Manipal Journal of Science and Technology

Volume 7 | Issue 1 Article 1

6-30-2022

Critical Information Infrastructure Protection, Vulnerabilities, Threats and Challenges: A Critical Review

Krishna Prakasha
Manipal Institute of Technology, Manipal, India, kkp.praksh@manipal.edu

Recommended Citation

Prakasha, Krishna (2022) "Critical Information Infrastructure Protection, Vulnerabilities, Threats and Challenges: A Critical Review," *Manipal Journal of Science and Technology*: Vol. 7: Iss. 1, Article 1.
Available at: https://impressions.manipal.edu/mjst/vol7/iss1/1

Review Article

Critical Information Infrastructure Protection, Vulnerabilities, Threats and Challenges: A Critical Review

Neeraj Saini, Tejas Sorte and Krishna Prakasha*

Email:kkp.praksh@manipal.edu

Abstract

Protection of Critical Information Infrastructure is a crucial requirement nowadays and requires immediate attention and a lot of prevention activities to avoid any cyber threat to critical IT services. This article aims to give a basic overview of Critical Information Infrastructure (CII) and Critical Sectors such as the Power and Energy Sector, Banking Financial Service and Insurance (BFSI), Telecommunications, Government Services, the Transport Sector, the Health Sector, etc. The consequences of attacks on these sectors have been examined, including their national and international challenges. This article shall also discuss the vulnerabilities of common CII, security controls, emerging trends, threats, and challenges towards protecting CII. Due to the occurrence of numerous cyber-attacks such as Distributed Denial-of-Service (DDoS), Advanced Persistent Threats (APTs), Phishing attacks, and others against critical systems, CII Protection has become a source of concern for every nation. Since information infrastructures are crucial to critical systems, an attack or disruption may spoil the operation of critical systems. Developed countries such as the USA, UK, Japan, etc., have already created a system; however, due to various additional particular issues and requirements, these solutions are not always appropriate for developing countries. On the other hand, emerging countries' information infrastructures undergo extraordinary expansion and problems. This article also covers the global demand for CII and the parameters for recognizing CII, which is a crucial endeavor. It also examines the existing state and potential development of India's and other countries' information infrastructures.

Key words: Critical Information Infrastructure (CII), Vulnerability, Threat, Protected System, Security Controls.

Introduction

Critical information infrastructure (CII) security is a global concern because it is one of the most vital assets for any nation's infrastructure. Apart from boosting social connections and information transfer, the technological revolution has enhanced the productivity of organizations across the board. CIIs are those computer resources upon which the core functionality of Critical Infrastructure is dependent. As per the Indian IT Act, CII can define "the computer resource, the incapacitation or destruction of which shall have a debilitating

impact on National Security, Economy, Public Health or safety" [1]. However, CII is the backbone of economic activities and national life in the USA. Businesses that provide crucial services that are exceedingly difficult to replace create them. If these services' functions are halted, weakened, or unavailable to the user, it could significantly impact economic and national life. Whereas in Australia, "The Information Communication Technology [ICT] component of critical infrastructure is CII". Different Nations define CII according to their importance and priority [2-3].

CII has two sides: on the one hand, it considers ICT and digital assets (as a stand-alone CI), and on the other hand, it requires that the inter-sectoral side of ICT and an asset within each of

Neeraj Saini, Tejas Sorte, Krishna Prakasha

Department of Computer Science & and Engineering, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal 576104, India.

Manuscript received: 12-01-2022

Revision accepted: 24-01-2022

* Corresponding Author

How to cite this article: Neeraj Saini, Tejas Sorte, Krishna Prakasha, “Critical Information Infrastructure Protection, Vulnerabilities, Threats and Challenges: A Critical Review” Manipal J. Sci. Tech., vol.7(1), 01-10, 2022.

Published by Impressions@MAHE, 2022

the CIs (Power and Energy, Finance, Telecom, Water and Food, etc.) [4].

CII can recognize in various ways (objects) in different ranges of activity and in other countries. Still, all of these objects share some common characteristics that define the CII's uniqueness in terms of national security.

In India, define the protected system (a highly critical component within CII) in the IT Act, where the "appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system". Any cyberattack on identified services/organizations will be considered Cyber Terrorism under Section 66F [5]. Some of the systems have already been declared as protected systems in India, such as Central Identities Data Repository (CIDR) in UIDAI [6], GST Database (GSTN) [7], and many more. Nowadays, ensuring the protection of CII is a challenging and critical task itself since critical sectors are interdependent. As the Internet of Things (IoT) becomes the standard model, the number of cyberattacks on information infrastructure, thefts, and data frauds will skyrocket. The failure to recognize the risks associated with information systems networks may result in the CII's demise.

