Scientific Research Publishing

Journal of Computer and Communications, 2021, 9, 80-102
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies

Maryam Roshanaei

Information, Science and Technology Department, The Pennsylvania State University Abington College, Abington, USA
Email: Mur45@psu.edu

How to cite this paper: Roshanaei, M. (2021) Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies. *Journal of Computer and Communications*, **9**, 80-102.
https://doi.org/10.4236/jcc.2021.98006

Received: July 19, 2021
Accepted: August 23, 2021
Published: August 26, 2021

Abstract

The importance of a nation's infrastructure is a vital core for economic growth, development, and innovation. Health, wealth, access to education, public safety, and helping prepare for global crises like pandemics are all dependent on functioning and reliable infrastructures. In decades, the substantial threats affecting infrastructures globally whether in the form of extreme weather, Covid-19 pandemic, or the threats of state and non-state actors' hackers, demanded urgency in building resilience infrastructures both during crises and in more stable conditions. At the same time, the adoption of emerging and innovative technologies boosts the development of the infrastructures using information, communication, and technology (ICT) platform. This shift accelerated its evolution toward digitization where interdependent and interconnected cyberspace demands collaborative and holistic strategies in protecting critical and high risks infrastructure assets from a growing number of disruptive cyberattacks. These ever-evolving cyber threats are creating increasingly dangerous and targeted cyberattacks to damage or disrupt the critical infrastructures delivering vital services to government, energy, healthcare, transportation, telecommunication, and other critical sectors. The infrastructure's high risks assets present serious challenges and are crucial to safety, efficiency, and reliability. Any nation must recognize and determine how to cope with any type of threats to their critical infrastructure as well as the strategies to remain resilient. This article first describes the challenges and the need for critical infrastructure protection including the related global risks challenges. It then reviews the United Nations, the European Union, and the United States' strategies, priorities, and urgencies of critical infrastructure protection. Subsequently, it surveys the critical infrastructure protection resilience strategies including ISO, IEC, ISA, NIST, CAF and CMM frameworks.

Keywords

Critical Infrastructure Protection, Critical Information Infrastructure Protection, Cybersecurity, Operational Technologies, Risk Management

1. Introduction

Understanding the challenge

Recognizing that the national and economic protection of any nation depends on the reliable functioning of critical infrastructures (CIs), nevertheless, the CIs are arguably now more at risk than ever. The highly digitized and connected of today's critical infrastructures such as healthcare, government, and other critical sectors have placed them firmly in the sights of domestic and nation-state threats. Historically, the goal of cybersecurity experts is to protect from cyber threats by providing confidentiality, integrity and availability of created, processed, stored, and transmitted IT assets. These cyber threats include internal, external actors and persistent attacks that are often sophisticated, systematic, regimented, and well-funded. In addition, with the responsibility of protecting IT infrastructure assets, cybersecurity experts need to consider the real threats that jeopardize the safety of critical infrastructure operators and their operational technologies (OT). However, addressing the security of OT vulnerabilities and the poorly protected operational system, control system, and connected devices has fallen behind IT infrastructure protection. According to [1] OT is a highly complex industrial control (IC) system such as Supervisory Control and Data Acquisition (SCADA) that manages the programmable systems or a piece of equipment interacting with the physical environment. The IC system or a piece of equipment monitors and controls devices, processes, and events such as power, water, transport, manufacturing, and other essential services. Traditionally, IT assets are considered as the sensitive resources for IT systems, technologies, and business continuity therefore addressing the system vulnerabilities and respond to attacks that are essential. Consequently, these assets' main concern is to provide confidentiality of sensitive information within IT systems by preventing any unauthorized access. In comparison, OT assets are considered as the power systems, known as cyber operational and physical systems; thus they have different security requirements and constraints in terms of applying security measures as well as providing availability, authentication, authorization, integrity, and safety levels. Additionally, any disruptive incidents on OT assets can harm the safety and reliability of power systems and cause catastrophic repercussions. The repercussion with the greatest consequence of safety as the intentional or accidental mis-operation of OT assets could cause harm or even death. At the same time, the repercussion of reliability is important as it will affect the power system such as generators, breakers, transformers, power, and gas lines [2]. **Figure 1** illustrates the different priorities and security requirements of critical infrastructures

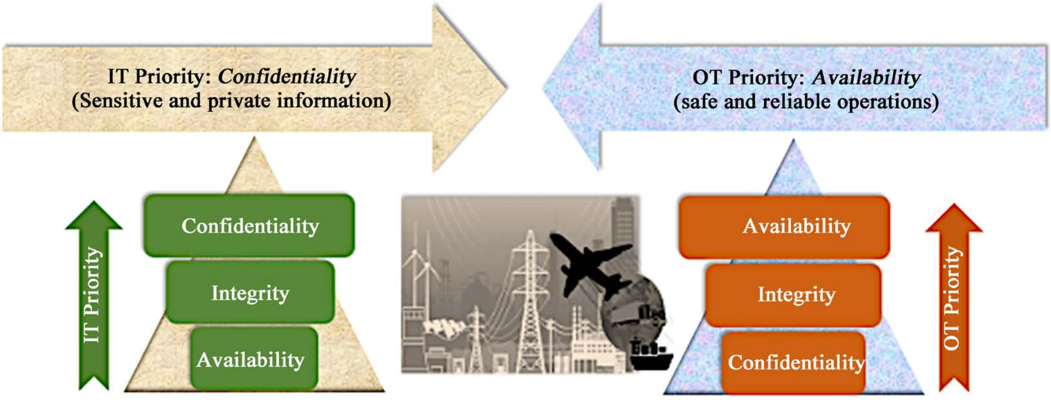
IT Priority: *Confidentiality*
(Sensitive and private information)
OT Priority: *Availability*
(safe and reliable operations)
IT Priority
Confidentiality
Integrity
Availability
Availability
Integrity
Confidentiality
OT Priority

Figure 1. Scope of IT and OT security priorities.

IT and OT systems.

The need for Critical Information Infrastructures Protection

The urgent need for Critical Infrastructures Protection (CIP) to strengthen the critical infrastructure operators and their operational technologies is today's goal to ensure sufficient trustworthiness of systems, products, and services and provide the necessary resilience to support the economy and security interests. Nations should recognize the importance of protecting critical infrastructures against natural disasters, terrorist activities, and now cyber threats. The CIP helps all critical infrastructure sectors to the highest standard and prepares them for disaster preparedness, response, and recovery. According to the Whitehouse fact sheet[1], the United States of America is recognized as the wealthiest country in the world, yet when it comes to the overall quality of infrastructure protection, it ranks 13th globally. In general, nations defined their critical Infrastructure sectors, however, the main four designated lifeline sectors are transportation, water, energy, and communication. Any disruption or loss of one of these sectors will directly affect the security and resilience of numerous sectors and cause harm and catastrophic consequences. While for decades governments and industries prioritized the protection of CI against physical attacks such as sabotage, it is recognized the rapid increase of cyberattacks by increasing the dependency on ICT infrastructures creating more security issues. The main factor in the nation's CI protection is not only physical disruption or destruction. It is also the accurate operation of CI using ICT-based services. It is important to recognize Critical Information Infrastructures (CII) as a vital component of CI in securing and protecting the availability of critical assets. The CII comprises the critical information and ICT process control systems such as increasing connectivity, remote monitoring, scalability, reliability. The compromised or disturbed CII nevertheless can be initiated by man-made, technical failures, vulnerabilities, and disasters that can jeopardize national security, economic growth, and stability of daily life. Therefore, the need for effective Critical Information Infrastructures Protection (CIIP) strategies, policies, and priorities are significantly essen-

[1] https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/31/fact-sheet-the-american-jobs-plan/.

tial for most nations. CIIP is considered a subset of CIP, however, governments and industries need to realize that CIP is considered a national security issue whereas CIIP is a global issue. Consequently, private-public sectors require to develop strong partnerships in information sharing and exchange capabilities. As shown in Figure 2, CII is a set of interconnected ICT infrastructures which are crucial for the safeguarding of vital CI functions such as health, safety, and economy. Any disruption or destruction of ICT functions will result in serious consequences and may cause a major impact on a nation [3].

