreats and vulnerabilities. The security framework must include the compulsory testing of cyber products, infrastructure skill capacity development, responsibilities of entities and individuals, and public-private partnerships.

An accountable integrated national cybersecurity apparatus to be structured/ restructured and it must be provided clear mandates and be empowered adequately. It must be able to supervise and enforce policies across India, including policies regulated by independent regulators.

National Trust Centre:

As per recommendations of Telecom Regulatory Authority of India (TRAI) on "Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications" released on 5th September 2017 National Trust Centre (NTC) must be set up without any further delay.

This NTC must be geared up to undertake the Security Testing and Evaluation comprehensively including but NOT limited to Devices, Systems, Networks, Application & System Softwares, Firmwares, Communication Stacks to ensure that the deployed Devices, systems and solutions are completely Trustworthy.

National Charter of Trust:

India needs its own National Charter of Trust to develop an ecosystem of Trustworthy vendors that Electricity Utilities and other Critical National Infrastructure agencies can TRUST absolutely by establishing the best practices in the domain of cyber security that are globally harmonized in Standards, Strategy, Innovation, Certification, Transparency and all other core characteristics required to build an absolutely TRUSTWORTHY ecosystem.

Improving cyber safety and resilience requires all stakeholders to act together at scale and in a coordinated way, including governments, the engineering professionals, operators of critical infrastructure and other systems, and developers of products and components. The evolving nature of the challenges will require continual responsiveness and agility by governments and other stakeholders.

The only approach would be to adopt top-down approach to standardization starting at the system or system-architecture rather than at the product level. We need to Study & Analyze the diverse Use Cases, Applications and corresponding Stakeholders & their respective requirements to understand their respective Characteristics and concerns. Develop a Granular Smart Grid Architecture followed by developing a Cyber Security Architecture mapping all the security, privacy, safety, resilience characteristics with the Granular Smart Grid Architecture.

The IEEMA Vision Electricity for All and Global Excellence leading to Human Enrichment – is based on the five building blocks viz. Credibility with Stakeholders, Excellence, Global Presence, Environment and Enabling Power to All.

The relevance - Ieema's membership base comprehensively covers the multitude of different aspects of the Smart Grid paradigm. Ieema has been major contributing stakeholder and partner in the Indian electricity ecosystem growth story for more than last six decades and, is in sync with the ground realities of electricity infrastructure deployments. Ieema smart grid division members have extensive pool of Individual and organizational competencies, knowledge base and understanding of Indian Power Systems and Utilities.

Ieema's perspective – Ieema views Smart grid as an integral yet one of the most critical components of a nationwide Integrated Smart Infrastructure. Thus, it believes that its architecture and the framework must not be considered or designed in isolation; rather it must form an integral part of the structured, Nationwide Homogeneous Framework and architecture defined and harmonized to the finest granularity. It must take into consideration the implications of other concurrent infrastructures and/or services running for the consumers/stakeholders to optimize the Life Cycle (Total) cost of all the infrastructures for a given geographical territory.

IEEMA Smart Grid Division Mission Enabling Indian Electricity infrastructure to become resilient, sustainable and secure…

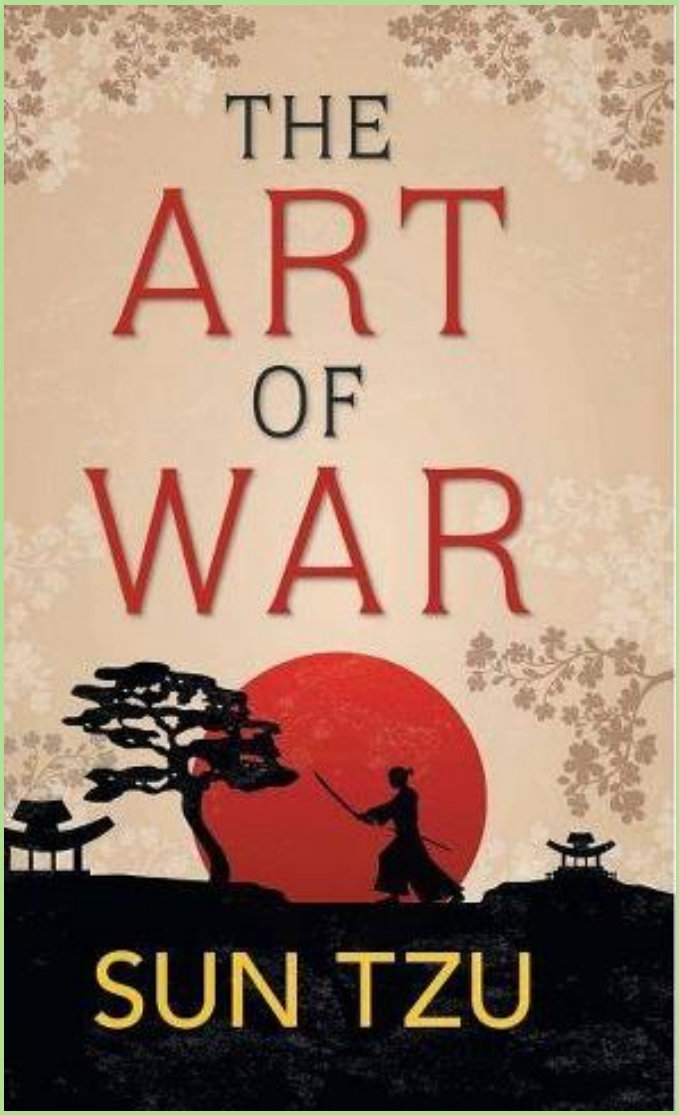
To ensure a comprehensive and structured deployment of nationwide smart grid infrastructure, it's Imperatives to address the current challenges like 'energy security', 'Electricity for all', and 'financial health of distribution utilities' along with 'Modernization of the Grid' in a holistic and sustainable manner.

Objective – Ieema smart grid division by virtue of its comprehensive members base covering the whole spectrum of the electricity infrastructure is uniquely positioned to support, advise and hand hold the government, utilities, policy makers, funding agencies and regulators in their endeavors to implement their restructuring, modernization and up gradation plans. Ieema smart grid division has taken upon itself to proactively support and enable the various government departments, ministries, utilities and other interested stakeholders to implement various relevant initiatives like National Smart Grid Mission (NSGM), National Mission for Enhanced Energy Efficiency (NMEEE), National and System Management (NSM) from IEC, National Electric Mobility Mission (NEMM).

Action Plan - To support the utilities and the government in their respective smart grid initiatives Ieema Smart Grid division has formed Focus Groups in critical areas, which need immediate co-operation amongst the various stakeholders to enable realization of Smart Grid Vision and Roadmap of Ministry of Power. The goal is to reach out to all the direct and indirect stakeholders in various government departments, research and academic institutions, industry associations, regulators and standards developing organizations to have inclusive deliberations and actionable insights to resolving the various challenges being faced by all the stakeholders in their respective endeavors to make our nation 'smart green & secure'. Initial few Focus Groups:

- ⇨ Smart Grid Architecture and Framework FG
- ⇨ Smart Grid Interoperability, Standards and Harmonization FG
- ⇨ Cyber Security FG

Cyber Security : Many Battles & A War



If you know the enemy and know yourself, you need not fear the result of a hundred battles.

If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat.

If you know neither the enemy nor yourself, you will succumb in every battle."

Each of these 3 points of 5th Century B.C. book directly applies to the world of Cyber Security.