International Journal of Nuclear Security

Volume 6 | Number 1 Article 3

7-6-2020

Regulatory Perspective on Nuclear Cyber Security: The Fundamental Issues

Uchechukwu Christian Arinze
Information and Communication Technology (ICT) Unit, Department of Radiological Safety, Nigerian Nuclear Regulatory Authority, Abuja.

Olumide Babatope Longe
Department of Information Systems, School of IT & Computing, American University of Nigeria, Yola.

Agozie Hyacinth Eneh
Computer Science Department, University of Nigeria, Nsukka

Regulatory Perspective on Nuclear Cyber Security: The Fundamental Issues

Cover Page Footnote

Special thanks to the Management of the Nigerian Nuclear Regulatory Authority, under the leadership of Professor Lawrence Anikwe Dim, for his support and encouragement to embark on this research.

International Journal of Nuclear Security, Vol.6 No.1, 2020

Regulatory Perspective on Nuclear Cyber Security: The Fundamental Issues

Arinze, U.C.[1], Eneh, A.H.[2], Longe, B.O.[3]
[1]Information and Communication Technology (ICT) Unit, Department of Radiological Safety, Nigerian Nuclear Regulatory Authority (NNRA), South East Zonal Office, Enugu, Enugu State.
[2]Computer Science Department, Faculty of Physical Sciences, University of Nigeria, Nsukka (UNN), Enugu.
[3]Department of Information Systems, School of Information Technology & Computing, American University of Nigeria (AUN), Yola, Adamawa State.
Email: [1]uchechukwu.arinze@nnra.gov.ng, [2]agozie.eneh@unn.edu.ng, [3]olumide.longe@aun.edu.ng
Tel: +2348066532557, +2348076756975, +2348160900893

Abstract

We are living in a digital and information-driven age and need to store information related to virtually every aspect of our lives, nuclear information included. For computer system to be reliable and secure in nuclear facilities, unauthorized event changes must be prevented (which means maintaining - confidentiality), field device inputs and outputs must remain immutable throughout their usable lifetime (which means maintaining - integrity), and all component parts should remain in an operable state (which means maintaining - availability).The dynamic and complex nature of cyber threats has made it a serious challenge to secure computer systems in nuclear facilities. A number of varied cyber security services, policies, mechanisms, strategies and regulatory frameworks have been adopted , including: confidentiality, integrity, availability, non-repudiation, encipherment, defense-in-depth (DID), design basis threat (DBT), IAEA technical guidance documents such as: GS-R-1, GS-R-2, GS-R-3, GS-G-3.1-3.5, NSS20, NSS23-G, NSS13, NSS17, NST036, NST045, and NST047, IEEE standard 7-4.3.2-2010, NIST SP 800-53, NIST SP 800-82, NEI 04-04, NEI 08-09 and country-specific requirements such as: 10 CFR 73.54, RG 5.71 (U.S.NRC), KINS/RG-N08.22 (South Korea). However, threats remain persistent. This paper is aimed at providing a regulatory perspective on nuclear cyber security, its relationship to nuclear safety and security, regulatory requirements and global best practice recommendations for nuclear cyber security, and strategies to prevent and counteract threats. This study is imperative as Nigeria prepares to join the league of countries with operational nuclear power plants and research reactors

International Journal of Nuclear Security, Vol.6 No.1, 2020

following approval and adoption of the nuclear power programme roadmap in 2007 and contract signing with Rosatom of Russia for NPP and research reactor construction.

Keywords: Cyber security, nuclear security, nuclear power plants, critical digital assets

I. Introduction, Motivation, Goals, Scope and Methodology

Cyber security includes all processes and mechanisms by which any digital equipment, information or service is protected from unintended or unauthorized access, change or destruction. As a component of nuclear security and the design basis threat (DBT) ***[1]***, cyber security is the range of measures enacted to prevent, detect, or respond to the theft of Category I nuclear material or to the sabotage of a nuclear facility, which could result in catastrophic radiological consequences by either exploiting vulnerabilities in information and computer systems alone or combined with physical attacks ***[2]***. According to the United States Nuclear Regulatory Commission (U.S. NRC) Regulatory Guide (RG) 5.71, cyber-attack is the manifestation of either physical or logical (i.e., electronic or digital) threats against computers, communication systems, or networks that may originate from either inside or outside the licensee's facility, have internal and external components, involve physical or logical threats, be directed or non-directed in nature, be conducted by threat agents having either malicious or non-malicious intent and have the potential to result in direct or indirect adverse effects or consequences to critical digital assets (CDAs) or critical systems (CSs). This includes attempts to gain unauthorized access to a CDA and/or CS's services, resources, or information, the attempt to compromise a CDA and/or CSs Integrity, Availability, or Confidentiality (C.I.A triad) or the attempt to cause an adverse impact to a Safety, Security and Emergency Preparedness (SSEP) functions.

The increasing wave of digitization of systems and processes has necessitated the upgrade of analog instrumentation and control (I&C) systems in nuclear power plants (NPPs) to digital I&C systems, i.e. systems based on computers and microprocessors to monitor, operate, control, and protect those facilities. Digital systems offer higher reliability, better plant performance and additional diagnostic capabilities. Analog systems will gradually become obsolete in the general IT paradigm shift to digital I&C systems. About 40% of the world's operating nuclear reactors have been modernized to include at least some digital I&C systems. Most new NPPs incorporate digital I&C systems. Digital I&C systems have posed new challenges for the nuclear industry and regulators, who are responsible for designing the methods, data and experience to assure themselves that the new systems meet all reliability and performance requirements. In general, countries that have more new builds have had greater incentives and opportunities to develop the needed capabilities. Other countries are still in the process of doing so. According to the 2018 Verizon DBIR report, more than 25% of cyber-attacks have been at the hands of insiders who exploit their authorized access. Trusted employees, contractors, and business partners pose a substantial risk to organizations. They often have the ability to bypass many security controls that focus on keeping outsiders out and are not capable of viewing insider activity or are tuned to ignore actions by authorized users. In the cloud, security teams have to understand the extent of these insider threats and enforce appropriate cloud controls to detect unauthorized actions by insiders. The threat posed by cyber-attacks often as a national and international security concern has grown in sophistication, frequency of occurrence and scale over the years, as shown in Figure 3. The problem is complicated by the involvement of nation states in these attacks as shown in Figure 4, attacks which had previously been the exclusive domain of private hackers, script kiddies and organized criminal groups. Attacks restricted to networks and financial computer systems have been extended to all IT and ICS components of nuclear facilities with all the implications, risks and potential radiological consequences such attacks pose to lives, property and the environment.

The importance of this paper is underscored by the fact that nuclear security is tremendously impacted by cyber security. Nuclear facilities made up of field devices, field controllers, supervisory control and data acquisition (SCADA) and instrumentation and control (I&C) systems as shown in Figure 1 are mission-critical infrastructure that are susceptible to attacks from Nation States and non-state actors like hactivist/hactivism, third-parties, organized crime, professional criminals, spies, voyeurs, corporate raiders, disgruntled insiders, vandals, script kiddies and cyber terrorists as shown in Table 1.1. The various threat actors have different motivations, intentions for their activities, and capabilities, which adds to the complexity of the problem and increases the need for comprehensive understanding of the risks at regional, industry, institutional and process levels.

Table 1.1 Cyber threat actors, Description of activities and Motivation

S. No.	Threat Actor	Description	Motivation
1.	Nation State	Hackers directly employed directly an arm of a national government to penetrate commercial and/or government computer systems in other countries.	• Cyber espionage
2.	Hactivist/Hactivism	Individuals or groups who use digital tools looking to advance their own social, political and ideological agendas.	• Political and/or social change • Thrill seeking • Reputational damage
3.	Third Parties	Third party vendors and service providers who: a. Have access to data b. Have access to systems c. Have access to facilities	• Immediate financial gain • Collect information for future financial gains • Competitive advantage • Collusion with other threat actors
4.	Organized Crime	Highly structured criminal organizations and groups of hackers that seek to attack under-defended targets and exploit vulnerabilities	• Immediate financial gain • Collect information for future financial gains
5.	Insiders	Current or former employees who may be disgruntled or under duress using internal access and authority for nefarious purposes	• Personal advantage, monetary gains • Malevolent behaviors (revenge) • Bribery, blackmail/coercion/ • collusion

In May 2018, there were 450 nuclear power plants (NPPs) in operation around the world, generating 393, 836 MW(e) total out of which 195 units (43.3%) were built in the last 30 years and 319 units (70.8%) were constructed during the last 25 years. Currently there are 439 operational nuclear reactors net installed capacity across 31 countries according to the International Atomic Energy Agency (IAEA) Power Reactor Information System (PRIS) database. These critical facilities use both analog and digital systems to monitor and operate plant processes, equipment, and store and retrieve information. In addition to physical and system operational security, cyber security of CDAs and computer instrumentation and control systems (ICS), networks have become a growing concern to both nuclear operators and nuclear facility regulators around the world. I&C components such as process control systems (PCS), supervisory control and data acquisition (SCADA), digital control systems (DCS) that interconnect plant systems performing safety, security, and emergency preparedness (SSEP) functions are not isolated from the Internet. This presents an attack vector for cyber threats as shown in Figure 1.1 and Figure 1.2 respectively.

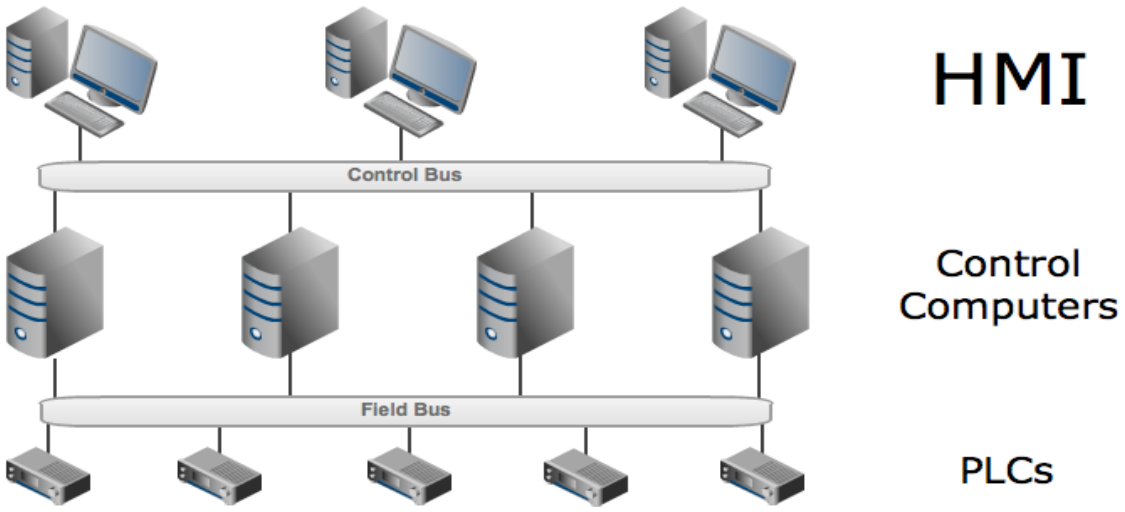

Figure 1.1: Highly simplified representation of process control system
Source: Kesler, B. (2011). The Vulnerability of Nuclear Facilities to Cyber Attack. Strategic Insights, Vol. 10, Issue 1, p.16.

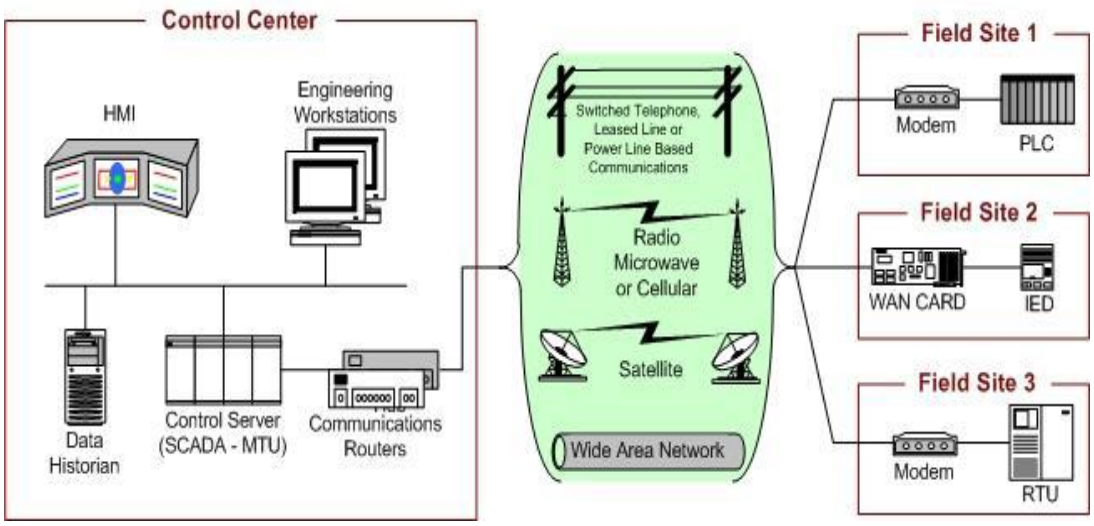

Figure 1.2: SCADA system in a nuclear facility
Source: NIST Special Publication 800-82 Rev 2 Draft: Guide to Industrial Control Systems (ICS) Security, p.2-6, 2014. (U.S)

According to the Insurance Information Institute (I.I.I) and J.D. Power 2018 Small Business Cyber Insurance and Security Spotlight Survey, 10 percent of small businesses surveyed suffered one or more cyber incidents in the prior year, and average cost of cyber-related losses over the past year was $188,400. Only about one-third of firms surveyed had cyber insurance, nearly 60 percent of respondents said their company is very concerned about cyber incidents - and 70 percent think that the risk of being victimized by a cyber-attack is growing at an alarming rate as shown in Figure 1.3. These attacks are orchestrated by Nation States and non-state actors like hactivist/hactivism, third-parties, organized crime, professional criminals, spies, voyeurs, corporate raiders, disgruntled insiders, vandals, script kiddies and cyber terrorists as shown in Figure 1.4.

