JISST
ISSN: 2545-5915

Journal of Information Science, Systems and Technology

Africa Regional Centre for Information Science, University of Ibadan, Nigeria
6 Benue Road, P. O. Box 22133, University of Ibadan, Nigeria 200001
Website: www.arcis.ui.edu.ng/jisst *Email:* jisst_arcis@ui.edu.ng ; jisst2015plus@gmail.com

Vol. 4, No. 3 (October 2020)

A Framework for Determination of Critical National Information Infrastructure in Nigeria

Uche M. Mbanaso [1]
uche.magnus@mbanaso.org

Victor E. Kulugh [1, 3]
vkulugh30@gmail.com

Julius A. Makinde [2]
julius.makinde@bazeuniversity.edu.ng

[1] Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria
[2] Computer Science Department, Baze University, Abuja, Nigeria
[3] Corresponding author

Abstract

Critical infrastructures (CI) at the national or organizational level is nowadays seen as both inclusive of and dependent on the Information Communications Technology (ICT) infrastructure for interconnecting and driving other infrastructures for sustained productivity, efficiency and growth. The interconnections that ICT facilitate through global and national networks however also make CI and Critical National Information Infrastructure (CNII) highly susceptible to malicious cyber-attacks sponsored by rival or antagonistic actors. Hence, nations must design and deploy strategic plans for CNII protection against such attacks. In Nigeria, the 2015 Cybercrimes (Prohibition and Prevention) Act empowers the President to designate and protect certain assets or services as CNII. However, there is currently no scientific framework or criteria in the country for determining which information assets, services and functions qualify as CNII. This paper presents a framework for identifying, characterizing and properly designating CNII in Nigeria based on descriptive, analytical and design research processes. The methodology entailed analysis and synthesis of concepts and ideas relating to CNII definitions, design, protection and management proposed or deployed for other countries. The outcome is a robust framework that defines logical steps for the identification, assessment and proper designation of CNI for Nigeria and possibly other developing countries. The research steps involved the characterization of CI, determination of CI dependencies on ICT, and measurement of the criticality of such dependencies. Planned future work would within the framework would then focus on the design and development of mathematical and computational constructs, algorithms to create automated tools for the computation, visualisation and comparison of the criticality metrics different components of CNII.

Keywords: Critical Infrastructure, Information Communication Technology, Critical National Information Infrastructure, Cybersecurity, Nigeria

1. Introduction

Infrastructure refers to interconnected basic facilities, devices, systems, services or functions, and so on that enable modern society or part thereof to function effectively, efficiently and sustainably. Critical National Infrastructure (CNI) refers to various usually interconnected infrastructure which failure or malfunction due to manmade or natural causes may likely result to debilitating effects to national security, economic security, safety and well-being of citizens (Tatar, Gokce, & Gheorghe, 2017; U.S. Department of Homeland Security, 2013; White, 2014). Today, CI at national or organizational levels is usually heavily dependent on Information and Communications Technology (ICT) required to ensure and enhance productivity and reliability of service delivery to and from intended anywhere and anytime. ICT infrastructure that supports CI is usually referred to as Critical Information Infrastructure (CII), or Critical National Information Infrastructure (CNII) at the national level. These are systems of electronic devices, computers and communication networks (Suter, 2007), essentially integrated to improve the synergy, productivity, efficiency, and performance of CI or CNI. In the rest of this paper, CI, CII and CNII are used in their broader or narrower contexts to refer to any infrastructure of strategic importance in modern society.

ICT and cyber-enabled CI unquestionably bring enormous economic and social benefits to society (Maglaras et al., 2018; Mbanaso & Dandaura, 2015). But, the resilience of interconnected CI nationally also depends crucially on the security and reliability of global cyber networks, which themselves are vulnerable as prey target of cyber-attacks sponsored by diverse actors with varying persuasions, including state or non-state actors and terrorists, who exploit vulnerabilities inherent in cyber technologies (Mbanaso & Dandaura, 2015; Setola, Luiijf, & Theocharidou, 2017). Such attacks can incapacitate or bring a nation-state to a standstill in a manner that makes it unable to function to provide basic essential services to the public.

The distinction between CNI and CNII is blurring, and both can be referred to simply as subsets of Critical infrastructure (CI). Notwithstanding, there is a subtle distinction as argued by Harašta (2018) since there are still traditional CI that are not ICT supported. This distinction is often viewed from the perspective of unidirectional or bidirectional dependency on ICT (Bashir & Christin, 2008; Luiijf, Nieuwenhuijs, Klaver, Van Eeten, & Cruz, 2010). It implies that traditional CI can depend on CII, and CII can equally depend on CI, as they become increasingly interconnected or integrated into a digital society. Consequently, the concepts of dependency and interdependency can have numerous effects with some degree of complexity and sophistication (Tweneboah-Koduah & Buchanan, 2018). The perspective that CI supported by ICT can introduce bidirectional interdependency further reinforces the debate that the line between CNI and CNII is getting blurred.

In Nigeria, the 2015 Cybercrime Act (Federal Government of Nigeria, 2015) empowers the President to designate certain assets, services, facilities, or systems as Critical National Information Infrastructure (CNII), and accord such infrastructure adequate national protection. But, there are no globally uniform and standardised criteria for an infrastructure to qualify and be designated as CNI or CNII in all countries. Thus, each nation is expected to individually identify and designate its CNI or CNII criteria and frameworks in the context of its national mission, interests or strategic objectives. Moreover, despite the Act, there is currently no known established scientific model or practical framework for determining what constitutes CNII in Nigeria. To help bridge this gap, this article presents initial works and results from ongoing research to develop models and frameworks to support the identification and determination of assets, facilities, services, or systems that qualify to be designated as CNII in the country. The study considers the peculiarity of Nigeria as a developing country, especially the need to gauge, firstly, the level of digitalisation in the various sectors of the economy, and secondly, the measurement of the criticality of CI dependency on ICT in each sector.

This paper provides the conceptual definitions, research design, methodological perspectives and frameworks that dictated the important steps and phases of the study. Accordingly, this article provides:

i. A comprehensive blueprint or research design framework that guides the rest of the research, which can be helpful to other researchers in this area;

ii. A robust framework that can aid in the process of identifying, assessing, and determining which infrastructure can qualify as CNII in Nigeria;

iii. The need that CII should be correctly identified, assessed, and so designated, to guarantee effective and proportionate protection against malicious activities or disruptions;

iv. That the steps, phases, approaches and important lessons described in this paper can be particularly useful to developing countries that may need to identify and designate CNII properly, using a scientific approach.

This work also introduces novel concepts in the identification and designation of CNII, including Criticality Index Factor (CIF), which is a composite value that depicts the degree of importance of infrastructure; and Criticality Indicator Quadrant (CIQ), a visual mechanism to rank the CIF of organisations into four bands of the quadrant. CIQ helps to visualise and compare the CIFs of various CII assets and organisations relative to others, thereby grouping them for better prioritisation and protection.

The rest of the paper is organized as follows: Section 2 presents the background and related works; section 3 presents the research questions; section 4 describes the overall methodology that underpins the study; Section 5 presents the development of the conceptual framework for the identification and determination of CNII; section 6 discusses the main findings and insights of the research; section 7 provides the conclusion and planned future work.