In regards to the importance of cybersecurity strategies, nations should adopt CIP and CIIP risk assessment as vital elements of cybersecurity. Figure 3 illustrates the perspective between elements and concepts of CIP, CIIP, and Cybersecurity strategies.

Critical Infrastructure Threats and Risks

The Global risks report 2021 [4] recognized cyberattacks among the top five risks along with extreme weather, climate action failure, natural disasters, and infectious diseases risks. The cyberattack risk can cause significant harmful impacts and adverse consequences on technological advances, critical infrastructures, and

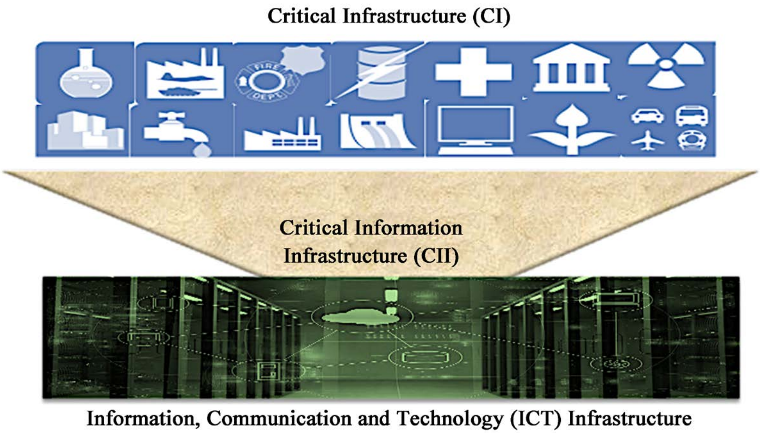
Critical Infrastructure (CI)
Critical Information Infrastructure (CII)
Information, Communication and Technology (ICT) Infrastructure

Figure 2. Interconnection of CI, CII and ICT infrastructures.

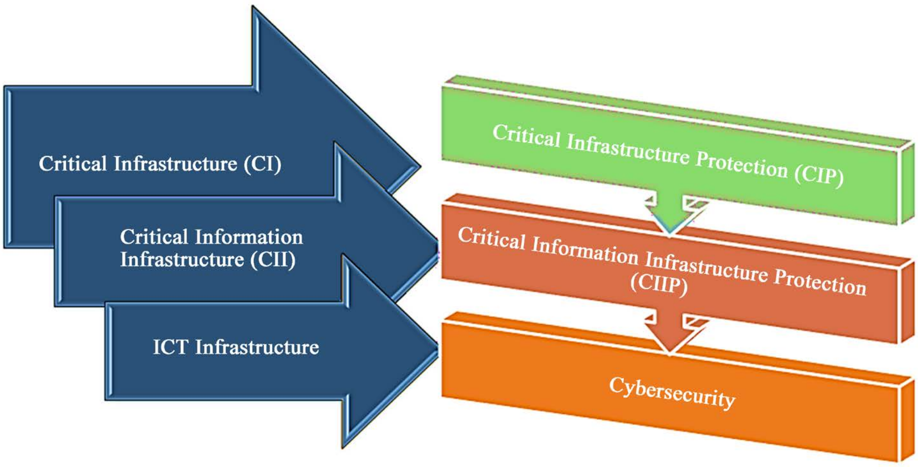
Critical Infrastructure (CI)
Critical Information Infrastructure (CII)
ICT Infrastructure
Critical Infrastructure Protection (CIP)
Critical Information Infrastructure Protection (CIIP)
Cybersecurity

Figure 3. Perspective of CIP, CIIP and Cybersecurity.

massive exploitation of data on an unprecedented scale. In addition, the Global risks report shows that in the last five years the cyberattacks were among the top five risks which consequently expose the critical infrastructures and their operational technologies subject to risks associated with physical and virtual threats such as natural disasters or risks in cyberspace respectively. Figure 4 illustrates the ranking of global risk in 2021 in terms of likelihood and impact on economic, environmental, geopolitical, societal, and technological risk factors.

This report shows the advancement of integration and interaction between physical and ICT in critical infrastructures shaped physical infrastructures more reliant using complex operational ICT systems. Consequently, this shift influenced the adversaries' focuses on exploiting potential cyber vulnerabilities. Due to the nature of interdependencies of the critical infrastructure sectors any damage, disruption, or destruction to one infrastructure sector or subsector can cause cascading effects, create a significant impact on other sectors' operations.

Significant critical infrastructures cyber incidents timeline

In 2021 [5], identified significant cyber-attacks on critical infrastructure sectors globally since 2006. Figure 5 shows the substantial cyber incidents between 2006 to March 2021. The cyber incident dataset are focuses globally on government agencies, defense and critical infrastructures (note that the 2021 data is YTD March).

[6] collected significant incidents worldwide using publicly available information against the different domains of critical infrastructures from January 1, 2009, to November 15, 2019. The dataset contains 130 incidents that were carried out against critical infrastructure sectors. Figure 6 shows the major incidents in different critical infrastructure sectors recorded between 2009 to 2019.

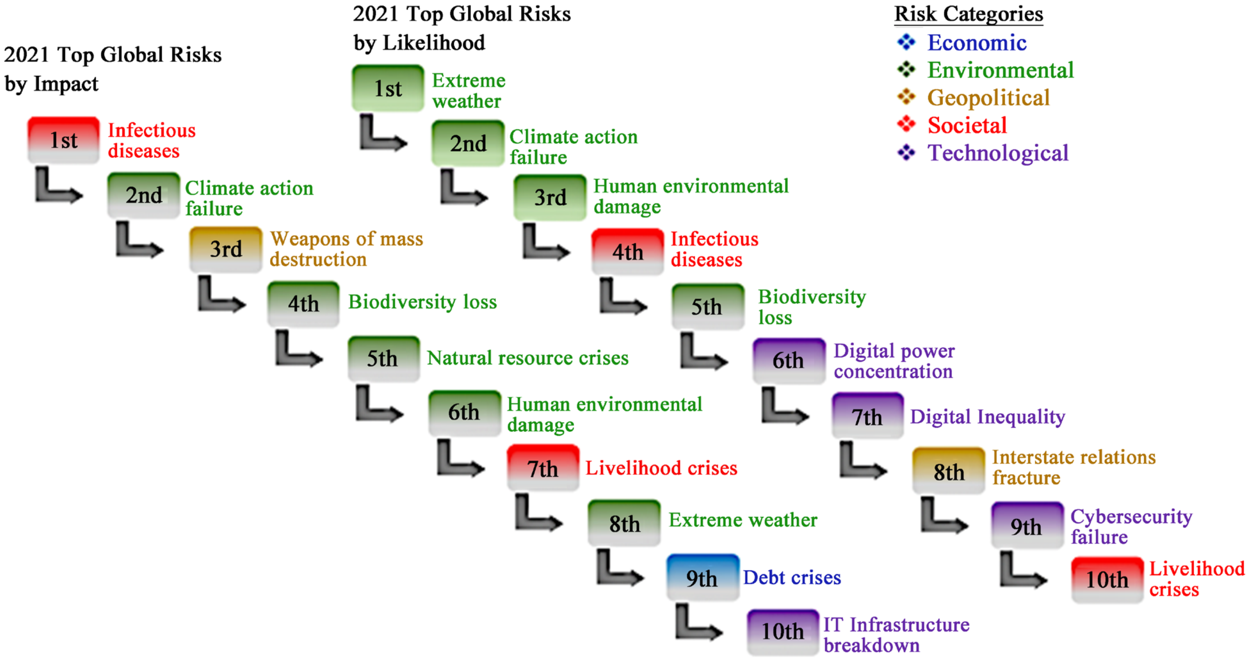
2021 Top Global Risks by Impact
1st Infectious diseases
2nd Climate action failure
3rd Weapons of mass destruction
4th Biodiversity loss
5th Natural resource crises
6th Human environmental damage
7th Livelihood crises
8th Extreme weather
9th Debt crises
10th IT Infrastructure breakdown
2021 Top Global Risks by Likelihood
1st Extreme weather
2nd Climate action failure
3rd Human environmental damage
4th Infectious diseases
5th Biodiversity loss
6th Digital power concentration
7th Digital Inequality
8th Interstate relations fracture
9th Cybersecurity failure
10th Livelihood crises
Risk Categories
Economic
Environmental
Geopolitical
Societal
Technological

Figure 4. Ranking of global risk in 2021.

