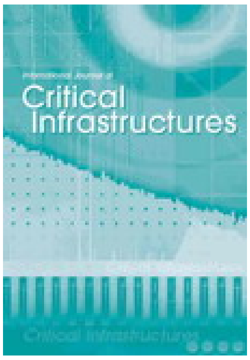


International Journal of Critical Infrastructures

ISSN online: 1741-8038 - ISSN print: 1475-3219
https://www.inderscience.com/ijcis

A methodological approach for characterisation of critical national infrastructure

Uche M. Mbanaso, Julius A. Makinde, Victor E. Kulugh

DOI: 10.1504/IJCIS.2023.10040420

Article History:

Received:	04 January 2021
Accepted:	07 April 2021
Published online:	21 April 2023

A methodological approach for characterisation of critical national infrastructure

Uche M. Mbanaso

Centre for Cyberspace Studies,
Nasarawa State University,
Keffi, Nigeria
Email: uche.magnus@mbanaso.org

Julius A. Makinde*

Department of Computer Science,
BAZE University,
Abuja, Nigeria
Email: julius.makinde@bazeuniversity.edu.ng
*Corresponding author

Victor E. Kulugh

Centre for Cyberspace Studies,
Nasarawa State University,
Keffi, Nigeria
Email: vkulugh30@gmail.com

Abstract: This article presents a methodological approach for the characterisation of critical national infrastructure (CNI). Despite several approaches to identifying CNI, there has not been any universally acceptable way that is agreeable because a country's CNI priority may differ. CNI enabled by information and communications technology (ICT) is usually referred to as critical national information infrastructure (CNII). Thus, the security of CNII requires a far-reaching approach that is harmonised and agile to mutually respond to global cyber threats. Without proportionate safeguards, the increasingly interconnected and interdependent infrastructures can create vulnerability opportunities that can cause failures with cascading or escalating effects. Consequently, proper characterisation, categorisation and designation of CNI are vital to effective CNII protection and resilience. We approached the study by extensive review, analysis and synthesis of CNI of selected countries around the globe. Then, we applied a multi-criteria decision making (MCDM) to show how CNI can be derived, and designated.

Keywords: critical national infrastructure; CNI; critical national information infrastructure; CNII; multi-criteria decision making; MCDM; comparative analysis; information and communications technology; ICT dependency.

Reference to this paper should be made as follows: Mbanaso, U.M., Makinde, J.A. and Kulugh, V.E. (2023) 'A methodological approach for characterisation of critical national infrastructure', *Int. J. Critical Infrastructures*, Vol. 19, No. 2, pp.172–197.

Biographical notes: Uche M. Mbanaso is a leading cybersecurity subject matter expert (SME), and currently the Executive Director at the Centre for Cyberspace Studies and lectures in the Computer Science Department, Nasarawa State University, Keffi, Nigeria. He is a visiting scholar at the LINK Centre, University of Witwatersrand, Johannesburg, South Africa. He is the Principal Investigator (PI) of TET Fund sponsored research on cybersecurity and critical national infrastructure (CNI). He earned his undergraduate qualification in Electronics and Communications Engineering, MSc in Information Technology and PhD Communications and Information Security.

Julius A. Makinde lectures in BAZE University, Nigeria and a PhD candidate at the Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria. His research interest is in the area of critical information infrastructure protection and resilience (CIIPR). He has over 14 years field experience in ICT with the private sector before joining academia. He earned his undergraduate qualification in Electronics and Communications Engineering and MSc in Information Technology.

Victor E. Kulugh is currently a Project Manager of the Cybersecurity and Critical National Infrastructure (CNI) Project and a PhD candidate at the Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria. His research interest is in the area of critical information infrastructure dependency and resilience. He obtained his BSc and MSc in Computer Science (Networking).

This paper is a revised and expanded version of a paper entitled 'Characterisation of critical infrastructure organisation in Nigeria' presented at 15th International Conference on Electronics, Computer and Computation (ICECCO), Nile University Abuja, Nigeria, 10–12 December 2019.

1 Introduction

This paper is an extension of work presented at the 15th International Conference on Electronics Computer and Computation (ICECCO 2019) (Mbanaso et al., 2019). The critical assets often referred to as critical national infrastructure (CNI) is so designated because of their roles in sustaining and improving the quality of the society, especially when they spread geographically across the country. It is publicly known that CNI is vital to the functioning of any modern society especially in this era of the digital economy. The disruption or destruction of such infrastructural assets can result in an undesirable effect on the nation and society (Katina and Keating, 2015; Lo et al., 2020; Singh et al., 2014; Srinivasu and Islamia, 2013). However, many countries are grappling with understanding the challenges faced by CNI, while some countries are yet to identify and designate certain critical infrastructure (CI) as CNI. Nonetheless, some countries have identified and classified CNI according to sectors (CIPedia, 2015).