2. Related works and frameworks

Infrastructure is the basic foundation for organised and structured facilities, systems, installations, services, etc. that provide the base for serving large populations for the proper functioning of modern society (Setola et al., 2017; UNCTAD, 2011). Infrastructure is man-made, consisting of technical structures, installations, or systems that facilitate the efficient delivery of goods and services to the public, economic growth or acceleration, and support national security. The notion of critical infrastructure differs from country to country due to differences in national environmental and contextual factors. For instance, Australian Government (2017) defines CI as *"physical facilities, supply chains, information technologies and communications networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic well-being of the nation, or affect Australia's ability to conduct national defence and ensure national security"*. Very similarly, CI is defined by the Government of Canada (Public Safety Canada, 2018) as *"processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government"*. And the United States ((USA Patriot Act, 2001) defines CI as *"systems and assets, physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health, and safety, or any combination of those matters."*

Nigeria's Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (Federal Government of Nigeria, 2015) defines CNII as *"certain computer systems and/or networks, whether physical or virtual and/or the computer programs, computer data and/or data traffic vital to this country that the incapacitation, destruction or interference of such systems and assets will have a debilitating impact on security, national or economic security, national public health, and safety or any combination of such matters as constituting critical national information infrastructure"*. Although the broader concept of CNI is not mentioned explicitly in the Act, it can be assumed that CNII was recognized as the ICT infrastructure and processes needed to interconnect, integrate and drive the various other critical traditional infrastructures in various others sectors of Nigeria's increasingly digital economy and society.

It can also be construed from various country-level definitions of CNI and CNII share common characteristics – the significance or criticality of the underlying national infrastructural assets that underpin and are needed for promoting the status, growth and national interests of each country and the social well-being of its citizens, as well as the criticality of the national information infrastructure needed to interconnects those infrastructural assets. The mutual parameters relate to the effects that can result from failures or disruptions whether natural events or manmade deliberate and targeted assaults and sabotage. While it can be true that countries can make deliberate efforts to contain natural failures, cyber threats are human originated with intents to either destroy, degrade or steal infrastructure assets. And they are becoming increasingly sophisticated as technology advances and society, infrastructures and activities become more digitally interconnected. Again, while every infrastructure serves a purpose, its significance, or the utility value (that is, the degree of criticality) to its dependents can differ across diverse environments. Consequently, the impact of failure or incapacitation can potentially affect society differently too. It is, therefore, important to pinpoint that due to resource constraints and limitations, it is impractical to protect all infrastructural assets equally (Izuakor & White, 2017). This reinforces the need to systematically propose models and frameworks and design strategies to identify, assess and designate CNI and CNII, as against the use of arbitrary or ad hoc approaches.

According to Serianu (2018), it is practically unfeasible to defend and protect critical assets without proper CII registry and defined national priorities. The uncertainty of the growing cyber risks suggests that risks associated with CII have to be nationally managed in a harmonized and coordinated fashion. Even if the task of identifying critical assets appear trivial, there are still unnerving challenges due to the complexity of CII dependency and interdependency (Luiijf et al., 2010; Mohamed, 2019; Tweneboah-Koduah & Buchanan, 2018). Equally, Izuakor and White (2017) contended that in the US, the government has continually grappled with CI assets identification amidst multiple critical assets and political disagreements on the basic criteria to determine CI.

The debate is that CII protection effort must start with correct identification based on defined metrics to ascertain the level of dependencies and degree of criticality (Moteff, 2005; Velasquez, 2016). The subject of critical infrastructure has continued to attract extensive studies about characterization, resilience, dependency, and interdependency, as well as a measure of criticality (Bloomfield, Popov, Salako, Stankovic, & Wright, 2017a; Kim & Kang, 2011; Kotzanikolaou, Theoharidou, & Gritzalis, 2013). The likelihood that a single cyber event has the potential to affect multiple critical infrastructures has been studied by (Kotzanikolaou et al., 2013), describing the high impact of common-cause failures as a result of CI dependencies and interdependencies, and it is vital to consider these factors when determining the criticality of an infrastructure (Panayiotis, Marianthi, & Dimitris, 2013). The foregoing underscores the fact that measurement of CI criticality is important for its identification, designation, and protection. It is the CI critical variables that define the degree of importance that countries should attach to the various components of their infrastructure which in turn should determine the suitable security controls including investment that should be applied to protect each component of the infrastructure.

Dependency has been categorised into physical dependency, cyber/informational dependency, geographic dependency, logical dependency, and social dependency (Rinaldi, Peerenboom, & Kelly, 2001), implying that dependency-interactions can bring multiple consequences that affect related infrastructures. Subsequently, CI failure has been characterised into cascading, escalating and common-cause (Bloomfield, Popov, Salako, Stankovic, & Wright, 2017b; Stergiopoulos, Vasilellis, Lykou, & Gritzalis, 2016). The work of Donzelli, Setola, & Tucci (2004) proposed a framework that identifies dependencies of an organisation on technological infrastructures, for evaluating the business impact of any possible failure, but did not provide scientifically define metrics for the evaluation.

Some existing critical infrastructure determination frameworks

As earlier alluded to, there are no global standards or criteria which all nations can apply without adaptations or modifications to the determination of which infrastructure can be designated as CNI or CNII. Certainly, it is the prerogative of every country or region to fashion out the modalities on how to identify, assess, and designate an infrastructure as a CNI or CNII.

Mattioli & Levy-Bencheton (2014) presented the methodology for the identification of critical information infrastructure assets and services for European member states. First, the authors discussed the current status and improvement aimed at building a defence for present and future cyber threats but identified "low-level maturity and lack of structured approach" by the member states, towards the identification of critical infrastructures in communication networks. The authors suggested two approaches: non-critical sector (non-CS) dependent and critical sector (CS) dependent. While the non-CS focuses on network architecture analysis, CS-dependent focuses on operator driven and state-driven processes. The CS-dependent approach is based on three steps: identification of critical sectors; identification of critical services; and identification of CII assets supporting critical services. These steps drew participation from the government and operators of critical infrastructure using a qualitative approach. One of the main drawbacks of the approach is that the selection of critical services is arbitrary, and not based on scientific principles, thereby not scientifically replicable. Being qualitative, the outcomes are mere narrative and descriptive of various states' experiences, which are not quantifiable and hence cannot be easily measured and comparatively analysed.

In Izuakor & White (2017), the key elements of the identification approach are drawn from the formal definitions of CI by nation-states, simplified and categorised under: (1) asset focus, which captures the characteristics of the assets that are critical to a nation; (2) consequences or concerns; and (3) the impact of the consequences on the nation and the population. This provided the philosophical understanding of the key components of critical asset identification without criteria on how to comparatively identify and categorise the assets.