The following critical sector needs to be functioning in a very secure manner so that crucial services under these sectors cannot be disturbed/attacked [8-9]:

a) Power and Energy,
b) Banking Financial Service and Insurance (BFSI),
c) Telecommunications,
d) Government Services
e) Transport (air, surface, rail, and water)
f) Public Health,
g) Water Supply,
h) Food,
i) Strategic and Public Enterprises,
j) Defense etc.

It is also required to develop awareness programs to reduce vulnerabilities, evolve policies, frameworks, and strategies for CII protection, and provide strategic leadership for a coherent government response in the event of a threat. Further, ICT directly impacts social behavior, economic growth, and business conduction. Controlling and monitoring various core critical services such as electricity, water supply, and medical services are getting computerized day by day, growing their dependency on ICT. Information infrastructure protection is vital as it has broad, direct, and indirect consequences on critical infrastructure [10-13].

Figure 1 [1], defines the CII to fit in our cyber world. The initial layer of cyberspace consists of physical and non-physical components. It indicates the virtual computer world, an electronic medium that allows us to communicate over the internet inside our cyber world, so many critical sectors, as mentioned above, where these individual sectors can affect the public health, economy, national security, etc., once they are under cyber-attack. These critical sectors define the most vital part, i.e., CII, which organizations need to prioritize to safeguard their national infrastructure [14-15].

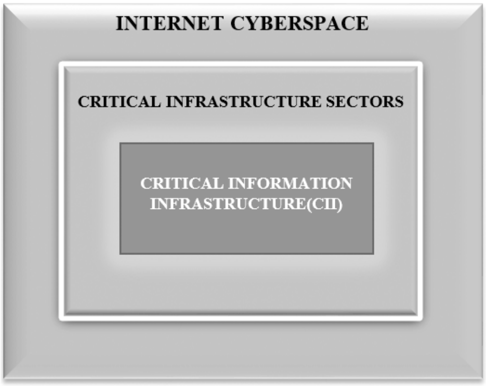
INTERNET CYBERSPACE
CRITICAL INFRASTRUCTURE SECTORS
CRITICAL INFORMATION INFRASTRUCTURE(CII)

Figure 1 Defining CII.

The evolving information infrastructure differs drastically in terms of various factors scale such as connectivity and dependencies from traditional structures. In addition, cyber-threats are fast evolving in terms of their character and ability to harm. The communication systems are interconnected resultant, interdependencies, and vulnerabilities globally, including damage and threats to the national security systems. Protective measures are required to minimize cyber threats and improvements in continual technological and new approaches [15-16].

The term CII appeared in the early 2000s. It denoted the "material and digital assets, networks, services, and installations that, if disrupted or destroyed, would have a serious impact on the health, security, or economic well-being of citizens and the efficient functioning of a country's Government". The physical component of the information infrastructure at an organizational level includes the location and disposition of network parameter devices and equipment (such as routers, servers, and critical information storage media), documents, and physical storage devices (HDDs) associated with the organization's own private data elements. Electronic information assets (like data and information held across systems), operating systems (OS), and numerous applications and software in the company have all been developed and implemented.

Critical Information Infrastructure Protection (CIIP) worldwide is an area of concern. Developed and developing countries managed several critical services and systems. On the other hand, the information infrastructure is a single point of failure. Information dependent on crucial systems can be disrupted and possibly inactivated [4,17].

Materials and methods

The literature review of relevant CIIs studies from domestic and international literature revealed the importance of CIIs in this dynamic technological environment. The study shows the interdependencies among the critical sectors below in Figure 2. The figure mentioned below has been taken from the “European Network and Information Security Agency (ENISA)” document. It is a European Union agency for cybersecurity. It shows that every critical sector is an individual critical domain in terms of parameters. If one critical sector was hit, it would cascade to the other remaining sectors.

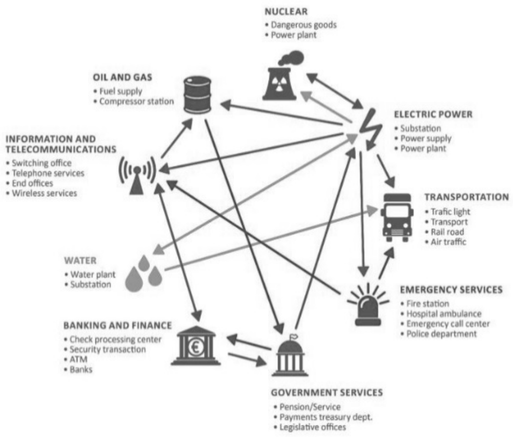

Figure 2 Representing Interdependency among Critical Sectors [8].