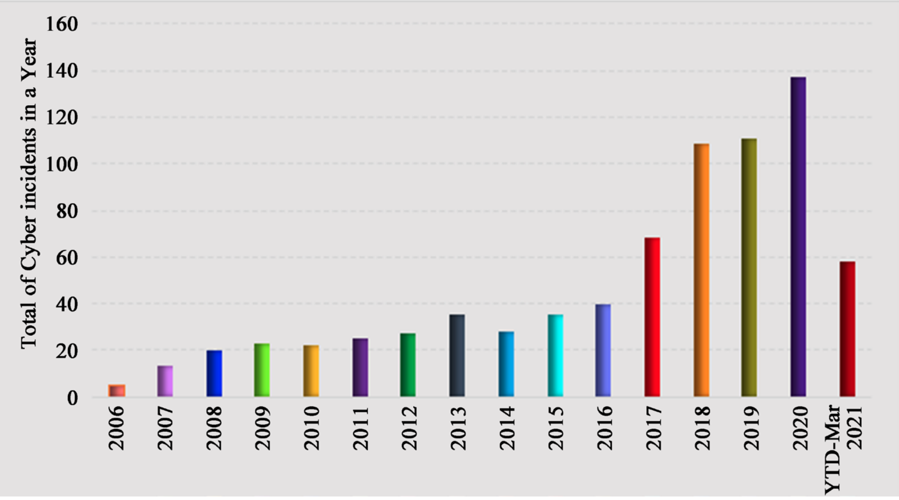

Figure 5. Recorded cyber incidents between 2006 to March 2021.

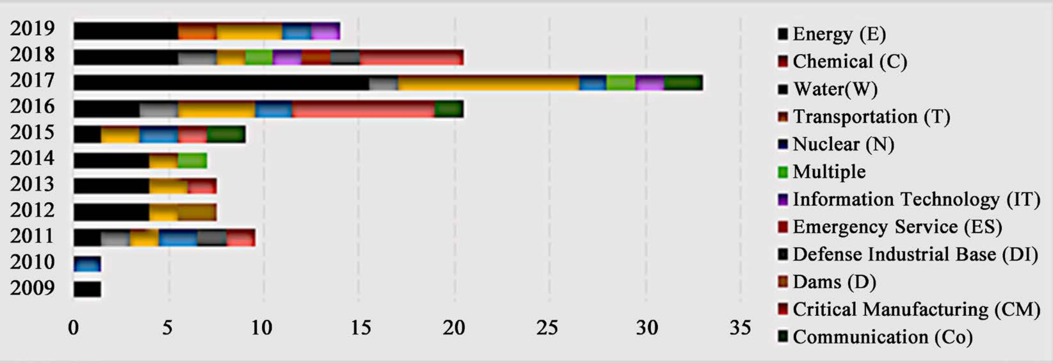

Figure 6. Incidents in critical infrastructure sectors between 2009 to 2019.

Based on the above graph, it is observed that the collected data on disruption of the critical infrastructure sectors are Energy and Transportation sectors. These sectors have significantly the highest spike followed by critical manufacturing and nuclear sectors, respectively. This observation emphasized that the spike is due to recent ransom ware attacks such as WannaCry and wiper malware such as NotPetya in 2017. The key factors of datasets are disruptive cyber-physical incidents as well as cyber-operational incidents. The disruptive cyber-physical incident initiated by the malicious activities executed with state or nonstate threat actors and had disruptive effects in the operational technology (OT) systems, devices, and processes compromising Industrial Control (IC) systems. The other key factor is disruptive cyber-operational incidents where a threat actor performs the malicious activities that disrupt IT systems attached to the ICS or Internet of things (IoT) systems and devices for managing inspection on intelligence preparation of the battlefield (IPB) or stealing intellectual property (IP) for economic commitments. Figure 7 shows the disruptive incidents cases by cyber-physical incidents, cyber-operational incidents, or unknown factors from January 1, 2009, to November 15, 2019.

The dataset collected by different threat agents that targeted critical infrastructure

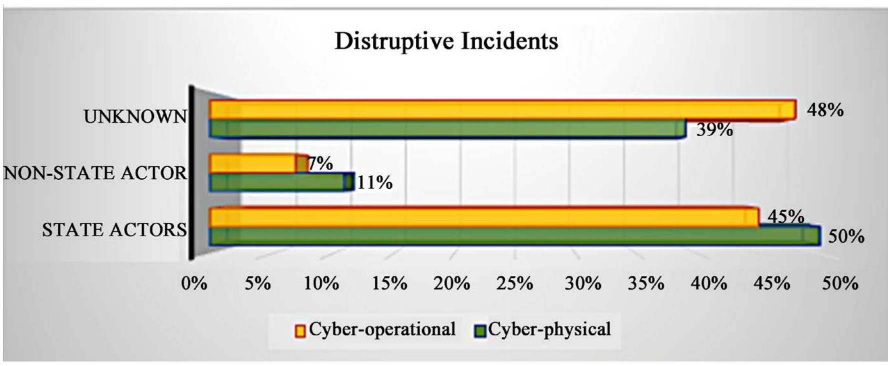

Figure 7. Disruptive incidents cases.

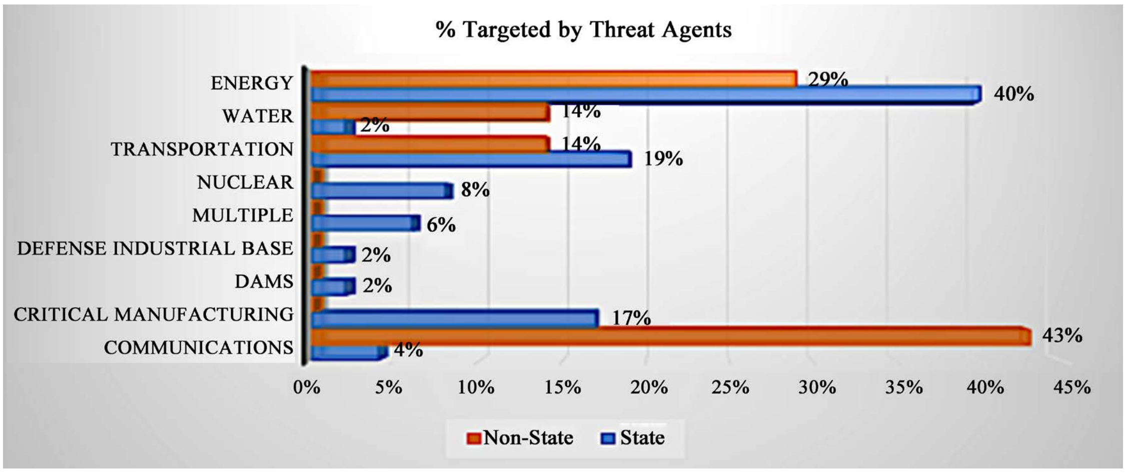

Figure 8. Sectors targeted by Threat agents.

sectors, shown in Figure 8, suggested that the sectors targeted by the state agents are higher than non-state agents due to the fact the non-state incidents in the cyber domain frequently remaining anonymous.