Nowadays, information and communications technology (ICT) has become an integral part of modern society, driving digital transformation, stimulating improved operational efficiency and high productivity. Nevertheless, the irresistible benefits of ICT are accompanied by cyber risks as a result of threats due to inherent vulnerabilities found in most ICT systems. Consequently, ICT enabled CI is highly susceptible to cyberattacks of various dimensions. So, CI has to contend with threats from diverse persuasions including state-sponsored threats – ideological and political, as well as high profile organised threats. Therefore, there is the need to identify, classify and map the infrastructures appropriately, and prioritise their protection based on their relevance to society (Elgin et al., 2010). Additionally, another factor that can influence the level of protection on any infrastructure is its relationship to other infrastructures. For instance, it is publicly known that ICT, transport, healthcare, financial sectors, etc. depend heavily on the availability of clean electrical power. It implies that any form of disruption or failure of the power grid will adversely affect these dependent sectors. Therefore, without appropriate national characterisation of CNI, it will be difficult to accurately quantify the damages or losses in an event of disruption or failure of the power grid. Nationally, the impact can be devastating, ranging from accidents due to traffic control system malfunction, loss of revenue, and other effects on critical sectors of the economy (Katina and Keating, 2015). The power incident of California, Canada and Europe is an example of such a devastating event (Andersson et al., 2005; Rinaldi et al., 2001). More so, the internet of things (IoT) and integration with cyber-physical systems is anticipated to alter the threats landscape of CNI. Then potentially, CNI supported by IoT can be expected to amplify the cyber risk exposure as the interconnection of devices will increase the opportunities for direct targeted cyber-attacks against CNI (Izuakor and White, 2016).

The fact that most of the cyberinfrastructure is owned by the private sector (Lo et al., 2020; Singh et al., 2014) infers that the government alone cannot be saddled with the responsibilities of protecting CI. It is open to debate whether many of the private sector CI organisations may find it demanding to invest proportionally to protect the CI they own. In some climes, the government owns some key national resources such as power grid, transportation, water, etc. which further complicates infrastructural interdependency relationships. It dictates that the government must work together with the private sector to develop suitable protection mechanisms (Reichard et al., 2016). The protection mechanism must include appropriate policy debate, clear comprehensible and anticipatory responses that is agreeable to all stakeholders. As a result, it is incumbent that every country decides how to consider an infrastructure criticality based on certain parameters or factors essential to the economic, social, political, security and the wellbeing of her citizens. Many countries have different approaches to the characterisation of CIs; the choice of criteria should be a function of national priorities but must be methodically consistent. For instances, the manufacturing sector is so considered as critically important infrastructure by China, the USA and Japan (West and Lansang, 2018). Similarly, the USA, Saudi Arabia and Russia consider the oil and gas sector very critical (Brown and Huntington, 2017). In some other countries, energy, transport, healthcare, water, power, finance, etc. are all considered CNI. The discrepancy in the identification of CI across the globe supports our earlier position that there is no standardised global formula that countries can adapt to so determine and designate a CI. It can also allude to that none of the approaches used by countries can be definitive. More so, what countries can identify and consider suitable as CI will continue to expand over time, implying that repeatability and methodical consistency are crucial factors. However, notwithstanding the liberty to so designate CNI by countries based on national priorities, how the concept of critical national information infrastructure (CNII) is related to CNI is so important since the cyber threat is global phenomena.

This article presents a study in an attempt to properly characterise CNI in the context of CNII since traditional CNI is increasingly dependent on ICT. In this regard, we carried out a comparative study of selected countries to identify how CNI are so characterised and categorised. This can be the basis to find similarities and divergences of how countries perceive CNI sectors and organisations. The outcome can help reshape the thinking of critical sector organisations, and possibly direct novel policy directions and protection strategy as well as infrastructural alignments. As it is already known, cybersecurity is a problem of all sectors in the society, which demands fundamental steps from both the private and public sectors. Therefore, this article seeks to provide an appropriate methodological approach in the characterisation and categorisation of CNI sectors and organisations, which can facilitate proper planning and proportionate CNI protection and resilience. The rest of the paper is organised as follows: Section 2 presents background and related works; Section 3 describes appraisal of critical sectors in selected countries; Section 4 comparatively analyses global critical sectors, and Section 5 demonstrates the categorisation approach. In Section 6, discussions on the result and analysis are presented, and Section 7 concludes with recommendations.