This article has included some case studies done by various countries, such as the USA, UK, Russia, Malaysia, EU countries, Ukraine, etc. These case studies reveal the important aspects of CII and focus on training and user awareness programs They did the same by conducting the surveys. One of the essential aspects they highlighted was the identification of CII. As a critical sector, identifying CII is equally and critically important. Everything cannot be a part of critical [16-19]. There are some components/services that are critical in each sector. They may define as follows:

- Identification of critical sectors (finance, energy, telecommunication, transport, health, etc.)
- Identify each sector's critical components/business process (power and energy, telecom, banking, health, etc.)
- Determine the infrastructure, related assets, processes, and operators required to provide these services [4-9].

Based on the study and specific facts, some parameters have been developed to evaluate critical sectors' CII components. Like in the case of infrastructure, it can be filtered using a number of sectoral and intersectoral parameters, such as the impacted geographic region, market share, the number of people who rely on the infrastructure, and the recovery time [11]. The same is discussed in the next section in a detailed manner to identify the CII.

Published by Impressions@MAHE, 2022

Results and discussion

CII has more chances to target an attacker to disrupt, hamper, or compromise IT-enabled services or processes, which are important for a nation. Organizations in critical sectors supply these services and capabilities through a variety of Business and Industrial Processes that run on the underlying Information Technology (IT) and Operation Technology (OT) platforms. The requirement for identifying CII within and across all Critical Sectors is the first step in having a consistent strategy [1, 17].

Identification and Assessment of CII

Any CII that identifies and assesses what is critical to a country will devote more resources to safeguarding services, processes, assets, and infrastructure where failure would have serious implications. In India, the National Critical Information Infrastructure Protection Centre (NCIIPC) is a Government Organization created under the Information Technology Act, 2000 (under Sec 70A). Guidelines for the Identification of Critical Information Infrastructure have already been published by this organization. Additionally, India's NCIIPC has declared 06 critical sectors. Depending on their requirements, these sectors may be different or given a higher priority in other countries [1, 18].

Similarly, different organizations in other countries are dealing with CII. Like the "Centre for the Protection of National Infrastructure (CPNI)" of the UK, the "Department of Homeland Security (DHS)" of the USA, the "National center of Incident readiness and Strategy for Cybersecurity (NISC)" of Japan, etc. To strengthen the security of critical infrastructure, the DHS agency of the USA is working towards resilience by generating a better understanding and voluntary partnership landscape across the country. It could be achieved by working with private and public stakeholders to resolve the security of infrastructure and resilience knowledge gaps, identify resilience-building prospects and strategies, and improve information-sharing systems among stakeholders [20].

Assess the criticality of functions and services in India based on the information provided by stakeholders. Then it also includes "the magnitude of impact on National Security, National Economy, Public Health, or Public Safety in case of incapacitation/destruction of its ICT infrastructure". Similarly, Critical infrastructures (Cis) are also taken into account by the US government as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" whereas in the UK, "Critical information infrastructure (CII) may refer to any IT systems that support key assets and services within the national infrastructure" [3, 21]. There are specific critical parameters based on a particular critical sector, such as the financial sector, defined as follows:

(a) Customer, business, and government services affected based on:

- The total number of daily transactions.
- Per day, the total value of all forms of transactions.
- The number of devices connected and the size of the network.
- The total number of customers in various categories.

(b) Apart from the above, timeframe (in hours, days, or weeks), after which the impact of non-availability of ICT infrastructure on "National Security, National Economy, Customers, Public Health, Public Safety, Business, and Government" will be very substantial. So, if the timeline is shorter, the situation is more severe.

(c) If any, the geographic or environmental impact of incapacitation/destruction of the underlying ICT infrastructure (in an area/city/district/state/region/nation-wide, or even beyond the international border)

(d) Dependency level to include:

- Non-availability of services and functions due to the failure and cascading effect of other critical sectors/subsectors and the breakdown or damage of the essential ICT infrastructure [11].
- Other critical sectors/sub-sectors rely on essential functions and services [1].

Based on the parameters mentioned above, the following services could be classified as adhering to CII under some of these Critical

Sectors [9, 17]:

- Power and Energy: Supervisory Control and Data Acquisition (SCADA) System
- Banking Financial Service and Insurance (BFSI): Core Banking Solution (CBS), Trading System (Stock Exchanges)
- Telecommunications: International Gateway Router, Network Management System (NMS)
- Government Services: Crime Data Records, Passport Services
- Transport (air, surface, rail, and water): Air Traffic Controller (ATC), port services

It is worth noting that determining the criticality of CII is a challenge in today's complex environment for ensuring a country's CIIP.

Vulnerabilities in CII.

Vulnerability refers to a flaw or weakness in a system that allows attackers to access it. An attacker can utilize vulnerabilities to achieve financial gain, steal confidential information, bring websites down, or damage data, making required information unavailable to authorized users [22].

CII is especially vulnerable to various cyberattacks. Large-scale Distributed Denial-of-Service (DDoS) attacks can be launched swiftly utilizing botnets to prevent national critical systems or services from reaching full operational capability. Such cyber-attacks substantially impact our daily routine services, such as train, flight, and bus ticketing systems [23-25].