2. Critical Infrastructure Protection (CIP)

The United State CIP

The United State relies on reliable critical infrastructures as a lifeline to their daily lives such as clean water, power, transportation, and communications. The Patriot Act of 2001 [7] redefined the critical infrastructures as a set of assets, systems, operational technologies, and other vital elements in the physical and cyber environments. As the United State critical infrastructure protection became a top priority for the nation, in 2013 the Executive Order 13,636 [8] was initiated for the development of improving critical Infrastructure's cybersecurity. It directs a policy of the United States "*to enhance the security and resilience of the Nation's critical infrastructures and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.*" [8]. In the U.S, both critical physical and cyber infrastructures are owned and operated by the private sector, federal, state, or regional governments. Following the Executive Order 13,636, in 2014 the Cybersecurity Enhancement Act 2014 (CEA) [9] was authorized through the National Institute of Standards and Technology (NIST) to facilitate and develop a framework for reducing risk to critical infrastructures by 1) Collaboration of public-private on cybersecurity; 2) Cybersecurity Research and Development; 3) Education and Workforce Development; 4) Cybersecurity Awareness and Preparedness; 5) Advancement of Cybersecurity Technical Standards. The framework is to identify "*a prioritized, flexible, repeatable, performance based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructures to help them identify, assess, and manage cyber risks.*" Furthermore, in 2015, Executive Order 13,691 [10] was issued to encourage and promote cybersecurity information sharing and to engage the private sectors in sharing information related to cybersecurity risks and disruptive incidents. In the U.S., Critical infrastructure is emphasized on four designated vital components 1) Communication, 2) Energy, 3) Water, and 4) Transportation. Numerous sectors rely on these four vital components. The Cybersecurity and Infrastructure Security Agency (CISA) identified a total of sixteen critical infrastructure sectors[2] and their Sector-Specify Agencies as defined in Presidential Policy Directive-21 [11] and the 2013 National Infrastructure Protection Plan[3], shown in **Table 1**.

Table 1. CISA critical infrastructure sectors and their sector-specify agencies.

Sector-Specify Agency	Critical infrastructure sectors
Department of Homeland Security (DHS)	Chemical Sector Communications Sector Dam Sector Emergency Services Sector Government Facilities Sector Information Technology Sector Transportation system Sector Commercial facilities Sector Critical Manufacturing Sector Nuclear Reactors, Materials & Waste Sector
Department of Treasury	Financial Services Sector
General Services Administration (GSA)	Government Facilities Sector
Department of Transportation (DOT)	Transportation system Sector
Department of Defense (DOD)	Defense Industrial Base Sector
Department of Energy (DOE)	Energy Sector
Department of Agriculture (USDA)	Food & Agriculture Sector
Department of Health & Human Services (HHS)	Food & Agriculture Sector
Environmental Protection Agency (EFA)	Water & Wastewater systems sector

[2] https://www.cisa.gov/critical-infrastructure-sectors.

[3] https://www.cisa.gov/national-infrastructure-protection-plan.

The sixteen CI sectors are interdependent and reliant on each other to provide reliable operations thus any disruption or loss of one of the critical sectors will directly affect the security and resilience of critical infrastructures operators and their operational technologies of other sectors. It is important to identify and understand the interdependencies between the sectors to evaluate the potential risks and vulnerabilities. Figure 9 illustrates the interdependencies of the U.S. critical infrastructure sectors.

The vast majority of the US critical infrastructure sectors owns and operates by the private sectors. The core commitments of private sector partnerships with the public sectors are essential to foster security and resilience through integrated, collaborative engagement and interaction. The partnerships play a central role in implementing an information sharing and awareness program to disseminate efficiently and effectively the critical threat information, risk mitigation, and other sensitive information from state, local, tribal and territorial governments and international partners. The Department of Homeland Security (DHS) and Cybersecurity and Infrastructures Security Agency (CISA) manage with public and private sector critical infrastructures partners engagement to boost the security and resilience of the US's critical infrastructures. The partnership between the public and private critical infrastructure sectors[4] is shown in Table 2.

In addition to partnership, facilitating information sharing and awareness programs[5] can be used voluntary and regulatory to provide security and resilience for critical infrastructures. They are a vital key to build a knowledge system to share and maintain crucial threat information, risk mitigation and other sensitive information and assets as shown in Table 3.

Furthermore, a set of guidelines has been provided to form a framework for private and public critical infrastructure sectors for sharing the threat information. This framework aims to facilitate information sharing platforms and accelerate the flow of threat information sharing with private and public critical infrastructures sectors. The vital resources for critical infrastructures security and

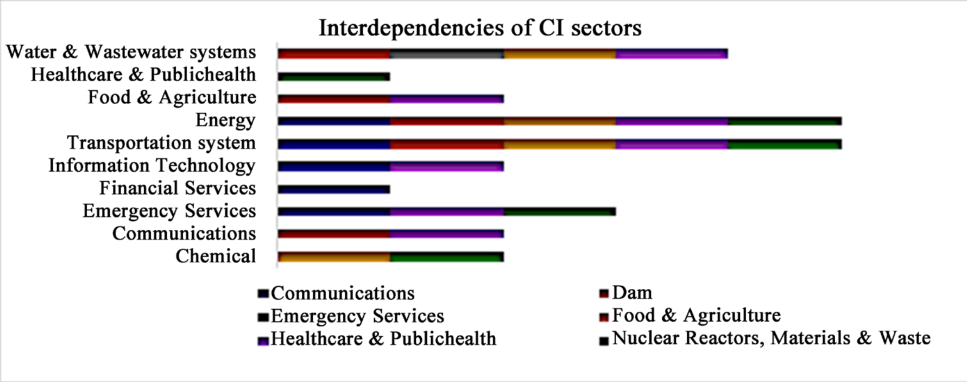

Figure 9. Interdependencies of the U.S. critical infrastructure sectors.

[4] https://www.cisa.gov/critical-infrastructure-sector-partnerships.

[5] https://www.cisa.gov/information-sharing-and-awareness.

Table 2. Partnership between the public-private critical infrastructures sectors.

Coordination	Description
National Infrastructures Protection Plan (NIPP) 2013: Partnering for Critical Infrastructures Security and Resilience	Provides an organized partnership approach between the public and the private sector for safeguard, security, and resilience of critical infrastructures
Critical Infrastructures Partnership Advisory Council (CIPAC)	Provides the operational framework for implementing NIPP partnership structure for jointly engagement in the public and private sector entities to coordinate councils in support of critical infrastructures security and resilience efforts.
Critical Infrastructures Cross-Sector Council	Provides a forum for CIPAC's Sector Coordinating Councils (SCCs) to address cross-sector issues and interdependencies.
Federal Senior Leadership Council (FSLC)	Composed of senior officials from the designated sector-specific agencies and other federal departments and agencies to facilitate enhanced federal communication and coordination across the sectors focused on critical infrastructures security and resilience.
State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC)	Provide a forum for active participants to assure that state, local, tribal, and territorial (SLTT) homeland security partners fully engaged in resilience efforts
Regional Consortium Coordinating Council (RC3)	Provides a framework to support and promote resilience activities existing regional groups in the public and private sectors.

Table 3. Information sharing and awareness programs.

Information sharing and awareness programs	Description
Traffic Light Protocol (TLP)	Set of descriptions to ensure greater sharing of information for directing the availability of sensitive information that can be shared to provide an efficient and regular partnership with the appropriate audience
Cyber Information Sharing and Collaboration Program (CISCP)	Enables information exchange and the establishment of a community to share public information exchange through reliable public-private partnerships across all critical infrastructures (CI) sectors
Information Sharing and Analysis Centers (ISACs)	Collect, analyze and disseminate actionable threat information and provide tools to mitigate risks and enhance resiliency to public-private partnerships across all critical infrastructures (CI) sectors
Information Sharing and Analysis organization (ISAOs)	Similar to ISACs, it gathers, analyzes, and disseminates cyber threat information, but unlike ISACs, ISAOs are not sector-affiliated
Automated Indicator Sharing (AIS)	Enables the cyber threat indicators and defensive measures to provide assistant in protecting public-private participants
Protected Critical Infrastructures Information (PCII)	Enables voluntary information sharing between public-private partnerships across all critical infrastructures (CI) sectors
Homeland Security Information Network (HSIN)	Share sensitive and unclassified information to public-private partnerships across all critical infrastructures (CI) sectors for operations management, evaluate data, send warnings and notifications as well as share the information they need to perform their duties
National Cyber Awareness System (NCAS)	Develop specific awareness with technical and non-technical audiences by implementing appropriate information including technical warnings, control systems advisories and reports, weekly vulnerability bulletins, and tips on cyber hygiene best practices.
National Information Exchange Model (NIEM)	Enables efficient risk-informed data exchange across public-private participants

resilience[6] are shown in Table 4.