Similarly, in (USA Patriot Act, 2001) critical infrastructure characterisation was examined from systems and assets perspective, as well as the consequences of potential incapacitation or destruction that may lead to debilitating impact. It provided the theoretical perceptions and identification of what is critical to the USA at a strategic level, and formulation of the National Infrastructure Protection Plan (NIPP) of the USA, (NIPP DHS, 2013). Furthermore, the Department of Defence (DoD) of the USA attempted to differentiate Defence Critical Infrastructure (DCI) and non-Defence networked assets and facilities for sustained military operations worldwide (US Department of Defense, 2016). The underlining philosophy aligned with the USA critical infrastructure identification, but from a defence operational perspective. Based on these consequences-based formal definitions of CI by the USA, the identification programme as outlined by the National Critical Infrastructure Prioritisation Programme (NCIPP) (USA Government Accountability Office, 2013) is driven by consequence thresholds based on fatalities, economic loss, mass evacuation duration and degradation of national security. The process involves the nomination of assets from states and federal partners, nominated assets are then benchmarked against the consequence thresholds, and an asset will qualify for the next level of evaluation if it meets two of the four consequences thresholds. Again, although, the approach is empirical, the major drawback is that the process is not scientifically repeatable and being qualitative, statistical analysis is too difficult to achieve comparatively. Besides, criticality in terms of dependencies and interdependencies are not adequately factored into the approach.

In the European Union (EU), there was an attempt to unify the identification and categorisation of CI asset, systems and functions across member states in the region (The Council of the European Union, 2008). In a further study (ENISA, 2014), the EU's approach to the identification of CII was based on three steps: identification of critical sectors, identification of critical services within the critical sectors, and finally, identification of critical information infrastructure supporting critical services. By implication, these steps are merely prescriptive without a concrete definition of scientific criteria that can be uniformly applied to achieve consistent and measurable results among member states. Besides, the methodology is restricted to communication assets. The European Programme on Critical Infrastructure Protection (EPCIP) (European Commission, 2012) CI identification methodology recommended a four-step approach that requires (1) member states to evaluate assets against sectorial criteria, (2) benchmark them against the formal definition of CI in the EU (The Council of the European Union, 2008), (3) national thresholds of consequences similar to those in NCIPP should then apply (if an asset meets this threshold, it can then move to the final stage) and (4) cross-border impacts evaluation. Again, the implication is that assets may be dropped in the process without having to be evaluated under the entire methodology. Also, apart from cross-border dependencies, other forms of dependencies were not considered. In another study (European Commission, 2009), Critical Dependencies of Energy, Finance and Transport Infrastructure on ICT Infrastructure was investigated without empirical data to support the determination of the CI level of dependency on ICT.

In Australia (Australian Government, 2010), the government is concerned about cyber-threats to critical information infrastructure and worried about the potential impact that can threaten public safety and confidence, economic security, Australia’s international competitiveness, or impediment of the continuity of government and its services.

In Nigeria, the Ministry of Communications and Digital Economy and National Information Technology Development Agency (NITDA) have formulated various policies that accelerated adoption of ICT as an enabler of modern economic growth (Jide Awe, Olatunji, & Oyebanji, 2014). The (Office of the National Security Adviser (ONSA), 2014) in a bid to formulate Critical Information Infrastructure Protection (CIIP), listed 15 critical infrastructure sectors as the basis to reduce cyber incidents to critical infrastructures. Again, while the policy effort provided the foundation for identification of CII sectors, the criteria that qualify an organisational asset as CII was lacking. Besides, this approach is simply narrow and never considered the intricacies of CI interdependency and criticality, since not all assets will have equal criticality.

There is a growing consensus within the CI research community that the increasing criticality and interdependencies of CIs are fuelled by continuous integration of ICT systems that operate the CIs (Kure, Islam, & Razzaque, 2018; Seppänen, Luokkala, Zhang, Torkki, & Virrantaus, 2018; Tweneboah-Koduah & Buchanan, 2018). This buttress the need for scientific and empirical approaches that can be used repeatedly to evaluate the extent of CI dependency on ICT and the criticality of this dependency based on statistical extrapolations. However, these previous studies mainly focused on developed countries which have already attained very high degrees of ICT dependency. The context of developing countries differs significantly as many of these countries are contending with the digitalisation of essential services or functions.

Consequently, while these approaches and frameworks influenced initial thinking in this research, the context of developing countries is taken into specific consideration. Thus, this work seeks to be scientific, empirical and risk-driven aiming to computationally quantify criteria parameters based on defined variable metrics and indicators. Moreover, besides identification, this work aims to deepen the understanding of the complexity of CI interdependency effects and attempt to quantify the dependencies, interdependencies and criticality in a bid to quantitatively establish the benchmark for the designation of CNII in Nigeria. In this way, various components of the CNII can be appropriately prioritised for relative protection, based on scientific and statistical approaches as opposed to using unscientific and ad hoc methods.

3. Research objectives and questions

Critical information infrastructures operate in multidimensional threat environments, which include human error, hardware and software defects, inefficient processes, flaws and weakness of systems as well as natural events (Hutchins et al., 2015). Considering the complexity of these operations (Carlsson, 2006), the study considered how these factors can amplify cyber risks and their direct relationship with the level of CI dependency on ICT infrastructure. Consequently, three main questions that direct the study are as follows:

i. What is the extent of CI dependency on ICT?
ii. What is the criticality of such CI dependency on ICT?
iii. What are the parameters to be considered when designating a CII as CNII?

These main research questions are framed based on the positivist outlook of the problem under study, which is scientifically driven through a quantitative approach. Implying that addressing the research questions will quantitatively expose the cyber risks of the infrastructure studied thereby providing the degree of importance of CII. Thus, our approach differs from the frameworks that influenced our work. Besides, the classification of the degree of importance of CII, it can provide useful insights on how to prioritise critical national information infrastructure protection. Thus, the answers to these three questions will support the proper identification, categorisation and designation of CNII in Nigeria.

4. Research design and methodology

In an attempt to answer the research questions, the research design took a holistic and pragmatic approach in methodology and philosophy. The CII operations span across the government and private sectors, and the individual, implying that these elements are vital to the context of the research design. Thus, Fig. 1 depicts the research design framework, which is a combination of descriptive, design and creation strategies, showing the components and phases that interrelate, and the different elements of the research leading to logical and coherent plan (Oates, 2006). It illustrates the necessary steps i.e. the research context, strategy, conceptualisation, framework, and model designs that support the investigation. The design and development of the framework are influenced by existing literature and relevant frameworks already described in section 2. The testing, verification and validation of the models will be based on the input of quantitative survey data from CII organisations, and the results will feature in future articles.