While given the increasing vulnerability of infrastructure and the sophistication of the threat, the necessity for CIIP has become a more prominent and pressing concern. An effective CIIP must consider the growing cyber threat in terms of new capabilities and vulnerabilities in digital and networked society [26].

The vulnerability may be defined in various categories, such as Software Vulnerabilities, Personnel Vulnerabilities, Disaster Recovery Planning Vulnerabilities, and Network Protocol Vulnerabilities [27].

Due to advanced and growing modern technologies, many essential systems are now susceptible to natural disasters (as indicated above), such as earthquakes, tsunamis, severe weather, and so on. Surprisingly, they have no physical consequence; nonetheless, abrupt demand spikes during crises might result in service denials or blackouts. This case happened in Mumbai, India (October 2020), where grid failure resulted in massive power outages [28].

CII has become particularly vulnerable to hacktivists, criminals, and even state actors and terrorists looking for an opportunity. They are usually used to attack important systems by transmitting malware (trojans, viruses, worms, etc.) that modifies and destroys critical data or disables services. The state actors use Advanced Persistent Threats (APT) mostly to gain any nation's confidential information. APT usually keeps watch on important aspects and resides in the system for many years without the user's knowledge. The important thing is that this type of virus could hardly be detected by an antivirus software engine. Detailed information and guidelines on vulnerabilities or configuration errors are available to everyone on the Internet, which quickly leads to CII breaches.

Emerging Trends, Threats, and Challenges in CII

After reviewing the relevant articles/papers, this section tried to bring up all pertinent issues in the following sector. In each case, possible solutions are also given in the form of a policy statement. From the higher management side, these policy-level solutions may help them better understand and implement them on the ground level.

BFSI Sector.

Banking Financial Services and Insurance (BFSI) is one of the critical sectors for every country due to its direct impact on its national economy. The cashless economy has made critical banking infrastructure a lucrative target for cybercriminals. Some of the issues and challenges that need deliberation are as under [21, 25]:

Mobile App Vulnerabilities.

Multiple security controls have to be used to secure managed and uncontrolled mobile devices and applications. Unpatched vulnerabilities can lead to the compromising of online shopping and banking credentials. Mobile application developers, wireless network service providers, and IT professionals in financial institutions must cooperate for the organization to succeed. The BFSI sector promises to address these concerns while also ensuring that financial transactions on mobile devices are as simple as possible.

Cloud Security.

Cloud-based platforms not only have financial benefits but also increase productivity. Despite this, the financial services industry is wary of fully embracing the cloud. It has numerous benefits as cloud computing becomes increasingly common in the financial sector. A hybrid strategy that uses both private and public clouds will emerge. Migration to cloud services, data protection/security, and regulatory compliance are all issues that the BFSI sector aims to address.

Combating Cyber Fraud.

Cyberattacks are becoming increasingly common in enterprises. Banks are increasing their online and mobile access, which increases the attack surface. Malicious, irresponsible, and compromised users are the most severe dangers and challenges to detect. These employees, contractors, and partners have lawful access to critical data and IT systems since they are already inside the bank's safe perimeter.

Vulnerabilities of ATM and Point of Sale (POS) Devices.

Fraud involving debit and credit cards is on the rise. Despite advancements in card security technology and the Payment Card Industry Data Security Standard (PCI DSS) standards, there are still security flaws in POS systems. Retailers are vulnerable to resourceful and organized cybercriminal gangs due to general security flaws in IT infrastructure. Malware explicitly designed to steal data from POS systems is freely available on the dark web. Furthermore, most ATMs operate on unsupported operating systems, which are vulnerable to various cyberattacks. An organization must follow the appropriate procedures to decrease the danger of POS system attacks and ensure secure transactions when using ATMs.

Poor stakeholders’ collaboration in financial services.

In this technological era where financial infrastructures become more interconnected than ever before, their flaws are likely to cascade onto other infrastructures and systems in the economic chain. In this scenario, stakeholder participation might be critical to quickly identifying and resolving difficulties. However, several approaches have been proposed to overcome these concerns. Still, cyber threat information (CTI) sharing is a procedure that has gained widespread support among cyber security professionals in both the public and private sectors. Any information used to identify, monitor, assess, and respond to risks can be included in this CTI [29].

Power and Energy Sector.

Several incidents in the recent past have exposed the vulnerabilities in the generation, transmission, and distribution sub-segments of the Power Sector and exploration/extraction, manufacturing, refining, and distribution segments of the Energy Sector. The Smart Grid rollout is a key initiative, but without a proper security framework, it can lead to a significant crisis and weaken the country’s stability.