2 Background and related works

Worldwide, the CNI provides mission-critical functions to a nation such that if interrupted during operational state or when required will have a devastating impact on delivering essential goods and services. Some disruptions may impact a single organisational unit while others can affect the entire organisations as well as another dependent (Mao and Li, 2018; Mohamed, 2019). This suggests that a disruption in infrastructure that affects the entire organisation or multiple organisations can qualify it to be classified as mission-critical or mission important infrastructure. ICT is increasingly enabling this mission-CI, resulting in susceptibility to cyberattacks (Ibrahim, 2016; Theron and Bologna, 2013). Examples of such include power grid, transportation networks, banking system networks, government treasury single account (TSA) system, national healthcare networks, and industrial control networks. Traditional CNI assets are increasingly connected through large networks of ICT to allow operational efficiency and higher productivity, central monitoring and remote or automated operations, making services and maintenance more effective. Thus, as more infrastructures connect to ICT networks, the high potential for amplified risks arises, which can even result in undesirable physical effects. A study by Ponemon Institute (2019) on cybersecurity in UK, Germany, Mexico, USA Japan and Australia, revealed that about 90% of the CI had been attacked between 2017 and 2019. It is argued that due to trends, cyberattacks or disruptions against CNI will continue to rise exponentially, and may equally affect smart home infrastructure (Khan et al., 2016; Siddiqui et al., 2018). Therefore, since these infrastructures support the functioning of modern society for economic prosperity, preservation of national security, safety and wellbeing of citizens, the impact of cyberattacks or disruptions can be far-reaching to the extent of bringing a nation to a standstill. As a consequence, many countries are building defensive mechanisms to protect and achieve some level of resilience against such disruptions or targeted cyber-attacks. The characteristics of cybersecurity events are such that a single incident has the potential to affect multiple organisations in a sector or escalate to other dependent sectors with its attendant of diverse effects. The inference that can be deduced so far is that most infrastructures do not exist in isolation but do have some sort of relationships either unidirectional or bidirectional, which exacerbates the intricacies of preserving such infrastructures against any form of disruptions (Moteff, 2005).

Thus, it is vital to identify and categorise CI according to the similarity of services or functions (Luiijf and Klaver, 2004). The Provincial Emergency Program (PEP, 2007) in Canada, used the concept of CI workbook to identify and categorise CNI. The workbook provides a simple framework for listing infrastructures under sectors they are relevant to. The number of other infrastructures supported by one infrastructure determines its importance. The drawback of the workbook framework is that it only deals with a geographical area with an emphasis on hazards such as flooding. According to the CRN Report (Elgin et al., 2010), the government of Dutch perceive CNI protection from crisis management and national security view. The UK and Canada pencil CNI protection and resilience as emergency and crisis management. In Ousmane et al. (2016), a study commissioned by the African Development Bank (ADB), to investigate the status of CNI between 2010 and 2013 in Nigeria, stated that water sanitation, transportation, power and ICT are supposedly critical to Nigeria were in deplorable conditions. The report suggested that the unacceptable condition may be as a result of a lack of adequate protection and maintenance. The study also revealed that the lack of relevant national policy and strategy about CNI protection may have affected the deplorable conditions. In (Rossella Mattioli, 2014), Rossella analysed the EU member states' approach to the identification of CNI based on a service-oriented approach; focused primarily on ICT infrastructures and (inter)dependencies, which confirms the increasing dependency on ICT. The sectors include energy, transport, water, food, healthcare, finance, public and legal order and safety, civil administration, chemical and nuclear industry, etc. Similarly, Canada categorised CNI based on factors such as geographical spread and interdependency (Herrera and Maennel, 2019; Islam and Moselhi, 2012). In Izuakor and White (2016), Izuakor and White approached the identification of CIs or assets from a risk assessment perspective – potential risk of an infrastructure being compromised. The approach focused on insider threat actors, arguing that risks should be recognised from the abuse of privileged users including trusted partners. The approach can be said to be a narrow view of the problem, as CI has a variety of vulnerability points. Besides, in Rossella Mattioli (2014), an assortment of approaches were enumerated including 'a non-critical service dependent approach' and 'critical service dependent approach', etc. which chiefly focused on the identification of critical services or functions within the infrastructure and non-critical functions. The idea is that the criticality of functions based on the impact that the disruptions can cause can be the basis for the identification. This method is considered from two perspectives: state and operator driven. These approaches have the downside of focusing on the identification, purely from network infrastructure components, since the organisation can have other critical assets other than network components. Besides, being network-centric, complexity can be introduced in the lower level of network components such as transport and access functions. In another study (Mcevoy, 2008), Mcevoy approached the identification of CI based on transmission critical asset decision tree scheme (TCADTS), with a flowchart of series of decisions built on defined criteria, which is from a risk assessment perspective.

Thus, the approaches reviewed addressed characterisation from different perspectives and environmental contexts, but are not consistent and repeatable since they lack the scientific approach. Since critical sector infrastructures share common attributes and characteristics, the alignment of the attributes or features should inform the basis for systematic and logical identification and categorisation. Therefore, we approached the study from a different methodological standpoint by a comparative survey of critical sectors to ascertain some similarities and discrepancies and then using linear multi-criteria decision making (MCDM) and weighted decision matrix (WDM) to derive the characterisation. Using a desktop search, we retrieved information about critical sectors in selected countries from various online repositories and databases. The selection of countries in continents depended on the ICT development index (IDI) ranking and with relevant CI information. The data after review, analysis and synthesis is comprehensively represented in Appendix.