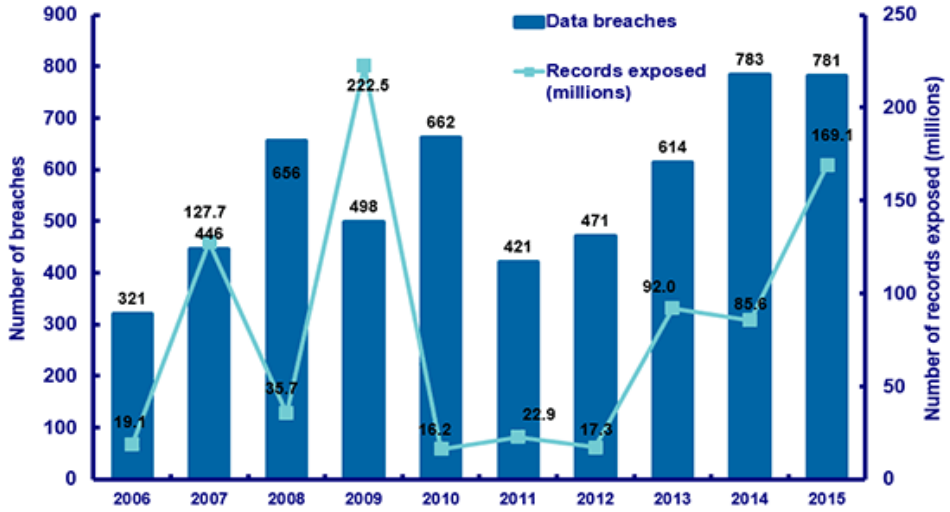

Figure 1.3: Number of data breaches 2006-2015
Source: Identity Theft Resource Centre: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

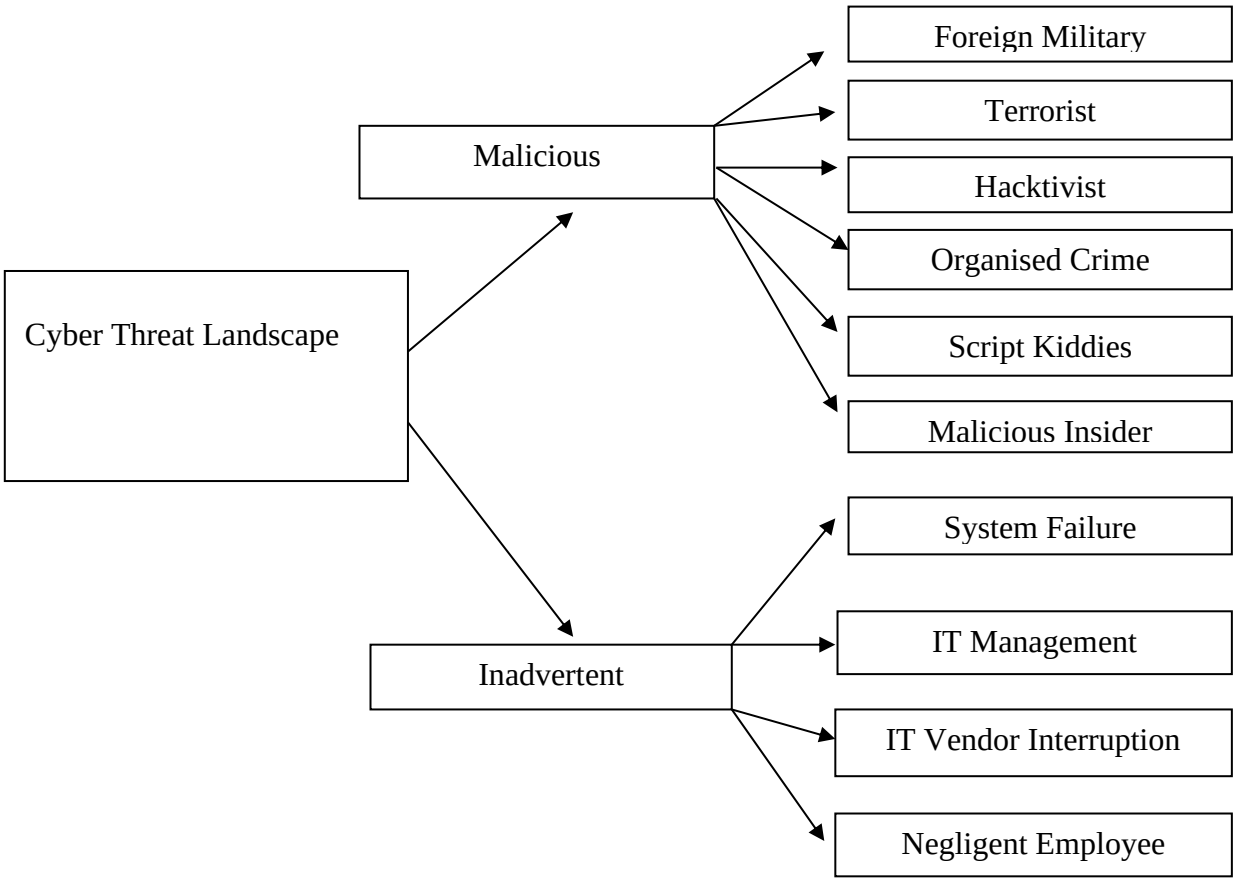

Figure 1.4: The cyber threat landscape
Source: https://emerginrisk.com/our-approach-4/threat-landscape/

Currently, the focus is not on new types of threats, but on existing types that are enhanced. As regards social engineering attacks, for example, a professionalization of the analysis followed by targeting can be observed. Perimeter security and cloud security measures are no longer sufficient. Increasingly, endpoint security is in demand again. It is also advisable to keep an eye on the hardware, as it may serve as target platform for firmware attacks. The impairment of products and standards continues to be a key issue. If these impairments affect widely used products and standards and remain undetected for a long time, they may be disastrous in terms of information security. A good example of this is Heartbleed. Therefore, it is advisable to reduce products' functionality to the maximum and, as a result, avoid the integration of potential vulnerabilities in unnecessary modules. It is also recommended not activating sensitive or hardly used modules by default (secure defaults). System providers using security-relevant products and standards should have several complementary security layers, including controls, in place. This allows them to reduce potential effects of such impairments (defense in depth). As a general rule, attacks are becoming more complex and more difficult to identify. For this reason, identifying misuse by means of user behavior analytics and adaptive security measures are gaining in importance.

In addition, game-changing events like the increase in the number of advanced persistent threats (APTs) such as the Taj Mahal framework and Stuxnet, malware, Trojan attacks and ransomware attacks at the personal, corporate and even state levels. A careful examination of cyber-attacks targeted at NPPs from 1980 to present reveals a pattern of increasing incidence of attack and sophistication. Particularly, 2014 presented multiple computer event that had direct impact or relevance for nuclear. Notable examples include: Bruce NPP (1990), Sellafield (1991), Ignalina (1991), Kurchatov (1991), Davis-Besse Nuclear

Power Plant Slammer worm attack on August 20, 2003 which started at the contractor's site and spread to the corporate plant network shutting down the digital portion of Safety Parameter Display (SPD) systems and Plant Process Control (PPC) for many hours. Others are: Brown's Ferry (2006), Hatch NPP (2008), Stuxnet at Iranian nuclear enrichment facility at Natanz in June 2010 (Figure 1.5); Oak Ridge National Laboratory (2011), Shamoon (2011), Areva (2011), RSA hack (2011), Aurora Test (2011), Red October (2011), Susquehanna NPP (2012), Monju NPP (2014), The Korea Hydro and Nuclear Power malware attack on December 9, 2014 meant to shut down the NPP, Anthem in 2014; Premera Blue Cross (2015), Target (2013), Japanese Nuclear Materials (2015), Gundremingen NPP (2016), University of Toyama (2016), Ukraine NPP (2017), Wolf Creek NPP (2017), U.S and European Union NPPs (2018) Heartbleed cyber breaches in 2014 resulting in the heating, ventilation and air-conditioning (HVAC) system of the vendor's remote access computer serving as the attack vector as shown in Figure 1.6. The cyber security sectoral budget of U.S expended to detect and prevent these losses is even greater and has resulted in financial losses in the billions of dollars as shown in Figure 1.7, while growing sophistication in attack is shown in Figure 1.8.

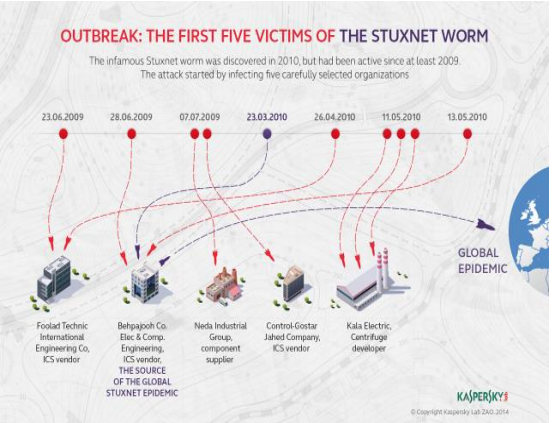

Figure 1.5: Timeline of Stuxnet at Natanz, Iran
Source: Kaspersky Labs, Russia

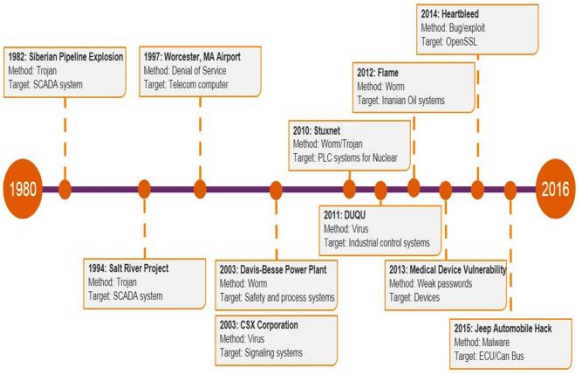

Figure 1.6: Cyber Incidents at NPPs 1980-2016
Source: Gemalto Inc, U.S

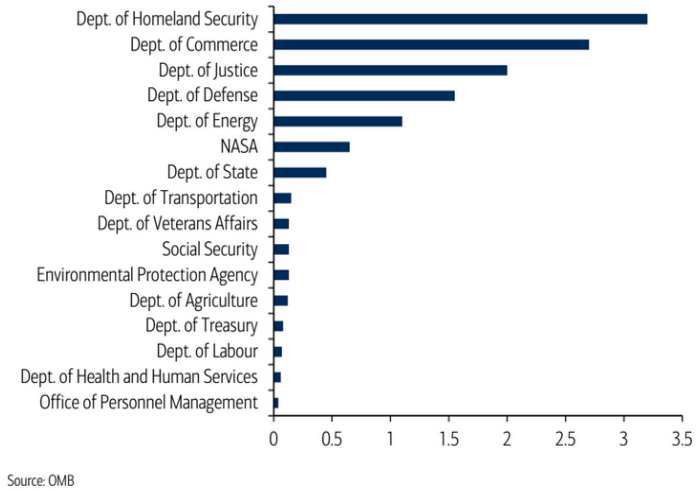

Figure 1.7: Sectoral budget on Cyber security by U.S.A Source: U.S Office of Management and Budget

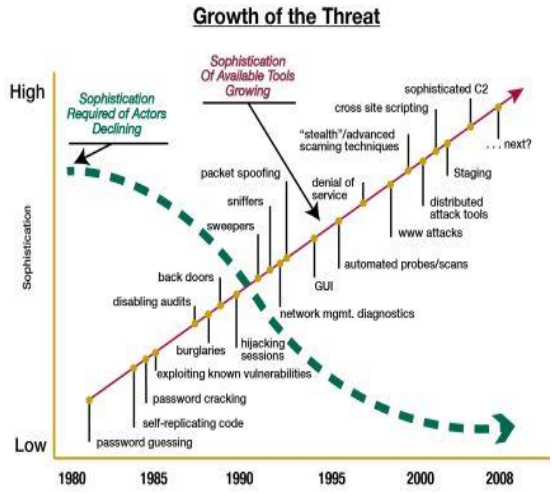

Figure 1.8: Cyber Attack Sophistication Source: https://www.nato.int/docu/review/2016/Also-in-2016/cyber-defense-nato-security-role/EN/index.htm

As a sub-set of nuclear security, the cyber threat landscape is highly dynamic and complex ***[1]***, it is a broad and wide-ranging discipline that interacts with all other areas of security in a nuclear facility. All disciplines of security complement each other to establish a facility's security posture, which is defined in the site security plan (SSP) as shown in Figures 1.9 and 1.10. A failure in any of the disciplines of security could severely impact the other domains and could place additional burdens on the remaining aspects of security.