In a recent critical incident in the USA (May 2021), Colonial Pipeline (an American oil pipeline system in Houston, Texas) halted its operations. A ransomware cyberattack crippled computerized pipeline management equipment [30]. Therefore, there is a need to highlight key cyber security threats across the entire Power and Energy Sector value chain:

Security of DCS/SCADA Networks.

The majority of DCS (Distributed Control Systems for industrial process automation, control, and monitoring) and supervisory control and data acquisition (SCADA) systems were developed before cyber threats existed, hardening and safeguarding them now presents a unique set of issues. The design does not account for quickly changing functional needs or the exponentially rising use of information technology in manufacturing and industrial settings. The volume, types, and severity of targeted threats to DCS/SCADA networks are increasing rapidly, which include External Threats (APTs, targeted attacks), Internal Threats (employees, contractors), and Human Errors (incorrect settings, configurations, and PLC programming).

Another issue is a lack of indigenous capability in developing state-of-the-art DCS/SCADA systems. The organization should develop a mitigation strategy for emerging cyber threats to DCS/SCADA networks [9,17].

Vulnerabilities in Smart Grid Systems.

Several sophisticated and intelligent devices are used in the Smart Grid to manage electricity supply and network demand. An attacker might use these devices' flaws to gain network access, compromise the security and integrity of transmitted data, and substantially impair or disrupt services. The smart grid network's size makes network monitoring and management extremely complex. The organization needs to address the issues of data spoofing, fraud detection, data loss prevention, denial of service, and similar concerns [27].

Convergence of IT and OT.

OT (operational technology) and IT (information technology) have traditionally been developed and managed as different areas, with various technology stacks, protocols, standards, governance frameworks, and organizational units in most businesses. These networks are increasingly frequently connected for business reasons. Legacy systems with unpatched vulnerabilities abound on OT networks, ready to be exploited. Maintenance and defense of OT networks necessitate specialized technical knowledge not found in standard IT skill sets. It is necessary to synchronize IT and OT plans and adopt shared governance and process frameworks. Security and data must be managed centrally, and resources must be retrained to understand the requirements of different domains. To address strategic, organizational, and technological issues, the company requires change management, and the implementation process goes smoothly.

While the integration of IT protocols and an internet connection has increased the efficiency of OT-based CII, it has also exposed IT systems to cyberspace threats, resulting in a considerable increase in the number of attacks. According to a poll of security professionals in six countries, at least one successful attack had impacted 90 percent of OT-based CII. According to another survey, half of the organizations that rely on OT have experienced downtime due to increasing cyberattacks in the past few years.

Existing Controls and Residual Risks.

Nowadays, higher management often considers cyber security a highly technical domain in any organization, perhaps best left to experts. It is referred to as a "cost of doing business" in the same way that insurance is. However, cyber security must be managed proactively as a critical component of overall operations in today's fast-paced environment. A company cannot presume that its present cyber security tactics and funding are sufficient because it has not been attacked recently. The widespread use of indigenous devices and systems can significantly reduce dangers.

Telecommunications Sector.

A successful cyberattack on a Telecommunications network could cripple critical services and disrupt governance. In the future, the telecommunication sector is very likely to encounter entirely new types of cybersecurity risks, ranging from known network flood attacks to highly complex Border Gateway Protocol (BGP) and Voice over IP (VoIP) multi-vector high-volume attacks [31]. There is a need for all stakeholders to deliberate on the technology and policy issues that are part of today’s security landscape.

Security of Network Devices and Operations.

Unified Threat Management (UTMs), Routers, Switches, Proxies, VPN Concentrators, Spam Filters, etc., are essential Network components. Vulnerabilities in these devices are often available in the public domain, and backdoors can never be ruled out. Similarly, Domain Name Systems (DNS) can be manipulated to launch attacks on CII. Currently, in India, the telecommunication sector relies almost totally on equipment of foreign origin. While TSPs/ISPs concentrate on performance and bandwidth, subscriber access devices' security is usually ignored [32]. Specific queries at the organizational level may arise in this scenario, such as how DNS can be secured against manipulations. What strategies should be adopted to provide secure access to subscribers, what should be the key ingredients of a coherent policy to support and fund indigenous development to achieve self-reliance and reduce the security risks etc.

Supply Chain Contamination.

Supply chain partners may provide attackers with a backdoor into the networks of host firms if they are not adequately maintained. Despite the increased threat and evidence around supply chain attack vectors, few compliance regulations specifically address third parties. The company needs to improve supply chain monitoring and implement strict security controls for people, processes, and technological changes.

Audit of Operations Support System.

Telecommunication networks are managed by Operations Support Systems (OSS), which provide network inventory, service provisioning, network configuration, and fault management. Management as a Service (MaaS) is becoming more popular in the telecom business. It brings many system management features and solutions into a single management environment, allowing for more flexibility and cost-effective implementation while scaling as customer needs evolve. In this scenario, the organization needed capacity development and a review of audit mechanisms to adapt to this emerging trend in OSS.