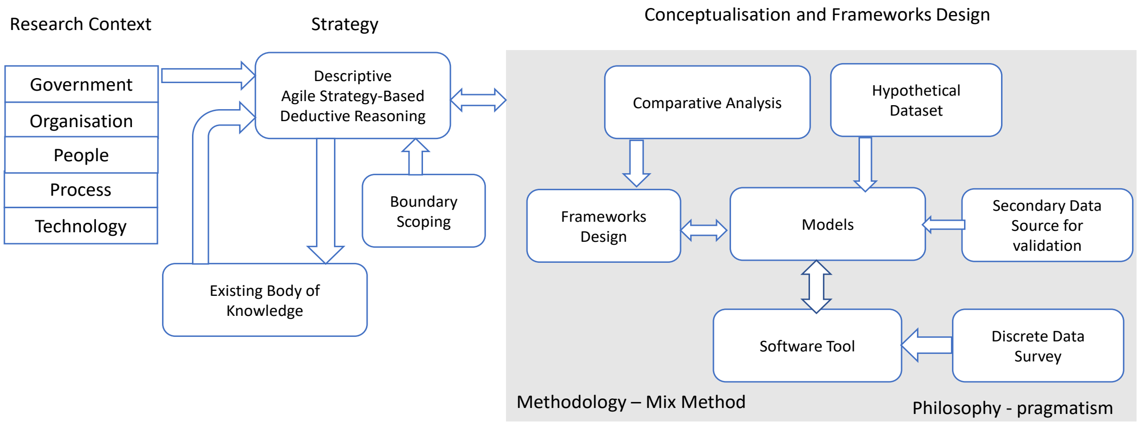

Fig. 1: Research Framework Design

The software tools will normally follow software development life cycle (SDLC), based on defined data structures, mathematical, computational, and statistical algorithms, for data generation, analysis, and visualization of the various findings. These phases as presented in Fig. 1 are explained as follows:

Phase 1: Research context

From a criticality measurement perspective, the underlying factors that influence how CII affects national security, the economy and well-being of citizens, and inter-relationships can be viewed from the backdrop of the government, CII organisation, process, people, and technology. The government plays a vital role in the CII protection and resilience; infrastructural dependency and interdependency factors affect organisations differently and should be considered. So, the research is situated within the context of the government, organisations, people, process, and technology, which are vital variables of importance to the study.

Phase 2: Implementation strategy

Cyberspace security breach events are unpredictable and require continuous research, assessment, and active solutions. The associated cybersecurity risks have made protection of CII an intricate task that requires dynamic approaches as opposed to static approaches. Thus, conceptually, this research is descriptive but requires an agile strategy (Dark, Linger, & Goldrich, 2015), to make it more interactive. The agile strategy helps the researcher to adopt a high iterative and adaptive methods that allow components of the research to be managed more effectively. Besides, it helps in the extensive review of related works and literature, which are the initial driver of the study. In the analysis, deductive principles are applied to ensure the reliability and objectivity of the effects of the variable factors. The primary source of data for model design and creation is accessible published documentation, along with the descriptive data source surveys, which are used to test, verify and validate the models.

Phase 3: Framework conceptualisation and design

The notion of ‘developing country’ influenced the very initial steps undertaken in the study. This informs the consideration of CI’s dependency on ICT - how much the traditional CI depends on ICT in quantitative terms, the degree of criticality of this dependency, and effects of CI relationships with other CIs, which can be unidirectional – dependency or bidirectional interdependency (Bloomfield et al., 2017b). This stage involves a mixed-method taking into consideration both quantitative and qualitative approaches. The numeric quantification of the metrics and indicators of measurements is key to the study. This phase characterises the core design of artefacts (or software tools), the testing, verification, and validation of the tools which are approached philosophically, from a pragmatic view in cognizance of various parameters.

5. Framework core

Arguably, not all traditional CIs completely depend on ICT to deliver their functions and services. However, it is anticipated that very shortly, the likelihood that most or all CI components will fully depend on ICT is high. This assumption influenced the conceptualisation of the framework models. Fig. 2 shows the abstract mapping view of the interrelation of dependency and interdependency that can exist among critical infrastructures. This depicts a complex structure of relationships, which exacerbates the multifaceted characteristics of determining the criticality of an infrastructure (Klinger & Cimiano, 2013).

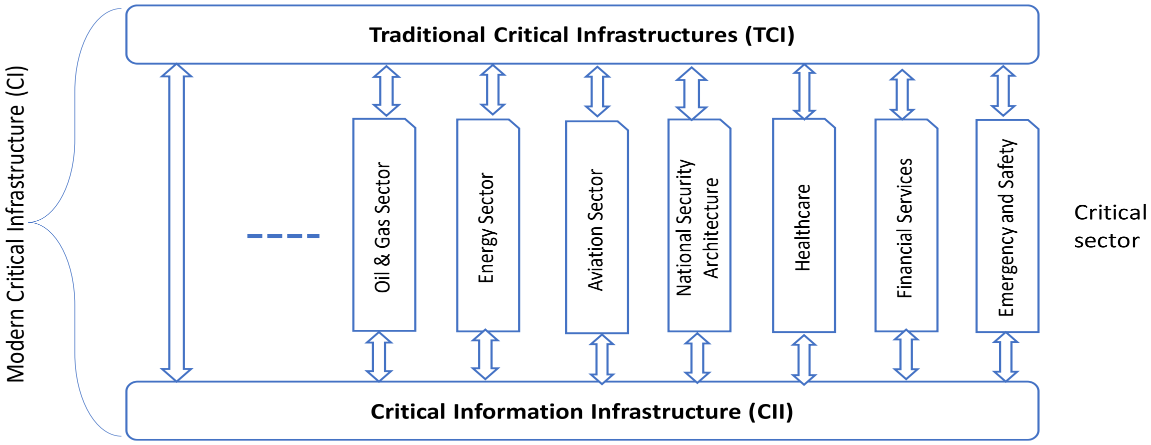
Traditional Critical Infrastructures (TCI)
Modern Critical Infrastructure (CI)
Oil & Gas Sector
Energy Sector
Aviation Sector
National Security Architecture
Healthcare
Financial Services
Emergency and Safety
Critical sector
Critical Information Infrastructure (CII)

Fig. 2: Interrelationships in Critical Sectors

The intricacy of dependency and interdependency can be viewed from internal and external dimensions spanning across physical, cyber, geographical, logical and social aspects of dependencies including operating environments, interconnectedness, and operational state (Argonne National Laboratory, 2015; Rinaldi et al., 2001). In Argonne National Laboratory (2015), it is viewed that cyber risk can be considered from the elements of vulnerability, threat, resilience, and impact. This implies that criticality is a function of risk, and cyber risk is not a static function. The implication is that the framework under consideration should be holistic and adaptive. More so, Fig. 2 illustrates that these structural maps of relationships have the potential to cause cascading and escalating effects or circular effects (Bloomfield et al., 2017b; Moteff, 2005).

Thus, the core framework design considers many causal variable parameters from the perspectives of ICT dependency, infrastructure dependency, and interdependency, the criticality of ICT dependency, environmental, logical, among other factors and indicators. Fig. 3 shows the core framework for the determination of infrastructure or assets as CNII. There are 8 core functional pillars, each pillar comprises sub-functions that may require the development of models or computational/mathematical components to support the dynamic quantification and summation of the variable factors. As shown, the determination of CNII depends on the influences of dependency and interdependency assessments and the quantification of criticality. This connotes that dependency, interdependency, and operational criticality should be quantitatively evaluated to determine the degree of importance of a CII. Also, the criteria should have a scale or a range since not all infrastructures will have equal criticality (Bloomfield et al., 2017b). The outcome provides the criticality value of a CII organisation's dependency on ICT and offers a single view to comparatively visualise critical sectors and organisations' criticality of dependency, i.e., the degree of importance of the various CIIs to support modern society (Fekete, 2011). The components, steps and interrelationships in the framework core are illustrated in Fig. 3, which are described further below.