Figure 1.9: Domains of nuclear security Source: [1, 9]IAEA Nuclear Security Series 17: Computer Security at Nuclear Facilities (Technical Guidance), p.12, 2011.

Figure 1.10: Nuclear security with safety & safeguards Source: [1.10]https://www.jaea.go.jp/04/iscn/activity/2011-12-08/2011-12-08-22.pdf

In order to counter this growing threat, this paper examines the current nuclear cyber security landscape vis-a-vis national and international regulatory frameworks and standards and also studies incidents and lessons learned with a view toward identifying critical gaps and making appropriate recommendations. This task was accomplished by adopting an open-source data gathering and analysis approach via International Atomic Energy Agency (IAEA) nuclear security and safety guidance documents and by examining country-specific cyber security standards and practices from five selected nuclear-powered nations namely: China, Germany, Russian Federation, South Africa and the United States. The scope of this study is restricted to legal, regulatory, and institutional frameworks for cyber security in civilian nuclear fuel cycle facilities, e.g., enrichment or fuel fabrication plants, power plants, reprocessing facilities, research reactors **[*2*]**, etc. The justification for the focus on cyber security is that it is one of the most significant new key elements that have entered the nuclear security lexicon in the last decade, quickly gaining momentum, prominence and significance due to the growing reliance on digital equipment **[*2*]**.

The objective of cyber security is to protect information and property from theft, corruption, or natural disaster, while allowing the information and property remain accessible and useful to authorized users. Currently cyber security issues are the most important challenge of Information Technology (IT) development. As global infrastructure increasingly depends on IT with increasing complexity, its vulnerability increases. The U.S in other to combat the threat of cyber terrorism and other security threats from adversaries, it categorizes 13 critical infrastructure sectors under its Federal Critical Infrastructure Protection Policy: Agriculture, Banking and Finance, Chemicals and hazardous materials, Defense industrial base, Emergency services, energy, Food, Government, Information and Communication Technology (ICT), Postal and shipping, Public health and healthcare, Transportation, Drinking water and water treatment systems. Electric power in particular is the most critical infrastructure upon which other infrastructure depends. Threats to the power infrastructure include natural disasters, human errors, power system component failures, ICT system failures, gaming in the markets, intrusion and sabotage.

Cyber security technologies have assisted in prevention, detection and response to cyber-attacks to critical digital assets (CDAs). Currently, there are a number of cyber security technologies that can be used to better protect CDAs from cyber-attacks according to Sklyar, 2012. In each of these categories, many technologies are currently available, while other technologies are still being researched and developed. Table 1.2 summarizes some of the common cyber security technologies, categorized by the type of security control they help to implement. Critical infrastructure sectors use all of these types of cyber security technologies to protect their systems. However, the level of use of technologies varies across sectors and across entities within sectors.

Table 1.2: Cyber Security Technologies Control Categories and Types [*3*]

	Control Category	**Control Type**
1.	Access Controls	Boundary protection: Firewalls, Content management Authentication: Biometrics, Smart tokens Authorization: User rights and privileges
2.	System Integrity	Antivirus software File integrity checkers
3.	Cryptography	Digital signatures and certificates Virtual private networks
4.	Audit and Monitoring	Intrusion detection systems Intrusion prevention systems Security event correlation tools Computer forensics tools

5.	Configuration management and assurance	Policy enforcement applications Network management Continuity of operations Scanners Patch management

There are a lot of different approaches to implement and manage cyber security measures. On from the approaches is Open Security Architecture (OSA). The OSA Metamodel depicts the entities and relationships that are relevant for OSA as shown in Figure 11. OSA can provide benefits to IT service consumers, IT service suppliers and IT vendors, giving the entire IT community an interest in using and improving. An open approach means that the patterns and catalogues will benefit the whole community and can be more quickly improved and refined by the common experience of participants.

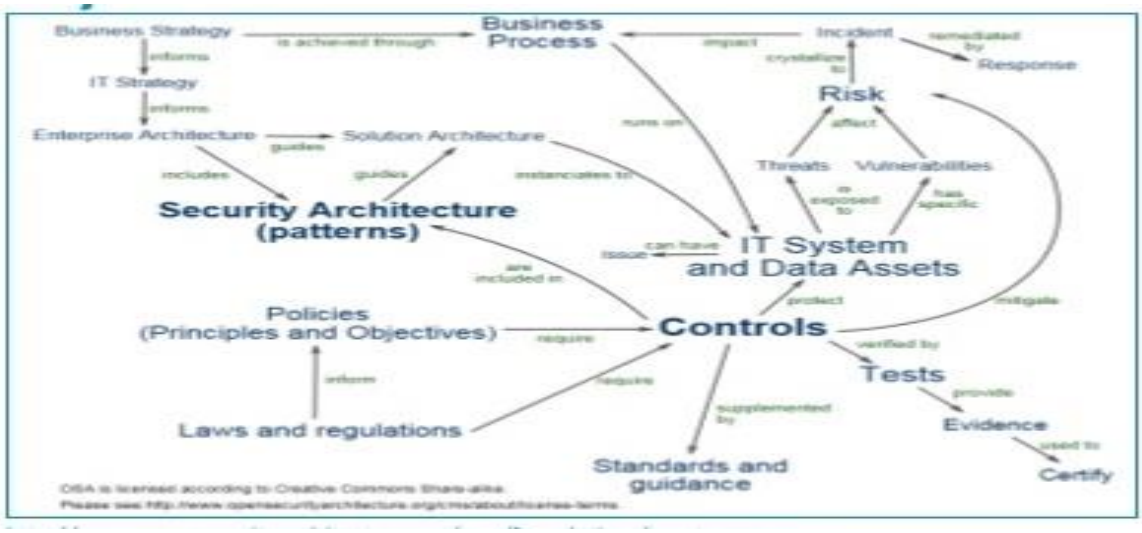

Figure 1.11: Open security architecture (OSA) Metamodel
Source: www.opensecurityarchitecture.org

The rest of the paper is organized as follows: section 2 provides an overview of related works in computer/information security and nuclear cyber security. Section 3 deals with nuclear cyber security model frameworks and standards. Section 4 highlight current status and examples of digital I&C systems in nuclear power plants. Section 5 deals with cyber security regulatory requirements for nuclear facilities. Section 6 outlines global best practice recommendations on nuclear cyber security for Regulators. Section 7 highlights the implications of cyber security incidents for research and practices. Section 8 points out the various lessons learned and section 9 is the summary and conclusion respectively.

II. Related Works

According to Tanenbaum and van Steen (2002), before one can evaluate attacks against a system and decide on appropriate mechanisms to fend off these threats, it is necessary to specify a security policy. A security policy defines the desired properties for each part of a secure computer system. It is a decision that has to take into account the value of the assets that should be protected, the expected threats and the cost of proper protection mechanisms. A security policy that is sufficient for the data of a normal home user may not be sufficient for a bank, as a bank is obviously a more likely target and has to protect more valuable resources. In general, there is a flow of data from a source (e.g., a host, a file, memory) to a destination (e.g., a remote host, another file, or a user) over a communication channel (e.g., a wire, a data bus). The task of the security system is to restrict access to this information to only those parties (persons

or processes) that are authorized to have access, according to the security policy in use. Although literature uses different approaches to categorizing network attacks, in this paper, I will classify them into three (3) groups related to confidentiality, integrity and availability, known as the C.I.A triad of network security goals as shown in Figure 2.1. Confidentiality in the nuclear context implies that unauthorized logic changes must be prevented; integrity implies that field device inputs and outputs must remain immutable throughout their usable lifetime and availability means that all components should remain in an operable state. The U.S.NRC RG 5.71 developed best practices over the years that include the basic tenet that information security is a life-cycle process. Figure 2.2 shows the U.S.NRC nuclear cyber security life cycle model and Figure 2.3 depicts the critical digital asset (CDA) identification process respectively.

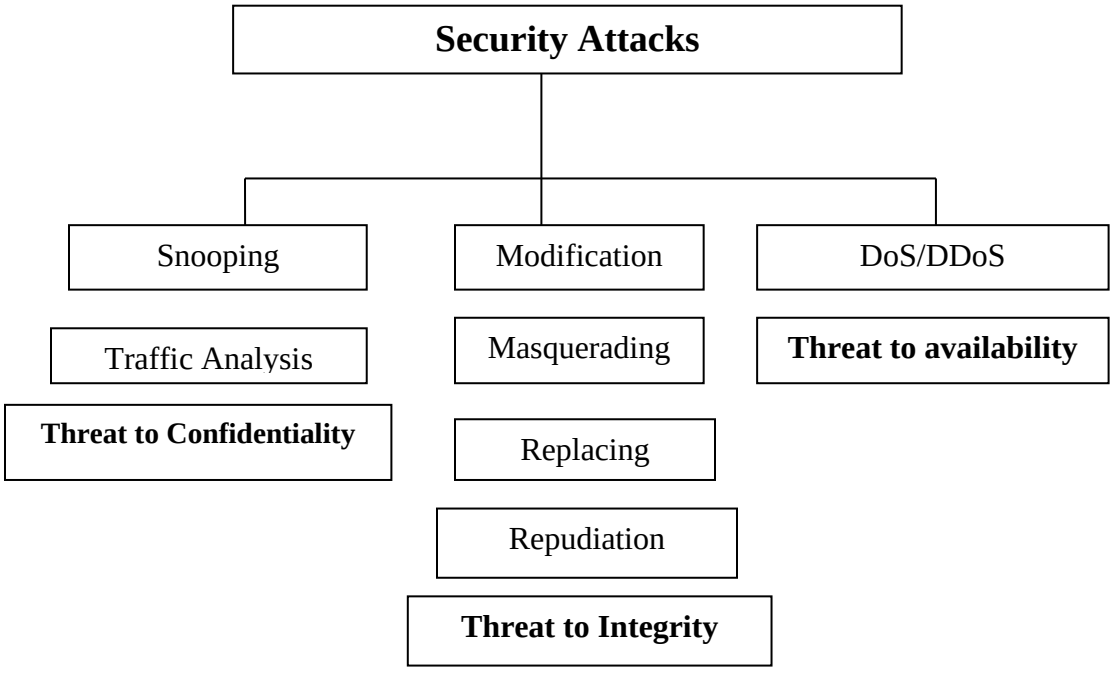

Figure 2.1: Classification of computer security attacks with relation to security goals
Source: Forouzan, B. (2003), p.733.

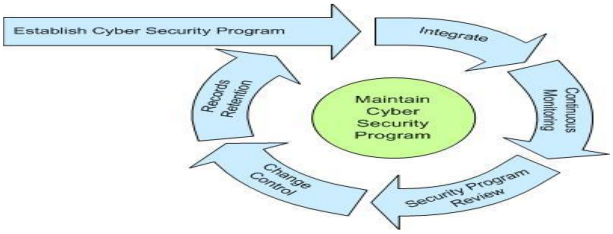

Figure 2.2: Cyber Security Life Cycle
Source: U.S.NRC RG 5.71, p.14

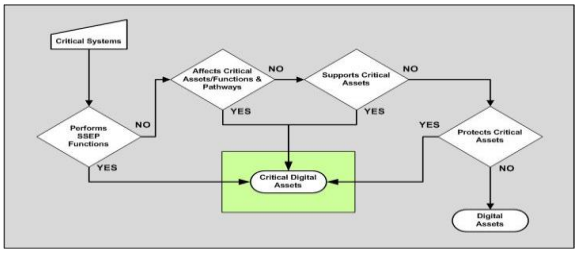

Figure 2.3: CDA Identification process
Source: U.S.NRC RG 5.71, p.16.