3 Appraisal of critical sectors in selected countries based on continent

3.1 Africa

Africa is made up of 54 countries (Encyclopedia, 2019; World, 2020; Worldatlas, 2020). Out of the ten countries we studied based on IDI, only nine have accessible information in the public domain about CNI. In Nigeria 15 critical sectors are recognised (Office of National Security Adviser, 2014), South Africa, 11 sectors (Pillay, 2017; Mitrovic, 2018), Libya has 11 sectors (Adrian and Co, 2020), Ghana has ten sectors (CIPedia, 2015), Morocco has five (Bank, 2020) and Cape Verde, four (Briceno-Garmendia and Benitez, 2014), Botswana, four (Dominguez and Briceno-Garmendia, 2011) as depicted in Table 1. Although Seychelles has the highest human development index (HDI) in Africa (Human Development Report, 2019), there is no publicly available information on its CNI.

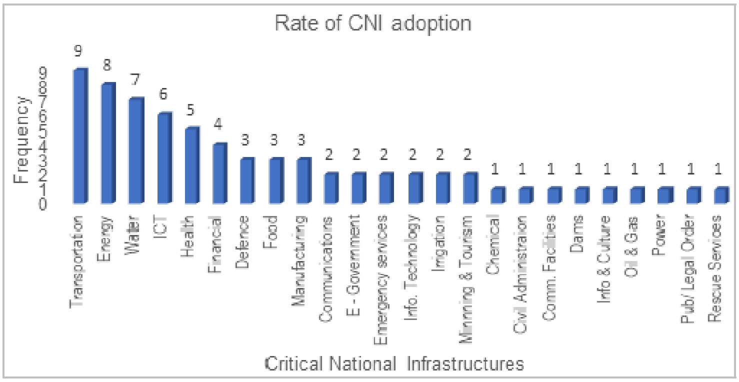
Table 1 CNI in of selected countries of Africa

Countries	*Number of CNIs*
Nigeria	15
South Africa	11
Libya	11
Ghana	10
Morocco	5
Kenya	5
Cape Verde	4
Egypt	4
Botswana	4

However, Nigeria, South Africa and Ghana have six sectors in common including defence, energy; financial, health, transportation and water (see Appendix). Similarly, Kenya and Egypt also identified energy, transportation, and ICT but differed in other infrastructure classification. Based on our study, transportation and energy are identified by nine and eight countries respectively in Africa, water is identified by seven countries, ICT, six health's by five, financial, four and defence, food and manufacturing are identified by three countries as shown in Figure 1.

This reveals the lack of publicly available data in most of the African countries and can be interpreted as a low level of awareness, and the perception of cyber threats in some of the countries. It further exposes the fact that some essential sectors such as food, emergency services by other countries were not considered. The detail is as shown in Tables A1 and A2 of Appendix.

Figure 1 Numbers of countries per CNI sector in Africa (see online version for colours)



3.2 Asia

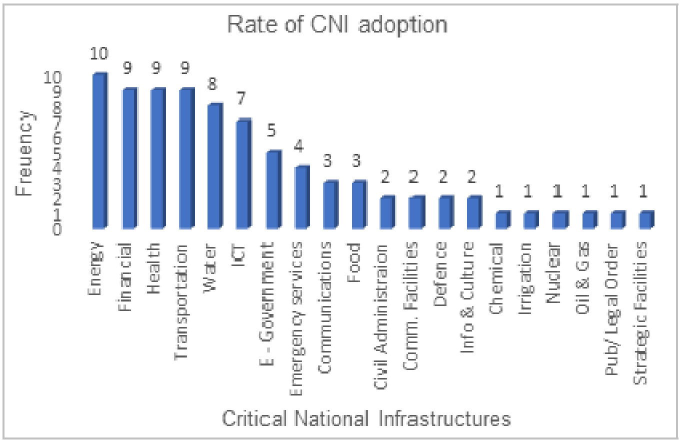
The Asian continent is made up of 48 countries (Worldatlas, 2020), and ten countries were examined. Table 2 shows the number of CNI sectors per selected country. Malaysia has the highest number of CNI of 10 (CIPedia, 2015). Malaysia and UAE have nine common CNI sectors including e-government, emergency, energy, financial, food, health, ICT, transportation and water sectors.

Table 2 CNIs in of selected countries of Asia

Countries	*Numbers of CNIs*
Malaysia	10
Rep. of Korea	9
Singapore	9
UAE	9
Philippines	9
Japan	8
Kuwait	8
China	7
Qatar	6
Turkey	6

Figure 2 shows that energy, financial, health, transportation and water are the topmost identified CNI in the Asian continent. Some countries, aside from identifying energy as a CNI also identified other sources of energy such as oil and gas, nuclear energy and power (Appendix). Arguably, this can be construed as exaggerated categorisation.