The United Nation Security Council (UNSC) CIP resolutions

The complexity of critical infrastructure protection becomes a complicated process to encompass the entire progression of potential cyberattacks. The

[6] https://www.cisa.gov/information-sharing-vital-resource.

Table 4. Critical Infrastructures security and resilience resources.

Resources	Description
Cybersecurity and Infrastructures Security Agency's Infrastructures Security division	Enable decision-making and information sharing to execute security and resilience activities
Information sharing tools	Support information sharing within and among the critical infrastructures sectors: Homeland Security Information Network - Critical Infrastructures (HSIN-CI) Infrastructures Protection Gateway (IP Gateway) National Infrastructures Coordinating Center (NICC) National Risk Management Center (NRMC) Protected Critical Infrastructures Information (PCII) Program Protective Security Advisors (PSAs) TRIP wire (Technical Resource for Incident Prevention)
Critical Infrastructures Threat Information Sharing Framework	Provides vital information and best practices for threat information-sharing entities
Critical Infrastructures Information Sharing Environment	An individual framework that implements the tools required to provide security partners to distribute vital information in their infrastructure's security and risk, respond to events, and enhance resilience management

United Nations has recognized the urgency of critical infrastructure protection that requires a partnership, cooperation, and obligation nationally and internationally as well as an immediate response plan to prevent the cascading effects of high-impact terrorist attacks. United Nations Security Council (UNSC) is one of the six organs of the United Nations (UN). UNSC is the premier global body with the principal goal and obligations of assessing, maintaining, and addressing international peace and security. UNSC issues resolutions to form a formal appeal for resolving security challenges and urgencies. The UNSC adopted resolution 1373 [12] in 2001 to establish an obligation on all UN member states a common core of a new campaign identifying good practices, early warning, and vulnerabilities as well as recognizing possible prevention measurement in strengthening national, international security strategies and policies. Following resolution 1373 (2001), in 2004 the UNSC adopted resolution 1566 [13] to strengthen effective measures and immediate response against terrorist activities that imposed on physical critical infrastructures producing cascading effects upon civilians. In 2005, The UN Secretary General established the global Counter-Terrorism Implementation Task Force (CTITF)[7], and subsequently in 2006, by consensus, it was endorsed by the General Assembly through the United Nations Global Counter-Terrorism Strategy. The mandate of the CTITF aims to coordinate, provide and maximize efforts by UN counter-terrorism four pillars strategy as shown in Table 5. Importantly, under pillars II member states committed to increase efforts to improve the security and protection of critical assets particularly the critical infrastructures as well as recognizing the support required by the states.

The UN council Counter-terrorism Committee (CTC) directed by security Council resolutions 1373 (2001) and 1624 (2005) [14] is to coordinate a common UN approach in implementing and preventing terrorist acts. The CTC is

[7] https://www.un.org/victimsofterrorism/en/about/ctitf.

supported by the Counter-Terrorism Committee Executive Directorate (CTED) to execute the committee's evaluations on the member state counter-terrorism technical assistance. The UNSC resolutions facilitate the assessment of the effectiveness of member state's policies to protect critical infrastructures including identifying good practices, deficiencies, and vulnerabilities as well as developing and sharing information analysis of counter-terrorism trends. Subsequently, UNSC resolution 2341 in 2017 [15] adopted the primary resolution on the protection of the critical infrastructures against emerging and rapidly evolving threats posed by cyberattacks and strengthening of States' capabilities of critical infrastructures. Resolution 2341 (2017) aims with the support of CTED to endorse a necessary step concerning the global awareness and preparedness to cyberattacks on critical infrastructures. The five key elements of the UNSC resolution 2341 (2017), shown in **Figure 10**, are recognized as 1) the *awareness* emphasizes the strengthening and reinforcing knowledge as well as recognizing the vulnerability and threats on critical infrastructures, 2) the *capabilities* evaluate the strength of states' capacities, the partnerships of private and public sectors to mitigate the risk of cyberattacks to a controllable level, 3) the *resilience* promotes methods of preparation, prevention, crisis management, and recovery to reduce cyberattacks intended to destroy or disable critical infrastructures, 4) the *distribution*

Table 5. UN counter-terrorism four pillars strategy[8].

Strategy	Description
Pillars I	"*Measures to address the conditions conducive to the spread of terrorism*"
Pillars II	"*Measures to prevent and combat terrorism*"
Pillars III	"*Measures to build states' capacity to prevent and combat terrorism and to strengthen the role of the United Nations system in that regard*"
Pillars IV	"*Measures to ensure respect for human rights for all and the rule of law as the fundamental basis for the Fig.ht against terrorism*"

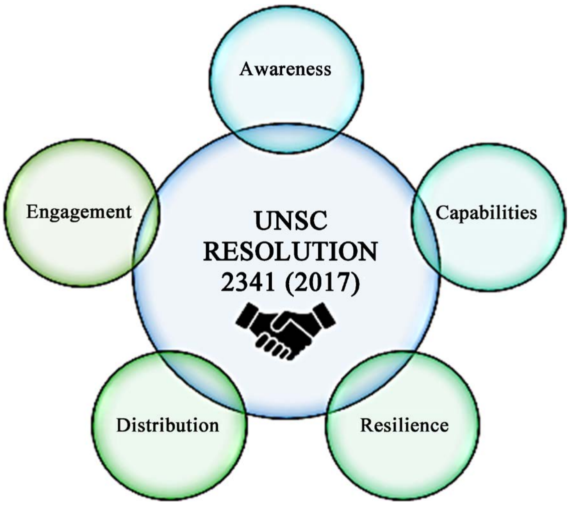

Figure 10. Key elements of the UNSC resolution 2341 (2017).

[8] https://www.un.org/counterterrorism/un-global-counter-terrorism-strategy.

intensifies an open exchange of operational information between a range of stakeholders such as governmental authorities, law enforcement, foreign partners and private sector owners and operators, 5) the *engagement* enhances the international and regional sectors to support regional connectivity projects and related cross-border infrastructures.

UNSC recognized three sectors of critical infrastructure: 1) Energy, 2) Transportation and 3) Water Supply, as well as the vulnerability of critical infrastructures to attacks committed by terrorists in cyberspace. UNSC resolution 2341 (2017) emphasized that terrorist attacks as a distinctive threat to critical infrastructures and urged all states to establish concrete and coordinated efforts in raising awareness and expanding knowledge and understanding to improve preparedness through international cooperation. It is also recognized that threats against critical infrastructures have multiple dimensions. While soft targets consider as sites or regions that are relatively vulnerable to terrorist attacks due to their unrestricted access with limited security, hard targets are intended to make it harder for a terrorist to strike. The classification of such threats caused by these targets depends on their nature, their origin, and the context in which they occur. Table 6 shows the specific threat classifications to critical infrastructures.

The European Union (EU) CIP

The European Council Directive 2008/114/EC was adopted in 2008 as a vital part of the European Program for Critical Infrastructure Protection (EPCIP). The Directive's purpose is to establish a framework for the identification and designation of critical infrastructure in the EU. The directive defines the European critical infrastructure (ECI) as [16] "an asset, system or part thereof located in the Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions." The scope of the EPCIP framework is to focus on the assessment and resilience of ECI as well as the need to improve the protection. The directive divides the framework into

Table 6. Threat classifications to critical infrastructures.

Threat Classification		
Nature	Physical	Destroy, weakening, and intervening in physical structure, mechanical, components, etc.
	Cyber	Manipulate, shut down or limit access to a crucial system, information, or data
Origin	Insider	Actors who linked to the organization, often as employees or suppliers with the ability to gain full or acquire knowledge
	External	Actors who can only gain access utilizing violent acts or espionage
Context	Isolated	Action launched to the same sector, operator, or geographical location
	Multiple targets	Action launched in a manner of campaigns or serial attacks

three ECI process stages as shown in Table 7.

The directive scope recognizes two CI sectors, 1) Energy and 2) Transport (excluding nuclear energy) as illustrated in Figure 11.

3. Cybersecurity Assessment Strategies

NIST Framework for improving critical Infrastructure's cybersecurity

The United State national and economic depends on reliable and functional critical infrastructures. It is recognized that the protection and security of critical

Table 7. ECI process under Directive 2008/114/EC.