For over 30 years, research in computer security has been ongoing. Notable intellectual successes include cryptographic protocols **[*4*]**, the star-property **[*5*]**, multilevel security using information flow **[*6, 7*]**, subject-object access matrix model **[*8*]**, public-key cryptography **[*9*]**, and access control lists **[*10*]**. In spite of these successes, it seems fair to say that the security of billions of deployed computer systems around

the world is suspect. Taxonomy defines what data are to be recorded and how like and unlike samplings are to be distinguished **[*11*]**. The C.I.A triad - Confidentiality, Integrity and Availability security goals can be threatened by security attacks. The snag is the lack of consensus on the approach to adopt in categorizing the attacks. Previous work has been done in the area of classifying threats and vulnerabilities.

Early taxonomies such as (Bishop, 1995) **[*12*]**, focused on categorizing security vulnerabilities in software to assist security practitioners in maintaining more robust and secure systems through an understanding of these vulnerabilities. One approach to gaining insight into an attacker's target is to consider the attack paths, or combination of exploits **[*13*]**. John Howard extended this idea in his 1997 doctoral work in which he analyzed and classified 4,299 security related incidents on the internet. Howard's work was notable because he included attackers, results and objectives as classification categories expanding threat taxonomies beyond the technical details of an attack to include more intangible factors such as an attacker's motivation for conducting an attack **[*14*]**. The vast majority of threat taxonomies are designed as attacker-centric frameworks which categorize attacks from the perspective of an attacker's tools, motivations and objectives. Killouri, Maxion and Tan created taxonomy in 2004 designed to be defense-centric based on how an attack manifested itself in the target systems. Based on a test set of 25 attacks, this taxonomy was able to predict whether or not the defender's detection systems would be able to detect a given type of an attack **[*15*]**.

In a similar effort, Mirkovic and Reiher created taxonomy of Distributed Denial of Service (DDoS) defenses, which categorized DDoS defense mechanisms based on activity level, degree of co-operation and deployment location **[*16*]**. These two taxonomies are among the few that classify threats or security incidents from a defensive viewpoint and show the importance of addressing such issues from different perspectives to gain a more holistic view of security issues. Researchers at the University of Memphis led by Simmons created a cyber-attack taxonomy called AVOIDIT in 2009, which described attacks using five (5), extensible classifications: Attack Vector, Operational Impact, Defense, Informational Impact, and Target **[*17*]**. In recent years, a number of researchers have begun to look at creating taxonomies specifically addressing SCADA systems. In 2010 Fovino, Coletta & Masera created a comprehensive taxonomy describing SCADA architecture, vulnerabilities, attacks and countermeasures **[*18*]**. In 2011 Zhu, Joseph, & Sastry highlighted the difference between what they termed standard information technology (IT) systems versus SCADA systems and focused on systematically identifying and classifying attacks against SCADA systems **[*19*]**.

The efforts present certain challenge: although they provide background information related to cyber threats that could be utilized to address future developments, the taxonomies in question do not properly capture the protection of nuclear facilities in the light of existing cyber threats and legal and regulatory frameworks. This is because nuclear digital systems are in nature different from general information and telecommunication systems. Because cyber-attacks against nuclear power plants can result in grievous consequences in the forms of human, environmental and infrastructural damages, nuclear digital systems are long-term, real-time systems that demands simultaneous responses to intrusions 24 hours a day, seven days a week for the entirety of their 30 to 40 years lifespan.

In 2015, Gluschke *et. al.* (2015) **[*2*]** characterized country-specific nuclear cyber regulatory practices and introduced a potential model for developing a national approach to cyber security at nuclear facilities. Similarly, in 2016 Dine, Assante, & Stoutland (2016) **[*20*]** highlighted the vulnerabilities of IT and ICS systems in nuclear facilities around the world, comparing country-specific nuclear cyber regulatory frameworks and best practices. Nuclear systems demand a comprehensive security measure that considers system life cycle, work processes and procedures as well as infrastructural protection spanning measures for system developers, system maintenance staffs, third-party contractors, consultants and workers within the plant. In [30], Gluschke, Mesut & Macori (2018) three levels of cyber threats protection are

established as requirements: the internet network, the intra-network, and the independently blocked network. Staff within the plant can work only within the intra-network. The internet and intra-network must be separated (air gap) to ensure full independence of the workspace and access. Internet access within the workspace must be authorized and separated from the intranet network. Although this separation can result in some inefficiencies and inconveniences, it provides an additional layer of security for the system to protect against cyber threats. The intra-network - must be connected with the independently blocked network, which controls specific nuclear infrastructure and critical information systems such as the nuclear reactors, computer systems, the centralized database management systems, the operating systems, turbine control systems, etc. This independently blocked network - transfers only simple operation information to the intra - network in order to ensure that new threats such as nuclear cyber terrorism and espionages are mitigated. In addition, a holistic approach that establishes legal and institutional frameworks for efficient radiation disaster management systems - must be in place to provide standards and procedures for regulating and controlling illegal transfer of radioactive and nuclear materials and for handling sabotage by cyber attackers.

In Cyber security at Nuclear Facilities: National Approaches, a research conducted by the Institute for Strategic Studies (ISS) at the Brandenburg University of Applied Sciences, Germany and United States Nuclear Threat Initiative (NTI), they focused on the legal, regulatory, and institutional frameworks for cyber security by examining in detail range of measures that affect the higher levels of the hierarchy of responsibilities **[*2*]**. The study's comparative analysis focuses on national legislation, regulatory frameworks, regulations and guidance, licensing and other associated regulatory activities. However, the limitation of their study is their decision not to discuss on the more operational and technical aspects of cyber security and their implementation at the facility level. The following figure shows the various tiers of cyber security needed to address the cyber threat at nuclear facilities and indicates the tiers at the nation state level, which is the focus of this study. The NSS20 approach is broader than is needed for cyber security; but most essential elements can play a role when assessing a nation state in terms of nuclear-cyber readiness, such as 'Identification and Definition of Nuclear Security Responsibilities', 'Legislative, Regulatory Framework' or 'Identification and Assessment of Nuclear Security Threats' **[*2*]**. Figure 2.4 illustrate the defense-in-depth (DID) model for nuclear cyber security.

A. National legislation

At the highest level, legislation should ideally reflect a contemporary approach to nuclear security, incorporating concepts expressed in the 2005 amendment to the Convention on the Physical Protection of Nuclear Material (CPPNM) **[*2, 21*]**, as well as including or referring to the security of information (or more explicitly cyber security) as one of the key elements of nuclear security. In this context it is probably more feasible to do so in those national legislations where nuclear security is separate from generic nuclear laws dealing with the promotion and regulation at large of any activity involving radioactive materials or nuclear energy generation **[*2*]**. Countries with or without specific nuclear security legislation are shown in table 2.1, while those with cyber legislation are shown in Table 2.2.

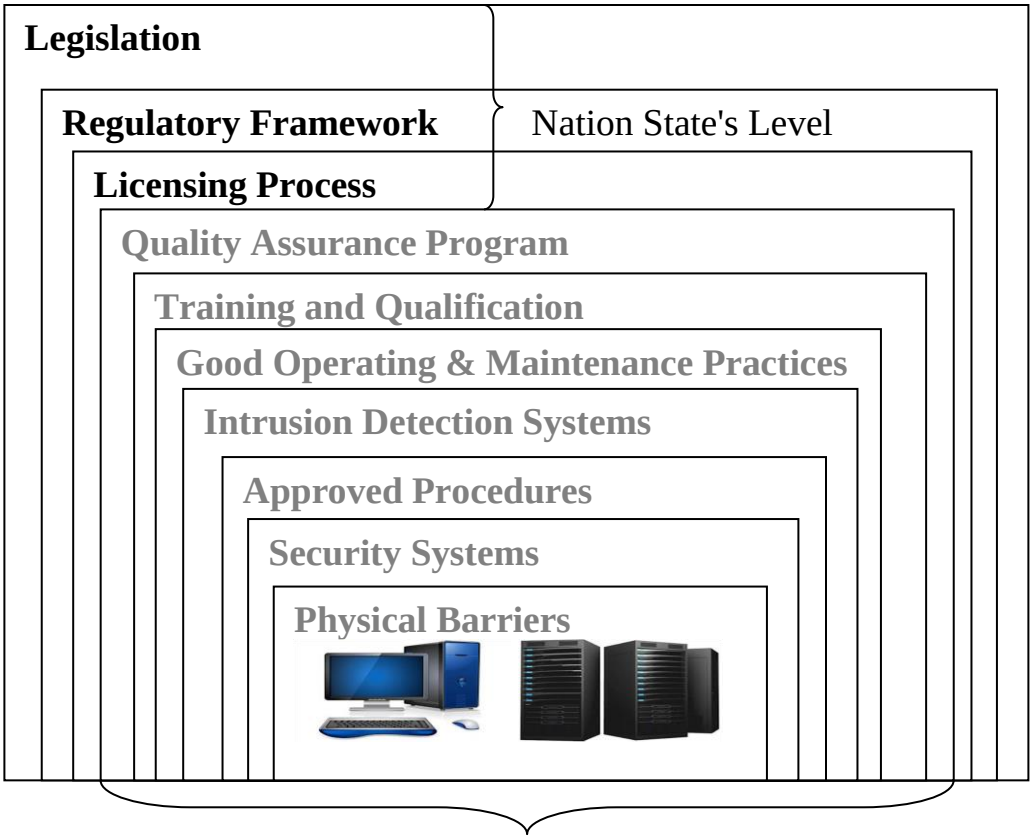

Figure 2.4: Defense-in-depth model for cyber security in the nuclear context, Source: [*2*]

Table 2.1: Specificity of nuclear security legislation [*2*]

Characteristics	Countries
No nuclear law	China
A generic "nuclear law" dealing broadly with issues relating to the implementation of nuclear power with few or no explicit references to nuclear security	South Africa **[*22*]**
A generic "nuclear law" with explicit references or detailed sections dedicated to nuclear security	
A law specifically dedicated to nuclear security (the latter often in conjunction with more generic "nuclear laws" within the same legal system)	U.S.A **[*23*]**, Germany **[*24*]** Russia **[*25, 26*]**

Table 2.2: Countries with Cyber security legislation [2]

Characteristics	Countries
No legislation regarding cyber security is in place	U.S.A., China
Legislation on cyber security is in place, no explicit provisions for critical infrastructure or nuclear facilities	South Africa **[*27, 28*]**
Legislation on cyber security is in place, and either has dedicated sections for critical infrastructure or nuclear facilities or separate laws covering the cyber security of these exist	Russia **[*29*]**, Germany **[*30*]**

B. Regulatory framework

Similarly, legislation should operate at the proper level and avoid rapid obsolescence by steering clear of legislating specific details which are bound to evolve rapidly (like technology) and should instead focus on establishing the framework for the correct operation of a regulatory authority, with regard to its ability to write and enforce regulation and to criminalize and prosecute relevant crimes **[*2*]**. Table 2.3 shows countries with or without competent authorities for cybersecurity at their respective nuclear facilities.

Table 2.3: Competent Authority for Cyber Security at Nuclear Facilities [*2*]

Characteristics	Countries
No competent authority explicitly regulating cyber security at nuclear facilities has been established	China
Cyber security at nuclear facilities is the responsibility of the nuclear regulatory body	Germany, U.S.A, South Africa
Cyber security at nuclear facilities is the responsibility of the cyber regulatory body	Russia

C. Regulations and guidance

Regulations instead, are standards adopted as rules by the relevant authority to implement, interpret, or make specific the laws enforced or administered by the authority itself. They are needed so that the industry may have clear and detailed instructions. At the same time, regulation can evolve and adapt more rapidly than legislation given a lighter approval/modification procedure that involves fewer stakeholders. A number of countries - for example, China and South Africa - have regulations pertaining to aspects of nuclear safety and cyber security that protect national infrastructure in general. There are no specific regulations in these countries related to the cyber security of nuclear facilities. Also, the status of the implementation of these regulations is elusive and can therefore not be said to be fully developed. The United States, Russia and Germany have written regulations in the cyber security of nuclear plants and the regulations are developed. **[*31*]**

D. Licensing

Ideally cyber security should be embedded into the design of nuclear facilities themselves and their associated security plans from the beginning. The crucial instruments to ensure that this occurs and is maintained through the lifecycle of an NPP – as a design goal and as an element of safety and security culture – are the licensing process and its enforcement **[*2*]**. In Germany and the United States considerations for cyber security are explicitly detailed in the licensing process and in the certification process of individual systems.