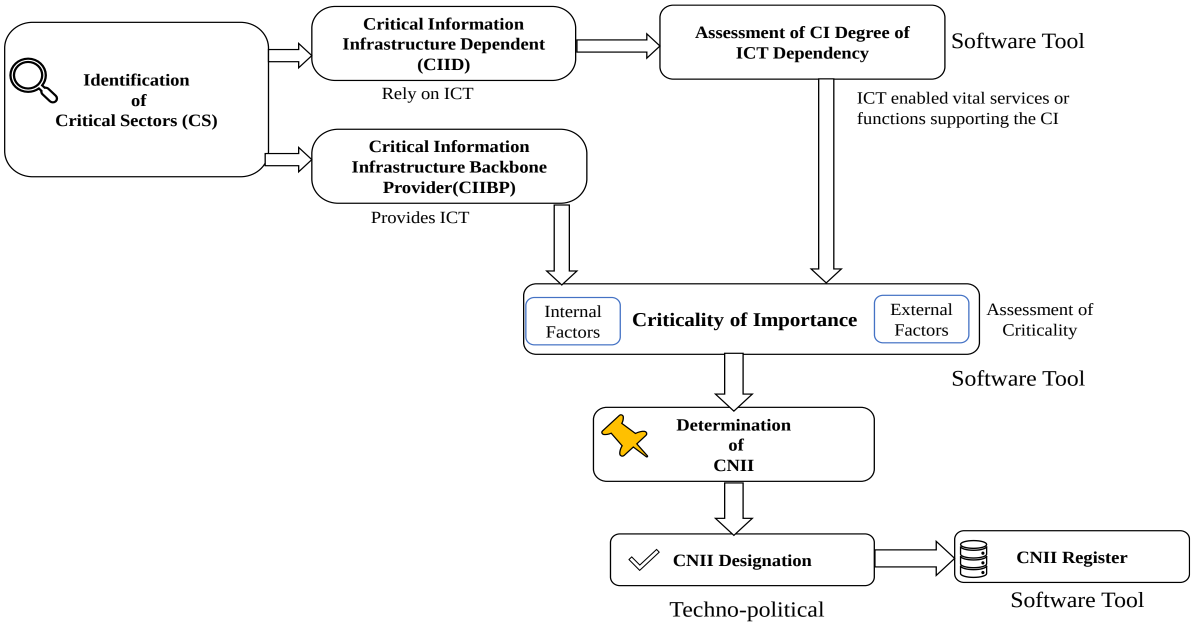
Identification of Critical Sectors (CS)
Critical Information Infrastructure Dependent (CIID)
Rely on ICT
Critical Information Infrastructure Backbone Provider(CIIBP)
Provides ICT
Assessment of CI Degree of ICT Dependency
Software Tool
ICT enabled vital services or functions supporting the CI
Internal Factors
Criticality of Importance
External Factors
Assessment of Criticality
Software Tool
Determination of CNII
CNII Designation
Techno-political
CNII Register
Software Tool

Fig. 3: The Framework Core

i. Identification of Critical Sectors (CS)

The first step in CI identification effort is to recognise the critical sectors (CS), which functions or services directly or indirectly significantly affect the wellness of modern society, as done in ENISA (2014) and European Commission (2012). The proper identification of critical sector organisations is a crucial precursor to determining CI's dependency on ICT; the list of critical services they provide, and their criticality, is crucial in determining the degree of importance of infrastructure. The initial asset baseline can be established accordingly as function-based, network-based, or logic-based (Izuakor & White, 2017). These concepts are described as follows:

a. The function-based approach also referred to as a mission-based approach, first, attempts to identify the functions that are critical to the mission of the asset under consideration. Subsequently, assets that support the functions can then be identified and evaluated against other variable factors.
b. In a network-based approach, all nodes and relationships in the system are identified, using the system mapping as a basis for the identification of their critical importance (Mattioli & Levy-Bencheton, 2014).
c. In the logic-based approach, assets are selected based on the best judgment of the investigator. A logic-based approach may complement other approaches in consideration of additional assets, external to the original scope. Intuitively, critical sectors are categorised into two: sectors that provide ICT infrastructure and sectors that depend on ICT, of which their services are critical to modern society. It is then assumed that the sector that provides ICT is already ICT dependent. And the sectors that depend on ICT require that their dependency on ICT should be gauged first instead of making an illogical assumption.

ii. Critical Information Infrastructure Dependency (CIID)

This refers to traditional CI that depends on ICT to correctly function and deliver optimal services to the society such as transport network, financial sector network, energy distribution, water supply, etc. that use components of ICT for improved efficiency and productivity. Presently, not all CIs depend on ICT; even those that depend on ICT may have varying degrees of ICT dependency. Consequently, it is important to identify those operations that are supported by ICT, the degree of ICT dependency, and the criticality of these dependencies. In methodologies for the identification of critical information infrastructure (ENISA, 2014), the third of the three steps outlined pointed to the identification of ICT infrastructure supporting critical society functions or services. However, the process of achieving identification was not highlighted. Also, there were no efforts in the work to measure the degree of dependency of CI components on ICT infrastructure.

iii. Critical Information Infrastructure Backbone Provider (CIIBP)

The CIIBP refers to communications networks infrastructure suppliers that provide the underlying connectivity, bandwidth, and other critical functions to other CI elements. This set of infrastructures do not need assessment of the degree of dependency on ICT, since they by default provide the underlying cyber infrastructure, but requires that criticality of their services or functions be quantified and properly categorised.

iv. Assessment of CI dependency on ICT

The developing world is grappling with digitalisation and the use of ICT to improve the way modern society is governed or services are delivered to citizens (Bilbao-Osorio, Dutta, & Lanvin, 2014). As a consequence, ICT infrastructures supporting CI remains underdeveloped with maturity level still low (WEF, 2016). So, there is the need to answer the pertinent question like *what exactly is the level of dependency of CI on ICT that can make it qualify as CNII?* The assessment of the degree of CI's dependency on ICT is a crucial task of the study. This assessment requires the identification of metrics and indicators as common underlying parameters that inform the measurements. These factors can be gauged in terms of their effects using a quantitative method. A software tool is required to automate the process based on a mathematical model, computational algorithms, and data structures.

v. Evaluation of criticality

The assessment of the criticality of a CII is an essential step to determining whether that infrastructure qualifies to be designated as CNII, which is essential to proportionate protection and resilience. Notably, an approach that can be used to conduct criticality assessment includes risk and impact assessments (Kotzanikolaou et al., 2013). Besides, consideration needs to be given to cross-sector effects and understanding the links to other dependent sectors. Some parameters need to be taken into account such as spatial distribution, severity (intensity or magnitude), effects of time (temporal distribution) as discussed in (Moteff, 2005). However, measuring the criticality of CII is a complicated task due to the diversity and complexity of the ICT environment that is constantly changing at a fast pace. As a consequence, factoring dynamic effect of failure in the context of social, economic, and environmental domains is vital. To automate the process, a mathematical model, computational algorithms, and data structures form the basis for the creation of a software tool to input data, analyse and visualise the criticality of the various identified CI elements.