Figure 2 Numbers of countries per CNI sector in Asia (see online version for colours)



3.3 Europe

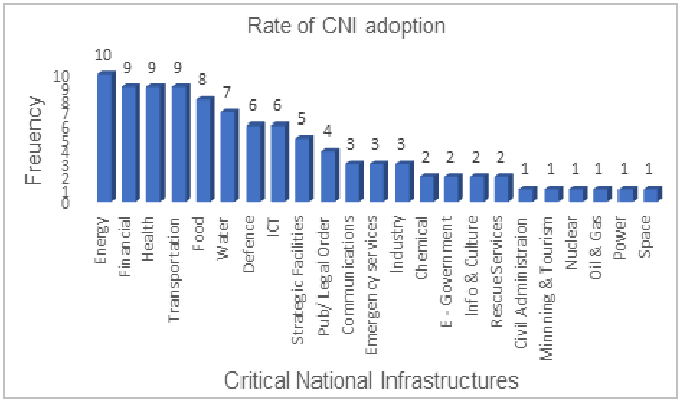
Europe has 44 countries (Worldatlas, 2020), and ten countries were studied, of which six countries identified 10 to 13 CNI as shown in Table 3. The UK tops the list with 13 CNI (Infrastructure, 2020). Below the UK are the Netherlands and France, each with 12 CNI sectors (CIPedia, 2015). Luxembourg has six CNI (Stéphane et al., 2018). Notwithstanding that Norway has the highest HDI in the world (Human Development Report, 2019) (Kovacevic et al., 2018), it has only six identified sectors. This can suggest that HDI does not influence how countries perceive and characterise CI.

Table 3 CNIs in of selected countries of Europe

Countries	*Numbers of CNIs*
United Kingdom	13
Netherlands	12
France	12
Sweden	11
Switzerland	10
Denmark	10
Germany	9
Iceland	7
Norway	6
Luxembourg	6

Figure 3 shows the number of countries per identified CNI. All the ten countries we studied identified energy. Financial, health and transportation are recognised by nine countries. Other identified CNI are food by eight countries and water in seven countries. Communication and ICT are separately identified. In Europe, most of the countries did not consider safety or rescue services as distinct CNI.

Figure 3 Numbers of countries per CNI sector in Europe (see online version for colours)



3.4 North America

Out of the 23 countries in the continent of North America (Worldatlas, 2020), seven countries were investigated. Table 4 shows the number of CNI recognised by each of the countries studied. The USA has 16 identified CNI to top the list, followed by St. Lucia 11 (UNOPS Lucia, 2020), Canada with ten identified CNI. The USA and Canada identified eight common CNI sectors including; energy, transportation, water, health, financial, civil admin, food and manufacturing. Equally, Mexico has seven identified CNI (Serre and Heinzlef, 2018). All the countries studied identified transportation and water as CNI.

Table 4 CNIs in of selected countries of North America

Countries	*Numbers of CNIs*
USA	16
St. Lucia	11
Canada	10
Mexico	7
Barbados	5
Bahamas	4
El Salvador	4

Figure 4 shows the numbers of countries that identified a particular CNI. Energy, transportation, and water top the list with seven countries identifying each of them. The dam sector is recognised by the USA, implying that she separated water infrastructure from that of the dam. In this continent, manufacturing and cybersecurity are also classified as CNI respectively (Appendix).

3.5 South America

In the South America continent, seven countries out of the 12 countries (Worldatlas, 2020) were studied. Chile topped the list of Table 5 with ten CNI (CIPedia, 2015; Compared, 2017) followed by Trinidad and Tobago with five CNI (CIPedia, 2015). Chile and Trinidad and Tobago (CIPedia, 2012) identified 4 common CNI including transportation, health, finance, and safety (Appendix). In Table 5, Peru and Venezuela recognised three sectors.

Figure 4 Numbers of countries per CNI sector in North America (see online version for colours)

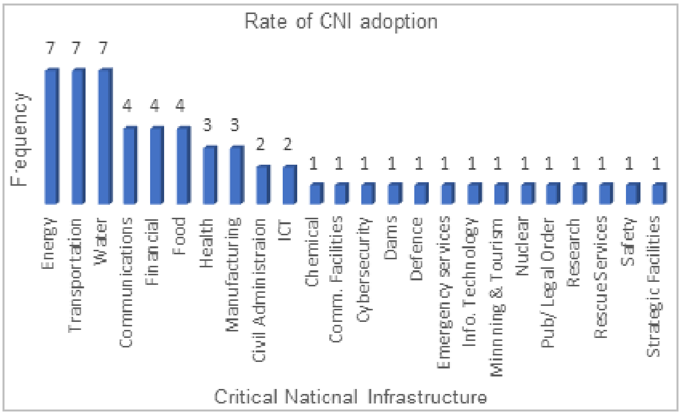


Table 5 CNIs in of selected countries of South America

Countries	*Numbers of CNIs*
Chile	10
Trinidad and Tobago	5
Brazil	4
Colombia	4
Argentina	4
Peru	3
Venezuela	3

Figure 5 Numbers of countries per CNI sector in South America (see online version for colours)

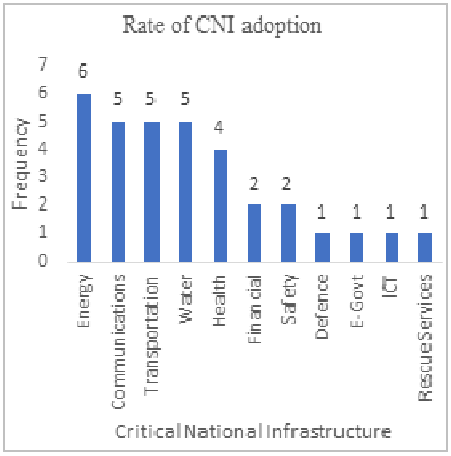


Figure 5 illustrates the number of countries that identified each CNI in South America. Energy topped the list with six countries identifying it. While transportation, water and communications CNIs are recognised by five countries, health is identified by four countries. Other details can be found in Appendix.