E. Associated regulatory activities

From supply chain control, to personnel security, to law enforcement training, many different issues may have a strong impact on the cyber security of nuclear facilities. Regulatory activities for nuclear facilities should encompass and characterize how threat assessment is done, how cyber security training is integrated in the programme, whether the nuclear supply chain is regulated, and whether cyber security is a component of those regulations. It is noteworthy that the United States and South Africa are nations that involve national intelligence agencies in the preparation of threat information and that this information is made available directly to nuclear facilities using the Design Basis Threat (DBT) model to communicate threats to facilities.

F. Cyber Security Education

Countries with very strong structure for nuclear facilities such as China and Russia, offer national level education and degree programmes in nuclear security. The majority of the countries delving into nuclear

facilities usage have educational programmes in cyber security, offered through universities. For example, Departments of Cyber Security now exist in Nigerian Universities. Although these programmes are new, often in their beginning stages, and the curriculum does not have contents that addresses nuclear cyber security. Russia, as of today, is one country where a national educational program for nuclear information technology (IT) and/or cyber security exists. Centers of higher education focused on cyber security or nuclear security can provide research, fundamental to advancing the field, as well as a highly trained workforce, which is necessary to ensure the adequate level of competence in the facilities **[*2*]**.

III. Analysis of Model Frameworks and Standards

This section provides detailed overview of cyber security Standards, Frameworks and Requirement specifications for addressing security vulnerabilities in IT/ICS systems used in NPPs. Cyber security Standards are set of specifications for the cyber security of I&C systems used in NPPs. A Framework is a risk-based approach to reducing cyber security risk. It comprises of three (3) parts: the Framework Core, the Framework Implementation Tiers and the Framework Profile **[*32*]** as shown in Figure 3.1.

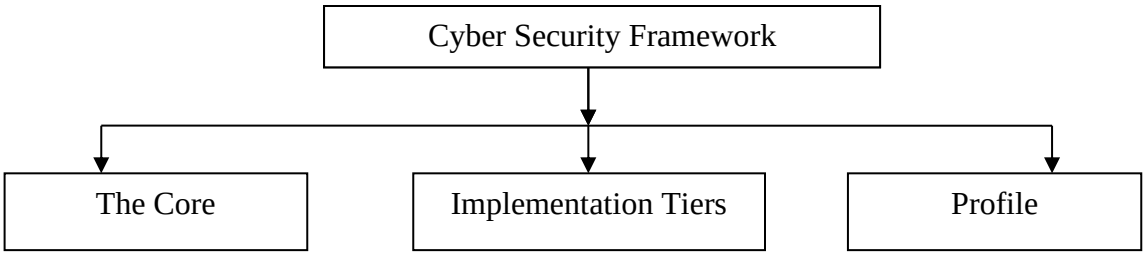

Figure 3.1: Cyber security Framework structure

The Framework Core is a set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. It comprises of four (4) types of elements: Functions, Categories, Sub-categories, and Informative References. The Framework Implementation Tier is a lens through which to view the characteristics of an organization's approach to risk - how an organization views cyber security risk and the processes in place to manage that risk. The Framework Profile is a representation of the outcomes that a particular system or organization has selected from the Framework Categories and Sub-Categories **[*32*]**.

In other to address the security vulnerabilities arising from cybersecurity threats, several frameworks have been developed by industry standardization organizations, International and national nuclear regulatory agencies like: the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), Institute of Electrical and Electronic Engineers (IEEE), Nuclear Energy Institute (NEI), International Atomic Energy Agency (IAEA), National Institutes of Standards and Technology (NIST), U.S. Nuclear Regulatory Commission (U.S.NRC), Canadian Nuclear Safety Commission (CNSC), the Korea Institute of Nuclear Safety (KINS) etc. These frameworks are vital tools that can be leveraged to systematically address cyber security concerns in the nuclear sector.

According to the U.S. Department of Homeland Security (DHS), the Nuclear Sector has a long history of addressing cyber security issues. In 1997, through the Nuclear Energy Institute (NEI), the industry began looking at potential issues associated with the increasing use of digital technologies at power reactors. At this time there was a concern regarding the potential impacts associated with the change in millennia—referred to at that time as the “Y2K” issue. Following the terrorist attacks of September 11, 2001, the industry turned its focus to potential cyber security-related issues. In January 2002, NEI established a Cyber Security Task Force (CSTF), initially composed of 23 members, to provide an industry-wide forum

for identifying, discussing, and resolving cyber security issues. In March 2002, the NRC issued Interim Compensatory Measures (ICM) Orders that directed licensees to consider and address cyber safety and security vulnerabilities **[*32*]**.

During 2003 and 2004, the industry was engaged in the development of guidance documents intended to support the uniform implementation of cyber security programs at power reactors. In July 2003, cyber security assessment pilots were completed at four U.S. nuclear power reactors. These pilots were designed to inform development of NUREG/CR-6847, "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants." The project team consisted of representatives from the Pacific Northwest National Laboratory (PNNL), the NRC, and the CSTF. NUREG/CR-6847 was released in November 2004. In November 2005, NEI released NEI 04-04, "Cyber Security Program for Power Reactors," Revision 1. NEI 04-04 provides guidance on establishing and maintaining a cyber security program and incorporates assessment methodology described in NUREG/CR-6847.

The NEI 04-04 program provides for the cyber security protection of all systems in the plant including those necessary for reliable electrical generation. The guidance provides a risk-informed approach, where consequences to plant functions are considered, and provides guidance on establishing a site cyber security defensive strategy incorporating multiple defensive layers with increasing levels of security protection. NEI 04-04 also provides guidance on incorporating cyber security considerations into the procurement process. The NEI 04-04 program includes the following steps **[*32*]**:

- Define current cyber security program
- Identify Critical Digital Assets (CDAs)
- Validate configuration
- Assess susceptibility
- Assess consequences
- Determine risk
- Refine defensive strategy
- Continue program management.

In December 2005, the NRC informed NEI by letter that Nuclear Energy Institute (NEI) 04-04, "Cyber Security Program for Power Reactors," Revision 1, dated November 18, 2005, is an acceptable method for establishing and maintaining a cyber security program at nuclear power plants. In 2006, the North American Electric Reliability Corporation (NERC) acknowledged that the NEI 04-04 program provides cyber security protection equivalent to the NERC Critical Infrastructure Protection (CIP) Reliability Standards **[*32*]**.

The nuclear industry established a Nuclear Strategic Issues Advisory Committee (NSIAC) that has the ability to establish initiatives binding to all nuclear power plants. The NSIAC is comprised of the Chief Nuclear Officers of each power plant site or fleet. Approved NSIAC initiatives are implemented at all U.S. nuclear power plants. In April 2006, the NSIAC established an initiative requiring nuclear power plants to implement NEI 04-04 within two years. All U.S. plants implemented the initiative by May 2008 **[*32*]**.

Power plants are required by the NRC to design, implement, and evaluate their physical and cyber security programs to defend against a Design Basis Threat (DBT). In response to the increasing threat of cyber-related attacks, the NRC amended its design basis threat requirements in 2007 to include a cyber-attack as an attribute of the adversary. The NRC describes a cyber-attack as:

> *"The capability to exploit site computer and communications system vulnerabilities to modify or destroy data and programming code, deny access to systems, and prevent the operation of the computer system and the equipment it controls."*

In March 2009, the NRC issued revised security requirements that included comprehensive programmatic cyber security requirements, principally codified in Title 10 of the Code of Federal Regulations (CFR), Section 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks" (Rule). The Rule requires power plants to submit a cyber security plan and implementation schedule for NRC review and approval. To support uniform implementation, the industry developed a template for the cyber security plan and the implementation schedule. In May 2010 the NRC endorsed NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6. NEI 08-09 provides a template for cyber security plans and a catalog of technical, operational, and management cyber security controls tailored from the NIST Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems," Revision 2. The template for the implementation schedule provides eight milestones—seven interim milestones and an eighth milestone for full implementation. The first seven milestones are designed to address the most prominent threats to the plant's most important systems **[*32*]**.

These milestones include the establishment of a cyber security assessment team, hardware-based isolation of key networks and assets, tightening controls over portable media and equipment, enhancing existing insider threat mitigation, instituting protective measures for digital equipment that could impact key safety systems, and establishing ongoing monitoring and assessment activities for implemented cyber security measures. By December 31, 2012, each plant completed the initial seven milestones. Post-2012 activities (the eighth milestone) include the completion of policy and procedural revisions that enhance existing capabilities, the completion of any remaining design-related modifications necessary to implement the cyber security plan, and institution of protective measures for lower consequence assets. In January 2013, the NRC began inspecting power plant cyber security program implementation of the initial seven milestones, and completed inspections at each power plant at the end of 2015 **[*32*]**.

The frameworks for providing cyber security controls at NPPs can be categorized into two (2) broad classes: International and Country-specific. These international publications are consistent with, and complement, international nuclear security instruments, such as the amended Convention on the Physical Protection of Nuclear Material CPPNM), the Code of Conduct (CoC) on the Safety and Security of Radioactive Sources, United Nations Security Council Resolutions (UNSCR) 1373 and 1540, and the International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT).

The structure of the legal framework as shown in Figure 3.2, which forms the basis for regulation, have Law, Act, decree and Statute as the principal legislation established by the national legislative body. It establishes the fundamental structures and concepts, sets infrastructure for regulatory control and defines out the scope of the legislation. Regulations are more specific in relation to nuclear Cybersecurity, are developed by the Regulatory Body, are issued by the legislative body, Ministry or Regulatory Body (varies depending on the national legal system). Licenses are authorizations issued by Regulatory Bodies as clearance to operate showing compliance with regulatory requirements as regards Cybersecurity. Regulatory documents include Codes of Practices (CoPs), Guidance documents et cetera. They are usually developed and issued by the Regulatory Body, give practice specific advice on how to achieve protection and safety requirements defined in legislation or regulations; may or may not be legally binding - other procedures might be followed to achieve the same protection and safety goals.

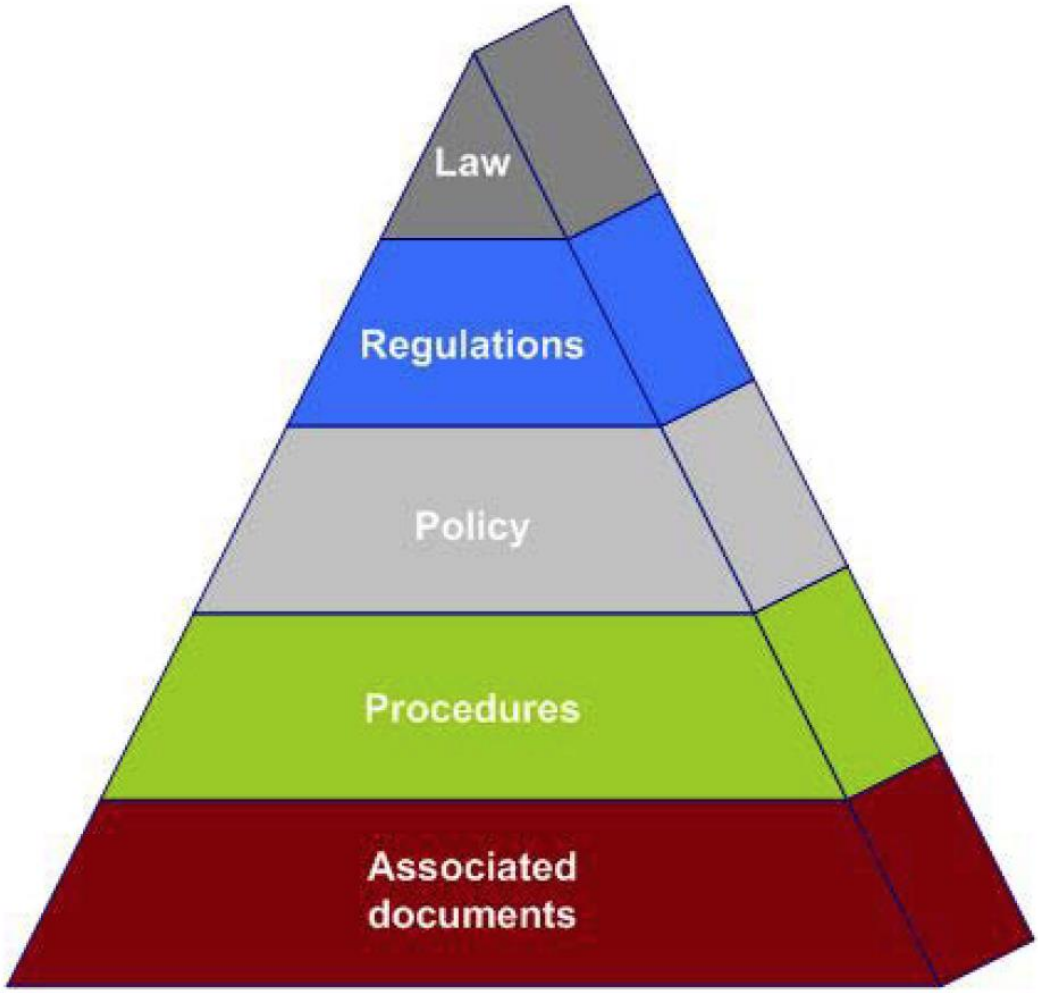

Figure 3.2: IAEA hierarchy of normative instruments for nuclear safety and security
Source: IAEA NSS No.17: Computer Security at Nuclear Facilities (Technical Guidance), p.9, 2011.