DDoS Mitigation.

Among the various security threats to the Telecommunication Sector, the most damaging effect is Distributed Denial-of-Service (DDoS). This kind of attack could be carried out in various ways, using various tools and codes. Institutional portals, banks, transit, newspapers, and broadcasting stations are all targeted by DDoS attacks, creating long-term outages. Even though services were restored without long-term or catastrophic consequences, this attack exposed CII's vulnerability. It demonstrated that cyberattacks are possible and can disrupt the delivery of critical services. It has also put tremendous pressure on security experts to bring out effective mitigation techniques ranging from a clean pipe, scrubbers, pattern matching, and AI/machine learning algorithms such as "Random Forest (RF), Decision Tree (DT), K-Nearest Neighbors (KNN), Support Vector Machine (SVM)", etc. [33-34]. The organization needs to focus on some of the most effective DDoS mitigation techniques for protecting the Telecommunications Sector.

CII Protection Measures.

The CII's strategic measurements and objectives are as follows [12,31]:

- Identify Critical Assets/Processes/Systems.
- Minimize the national vulnerabilities, which are at least in critical nature.
- Minimize recovery time and damage from cyberattacks.
- Security hardening and testing of critical equipment.
- Dissemination and sharing of information on varieties of cyberattacks.
- Preventive measures need to be taken at all levels.
- For damage management, the IDS system's early detection and rapid response capabilities must be improved.
- Reduce or eliminate the adverse impact of service disruptions on government and society.
- The affected system must be restored within the shortest possible time to ensure that it continues to function at a minimum level.
- Frequent auditing of CII components.

Apart from the above, there is also a requirement to take necessary steps at the National Level such as [31-35]:

- Require to develop a national program to minimize cyberspace security threats and vulnerabilities.
- Launch a national awareness and training campaign for online security.
- Improving the security of Government systems.

- Need to focus on Critical Information Infrastructure Protection.
- Requires national security and international collaboration on cyber security challenges to be strengthened.
- Collaboration with international partners on CII Protection.
- Need to strengthen the Public/Private Cooperation (Industry and Government): In most countries, many CIIs have private actors. Therefore, building public-private partnerships is a critical component of CIIP. The following may include [17]:
- Identify the issue and threats to national CII.
- Evolving the security policy for vendors and the protection of their products.
- Require an efficient policy and its implementation for a fast resolution to all incidents related to CII.
- System development to disseminate formal and informal information on crimes and cyber-terrorism.
- Blockchain Infrastructure may help accomplish the Confidentiality, Integrity, and Availability (CIA) features [29].

Important Security Controls to Protect CII [13, 29].

Preventive, detective, and remedial controls are the three types of security controls. Preventive controls prevent security incidents, whereas detective controls identify security events that violate preventive controls, and corrective controls address the discovered problems.

- Preventive Controls: Policies, Firewalls, Antivirus Software, Penetration Testing, etc.
- Detective Controls: Antivirus Software, Intrusion Detection Systems (IDS), Honeypots, etc.
- Corrective Controls: Antivirus Software, Disaster Recovery Plan, Zombie Zapper (a tool to stop flooding a network with traffic), etc.

Modern cultures are becoming increasingly interconnected and reliant on CII. Increased speed has also scaled up with inherent hazards and risks in the case of 4G or 5G networks. In this case, it is necessary to enforce the CIIP policy at the organizational level [32]. In a country's CIIP policy, many people/actors with various backgrounds and interests are involved. To develop a shared understanding and handle the issue, the government must interact with these individuals/actors. According to the research, in CIIP, various government activities have emerged, such as training and awareness-raising programs, information-sharing, developing the required framework, detecting vulnerability, developing incident-related activities, and weighting to implement the crisis management program. Apart from this, a Government’s CIIP policy must include some necessary guidelines and a comprehensive strategy. There is an urgent requirement for an effective CIIP policy that should follow a holistic approach, including challenges and problems faced by the organization/stakeholders. Since enough different agencies are working for CIIP, at the same time, Government roles in each country become essential.

Conclusions

This study provided the details of Critical Information Infrastructure (CII), including the current threat and challenges concerning information infrastructure in some critical sectors. For Practical CIIP, one has to cooperate and share the relevant information with the Governments to secure this environment.

Therefore, to ensure the success and protection of the National CII, it is required that the private sectors and government bodies, such as law enforcement intelligence agencies in specific fields, work together. Since the private sector operates and owns the bulk of a country's CII, public-private partnerships are one of the most important aspects of CII protection. To do this, the government should provide a well-organized, dependable, and effective network to the private sector and their support.