ECI process	Stages
Identification	Apply sectoral criteria for critical infrastructures Apply the definition of critical infrastructure, according to Article 2(a) of the directive Apply transboundary element according to Article 2(b) Apply cross-cutting criteria to identify potential ECIs
Designation	Inform other Member States affected by a potential ECI Critical Infrastructure Warning Information Network (CIWIN) Engage in bilateral/multilateral dialogue with the Member States affected Agree with the Member States affected on ECI Inform European Commission and ECI owner/operator
Protection	Apply operator security plan (OSP) procedure in accordance with Article 5 and Annex II, and review OSP regularly Designate security liaison officer (Article 6) Report to Commission every 2 years on types of risks, threats and vulnerabilities encountered per ECI sector Classify reports at an appropriate level

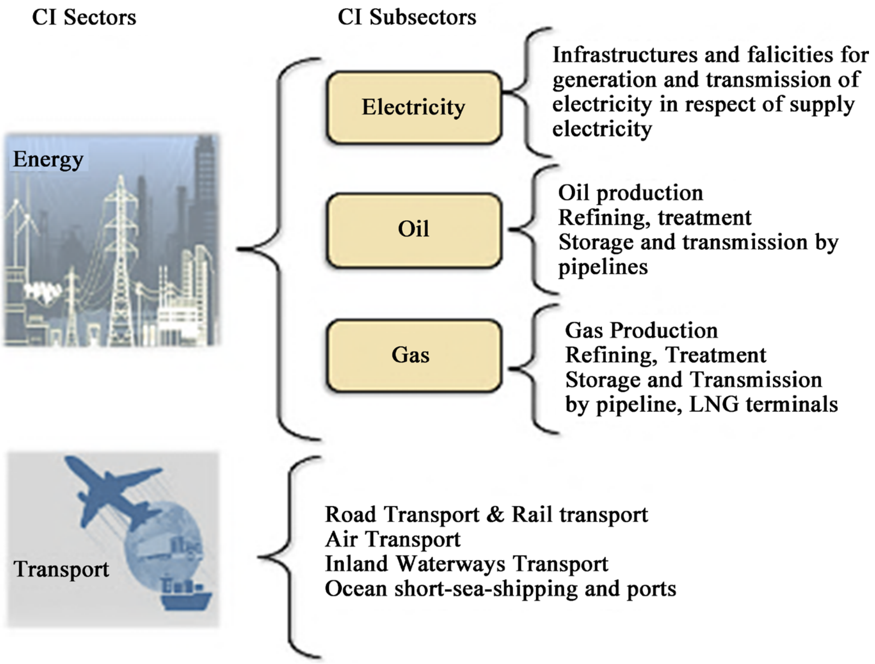
CI Sectors
CI Subsectors
Energy
Electricity
Infrastructures and falicities for generation and transmission of electricity in respect of supply electricity
Oil
Oil production
Refining, treatment
Storage and transmission by pipelines
Gas
Gas Production
Refining, Treatment
Storage and Transmission by pipeline, LNG terminals
Transport
Road Transport & Rail transport
Air Transport
Inland Waterways Transport
Ocean short-sea-shipping and ports

Figure 11. Critical infrastructure sectors covered by Directive 2008/114/EC.

infrastructures became a top priority. In response, NIST [17] released the Cybersecurity Framework in strengthening the resilience of critical Infrastructures by engaging organizations to consider cybersecurity risks as part of their risk assessment and management practices. The NIST Cybersecurity Framework (NIST CSF) was first released in 2014 under executive order 13,636 and updated in 2018. Consequently, the executive order in 2017, required compliance for federal government agencies and entities in their supply chain. The NIST CSF aimed to launch harmonized approach and a common set of practices, standards, goals, and guidelines for managing cybersecurity-related risk. The framework promotes flexible, cost-effective, and prioritized approaches for the protection and resilience of critical infrastructure sectors vital to the US economy and national security. NIST CSF is a voluntary framework that any organization of any size can apply to deliver services and products linked to the nation's critical infrastructures and the entities in their supply chain. While NIST CSF was responsible for creating a framework to reduce risks in critical infrastructures, the Department of Homeland Security (DHS) launched public and private partnerships to align critical infrastructure owners and operators with existing resources regardless of size or cybersecurity complexity. The Framework's risk-based and flexible approach is to address cybersecurity complexity attributes including the effect on physical, cyber, and society. The Framework can be implemented in any organization that directly or indirectly relies on the technology including information technology (IT), operational technologies (OT), cyber-physical systems (CPS), or connected devices. Three main components formed the framework: a) Framework core, b) Implementation tiers and c) Framework profiles. The components aim to strengthen the partnership across critical infrastructure sectors in recognizing, prioritizing, and reducing cybersecurity risks including cybersecurity achievable outcomes and their relevant recommendations.

1) Framework Core

The Framework Core consists of a set of industry standards, guidelines, and organizational best practices to manage cybersecurity risk that is recognized and identified by stakeholders. The Framework Core has four key elements: 1) *Functions* form necessary attributes to assist organizations in managing cybersecurity risks, 2) *Categories* are a subset of a Function that group the cybersecurity issues such as detection methods, asset management, and controls 3) *Subcategories* are a subset of a Category that assists in achieving the outcomes of each Category such as the investigation of notification from detection systems 4) *Information References* represent as a section of standards, guidelines, and practices that is frequently used in critical infrastructure sectors. The functions are *Identify*, *Protect*, *Detect*, *Respond*, and *Recover* as shown in **Table 8**.

The functions are facilitating risk management evaluations, addressing threats, and improving the incident post-analysis. **Figure 12** demonstrates the Framework Core structure.

Table 8. Framework core functions.

Functions	Description
Identify	Promote an organizational knowledge in managing cybersecurity risks “system, people, assets, data, and capabilities”
Protect	Ensure that applicable security control in the safeguarding of availability of critical services
Detect	Utilize and execute applicable actions to discover the occurrence of a cybersecurity event
Respond	Apply and achieve detection responses to a cybersecurity incident
Recover	Perform and execute applicable actions to recover any damaged services promptly caused by a cybersecurity incident

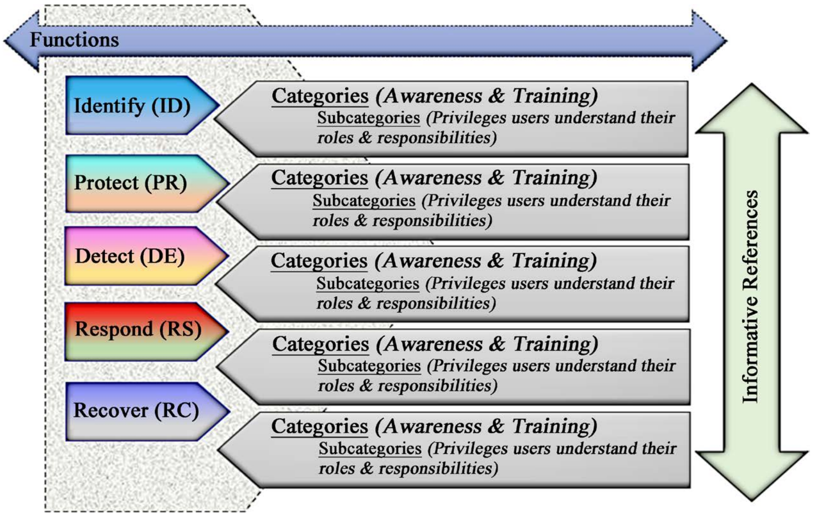
Functions
Identify (ID)
Protect (PR)
Detect (DE)
Respond (RS)
Recover (RC)
Categories (Awareness & Training)
Subcategories (Privileges users understand their roles & responsibilities)
Categories (Awareness & Training)
Subcategories (Privileges users understand their roles & responsibilities)
Categories (Awareness & Training)
Subcategories (Privileges users understand their roles & responsibilities)
Categories (Awareness & Training)
Subcategories (Privileges users understand their roles & responsibilities)
Categories (Awareness & Training)
Subcategories (Privileges users understand their roles & responsibilities)
Informative References

Figure 12. Framework core structure.