The international frameworks and Standards like IAEA publications in the IAEA Nuclear Security Series (NSS) and Basic Safety Standards (BSS) are issued in the following categories as shown in Figure 3.3:

- **Nuclear Security Fundamentals:** contain objectives, concepts and principles of nuclear security and provide the basis for security recommendations.
- **Recommendations** present best practices that should be adopted by Member States in the application of the Nuclear Security Fundamentals.
- **Implementing Guides** provide further elaboration of the Recommendations in broad areas and suggest measures for their implementation.
- **Technical Guidance:** publications include: Reference Manuals, with detailed measures and/or guidance on how to apply the Implementing Guides in specific fields or activities; Training Guides, covering the syllabus and/or manuals for IAEA training courses in the area of nuclear security; and Service Guides, which provide guidance on the conduct and scope of IAEA nuclear security advisory missions.

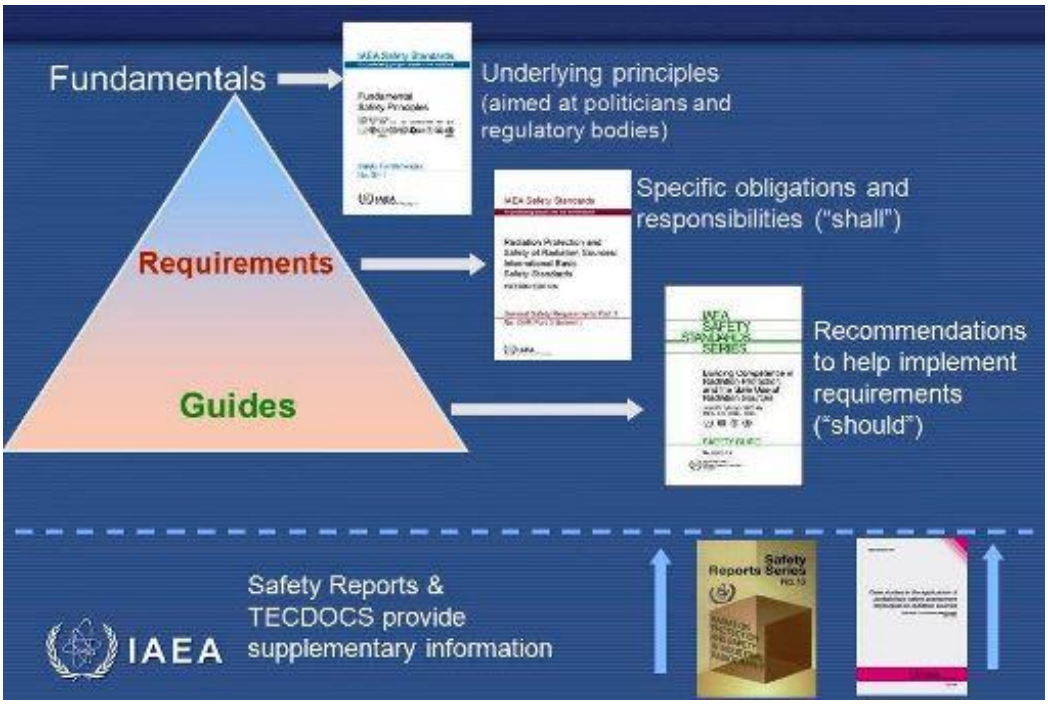

Figure 3.3: IAEA Safety Standard Series hierarchy
Source: IAEA NSS No.17: Computer Security at Nuclear Facilities (Technical Guidance), p.9, 2011.

The selection of a framework should be informed by baseline assessment, risk appetite and governance model. The primary consideration to be made by those with accountability for cyber security of nuclear facilities is ensuring that when implementing a framework, linkages and integration are created with the governance model, risk appetite, strategic plan and the broader enterprise risk management functions. It is also important to consider the broader regulatory framework and environment to inform framework selection. These nuclear cyber security frameworks are categorized into IAEA and country-specific frameworks. The lists of nuclear cyber security frameworks, requirements, guidance are provided in Tables 3.1-3.3, while Table 3.4 highlights the comparative analysis of the main requirements of IAEA Draft, U.S NRC RG 5.71 and IEC 62645 CDI.

Table 3.1: IAEA Nuclear Computer/Cyber Security Requirement Sources

.	Title of Publication	Type	Summary
1	IAEA Nuclear Security Series Number 20 (NSS 20): Objective and Essential Elements of a State's Nuclear Security Regime, 2013.	Fundamentals	Provide for the establishment of regulations and requirements for protecting the confidentiality of sensitive information and sensitive information assets.
2.	IAEA NSS 13: Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Rev 5), 2005.	Recommendation	Provides a set of recommended requirements to achieve the four Physical Protection Objectives and to apply the 12

			Fundamental Principles. Section 4.10 states: "Computer-based systems used for - physical protection, nuclear safety, and nuclear material accountancy and control should be protected against compromise (e.g. cyber-attack, manipulation or falsification) consistent with the threat assessment or DBT."
3.	IAEA NSS No. 17: Computer Security at Nuclear Facilities, 2011.	Technical Guidance	Provide guidelines to personnel designing, implementing, and managing I&C and information systems (IS) and networks at nuclear facilities. It addresses prevention and detection of potential attacks through reference to best practices in architecture, assurance and management of security information and I&C systems.
4.	IAEA NSS No. 23-G: Security of Nuclear Information	Technical Guidance	Provides guidance on implementing the principle of confidentiality and on the broader aspects of information security (i.e. integrity and availability). It specifically seeks to assist Member States in the identification, classification, and assignment of appropriate security controls to information that could adversely impact nuclear security if compromised.
5.	IAEA Defense in Depth in Nuclear Safety (INSAG 10), 1996.	Implementing Guide	Provide NPPs with DID implementing guidelines. Outlines five (5) levels of DID that should be sustained at NPPs.
6.	IAEA NSS No. 33-T: Computer Security of Instrumentation and Control Systems at Nuclear Facilities, 2018.	Technical Guidance	Provides guidance for the protection of I&C systems at nuclear facilities on

			computer security against malicious acts that could prevent such systems from performing their SSEP functions. Its scope includes application of computer security measures to I&C systems, application of such measures to the development, simulation and maintenance environments of these systems.
7.	IAEA Computer Security for Nuclear Security (NST045), 2016.	Implementing Guide (Under development)	Provide guidance on developing, implementing and integrating computer security as key component of nuclear security. Applies to the computer security aspects of nuclear security regime.
8.	IAEA Computer Security Techniques for Nuclear Facilities (NST047).	Technical Guidance Under development)	Provides discussion on good practices for implementing computer security associated digital technologies at nuclear facilities.
9.	IAEA Computer Security of I&C Systems at Nuclear Facilities (NST036), 2016.	Technical Guidance	Provides guidance on implementing computer security controls across the life cycle of nuclear I&C and control systems.
10.	IAEA Conducting Computer Security Assessments (NST037), 2015.	TECDOC Series	Provides good practices for organizing and conducting computer security assessments associated with nuclear security.
11.	IAEA Computer Security Incident Response (NST038), 2015.	TECDOC Series	Provides good practices for implementing computer security incident response processes between competent authorities, operators, and technical support organizations.
12.	IAEA Computer Security during the Lifetime of a Nuclear Facility (NST051), 2016.	Technical Guidance	Provide guidance to States, competent Authorities and operators on appropriate nuclear security measures during the different stages

			in the lifetime of a nuclear facility. Covers nuclear safety, security and safeguards.

Table 3.2: International Standards Organizations Cyber Security Requirement Sources

.	Title of Publication	Type	Summary
1.	IEEE 7-4.3.2-2016: Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations, 2016.	Standard	This standard serves to amplify criteria to IEEE Std 603(TM)-2009, to address the use of programmable digital devices as part of safety systems in nuclear power generating stations. The criteria contained herein, in conjunction with criteria in IEEE Std 603-2009, establish minimum functional and design requirements for programmable digital devices used as components of safety systems.
2.	IEEE 1686-2013: Standard for Intelligent Electronic Devices (IEDs) Cyber Security Capabilities, 2008.	Reference	The standard defines functions and features to be provided in intelligent electronic devices (IEDs) to accommodate cybersecurity programs. It addresses security regarding the access, operation, configuration, firmware revision and data retrieval from an IED. Confidentiality, integrity and availability of external interface of the IED is also addressed.
3.	IEC 61513: Nuclear Power Plant - Implementation and Control Important to Safety General Requirements for Systems, 2011.	Standard	Provides requirements and recommendations for the overall I&C architecture which may contain either or both technologies. The main technical changes are alignment with the latest revisions of IAEA documents, alignment with the new editions of IEC 60880, IEC 61226, IEC 62138, IEC 62340, IEC 60987, alignment with significant advances of software engineering techniques and integration of requirements for staff training.
4.	ISO/IEC TR 13335-1: Information Technology - Guidelines for the Management of Information Technology Security, 2001.	Standard	Provide a standard for IT security. Consists of Five (5) parts: Concepts & models for managing & planning IT Security, Techniques for the Management of IT Security, Selection of safeguards & Management guidance on Network Security.

5.	ISO/IEC 27000:2009 ISO/IEC 27001:2005 ISO/IEC 27002:2005 ISO/IEC 27005:2008 ISO/IEC 27006:2007	Standard	Developed from BS7799 published in the mid-1990. The British Standard accepted by ISO/IEC as ISO/IEC 17799:2000 revised in 2005 and re-numbered in 2007 to align with other ISO/IEC 2700 series standards. It provides best practice recommendation on information security management for use by those with accountabilities for initiating, designing, maintaining information security management systems.

Table 3.3: Country-Specific Cyber Security Requirement Sources

.	Title of Publication	Country	Type	Summary
1.	NIST Special Publication 800-82 Rev 2: Guide to Industrial Control Systems (ICS) Security, 2014.	U.S	Standard	Provide guidance for securing ICS, including SCADA, DCS and other systems performing control functions. Outlines notional overview of ICS, reviews typical system topologies and architectures, identifies known threats and vulnerabilities to these systems etc.
2.	NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems, 2002.	U.S	Reference	Provide guidance for conducting risk assessments of Federal Information Systems and organizations, simplifying the guidance in SP 800-39. It satisfies the requirement of FISMA.
3.	NIST Special Publication SP 800-53A Rev 1: Guide for Assessing the Security Controls in Federal Information Systems in Organizations, 2008.	U.S	Reference	Provides guidelines for developing security assessment plans and associated security control assessment procedures that are consistent with SP 800-53, Revision 3 in all phases of the development life cycle.
4.	NIST Special Publication 800-53 Rev 3: Recommended Security Controls for Federal Information Systems and Organizations, 2009.	U.S	Reference	This standard supersedes NIST SP 800-53A Rev 1. It provides a set of security controls that can satisfy the breadth and depth of security requirements levied on information systems and organizations and that is consistent with and complementary to other established information security standards.
5.	NIST FIPS PUB 140-2: Security Requirements for Cryptographic Modules, 2002.	U.S	Reference	Is a Computer Security Standard used to approve cryptographic modules that include both software and hardware components? An

				initial publication was on May 25, 2001 and was last updated December 3, 2002.
6.	NEI 04-04 Rev 1/NEI 08-09 Rev 6: Cyber Security Program for Power Reactors, 2005/2010	U.S.	Rule	Provides a template for nuclear power reactor licensees with a means for developing and maintaining a cyber security program at their sites. The plan includes a defensive strategy that consists of a defensive architecture and a set of security controls that are based on NIST SP 800-82, Final Public Draft, Dated September 29, 2008, "Guide to ICS," and NIST SP 800-53, Revision 2, Recommended.
7.	NEI 10-04 Rev 2: Identifying Systems and Assets Subject to the Cyber Security Rules, 2012.	U.S.	Rule	Provide guidance on the identification of digital computer and communication systems & networks subject to the requirements of 10 CFR 73.54. Utilizes the licensee's Current Licensing Basis (CLB) to ascertain important-to-safety functions in the context of the NRC Cyber Security Rule.
8.	Nuclear Regulatory Commission (N.R.C) Regulatory Guide (RG) 5.71: Cyber Security Programs for Nuclear Facilities, 2010.	U.S.	Regulatory Guide	Provides comprehensive guidance to applicants and licensees on satisfying the requirements of 10 CFR 73.54 that the OMB approved under OMB control number 3150-002 by using NIST SP 800-53, Rev 3 framework.
9.	N.R.C Regulatory Guide (RG) 73.54: Protection of Digital Computer and Communication Systems and Networks	U.S.	Reference	Performance-based programmatic requirement that ensures that the functions of digital computers, communication systems, and networks associated with SSEP functions are protected from cyber-attacks. Licensees provide high assurance that digital computer and communication systems and networks are adequately protected against cyber-attacks, up to and including the design-basis threat (DBT), as described in 10 CFR 73.1, "Purpose and Scope".
10.	N.R.C Regulatory Guide 5.83 (RG 5.83): Cyber Security Event Notifications, 2015.	U.S	Rule	Addresses cyber security event notification requirements. Describes approaches and methodologies that staff of the U.S. N.R.C considers acceptable for use by NPP licensees