With the cooperation between government and private industries, it is also essential that the private sectors know whom to talk to in the Government and public sectors. Therefore, every organization has designated a “Chief Information

Security Officer (CISO)/Information Security Officer (ISO)" to look after this area. He will be the single point of contact for everyone, whether internal or external, especially in the case of a cyber incident. By doing so, public-private partnerships will be boosted, and information sharing between public/government departments at various levels will also be promoted.

Importantly, each country's government should consider having an open dialogue and conversation with academics and research institutes. They may be crucial in determining the best process, tools, and procedures for CIIP.

It is a reality that CII vulnerabilities will continue to exist and grow as ICT technologies evolve and improve. Furthermore, as the number of networked, interdependent operations increases, cyber security issues will only grow. Any damage or disruption to CII will directly impact national security, the economy, and public health and safety. To secure and safeguard CII, all stakeholders, public and private, must collaborate to achieve the CIA for CIIP and develop novel security solutions. As a result, a structure for coordination between industry and government must be designed. As a result, CII security is not a one-person job. Instead, it is a team effort, a comprehensive, multi-stakeholder approach requiring a distinct design with appropriate standards and resources.

References

[1] NCIIPC Guidelines for CII Identification, Available at: https://nciipc.gov.in/documents/Guidelines_for_Identification_of_CII.pdf, accessed January 2022.

[2] L. O. Nweke and S. Wolthusen, "Legal Issues Related to Cyber Threat Information Sharing Among Private Entities for Critical Infrastructure Protection," *2020 12th International Conference on Cyber Conflict (CyCon)*, 2020, pp. 63-78, doi: 10.23919/CyCon49761.2020.9131721.

[3] Critical Information Infrastructure, Available at: https://websites.fraunhofer.de/CIPedia/index.php/ Critical_Information_Infrastructure, accessed January 2022.

[4] Safeguarding Critical Information Infrastructure: Risk & Opportunities, Available at: https://www.itu.int, accessed January 2022.

[5] The Information Technology Act, 2000, Available at: https://www.meity.gov.in/content/information-technology-act-2000, accessed January 2022.

[6] UIDAI Notification, Available at: https://www.meity.gov.in/content/gazettes, accessed January 2022.

[7] GST update Available at https://www.cbic.gov.in/resources//htdocs-cbec/gst/GST-Update150220new.pdf, accessed January 2022.

[8] Communication network dependencies for ICS/SCADA Systems, Available at: https://www.enisa.europa.eu/publications/ics-scada-dependencies, accessed January 2022.

[9] Mariana Hentea, "Critical Infrastructure Protection," in Building an Effective Security Program for Distributed Energy Resources and Systems, *John Wiley & Sons*, 2021, pp.243-275, doi: 10.1002/9781119070740.ch7.

[10] S. Erokhin, A. Petukhov and P. Pilyugin, "Comparison of Information Security Systems for Asymptotic Information Security Management Critical Information Infrastructures," *2021 28th Conference of Open Innovations Association (FRUCT)*, 2021, pp. 89-95, doi: 10.23919/FRUCT50888.2021.9347608.

[11] Herrera, Luis-Carlos & Maennel, Olaf, "A Comprehensive Instrument for Identifying Critical Information Infrastructure Services", *2019 International Journal of Critical Infrastructure Protection*.25. 10.1016/j.ijcip.2019.02.001.

[12] Best Practices for Critical Information Infrastructure Protection (CIIP), Available at: https://publications.iadb.org/, accessed January 2022.

[13] Special Issue on Cybersecurity, Available at: https://www.nec.com/en/global/techrep/jou

rnal/g17/n02/ g1702pa.html, accessed January 2022.

[14] N. Kushwaha, K. Giles, T. Singer and B. W. Watson, "Cyber Personhood," *2021 13th International Conference on Cyber Conflict (CyCon)*, 2021, pp. 275-289, doi: 10.23919/CyCon51939.2021.9468299.

[15] E. Abdulova and A. Kalashnikov, "Some aspects of critical information infrastructure risk management," *2021 14th International Conference Management of large-scale system development (MLSD)*, 2021, pp. 1-5, doi: 10.1109/MLSD52249.2021.9600202.

[16] S. B. M. Sabtu and K. M. Mohamad, "Critical Information Infrastructure Protection Framework Development: Preliminary Findings from the Malaysian Public Sector," *2020 8th International Conference on Information Technology and Multimedia (ICIMU)*, 2020, pp. 1-6, doi: 10.1109/ICIMU49871.2020.9263397.

[17] Assenza, G., Cozzani, V., Flammini, F., Gotcheva, N., Gustafsson, T., Hansson, A., Heikkila, J., Iaiani, M., Katsikas, S., Nissilä, M., Oliva, G., Richter, E., Roelofs, M., Azari, M. S., Setola, R., Stejin, W., Tugnoli, A., Vanderbeek, D., Westerdahl, L., ... Young, H. (2020), "White paper on industry experiences in critical information infrastructure security": A special session at CRITIS 2019, *14th International Conference, CRITIS 2019, Revised Selected Papers* (pp. 197-207). Springer. Lecture Notes in Computer Science Vol. 11777 https://doi.org/10.1007/978-3-030-37670-3_18

[18] O. Potii and Y. Tsyplinsky, "Methods of Classification and Assessment of Critical Information Infrastructure Objects*," 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, 2020, pp. 389-393, doi: 10.1109/DESSERT50317.2020.9125028.