CI dependency is a function of the level of coupling either directly or indirectly with other infrastructure. It is common knowledge that a single disruption or attack at one infrastructure is capable of extending the effects i.e. cascading consequences across the chain of CI elements. Against this backdrop, gauging dependency and interdependency to determine criticality is not trivial. This interconnectedness makes it incomplete to consider CNII without adequate analysis or understanding of the effects of a particular CI element vis-à-vis other elements. As stated in (Argonne National Laboratory, 2015), CI elements may have either unidirectional dependency or bidirectional dependency relationships. This gave rise to the definition of categories of dependencies as follows:

a. *Upstream dependencies (U_d):* Services provided by external infrastructure elements that are vital in supporting the operations and functions of a particular element.
b. *Internal dependencies (I_d):* Internal dependencies refer to the internal links among the assets making a particular CI element (e.g., a water-cooling mechanism is required to cool electrical generating plant).

c. *Downstream dependencies (D_d)*: The services provided by a CI element to other dependent infrastructures, i.e. consuming parties that may be affected in the event of failure or disruption.

The types of dependency are further classified into physical, cyber, geographic, logical and social (Rinaldi et al., 2001). The authors further described five elements that characterise dependency and interdependency namely: operating environment, coupling and response behaviour, type of failure, infrastructure characteristics, and state of operations (Rinaldi et al., 2001). These factors in some way can affect the criticality of the importance of a given critical information infrastructure.

vi. Determination of CNII

The determination of CNII is a function of service criticality that takes into cognisance, the effect of dependency and interdependency. Applying a quantitative approach, and a mathematical model that combines the inputs of the upstream dependency, internal dependency and downstream dependency, the criticality of importance can be computed to ascertain whether infrastructure can qualify as CNII. The computational outcome of the criticality measurement assessment is then aggregated into an overall score called Criticality Index Factor (CIF). The CIF, which is a composite value depicts the degree of importance, which is a derivation of the quantitative variable factors based on the mathematical and computational constructs. (The details of CIF constructs shall be presented in a subsequent article.)

Then, the concept of Criticality Indicator Quadrant (CIQ) is proposed to provide a mechanism to rank and place the CIF of assets/organisations visually into the four bands of the quadrant. The CIQ concept and framework helps to compare the CIFs of various CII organisations relative to other composite values, thereby grouping them according to their quad. This CIQ is, therefore, a pre-defined scale that supports the ranking of the CIF based on the division of the maximum achievable value of the CIF per CI or organisation, i.e. 1.00 by 4 to arrive at the 4 quads. The bands of CIQ are as defined in Table 1. A software tool based on the mathematical and computational constructs forms the basis for the automation of data generation and collection, analysis, ranking, and visualisation.

Table 1: Criticality Indicator Quadrant (CIQ) Description

	CIQ range	*CIQ Quadrant*	*CIQ Description*
Q1	0.00 – 0.25	Essential	Loosely achieved – the adoption of ICT is in its infancy
Q2	0.26 – 0.50	Important	Partially achieved – ICT in place, but not consistently and structurally organised; some important integration is lacking
Q3	0.51– 0.75	Critical	Largely achieved – ICT structurally implemented, only a few, and/or only minor integration is lacking
Q4	0.76 – 1.00	Highly Critical	Fully achieved – fully dependent upon CNII to function correctly and deliver services.

ii. CNII designation

In Nigeria, the protocol for the designation of infrastructure as CNII is a power vested by law on the President; however, the above-described frameworks and tools can then be used to facilitate evidence-based decision-making to that effect, instead of unscientific and arbitrary approaches. The CIQ provides a single view of each identified asset or organisation’s criticality level i.e., the degree of importance. In this way, the President can officially decorate an infrastructure and authorise it to be formally entered in the national CNII register.

iii. CNII Register

The concept of CNII Register is to maintain a database that formally gazettes all CNII sectors and their organisations with functional capability and profile mapping. This has numerous benefits. For instance, in time of crisis, it can quickly support the management of incident responses; it can form the basis for proportionate investment for CNII protection. The entries will contain all necessary updatable data required for the management of CNII protection and building of resilience. The register is a combination of software tools and managed database system based on data structures and algorithms.

6. Discussion

The concept of the designation of infrastructure as critical national infrastructure is not new, although it may be construed as a political activity, what is fresh is the underlying operational environments and complexity that exist today. The cyberspace and its infrastructure – computers, networks, functions, and the people element have altered the landscape of national risks. The characteristics of the new environment are such that a single operational failure of one infrastructure can heavily affect other infrastructures in what has been described as common-cause, cascading, and escalating effects (Clark, Berson, Lin, Science, & Board, 2015; Panayiotis et al., 2013). A good example is the interdependency relationships amongst transport networks, power grid networks, and communication networks, and with the notion of Supervisory Control and Data Acquisition (SCADA) (Maglaras et al., 2018), which can interconnect these networks for high productivity and efficiency. The interaction of constituent parts of these infrastructures can happen in multilayer fashion, therefore, further exacerbating the complexity in the degree of criticality (Banerjee, Das, Sen, & Science, 2017). The degree of criticality is a function of certain factors, and some infrastructures or assets may be more critical than others, buttressing the need for a common criterion to uniformly determine criticality. It implies that a variety of infrastructures can have a differing degree of importance, which should be quantified, ranked, and compared.

Consequently, the factors that contribute to the measurement of criticality, which includes: external factors, internal factors, and other dynamic value-sensitive factors should be taken into cognizance (Kim & Kang, 2011). The fact that any failure or disruption of any form can have debilitating effects to the extent of affecting other infrastructures implies that combined effects must be considered. Again, the perception of criticality can no longer be isolated among stakeholders but should be such that a better understanding of the value chain is taken into account. Thus, since the degree of criticality can be said to be directly proportional to the risk, critical sectors must have a uniform approach to CII protection and resilience (Gheorghe, Vamanu, Katina, & Pulfer, 2018). Equally, the criticality of infrastructure or asset is unlikely to remain static, as such value-sensitive factors have the potential to continuously alter the degree of criticality. Likewise, a particular infrastructure or asset may have a divergent degree of criticality in different environments. For instance, an internet bandwidth supply in the financial sector may likely have a high degree of criticality than the same internet bandwidth in the manufacturing sector (Kim & Kang, 2011). Another consideration is the depth of dependency (n^{th} order of dependencies); a minor failure or disruption i.e. relatively minor security incident in one CII may have the potential to cause escalating or cascading impacts to second or third order dependent CIIs. This brings the fact that identifying a multi-order dependency of infrastructures is vital to the cumulative effect or overall degree of criticality.

Hence, this paper presents a framework that provides comprehensive scientific and empirical constructs that can be used as a basis to identify, assess, and designate an infrastructure as CNII. It differs from the current state of research in this domain by approach and philosophy. Our work is scientifically based on design and creation research approach, and empirical-based on descriptive strategy using a mixed-methods approach. Besides, it has provided rigorous conceptual phases and designs, introduced new concepts, which are significant contributions to the body of literature. Also, the outcome can help the government and other stakeholders to understand the degree of criticality of various sector organisations. As a result, it has established a benchmark for risk-point of view rather than an arbitrary point of view, in a repeatable and uniform way.