				when categorizing certain cyber security event, and the process for conducting notifications and submitting written security follow-up reports to the NRC for cyber security events.
11.	N.R.C Regulatory Guide (RG) 1.152 Rev 2 & 3: Criteria for Use of Computer in Safety Systems of Nuclear Power Plants, 2006. (U.S.)	U.S	Rule	Provided specific guidance to nuclear power plant licensees for use in the design, development and implementation of IT/ICS systems.
12.	Template for the Cyber Security Plan Implementation Schedule	U.S	Rule	Provides a template used by each operating power plant to establish the schedule for the implementation of their cyber security plans.
13.	Department of Homeland Security (D.H.S) Catalog of Control Systems Security: Recommendations for Standards Developers, 2009.	U.S	Reference	The catalog presents a compilation of practices that various industry bodies have recommended to increase the security of control systems from both physical and cyber-attacks.
14.	D.H.S Cyber Security Procurement Language for Control Systems, Version 1.8, 2008.	U.S	Reference	Summarize security principles that should be considered when designing and procuring control systems products (software, systems, and networks) and provide example language to incorporate into procurement specifications.
15.	D.H.S Cyber Security Assessments of Industrial Control System, 2017.	U.S	Reference	Covers the process of planning an ICS cyber security assessment, including how to select testing areas and reporting process.
16.	D.H.S Recommended Practice for Patch Management of Control Systems, 2008	U.S	Reference	The report recommends patch management practices for consideration and deployment by ICS asset owners. It specifically identifies issues and recommends practices for ICS patch management in order to strengthen overall ICS security.
17.	D.H.S Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-in-Depth (DID) Strategies	U.S	Reference	The report provides guidance for developing defense-in-depth strategies for organizations that use control systems networks while maintaining multi-tier information architectures.
18.	Regulatory Document (REGDOC) - 2.5.1: Design of Reactor Facilities - Nuclear Power Plants, 2014.	Canada	Regulatory Guide	Provides overall status of Canadian regulatory framework for cyber security, as well as key requirements of new CSA standard N290.7-14.

				Cyber Security aspects of Computer-based I&C systems.
19.	Korea Institute of Nuclear Safety Regulatory Guide - KINS/RG N08.22: Cyber Security for I&C System, 2009. (South Korea)	Republic of Korea	Regulatory Guide	Provides a framework for guidance in implementing cyber security controls at Korean NPPs.

Table 3.4: Comparative analysis of the main requirements of IAEA Draft, U.S NRC RG 5.71 and IEC 62645 CDI [*3*]

Document Categories	IAEA Draft (66 pages)	U.S NRC RG 5.71 (105 pages)	IEC 62645 CDI (37 pages)
Main entity and definition	Computer security (synonym of cyber security) is a particular aspect of information security related to computer-based systems, networks and digital systems. Information security - the security of any information regardless of the media used to store or transmit the information. Includes the preservation of the confidentiality, integrity and availability attributes of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.	There is no security definitions Cyber security – protection against cyber-attacks is meant.	No security definitions Computer security - reference to IAEA guidance The goal of the computer-based security is to protect the I&C systems from deliberate and intelligent attacks that may jeopardize overall plant safety and availability.
Security Control	Personnel security, Physical security, Nuclear security (in 1.2.1, not in Glossary) Management systems, Organizational issues, Implementing computer security.	Technical, Operational and Management control	11 security categories and Security Programme management.
Related documents	Site Security Plan Computer Security Plan (can be a part of SSP)	Cyber Security Plan Cyber Security Program	Security Programme Computer Security Plan

Requirements to vendors	It is paramount that the security department works closely with the contracts department to ensure that the security provisions are incorporated in each contract. When considered necessary, checks and audits should be made to ensure that the contracting organization's management system adequately addresses security issues, and that the organization's practices and measures are in compliance with the system.	There are no direct requirements, only from utility point of view	There are no direct requirements. Platform and application security are a part of operational security procedures.
Life cycle	Security management lifecycle (spiral shape)	Security lifecycle process (spiral shape)	Linear Life Cycle Implementation of Computer Security
Levels of Security	Five levels of security (strength of Measures)	Five levels of cyber security defensive architecture	Five levels of computer security protective measures

IV. Status and Examples of Digital I&C Systems in Nuclear Power Plants

Nuclear power plants (NPPs) rely on I&C systems for protection, control, supervision and monitoring. A typical unit has approximately 10 000 sensors and detectors and 5000 km of I&C cables. The total mass of I&C related components is on the order of 1000 tonnes. This makes I&C system one of the heaviest and most extensive non-building structures in any nuclear power plant. No globally comprehensive statistics are available on the numbers of plants with fully analog, fully digital or hybrid I&C systems. However, approximately 40% of the world's 439 operating power reactors, accounting for nearly all of the 30 countries with operating NPPs, have had some level of digital I&C upgrade to, at least, important safety systems. From another perspective, 90% of all the digital I&C installations that have been done have been modernization projects at existing reactors. 10% have been at new reactors. Of the 34 reactors currently under construction around the world, all of those for which construction began after 1990 have some digital I&C components in their control and safety systems.

In Japan, the first fully digital I&C system was integrated into the Kashiwazaki-Kariwa-6 advanced boiling water reactor (ABWR) in 1996, followed shortly by Kashiwazaki-Kariwa-7 (KK-7). Similar digital I&C systems are used in Hamaoka-5. Tomari-3, which will feature the first all-digital reactor control room, is scheduled to begin operation in 2009.

In China, Qinshan Phase III, with two 700 MW(e) CANDU reactors, and Tianwan-1 and -2, with two 1000 MW(e) VVERs, have fully digital I&C systems, including both the safety and control systems, and partly computerized, i.e. hybrid, human-system interfaces (HSIs). China's high-temperature gas cooled experimental reactor, the HTGR-10, also has fully digital safety and control I&C systems, plus a hybrid human-system interface in its main control room.

In the UK at Sizewell B, a 1250 MW(e) PWR, all automatic functions of the safety I&C systems are digital, and in the main control room, all the qualified displays used in the human-system interface are computerized.

In Russia, Kalinin-3, which was commissioned in 2004, is the first VVER-1000 equipped with digital I&C safety systems and digital process control systems. In addition, both its main and emergency control rooms have hybrid human-system interfaces. A dynamic simulator was also installed for the purpose of testing control functions.

In the Republic of Korea, three 1000 MW(e) PWRs are under construction (Shin-Kori-1 and -2 and Shin-Wolsong-1), all with fully digital I&C safety and control systems and hybrid human-system interfaces in the control rooms.

In the USA, 1978 was the last year in which construction started on a reactor that eventually came online. The US Nuclear Regulatory Commission (NRC) has therefore not had the same experience with digital I&C systems as have regulators in China, India, Japan and the Republic of Korea, where the expansion of nuclear power is centred. Partly as a result, digital systems have not yet been approved for use as safety systems in operating US NPPs. Figure 4.1 is a simplified illustration of a U.S case where the I&C systems for controlling the plant, on the left side of the figure, are digital (computers, digital data networks, automatic calculations, and microprocessor-based sensors), and the I&C systems for safety, labelled "protection" on the right side of the figure, are analog. The figure also illustrates the features of independence, redundancy, and diversity that are essential in I&C systems and are outlined below.

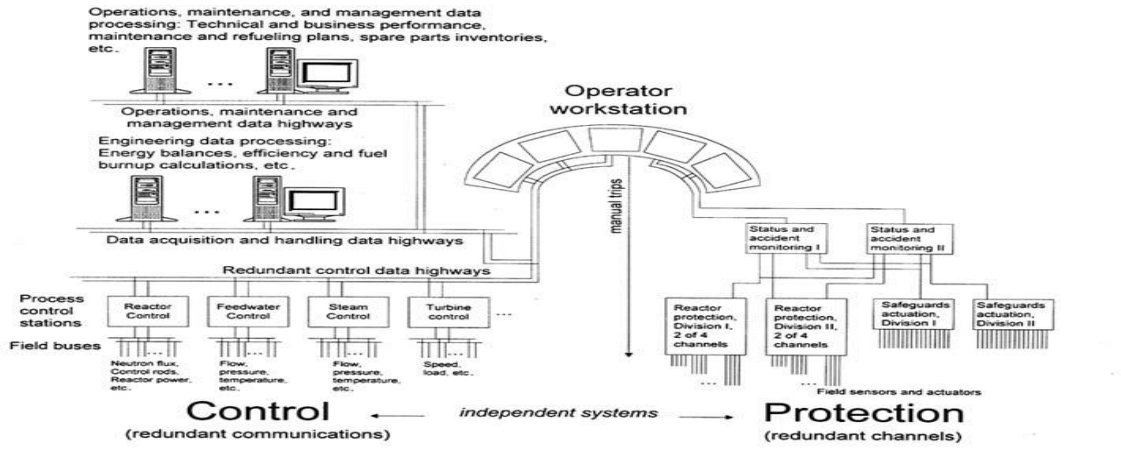

Figure 4.1: Typical I&C architecture for a plant with a digital I&C system for control and an analog I&C system for safety (labelled "protection" in the figure).
Source: US National Research Council, Digital Instrumentation and Control Systems in NPPs - Safety and Reliability Issues, 1997).

V. Cyber Security Regulatory Requirements for Nuclear Facilities

All nuclear power plant licensees are required by regulation to establish, implement, and maintain a cyber security program that provides a high assurance of adequate protection against cyber-attacks. There are three (3) distinct groups or types of requirements that the cyber security program must satisfy:

- Performance Requirements,
- Programmatic Requirements and
- Documentary Requirements respectively **[*33*]**.

This perspective provides a distinction between what outcomes are expected versus the necessary programmatic and documentary articles required to demonstrate the achievement of those outcomes **[*33*]**.

VI. Global Best Practice Recommendations on Nuclear Cyber Security for Regulators

Crafting a cyber security regulatory framework is a difficult and complex task for any nuclear regulator. The following global best practice recommendations, if strictly followed, will help in simplifying the process of implementing a robust nuclear cyber security defense system:

a) Adopt a risk-based cyber security framework for isolating critical digital assets (CDAs) by thoroughly analyzing systems and processes to classify their criticality and attack paths.
b) Institutionalize cyber security. The most challenging issue for nuclear cyber security is configuration integrity. The licensee must be compelled by the regulator to establish and demonstrate how configuration integrity is maintained in their facility.
c) Set the scope by limiting consequences of radiological hazards.
d) Demand verifiability and accurate system documentation on the digital characteristics of the plant systems, including details on system and network configuration, data flows, authorized software applications, engineering systems, etc.
e) Implement an active cyber defense system rather than being reactive to cyber threats.
f) Reduce digital complexity of CDAs as it complicates the task of securing CDAs.
g) Avoid blind adoption of information security concepts. Refer to concepts from safety and control systems engineering.
h) Get the cyber design basis threat right. Defining a DBT based on hackers and malware attack is too simplistic. Consider the design of modified products.
i) Implement a cyber incident response strategy. A sophisticated cyber-attack against a nuclear facility implies the risk of radiological release, thereby creating a hazard to public safety and compromising national security. Responding to such an event is not the sole responsibility of the licensees. Just like in the case of physical attacks, have a solid response plan ready and tell the licensees what you expect from them in terms of first response.

VII. Implications for Research and Practices

Based on the foregoing, the questions that result from the discourse are:

- What effect will an increase in the cost of cyber security/system protection have on nuclear renaissance?
- What is the overall lesson for nuclear-emerging countries like Nigeria when it comes to embracing cyber security as an important piece of nuclear power program implementation?

- At what point will a break in the link in Cyber Attack Sophistication model become a threat to safety or security in terms of operation or plant availability? It is necessary to answer these pertinent questions in order to properly situate the findings from our discourse in line with the evolution of nuclear facilities in developing countries such as Nigeria.