2) Implementation Tiers

The Implementation Tiers provide the degree of implementing cybersecurity risk controls. As Table 9 shows, four tiers measure the degree of organizational decision making on consistency and difficulty in cybersecurity risk management practices as well as identifying responses for the prioritized organization assets that could have potential risk.

3) Framework Profiles

The Framework Profile, known as *Profile* is the association of the functions, categories, and subcategories that measures the security requirement, quantitative and qualitative risks estimated values as well as risk sensitivity, acceptance, and resources to achieve the desired outcomes in the Framework Core.

ISO/IEC 27000 Series of Standards

The International Standard Organization (ISO) is an independent, non-governmental international organization that closely works with the International Electrotechnical Commission (IEC), the International Telecommunication Union (ITU), and World Trade Organization (WTO) as well as liaison with United Nations (UN) and its partners. The ISO/IEC Joint Technical Committee (JTC1) developed the ISO/IEC 27,000 family of Standards for information technology

Table 9. Implementation tiers and description.

Tiers	Implementation Methods	Description
Tier 1: Partial	*Risk Management Process*	Informal practices
	Integrated Risk Management Program	Limited awareness of cybersecurity risk
	External Participation	Sparse cybersecurity coordination
Tier 2: Risk Informed	*Risk Management Process*	Management approves the risk management practices
	Integrated Risk Management Program	High-level awareness of cybersecurity risk
	External Participation	Shared cybersecurity coordination
Tier 3: Repeatable	*Risk Management Process*	Formal policies practices
	Integrated Risk Management Program	Organizational wide awareness of cybersecurity risk
	External Participation	Implemented processes, and regular formal coordination.
Tier 4: Adaptive	*Risk Management Process*	Adaptive policies practices
	Integrated Risk Management Program	Implemented processes, and regular formal coordination as part of the organization culture
	External Participation	Promotes active cybersecurity coordination

(IT) systems to help and support the best practices for improving organizations' information security. The ISO/IEC 27000 series of standards were published by ISO and IEC to provide a systematic approach of Information Security Management System (ISMS) for risk management for all organization sizes and sectors. The series consists of inter-related standards that ready for adoption by organizations to develop and implement a framework for managing the security of critical infrastructure assets. Table 10 explains the ISO/IEC 27000 series standards [18].

As shown in table [10], for effective critical infrastructures cybersecurity risk management, ISO/IEC 27001 and ISO/IEC 27010 parts of ISO/IEC 27000 series are used. While ISO/IEC 27001 is designed to protect the confidentiality, integrity, and availability of their information assets, ISO/IEC 27010 provides controls and guidance for implementing information exchanging and sharing of sensitive information as well as provisioning, maintaining, and protecting organizations or state's critical infrastructures.

ISO/IEC 27001

The first and second versions of ISO 27001 were released in 2005 (ISO/IEC 27001:2005), 2013, respectively and it was reviewed in 2019. Additionally, the ISO/IEC 27001 is supported by the ISO/IEC 27002 code of practice for information security management describing how to implement information security controls for managing information security risks. ISO/IEC 27001 Information Security Management System (ISMS) consists [19] of 1) highlights the importance of achieving objectives of ISMS; 2) provides management leaderships to

Table 10. ISO/IEC 27000 standards series.

ISO/IEC 27000 series	Standards	Information technology—Security techniques—Information security management systems
Vocabulary Standards	27000	Overview and vocabulary
Requirement Standards	27001	Requirements
	27006	Requirements for bodies providing audit and certification of information security management systems
	27009	Requirements
Guidelines Standards	27002	Code of practice for information security controls
	27003	Guidance
	27004	Monitoring, measurement, analysis and evaluation
	27005	Information security risk management
	27007	Guidelines for information security management systems auditing
	TR 27008	Guidelines on information security controls
	27013	Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1[a]
	27014	Governance of information security
	TR 27016	Organizational economics
	27021	Information security management for inter-sector and inter-organizational communications
Sector-Specific Guidelines Standards	27010	Information security management for inter-sector and inter-organizational communications
	27011	Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations
	27017	Code of practice for information security controls based on ISO/IEC 27002 for cloud services
	27018	Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
	27019	Information security controls for the energy utility industry

[a] ISO/IEC 20000-1:2011, Information technology—Service management—Part 1: Service ISO/IEC 27001, Information technology.

support the ISMS measures for implementing and monitoring the information security objectives; 3) addresses the risks in information security objectives; 4) support trustworthy resources for managing and maintaining the ISMS; 5) provide operational strategies for the execution of documentation needs to be delivered; 6) performs evaluation, measurement, analyses and monitor the ISMS; 7) improves performance and continual advancement requirements.

ISO/IEC 27010

ISO/IEC 27010 was published in 2012 and had minor editorial changes in 2015. While ISO/IEC 27010:2015 complements ISO/IEC 27001:2013, the ISO/IEC 27010 provides guidance and guidelines on adopting, implementing, meaning information in inter-organizational and inter-sector communications. ISO/IEC

27010 [20] consists of 1) highlighting the Information sharing, management, and supportive entities for communities as well as inter-sector communication, compliance, and communication model and provides the management direction for information security; 2) addressing the information security for organizations and the status change of employment; 3) providing responsibility for assets, information classification and information exchanges protections and physical and environmental security; 4) addressing the access control, cryptographic control, Operational procedures, protection responsibilities, and technical vulnerability management; 5) providing Information security, delivery management, and incident management in supplier relationships; 6) addressing the management of Information security incident management and improvements and the information security continuity and redundancies vii) compliance with legal and contractual requirements and Information security reviews

ISO 22301

ISO 22301 was released in 2012 and was reviewed in 2019. ISO 22301 provides the requirements of security and resilience for business continuity management systems. The standard identifies a set of requirements to implement, maintain and improve a management system to safeguard, protect risks and disruptions as well as prepare a response/recovery to any incident. The standard [21] provides four key requirements for implementing business continuity 1) understanding of organization by Planning, implementing, maintaining, and continually improving Business Continuity Management System (BCMS), 2) provide framework and methodology to support compliance with stated business continuity policy, 3) plan and support actions, resources, and awareness to deliver products and services at an acceptable predefined capacity during a disruption, 4) evaluate the monitoring, measurement, and analysis to enhance the business continuity resilience through the effective application of the Business Continuity Management System (BCMS).

ISA/IEC 62443 series

The ISA/IEC 62443 series is a series of standards developed by the International Society of Automation (ISA) and International Electrotechnical Commission (IEC) for industrial and critical infrastructures operational technology, including but not restricted to power utilities, water management systems, healthcare, and transport systems. The ISA/IEC 62443 has four categories to assess the cybersecurity risks and recognize the critical systems. **Table 11** shows the series categories and their descriptions[9].

Cyber Assessment Framework (CAF)

The United Kingdom (UK)'s National Security Strategy recognized the security, protection, and resilience of the UK's Critical National Infrastructures (CNI) remains crucial for the functioning of society, such as those associated with energy supply, water supply, transportation, health, and telecommunication. The UK National Cyber Security Center (NCSC) developed the Cyber As-

[9] https://webstore.iec.ch/searchform&q=IEC%2062443.

sessment Framework (CAF) [22] known as the NCSC CAF collection to provide a set of fourteen cybersecurity and resilience principles for securing CI sectors. NCSC CAF collection adopted the EU Security of Networks & Information Systems (NIS) Directive that aims to raise levels of cybersecurity and resilience of crucial systems across the EU. The CAF collection is intended for use of any organizations that are part of UK Critical National Infrastructures (CNI) or responsible to provide services to CNI sectors. Table 12 provides an overview of the fourteen CAF cybersecurity and resilience principles as well as classifies the

Table 11. ISA/IEC 62443 Series categories.

Categories	Description
General documents *IEC* 62443-1	Present essential concepts and secure development lifecycle requirements
Policies & Procedures *IEC* 62443-2	Highlights the security measures and system integration
System *IEC* 62443-3	Guidance on designing and implementing secure systems levels
Component *IEC* 62443-4	Describe a set of requirements to support secured industrial components

Table 12. CAF cybersecurity and resilience principles.