7. Conclusion and future work

The development of a framework for assigning services or assets as critical national information infrastructure or CNII is a complex task. The function of criticality, dependencies, and interdependencies due to the complexity of interconnectedness are intricate issues to investigate. This is exacerbated by the characterization of diverse operational environments including, operational technology, operating conditions, interdependency behaviours, and coupling, category of failures, process characteristics as well as the operational state. Several variable factors influence the determination of the degree of criticality and can affect CI protection and resilience. The multilayer dimension of factors raised can lead to the proliferation of cascading and escalating effects, and this can bring difficulties. Therefore, this article provides scientific and empirical approaches to solving a multifaceted cybersecurity problem. Finally, the CNII determination is achievable by quantitatively combining the various effects of dependencies and criticality; and the representation of Critical Index Factor and Criticality Indicator Quadrant for better visualisation, ranking, and comparisons are novel constructs.

This article has provided a comprehensive conceptual framework that guides ongoing research in CNI and Cybersecurity towards developing a robust scientific model for the proper identification and designation of CII as CNII in Nigeria. The next stage of work will focus on the design and development of mathematical and computational constructs and tools for:

i. ICT Dependency measurement model
ii. Dependency and Interdependency of critical infrastructure measurements
iii. Degree of Importance or Criticality Measurement model
iv. CNII Register.

References

Argonne National Laboratory. (2015). *Analysis of Critical Infrastructure Dependencies and Interdependencies*. Retrieved from http://www.osti.gov/scitech/

Australian Government. (2010). Critical infrastructure resilience strategy. In *Report*. Retrieved from papers2://publication/uuid/C8ECF2E8-3ED2-4881-86E2-39F8F0581282%5Cnhttp://www.tisn.gov.au/documents/australian+government+s+critical+infrastructure+resilience+strategy.pdf

Australian Government. (2017). Australia-New Zealand Counter-Terrorism Committee. *Australian National Security*. Retrieved from https://www.nationalsecurity.gov.au/WhatAustraliaisdoing/Pages/Australia-New-Zealand-Counter-Terrorism-Committee.aspx

Awe, J., Olatunji, V., & Oyebanji, O. (2014). *ICT4D Strategic Action Plan Implementation Status Update and Illustrations Book*. Retrieved from http://nitda.gov.ng/wp-content/uploads/2018/07/ICT4D-SAPI-Book.pdf

Banerjee, J., Das, A., Sen, A., & Science, C. (2017). A Survey of Interdependency Models for Critical Infrastructure Networks. *Physics.Soc-Ph*. https://doi.org/DOI:3233/978-1-61499-391-9-1

Bashir, M. A., & Christin, N. (2008). Three Case Studies in Quantitative Information Risk Analysis. *Proceedings of the CERT/SEI Making the Business Case for Software Assurance Workshop*, 77–86.

Bilbao-Osorio, B., Dutta, S., & Lanvin, B. (2014). *The Global Information Technology Report 2014 Rewards and Risks of Big Data*. Retrieved from https://www.weforum.org/reports/global-information-technology-report-2014

Bloomfield, R. E., Popov, P., Salako, K., Stankovic, V., & Wright, D. (2017a). Preliminary interdependency analysis: An approach to support critical-infrastructure risk-assessment. *Reliability Engineering and System Safety*, *167*(March), 198–217. https://doi.org/10.1016/j.ress.2017.05.030

Bloomfield, R. E., Popov, P., Salako, K., Stankovic, V., & Wright, D. (2017b). Preliminary interdependency analysis: An approach to support critical-infrastructure risk-assessment. *Reliability Engineering and System Safety*, *167*(July 2015), 198–217. https://doi.org/10.1016/j.ress.2017.05.030

Carlsson, S. A. (2006). Design science research in information systems: A critical realist perspective. *ACIS 2006 Proceedings - 17th Australasian Conference on Information Systems*.

Clark, D., Berson, T., Lin, H. S., Science, C., & Board, T. (2015). At the Nexus of Cybersecurity and Public Policy. *At the Nexus of Cybersecurity and Public Policy*. https://doi.org/10.17226/18749

Dark, M., B, M. B., Linger, R., & Goldrich, L. (2015). Realism in Teaching Cybersecurity Research : The Agile Research Process A New Approach to Teaching Cybersecurity Research. *Conference: IFIP World Conference on Information Security Education, May 2015*, *2*, 3–14. https://doi.org/10.1007/978-3-319-18500-2

Department of Defense (DoD). (2016). *Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms*. *2010*(November 2010).

Donzelli, P., Setola, R., & Tucci, S. (2004). Identifying and Evaluating Critical Infrastructures - A Goal-driven Dependability Analysis Framework -. *Proceedings of the International Conference on Communications in Computing, CIC '04, June 21-24, 2004, Las Vegas, Nevada, USA*.

ENISA. (2014). *Methodologies for the identification of Critical Information Infrastructure assets and services*. https://doi.org/10.3892/ijmm.2018.3420

European Commission. (2009). *Final Report On Study on Critical Dependencies of Energy, Finance and Transport Infrastructures on ICT Infrastructure On behalf of the European Commission DG Justice, Freedom and Security*.

European Commission. (2012). *Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP)*. Brussels, Belgium, 2012.

Federal Government of Nigeria. *Cybercrimes (Prohibition, Prevention, etc) Act.*, 3 § (2015).

Fekete, A. (2011). Common criteria for the assessment of critical infrastructures. *International Journal of Disaster Risk Science*, *2*(1), 15–24. https://doi.org/10.1007/s13753-011-0002-y

Gheorghe, A. V., Vamanu, D. V., Katina, P. F., & Pulfer, R. (2018). Critical infrastructures, key resources, and key assets. In *Topics in Safety, Risk, Reliability and Quality* (Vol. 34). https://doi.org/10.1007/978-3-319-69224-1_1

Harašta, J. (2018). Legally critical : Defining critical infrastructure in an interconnected world. *IJCIP*, *000*, 1–10. https://doi.org/10.1016/j.ijcip.2018.05.007

Hutchins, M. J., Bhinge, R., Micali, M. K., Robinson, S. L., Sutherland, J. W., & Dornfeld, D. (2015). Framework for Identifying Cybersecurity Risks in Manufacturing. *Procedia Manufacturing*, *1*. https://doi.org/10.1016/j.promfg.2015.09.060

Izuakor, C., & White, R. (2017). *Critical Infrastructure Protection XI*. *512*, 27–41. https://doi.org/10.1007/978-3-319-70395-4

Kim, A., & Kang, M. H. (2011). Determining Asset Criticality for Cyber Defense. *Centre for High Assurance Computer Systems Information Technology Division, Naval Research Laboratory, Washington, DC 20375-5320*, *NRL/MR/155*.

Klinger, R., & Cimiano, P. (2013). Bidirectional Inter-dependencies of Subjective Expressions and Targets and their Value for a Joint Model. *Association for Computational Linguistics*, 848–854.