3.6 Oceania

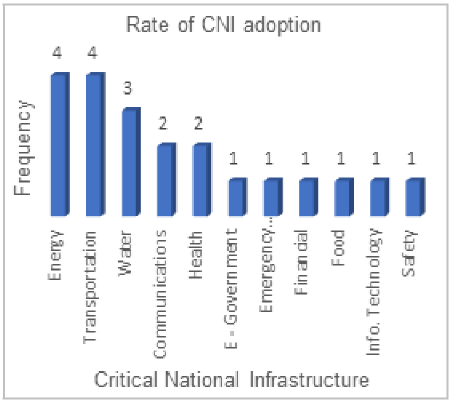
In this continent of 14 countries (Worldatlas, 2020), we examined four countries to ascertain the status of the CNI. Table 6 shows that Australia topped the list with eight CNI. Next is Papua New Guinea with six sectors. Other countries do not have any publicly available information about CNI sectors.

Table 6 CNIs in of selected countries of Oceania

Countries	*Numbers of CNIs*
Australia	7
New Zealand	6
Fiji	4
Solomon Island	4

Figure 6 illustrates the number of countries that identified each CNI sector. Transportation topped the list with four countries identifying it. Energy and water are recognised in three countries. Information technology (IT) and food are listed in two countries.

Figure 6 Numbers of countries per CNI sector in Oceania (see online version for colours)



4 Comparative analysis of global critical sectors

From the study so far, it is important to reiterate as earlier alluded to that countries identify and categorise CI based on national priorities, and the utility value attached to each CI (Herrera and Maennel, 2019; Mbanaso et al., 2019; Rossella Mattioli, 2014). It implies that national priorities and perceived level of importance by the government in most cases inform how CIs are so recognised. Arguably, the non-availability of CNI records in some countries may not necessarily mean that the country has not recognised certain infrastructure as critical. It could be due to inaccessibility or not digitally presented on the web. Still, it could mean that the country has not formally recognised and designated critical assets, functions or services as CNI or CNII. The examination of 47 countries across the globe, throw insights into how some countries so identified and categorised mainstream CNI. The results are shown in Tables 7a and 7b illustrating the numbers of CNI per country. The analysis revealed that the USA topped the list with 16 CNI, followed by Nigeria with 15, then Indonesia, UK and Austria, with 13 CNI each. India and Australia respectively both have 12 CNI. However, contextualising with the current HDI ranking (UNDP, 2019) and the studied countries, it is evident that HDI does not influence how countries characterise and designate CI. For instant, Australia has an index value of 0.938, against the USA and the UK with 0.920 index values but the UK has more designated sectors than Australia. Theoretically, the expectation is that Australia with the highest development index, which is an indicator of sustainable development, should have more designated critical sector sectors. Also, South Africa with an HDI of 0.705, the highest in Africa has 12 CNI while India with an HDI of 0.647, has 12 CNI. Also, Chile, Canada, and Denmark have the same 10 CNI.

Table 7a Numbers of CNIs per country

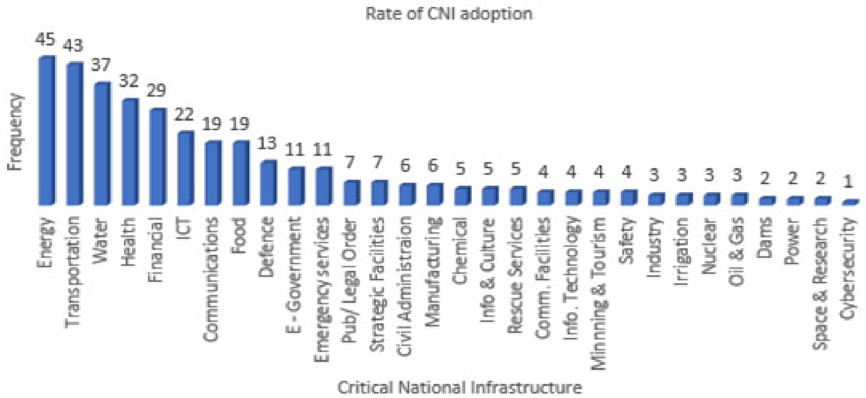
No.	*Countries*	*Numbers of CNI*
1	USA	16
2	Nigeria	15
3	Indonesia	13
4	United Kingdom	13
5	Austria	13
6	India	12
7	Netherlands	12
8	Spain	12
9	France	12
10	South Africa	12
11	Sweden	11
12	Ghana	10
13	Malaysia	10
14	Switzerland	10
15	Ukraine	10
16	Denmark	10
17	Canada	10
18	Chile	10
19	Singapore	9
20	Rep. of Korea	9
21	UAE	9
22	Philippine	9
23	Ireland	9
24	Germany	9
25	Estonia	9