With regard to the first and second questions the cost benefit analysis of the nuclear renaissance, with all of its ramifications is skews positively, as the deliverables from nuclear energy provides many resources that result in earned revenue that can be used to address security issues. Although cyber security of nuclear facilities will increase the cost of operations, planning cybersecurity for nuclear facilities should be an integral part of the overall security processes and strategy. With regard to the third question, looking at the Cyber Attack Sophistication model, it is pertinent to mention that any form of vulnerability poses a major threat to the safety or security of nuclear facilities in terms of operation or plant availability.

VIII. Lessons Learned

The various cyber security incidents reported in this paper and vulnerabilities of I&Cs deployed in NPPs around the world hold important lessons for the cyber security of nuclear facilities and critical digital infrastructure in general.

a. The notion of airgap separating control and protection sections of NPPs has been proved wrong. The case of Davis-Besse NPP shows that this is a misconception. Operators who try to monitor and protect every connection cannot be sure they know about all of them. Stuxnet was transmitted via thumb drives to infect computers that were not connected to the internet.

b. Security vulnerabilities as a result of digital I&C deployment across CDAs are more complicated than earlier thought by alarmists and sceptics.

c. The various cyber security incidents reveal that Process Control Systems (PCSs) are not immune from attacks since they are different from ordinary computers as widely believed.

d. There is need for an understanding of current cyber security challenges and threat. NPPs responsible for power generation, enrichment and storage are complex computing environments consisting of hundreds to thousands of individual devices. These devices and computer systems that manage them are built from a combination of common, off-the-shell (OTS) computing technologies and custom, one-of-a-kind hardware, software and networking protocols. The only commonality between these facilities is that a large number of their critical systems tend to be built on legacy technologies. The current ad hoc approach to computer security that attempt to detect and block cyber-attacks using intrusion detection systems (IDS) is attack-centric and needs to change to a proactive, risk-based approach.

e. Due to dynamic and complex threat landscape confronting computer systems deployed at NPPs, a new approach to computer security is needed, centered on sound principles and technologies that can be used to construct effective defenses. The vulnerability-centric security approach seeks to address the root cause of system insecurity - system vulnerabilities - and creates the opportunity for security to be more constructive.

IX. Summary and Conclusion

From this study, only three out of the five countries possess written cyber regulations (U.S.A, Germany and Russia); China and South Africa do not have these regulations. The diversity in the ways in which cyber capabilities can be used poses one of the greatest challenges in Information technology. Computer security must be an essential component in an effective and robust nuclear security regime, so as to guard against increasingly sophisticated cyber threats in a digitally dependent environment. Nonetheless, particularly the computers used in safety and safety-related systems must be very well protected from possible intrusions. But other computers must be protected as well. The computers used to control the plant are essential to assure the continuity of power production. The computers used to control access to sensitive areas are needed both to prevent unauthorized access that might be part of an attack, and to assure authorized access both for safety and security reasons. Computers that store important and sensitive data have to be protected to assure that those data are not erased or stolen. Possible cyber-attacks could be associated with business espionage, technology theft, a disgruntled employee, a recreational hacker, a cyber activist, organized crime, a nation state, or a terrorist organization.

X. Works Cited

1. C. Haney, Cyber Security (2013), (available at https://www.nrc.gov/docs/ML1319/ML13198A405.pdf).

2. G. Gluschke, “Cyber Security at Nuclear Facilities: National Approaches” (Research project, Institute for Security and Safety, Fachhochschule Brandenburg University of Applied Sciences, randenburg an der Havel, Germany, 2015), (available at https://media.nti.org/pdfs/Cyber_Security_in_Nuclear_FINAL_UZNMggd.pdf).

3. V. Sklyar, Cyber Security of Safety-Critical Infrastructures: A Case Study for Nuclear Facilities. *Inf. Secur. Int. J.* **28**, 98–107 (2012).

4. M. Abadi, R. Needham, Prudent Engineering Practice for Cryptographic Protocols. *IEEE Trans. Softw. Eng.* **22**, 6–15 (1996).

5. D. E. Bell, L. J. L. Padula, Secure computer systems: Mathematical foundations, MTR-2547, Vol. I-III. *MITRE Corp. Bedford MA Tech Rep* (1973).

6. D. E. Denning, A Lattice Model of Secure Information Flow. *Commun. ACM*. **19**, 236–243 (1976).

7. A. C. Myers, B. Liskov, A Decentralized Model for Information Flow Control. *ACM SIGOPS Oper. Syst. Rev.* **31**, 129–142 (1997).

8. B. W. Lampson, Protection. *ACM SIGOPS Oper. Syst. Rev.* **8**, 18–24 (1974).

9. R. L. Rivest, A. Shamir, L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM*. **21**, 120–126 (1978).

10. J. H. Saltzer, Protection and the Control of Information Sharing in Multics. *Commun. ACM*. **17**, 388–402 (1974).

11. S. D. Applegate, A. Stavrou, in *2013 5th International Conference on Cyber Conflict (CYCON 2013)* (2013), pp. 1–18.

12. M. Bishop, "A Taxonomy of Unix System and Network Vulnerabilities" (Technical report CSE-95-10, Department of Computer Science, University of California at Davis, Davis, California, 1995), (available at http://www.windowsecurity.com/uplarticle/1/ucd-ecs-95-10.pdf).

13. S. Noel, Sushil Jajodia, B. O'Berry, M. Jacobs, in *19th Annual Computer Security Applications Conference, 2003. Proceedings.* (2003), pp. 86–95.

14. J. D. Howard, thesis, Carnegie Melon, Pittsburgh, PA (1997).

15. K. S. Killourhy, R. A. Maxion, K. M. C. Tan, in *International Conference on Dependable Systems and Networks, 2004* (2004), pp. 102–111.

16. J. Mirkovic, P. Reiher, A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. *ACM SIGCOMM Comput. Commun. Rev.* **34**, 39–53 (2004).

17. C. Simmons, C. Ellis, S. Shiva, D. Dasgupta, C. Wu, AVOIDIT: A Cyber Attack Taxonomy (2009).

18. I. N. Fovino, A. Coletta, M. Masera, Taxonomy of security solutions for the SCADA sector. *Proj. ESCORTS Deliv.* **2** (2010).

19. B. Zhu, A. Joseph, S. Sastry, in *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing* (IEEE, Dalian, China, 2011; http://ieeexplore.ieee.org/document/6142258/), pp. 380–388.

20. M. Assante, P. Stoutland, A. Van Dine, "Outpacing Cyber Threats: Priorities for Cyber Security at Nuclear Facilities" (CN-244-64, Nuclear Threat Initiative, Washington, D.C., 2016), (available at https://media.nti.org/documents/NTI_CyberThreats__FINAL.pdf).

21. "Nuclear Security - Measures to Protect Against Nuclear Terrorism | Amendment to the Convention on the Physical Protection of Nuclear Material" (GOV/INF/2005/10-GC(49)/INF/6, International Atomic Energy Agency, 2005).

22. Republic of South Africa, *Nuclear Energy Act, Act No. 46 of 1999* (https://cisp.cachefly.net/assets/articles/attachments/03513_nucenergact46.pdf).

23. The Government of the United States of America, *An Act to Amend the Atomic Energy Act of 1946, as Amended and for Other Purposes* (1954), vol. 68 Stat. 919.

24. Bundestag, *Act on the Peaceful Utilization of Atomic Energy and the Protection against its Hazards (Atomic Energy Act(*.

25. Government of Russia, *Regulation of the System of State Accounting and Control of Nuclear Materials* (2008), vol. 352.

26. Government of Russia, *Rules of Physical Protection of Nuclear Material, Nuclear Facilities, and Nuclear Material Storage Points* (2007), vol. 456.

27. Republic of South Africa, *Electronic Communications and Transactions Act, 2002, No. 25* (https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf).

28. Republic of South Africa, *Minimum Information Security Standards* (1996).

29. Duma, *On Information, Information Technologies, and Information Protection* (2006; http://asozd2.duma.gov.ru/main.nsf/%28Spravka%29?OpenAgent&RN=89417-6), vols. 89417–6.

30. Bundestag, Taking Advantage of Opportunities - Avoiding Risks (Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes). *Ger. Fed. Off. Inf. Secur.* (2009), (available at https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html;jsessionid=95DD7F9A952823A2B846929BC7E232E6.2_cid503).

31. G. Gluschke, M. H. Casin, *Cyber Security Policies and Critical Infrastructure Protection* (Institute for Security and Safety Press, 2018).

32. US Department of Homeland Securitu, "Nuclear Sector Cybersecurity Framework Implementation Guidance for U.S. Nuclear Power Reactors" (Implementation Guide, United States Cybersecurity and Infrastructure Agency, 2019), (available at U.S. Department of Homeland Security (DHS) Nuclear Sector Cybersecurity Framework Implementation Guidance for U.S. Nuclear Power Reactors).

33. Perry Pederson, Regulating Nuclear Cyber Security: The Core Issues. *Data-Driven OTICS Secur. Langner* (2015), (available at https://www.langner.com/2015/01/regulating-nuclear-cyber-security-the-core-issues/).

Author(s)

Professor LONGE Olumide holds a PhD degree in Computer Science (Information Systems Security Specialization) from the University of Benin, Benin City Nigeria; a Master's degree in Computer Technology (Information Systems) from the Federal University of Technology Akure, Nigeria, a BSc in Computing from the University of Benin, Benin City, Nigeria and National Diploma in Electrical/Electronic Engineering from the Federal Polytechnic, Ado Ekiti, Nigeria. A recipient of several national and international awards and recognitions, he is an alumnus Fulbright Scholar, Google Scholar, MacArthur Scholar and an alumnus MIT Scholar. Prof Longe has had a Progressive and accomplished academic and professional career demonstrating consistent success in research and development, professional impact, national, regional and global recognition and assuring students success. He is Seasoned in conceiving management information systems theories (evidenced by scholastic publications), and initiatives in ICT diffusion and uptake. Longe has been named by Microsoft research as one of the leading experts on privacy and security research in Africa. Prof Longe has been honored both locally and internationally for initiating research collaboration and exchange programs. He was at a time the lead researcher on the New Partnership for Africa's Development (NE PAD) Council's Cyber Security Program for Africa. His current research focuses on Management Information Systems Security, social and enterprise informatics (using ubiquitous computing and social theories to aid management decision making processes). He is also involved in Cyber criminality profiling for identifying causation, assisting apprehension and providing treatments for cybercrime cases.

Dr. Agozie Eneh is a Senior Lecturer in Computer Science. His research interests include computer network security, analysis of authentication protocols, performance evaluation of systems, optimization theories, and communicating sequential processes. He teaches on both the undergraduate and postgraduate programmes of Computer Science and has supervised several projects since joining the University of Nigeria. Dr. Eneh has worked both in the private and public sectors of the economy before joining the world of academia.

Uchechukwu Christian Arinze is a Doctoral candidate in Computer Science at the University of Nigeria. He holds B.Sc and M.Sc in Computer Science. As a WINS Academy Certified Nuclear Security Professional, his research interest in addition to nuclear security, Safeguards and non-proliferation spans the development of improved algorithms for Congestion Control in Wireless Telecommunication and Data Communication Networks, Data center costing models; numerical algorithms, cloud computing, big data and Database systems. He has broad range of professional certifications in Computer Security, Radiation Detection Techniques for Front Line Officers (FLOs); Transport Security; Information and Computer Security; Nuclear Material Accounting and Control (NMAC);Radiological Crime Scene Management (RCSM); Physical Protection of Nuclear Material & Nuclear Facilities; Introduction to Radioactive Sources and their Applications; Overview of Nuclear Security Threats and Risks; Nuclear Security Threats and Risks: Material & Facilities; Nuclear Security Threats and Risks: Material out of Regulatory Control (MoRC); Nuclear Security Threats and Risks: Cyber Threat; Preventive and Protective Measures against Insider Threats; Introduction and Overview of IAEA Nuclear Security Series Publications; Radiation Basics and Consequences of Exposure to Radiation. Others include: Texas A&M University Nuclear Security Science and Policy Institute (NSSPI) certificate of completion on the Nuclear Security and Safeguards Education Portal (NSSEP) in: Basic Nuclear and Atomic Physics; The Nuclear Fuel Cycle (NFC); Basic Radiation Detection; Threats to Nuclear Security; Nuclear Security Culture; Introduction to Statistics; Introduction to Safeguards and Security; Containment and Surveillance; Nuclear Material Accountancy; Spent Nuclear Fuel Safeguards; Uranium Enrichment Safeguards; Physical Protection Systems (PPS) and Insider Threats. As a World Institute for Nuclear Security (WINS) Alumni since 2016, he has enrolled and successfully completed the WINS Academy Foundation, Nuclear Security for Scientists, Technicians and Engineers (M-04S), Nuclear Security Regulation (M-09S), Nuclear Security Governance (M-02S) modules respectively - first to sit and pass the examination globally. He is currently an ICT Engineer with the Nigerian Nuclear Regulatory Authority (NNRA).