Kotzanikolaou, P., Theoharidou, M., & Gritzalis, D. (2013). Chapter 12 COMMON-CAUSE

FAILURES IN. In J. Butts & S. Shenoi (Eds.), *Critical Infrastructure Protection VII* (VII, pp. 171–182). https://doi.org/10.1007/978-3-642-45330-4

Kure, H., Islam, S., & Razzaque, M. (2018). An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. *Applied Sciences*, *8*(6), 898. https://doi.org/10.3390/app8060898

Luiijf, H. A. M., Nieuwenhuijs, A. H., Klaver, M. H. A., Van Eeten, M. J. G., & Cruz, E. (2010). Empirical findings on European critical infrastructure dependencies. *International Journal of System of Systems Engineering*, *2*(1), 3–18. https://doi.org/10.1504/IJSSE.2010.035378

Maglaras, L. A., Kim, K. H., Janicke, H., Ferrag, M. A., Rallis, S., Fragkou, P., … Cruz, T. J. (2018, March). *Cybersecurity of critical infrastructures* (Vol. 4, pp. 42–45). Vol. 4, pp. 42–45. https://doi.org/10.1016/j.icte.2018.02.001

Mattioli, R., & Levy-Bencheton, C. (2014). *Methodologies for the identification of Critical Information Infrastructure assets and services*. https://doi.org/10.2824/38100

Mbanaso, U. M., & Dandaura, E. S. (2015). The Cyberspace: Redefining A New World. *IOSR Journal of Computer Engineering*, *17*(3), 2278–2661. https://doi.org/10.9790/0661-17361724

Mohamed, A. A. A. (2019). On the rising interdependency between the power grid, ICT network, and e-mobility: Modeling and analysis. *Energies*, *12*(10). https://doi.org/10.3390/en12101874

Moteff, J. (2005). Risk Management and Critical Infrastructure Protection : Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences. *Science And Technology*, 1–29.

NIPP DHS. (2013). National Infrastructure Protection Plan - DHS. *Dhs*, (December), 1–57.

Oates, B. J. (2006). *Researching Information Systems and Computing*. SAGE Publications Ltd.

Office of the National Security Adviser (ONSA). (2014). *National Cybersecurity Policy*. Retrieved from https://cert.gov.ng/ngcert/resources/National_Cybesecurity_Strategy.pdf

Panayiotis, K., Marianthi, T., & Dimitris, G. (2013). Risk assessment of multi-order dependencies between critical information and communication infrastructures. *Critical Information Infrastructure Protection and Resilience in the ICT Sector*, 153–172. https://doi.org/10.4018/978-1-4666-2964-6.ch008

Public Safety Canada. (2018). *National Cross Sector Forum 2018-2020 Action Plan for Critical Infrastructure*. 1–21.

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, *21*(6), 11–25. https://doi.org/10.1109/37.969131

Seppänen, H., Luokkala, P., Zhang, Z., Torkki, P., & Virrantaus, K. (2018). Critical infrastructure vulnerability—a method for identifying the infrastructure service failure interdependencies, Hannes. *International Journal of Critical Infrastructure Protection*. https://doi.org/10.1016/j.ijcip.2018.05.002

Serianu. (2018). *SACCO Cybersecurity Report 2018: Demystifying Cybersecurity for Saccos*. Retrieved from https://africasustainabilitymatters.com/download/sacco-cyber-security-report-2018/

Setola, R., Luiijf, E., & Theocharidou, M. (2017). Managing the Complexity of Critical Infrastructures. *Managing the Complexity of Critical InfrastructuresA Modelling and Simulation Approach*, *90*(Ci), 1–18. https://doi.org/10.1007/978-3-319-51043-9

Stergiopoulos, G., Vasilellis, E., Lykou, G., & Gritzalis, D. (2016). *Chapter 14 Classification and Comparison of Critical Infrastructure Protection Tools*. 239–240. https://doi.org/10.1007/978-3-319-48737-3

Suter, M. (2007). A Generic National Framework For Critical Information Infrastructure Protection (CIIP). *Security Studies*, (August).

Tatar, U., Gokce, Y., & Gheorghe, A. (2017). Strategic Cyber Defense: A Multidisciplinary

Perspective. *NATO Advanced Research Workshop on A Framework for a Military Cyber Defense Strategy*.

The Council of the European Union. (2008). Council Directive 2008/114/EC: on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. In the *Official Journal of the European Union*.

Tweneboah-Koduah, S., & Buchanan, W. J. (2018). Security risk assessment of critical infrastructure systems: A comparative study. *Computer Journal*, *61*(9), 1389–1406. https://doi.org/10.1093/comjnl/bxy002

U.S. Department of Homeland Security. (2013). *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*.

UNCTAD. (2011). Measuring the Impacts of Information and Communication Technology for Development. In the *United Nations Conference on Trade and Development*. New York.

US Government Accountability Office. (2013). *Critical Infrastructure Protection: DHS List of Priority Assets Needs to Be Validated and Reported to Congress, Report to Congressional Requesters, GAO-13-296, Washington, DC*.

USA Patriot Act. (2001). *USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006 (S. 2271). 2005*, 1–6. Retrieved from http://www.fas.org/sgp/crs/intel/RS22384.pdf

Velasquez, L. C. H. (2016). *A Comprehensive Instrument for Identifying Critical Information Infrastructure Services*. The University of Tartu.

WEF. (2016). The Global Information Technology Report 2016. In *Insight Report*. Retrieved from http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf%0Ahttps://www.weforum.org/reports/the-global-information-technology-report-2016

White, R. (2014). Towards a unified homeland security strategy: An asset vulnerability model. *Homeland Security Affairs*, *10* (February), 1–15.

Acknowledgement

This research is supported by the Nigeria TETFund National Research Fund (NRF) research grant TETF/DR&D/CE/NRF/UNI/KEFFI/VOL.1/B5 to Nasarawa State University, Keffi, Nigeria.

Profiles of the Authors

Uche M. Mbanaso is a cybersecurity expert and currently the Executive Director, Centre for Cyberspace Studies, Computer Science Department, Nasarawa State University, Keffi, Nigeria, and a visiting scholar at the LINK Centre, University of Witwatersrand, Johannesburg, South Africa. He played key roles in the Nigeria Cybercrimes Act 2015, National Cybersecurity Strategy and Policy 2015, Data and Privacy Protection Bill 2019, and other cybersecurity framework developments in Nigeria. He possesses MSc in Information Technology (Bradford UK, 2003) and PhD Communications and Information Security (Salford UK, 2009). He is actively involved in Cyberspace and Networks Security, Data Privacy Protections and Public Key Technologies.

Victor Emmanuel Kulugh is currently the Project Manager of the Cybersecurity And Critical National Infrastructure Project and a PhD candidate at the Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria. His research interest is in critical information infrastructure dependency and resilience. He obtained B.Sc. from Enugu State University of Science and Technology, Enugu, Nigeria in 2013 and received an M.Sc. degree in Computer Science (Networking) in 2017 from the Nasarawa State University, Keffi, Nigeria.

Julius Adebowale Makinde lectures at the Baze University, Nigeria and is a PhD candidate at the Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria. His research interest is in critical information infrastructure protection and resilience (CIIPR). He has over 14 years' experience in ICT in the private sector before joining academia. He earned his undergraduate qualification in Electronics and Communications Engineering in Nigeria, and MSc in Information Technology from DE Montfort University, UK in 2007.