Table 7b Numbers of CNIs per country

No.	*Countries*	*Numbers of CNI*
26	Kuwait	8
27	Japan	8
28	Mexico	8
29	Iceland	7
30	China	7
31	Australia	7
32	Papua New Guinea	6
33	Qatar	6
34	Turkey	6
35	Norway	6
36	P. New Guinea	6
37	New Zealand	6
38	Kenya	5
39	Trinidad and Tobago	5
40	Egypt	4
41	Bahamas	4
42	El Salvador	4
43	Brazil	4
44	Colombia	4
45	Argentina	4
46	Fiji	4
47	Solomon Island	4
48	Peru	3
49	Venezuela	3

Figure 7 depicts a chart of sectors, and the number of countries that recognised each sector. The chart shows that out of 47 countries, 45 recognised energy, which topped the list, followed by transportation recognised by 43 countries. The republic of Trinidad and Tobago is the only country that did not recognise energy as a sector (CIPedia, 2012). The sector that is recognised only a country such as cybersecurity, is indicated in Appendix. Sectors such as dams, irrigation, and research are recognised by two countries each. Figure 7 shows clearly the arbitrariness of critical sectors designation. Besides, sectors with a smaller number of countries are sub-sectors of some other core sectors. For example, the dam and underwater are sub-sectors of water in some countries. Consequently, the similarities and divergences are undoubtedly evident in Figure 7. Interestingly, only Mexico recognised cybersecurity as CI (Serre and Heinzlef, 2018). Besides, it can be argued that cybersecurity is an abstract imaginary infrastructure to be so identified and recognised as a critical sector. Notwithstanding this, cybersecurity is an important function so vital for the wellbeing of a country that requires special attention. Arguably, the perception of cybersecurity as an intangible infrastructure in the context of CNII can simply be the basis of its exclusion as a CI. Aside, cybersecurity as a critical function or service can be intrinsically categorised and recognised but not as a sector since it pervades across sectors of CNII. Figure 8 presents the map view of numbers of CNIs of selected countries.

Figure 7 Global view of numbers of countries per CNI (see online version for colours)



5 Characterisation and categorisation of CI

It is evident from the previous sections that there is no publicly available standard or consensus for the characterisation and designation of CI; different countries use different criteria for the identification and designation of an infrastructure, asset, service or function as a CNI or CNII. We can leverage the insights gained from the survey of CI in 49 countries from six continents, to derive a systematic approach for the characterisation of CNI or CNII. Figure 7 shows the CNI sectors and the number of countries that recognised each CNI, which we coin as the global popularity (Gp) of each sector. If we take Gp as one of the criteria and consider other peculiar criteria (or indicators) such as geographical spread (Gs), dependency factor (Df), alignment with existing structure (As) and potential cyber risk (Pr), we can therefore use a multi-criteria-decision methodology (Almeida and Técnico, 2008) as the basis to formulate the characterisation and categorisation. Consequently, we adopted the MCDM (Kazimieras Zavadskas et al., 2018), based on WDM. We assign weight factors to the indicators as described in Table 8 based on the researchers' judgement.

The rationale for the assignment of the weighting factor to each indicator is a proportion of assumed relative importance to the overall goal, and the total of the weight factor (*wf*) must be equal to 1 (or 100%), (ITU, 2017) according to equation (1).

$$\sum_{k=1}^{n} wf = 1 \tag{1}$$

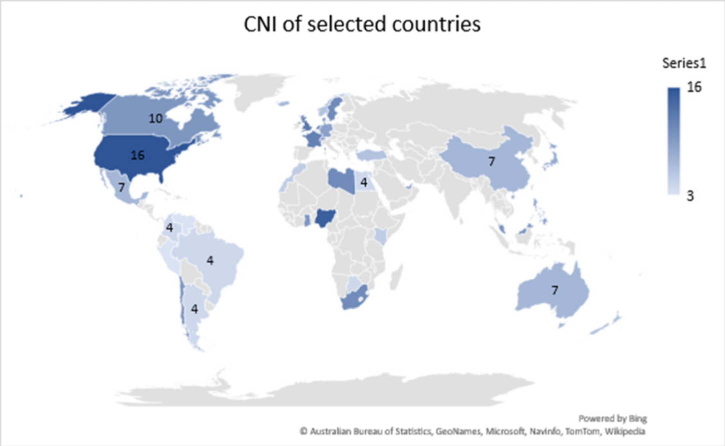
where k = from 1 to n and n is the number of indicators.

We apply the five-point Likert scale shown in Table 9 for the quantitative evaluation of the rest of the indicators except for Gp shown in Figure 8. The assignment of the scale to other indicators was done by a combination of the research team and subject matter experts (SMEs). The outcome is the matrix table shown in Table 10.