[19] S. Gnatyuk, Y. Polishchuk, V. Sydorenko and Y. Sotnichenko, "Determining the Level of Importance for Critical Information Infrastructure Objects," *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*, 2019, pp. 829-834, doi: 10.1109/PICST47496.2019.9061390.

[20] S. Breor, "Assessing Critical Infrastructure Dependencies And Interdependencies," *2018 Winter Simulation Conference (WSC)*, 2018, pp. 1-9, doi: 10.1109/WSC.2018.8632498.

[21] L. Cazorla, C. Alcaraz and J. Lopez, "Cyber Stealth Attacks in Critical Information Infrastructures," *in IEEE Systems Journal*, vol. 12, no. 2, pp. 1778-1792, June 2018, doi: 10.1109/JSYST.2015.2487684.

[22] T. V. Karlova, A. Y. Bekmeshov and N. M. Kuznetsova, "Protection the Data Banks in State Critical Information Infrastructure Organizations," *2019 International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS)*, 2019, pp. 155-157, doi: 10.1109/ITQMIS.2019.8928412.

[23] S. Mazepa, L. Dostàlek, O. Sharmar and S. Banakh, "Cybercrime and Vulnerability of Ukrainian Critical Information Infrastructure," *2020 10th International Conference on Advanced Computer Information Technologies (ACIT)*, 2020, pp. 783-786, doi: 10.1109/ACIT49673.2020.9208965.

[24] A. S. Shaburov and V. R. Alekseev, "Protection Models of Critical Information Infrastructure Objects from Targeted Computer Attacks," *2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, 2019, pp. 335-338, doi: 10.1109/EIConRus.2019.8656722.

[25] S. D. Erokhin, "Managing Security of Critical Information Infrastructure," *2019 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO)*, 2019, pp. 1-4, doi: 10.1109/SYNCHROINFO.2019.8814097.

[26] Y. A. Gatchin and V. V. Sukhostat, "Research of Vulnerabilities of Information Processing Processes Systems of Critical Information Infrastructure," *2019 Wave Electronics and its Application in Information and*

Telecommunication Systems (WECONF), 2019, pp. 1-4, doi: 10.1109/WECONF.2019.8840618.

[27] P. A. Wibowo Putro and D. I. Sensuse, "Threats, Vulnerabilities and Security Functions in Critical Information Infrastructure," *2021 8th International Conference on Information Technology, Computer and Electrical Engineering (ICITACEE)*, 2021, pp. 113-117, doi: 10.1109/ICITACEE53184.2021.9617515.

[28] Mumbai Power Outage, Available at: https://thewire.in, accessed January 2022.

[29] Karagiannis, I., Mavrogiannis, K., Soldatos, J., Drakoulis, D., Troiano, E., & Polyviou, A. (2020), "Blockchain Based Sharing of Security Information for Critical Infrastructures of the Finance Sector", *Computer Security - ESORICS 2019 International Workshops*, Revised Selected Papers (pp. 226-241).https://doi.org/10.1007/978-3-030-42051-2_16.

[30] Colonial Pipeline: The DarkSide Strikes, Available at: https://crsreports.congress.gov/product/pdf/IN/ IN11667, accessed January 2022.

[31] Vincent, Torty & Prince, Udoyen, "Implementation Of Critical Information Infrastructure Protection Techniques Against Cyber Attack Using Big Data Analytics", 2021, 10.13140/RG.2.2.12116.53124.

[32] D. Lučić and P. Mišević, "An Impact of Implementation of 5G Technology on Information Security," *2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO)*, 2021, pp. 412-416, doi: 10.23919/MIPRO52101.2021.9596777.

[33] A. S. Shaburov and V. R. Alekseev, "On the Assessment of Information Security Ensuring Models of Critical Information Infrastructure Facilities," *2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, 2020, pp. 492-496, doi: 10.1109/EIConRus49466.2020.9039481.

[34] P. Perrone, F. Flammini and R. Setola, "Machine Learning for Threat Recognition in Critical Cyber-Physical Systems," *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, 2021, pp. 298-303, doi: 10.1109/CSR51186.2021.9527979.

[35] Besenyo, Janos & Feher, Andras. (2020), "Critical Infrastructure Protection (CIP) as new soft targets: private security vs. common security", *Journal of Security and Sustainability Issues*. 2020/3. 10.9770/jssi.2020.10.1(1).