Objectives	Principles	Description
Objective A *Managing security risk*	A.1 Governance	Acceptable policies and processes to approach the security of network and information systems.
	A.2 Risk management	Recognition, evaluation and awareness of security risks to approach risk management.
	A.3 Asset management	Regulating and awareness of all critical systems and/or services required for support
	A.4 Supply chain	Awareness and control of the security risks for the systems that have external dependencies
Objective B *Protecting against cyber attack*	B.1 Service protection policies and processes	Measuring and communicating acceptable policies and processes to secure critical systems operations.
	B.2 Identity and access control	Awareness, verifying and regulating access to networks and information systems supporting essential functions.
	B.3 Data security	Safeguarding data used in essential functions from adverse actions.
	B.4 System security	Safeguarding critical network and information systems and technology from cyberattack.
	B.5 Resilient networks and systems	Developing resilience against adverse actions.
	B.6 Staff awareness and training	Involving staff to make a positive contribution to the cybersecurity of essential functions.
Objective C *Detecting cyber security events*	C.1 Security monitoring	Observing and monitoring the potential security problems and the effectiveness of existing security measures.
	C.2 Proactive security event discovery	Identifying anomalous incidents in relevant network and information systems.
Objective D *Minimizing the impact of cyber security incidents*	D.1 Response and recovery planning	Placing suitable incident management and mitigation processes.

fourteen objectives, principles with related guidance and reference for CAF collection[10].

Cybersecurity Capacity Maturity Model for Nations (CMM) Framework

The Cybersecurity Capacity Maturity Model for Nations (CMM) framework was developed in 2016 by the Global Cyber Security Capacity Centre (GCSCC) of the University of Oxford to assess, measure, and evaluate the nations' cybersecurity capacity. The CMM framework [23] is comprised of five Dimensions to measure and evaluate the effectiveness of security, protection, and resilience of national cybersecurity strategies as shown in Table 13.

4. Conclusion

Conclusion and Future Improvements

Critical infrastructure is a crucial requirement for any society to survive. This article assessed that CI protection strategies only are effective if security and resilience are seen as critical requirements in CI. This article reviewed the NIST, ISO/IEC, ISA/IEC, CAF, and CMM cybersecurity assessment frameworks and strategies and their common goal of an assessment framework for increasing the effectiveness of cybersecurity capacity. The assessments focus on evaluating the level of the cybersecurity capabilities by fostering best practices, safeguard information, guiding cybersecurity activities, and managing risks within organizations as well as enabling structures to maintain the desire security posture, determining the current status of cyber preparedness, and develop operational resilience. The CI protections frameworks' future improvement can develop by a measurement system to evaluate the capabilities of assessment methods, measure the effectiveness of the activities and action plans using meaningful indicators on a

Table 13. CMM framework.

Dimension	Description
Dimension 1 *Cybersecurity Policy and Strategy*	Evaluate and enhance the level of national cybersecurity strategy and resilience by improving its incident response, cyber defense, and critical infrastructure capabilities.
Dimension 2 *Cybersecurity Culture and Society*	Assess and measure the key elements of national cybersecurity awareness and values of cyber-related risks and the trust level
Dimension 3 *Building Cybersecurity Knowledge and Capabilities*	Evaluate the level of availability and quality of national cybersecurity awareness, educational and professional training programs.
Dimension 4 *Legal and Regulatory Frameworks*	Assess and observes the direct and indirect cybersecurity national legislation including regulatory requirements for cybersecurity, cyber-crime-related legislation, and related legislation.
Dimension 5 *Standards and Technologies*	Observe and addresses the effectiveness of cybersecurity technology, standards, and good practices in protecting critical assets of organizations, national infrastructures, and individuals.

[10] https://www.ncsc.gov.uk/collection/caf/table-view-principles-and-related-guidance.

shared platform, shift voluntary and self-assessment methods to a more consistent and comprehensive assessment approach.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] U.S. Department of Commerce (2018) Risk Management Framework for Information Systems and Organizations a System Life Cycle Approach for Security and Privacy. Special Publication No. 800-37, Revision 2, National Institute of Standards and Technology, Gaithersburg. https://nvlpubs.nist.gov/Nistpubs/SpecialPublications/NIST.SP.800-37r2.Pdf

[2] International Electrotechnical Commission (IEC) (2019) Cyber Security and Resilience Guidelines for the Smart Energy Operational Environment. International Electrotechnical Commission, Geneva. http://www.iec.ch/basecamp/cyber-security-and-resilience-guidelines-smart-energy-operational-environment

[3] (2017) GFCE Global Good Practices Critical Information Infrastructure Protection (CIIP). *Global Forum on Cyber Expertise*, Brussels, 31 May-1 June 2017. https://cybilportal.org/tools/gfce-global-good-practices-critical-information-infrastructure-protection-ciip/

[4] World Economic Forum (2021) The Global Risks Report 2021. 16th Edition, World Economic Forum, Cologny. http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

[5] Center for Strategic & International Studies (2021) Significant Cyber Incidents since 2006. Center for Strategic & International Studies (CSIS), Washington DC. https://csis-website-prod.s3.amazonaws.com/s3fs-public/210604_Significant_Cyber_Events.pdf?Ig0rKRzJ9Bc2WS95MJVt1pkZll5eJLE7

[6] National Consortium for the Study of Terrorism and Responses to Terrorism (2019) Significant Multi-Domain Incidents against Critical Infrastructure (SMICI) Dataset. National Consortium for the Study of Terrorism and Responses to Terrorism, College Park. http://www.start.umd.edu/pubs/START_UWT_SignificantMultiDomainIncidentsAgainstCriticalInfrastructure_Dec2019.pdf

[7] Patriot Act of 2001. https://www.justice.gov/archive/ll/highlights.htm

[8] Federal Register (2013) Executive Order 13636: Improving Critical Infrastructure Cybersecurity. https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity

[9] Congress.gov (2014) Cybersecurity Enhancement Act 2014 (CEA). https://www.congress.gov/bill/113th-congress/senate-bill/1353/text

[10] Federal Register (2015) Executive Order 13691: Promoting Private Sector Cybersecurity Information Sharing. https://www.federalregister.gov/documents/2015/02/20/2015-03714/promoting-private-sector-cybersecurity-information-sharing

[11] (2013) Presidential Policy Directive-21—Critical Infrastructure Security and Resilience.

https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[12] United Nations Security Council (2001) UNSC Resolution 1373. United Nations Security Council, New York. https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf

[13] United Nations Security Council (2004) UNSC Resolution 1566. United Nations Security Council, New York. https://undocs.org/S/RES/1566(2004)

[14] United Nations Security Council (2005) UNSC Resolution 1624. United Nations Security Council, New York. https://digitallibrary.un.org/record/556538?ln=en

[15] United Nations Security Council (2017) UNSC Resolution 2341. United Nations Security Council, New York. https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_res_2341.pdf

[16] Council of the European Union (2008) Directive 2008/114/EC—The Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection. *Official Journal of the European Union*, **51**, 75. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008L0114&from=EN

[17] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology, Gaithersburg. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[18] International Organization for Standardization (2018) Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary. ISO/IEC 27000, International Organization for Standardization, Geneva.

[19] International Organization for Standardization (2013) Information Technology—Security Techniques—Information Security Management Systems—Requirements. ISO/IEC 27001, International Organization for Standardization, Geneva.

[20] International Organization for Standardization (2015) Information Technology—Security Techniques—Information Security Management for Inter-Sector and Inter-Organizational Communications. ISO/IEC 27010, International Organization for Standardization, Geneva.

[21] International Organization for Standardization (2019) Security and Resilience—Business Continuity Management Systems—Requirements. ISO 22301, International Organization for Standardization, Geneva.

[22] National Cyber Security Center (2019) Cyber Assessment Framework V3.0. National Cyber Security Center, London. https://www.ncsc.gov.uk/information/cyber-assessment-framework--caf--changelog

[23] Global Cybersecurity Capacity Centre (2021) Cybersecurity Capacity Maturity Model for Nations (CMM) Report. Global Cybersecurity Capacity Centre, Oxford. https://cybilportal.org/wp-content/uploads/2021/03/CMM2021-Edition-March-2021.pdf