Table 8 Indicator weight factors

Indicator	*Description*	*Weight factor*
Global popularity (Gp)	The frequency of appearance of a CNI in the number of countries studied.	0.25
Geographical Spread (Gs)	The geographic spread or influence of the considered CNI such that the effects of its failure cuts across wide geographic locations.	0.20
Dependency factor (Df)	A measure of the level of (inter)dependence of other CNIs on the considered CNI.	0.20
Alignment with existing structure (As)	The level of integration of the considered CNI with existing traditional CNIs (whether it is tightly or loosely coupled).	0.10
Potential cyber risk (Pr)	A measure of the cyber vulnerabilities and threats that may potentially expose the CNI to cyber risk.	0.25
	Total	1.00

Figure 8 Map view of number of CNI per country studied (see online version for colours)


CNI of selected countries
Series1
16
3
10
16
7
4
4
4
4
7
7
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, TomTom, Wikipedia

The MCDM considers many factors as described in Table 8 of which each influences the economy and social wellbeing of a nation. To derive composite values, we use linear MCDM (Fu et al., 2020; Kazimieras Zavadskas et al., 2018) to transform and normalise the values. The linear algorithm used to arrive at our decision is as follows:

1 normalisation of performance values

2 introduction of weighted values

3 summation of weighted normalised values.

In step (1), we make all the performance values to be comparable based on equation (2), where performance value = x and transformed value = X_n. Thus, the value X_n is:

$$X_n = \frac{X}{X \max} \tag{2}$$

Table 9 Likert rating scale

Rating	*Very low*	*Low*	*Medium*	*High*	*Very high*
Scale	1	2	3	4	5

Table 10 Matrix table of sectors and rating of indicators

Sectors	*Gp*	*Gs*	*Df*	*As*	*Pr*
Energy	45	5	4	3	4
Transportation	43	4	4	4	4
Water	37	4	4	3	4
Health	32	5	5	4	4
Financial	29	4	4	3	5
ICT	22	3	4	4	5
Communications	19	3	4	4	4
Food	19	4	4	3	4
Defence	13	3	3	2	3
E-government	11	2	2	2	3
Emergency services	11	3	2	1	2
Pub/legal/others	7	2	4	1	2
Strategic facilities	7	1	1	3	2
Civil admin.	6	3	4	4	3
Manufacturing	6	4	4	4	3
Chemical	5	3	1	3	3
Information and culture	5	2	2	1	1
Rescue services	5	2	2	2	2
Commercial facilities	4	4	2	3	4
Info. technology	4	4	2	3	4
Mining and tourism	4	3	2	2	1
Safety	4	3	2	3	2
Industry	3	3	3	3	3
Irrigation	3	3	1	2	1
Nuclear	3	2	1	1	4
Oil and Gas	3	3	4	4	4
Dams	2	4	1	1	2
Power	2	4	4	4	3
Space and research	2	3	4	3	4
Cybersecurity	1	1	2	2	5
Xmax	*45*	*5*	*5*	*4*	*5*

Table 11 demonstrates the transformation of Table 10 based on equation (2).

Table 11 Example of transformed table

CNI	*Gp*	*Gs*	*Df*	*As*	*Pr*
Energy	1.000	1.000	0.800	0.750	0.800
Transportation	0.958	0.800	1.000	1.000	0.800
Space and research	0.042	0.600	1.000	0.750	0.800
Cybersecurity	0.021	0.200	0.500	0.500	1.000

In step (2), we apply the weighted factors to the normalised values (X_n). This is achieved by finding the product of transformed value and the weighted factors as shown in equation (3).

The next step (3) is, to sum up, the normalised values for each sector to arrive at the decision index (*Di*) as shown in equation (4).

$$Xwn = WfX_n \tag{3}$$

$$Di = \sum_{k=1}^{n} Xwn \tag{4}$$

where k is in the range of 1 to n.

Thus, using equation (4), Table 12 is derived and ranked based on the linear MCDM. After the calculation and normalisation, the health sector topped the list of 31 CNIs followed by energy, indicating that they are the most universally recognised CNI sectors. The fact that the health sector ranked first, demonstrates the importance attached to health by many countries, and arguably reflects on the consequences of the COVID-19 pandemic. This single factor can be said to validate the weighting used in our MCDM. The Information and culture on the other hand ranked last, implying that it is the least universally recognised CNI sector. The ranking outcome order arrived, i.e., energy, transportation, financial, water, ICT, food, communications, manufacturing, oil and gas, power, etc. can be said to reflect in Tables 7(a) and 7(b), identifying about 80% of the listed CNI.

Table 12 Ranked CNIs based on multi-criteria decision matrix

CNI	*Gp*	*Gs*	*Df*	*As*	*Pr*	*Score*	*Rank*
Health	0.198	0.200	0.250	0.100	0.200	0.948	1
Energy	0.250	0.200	0.200	0.075	0.200	0.925	2
Transportation	0.240	0.160	0.200	0.100	0.200	0.900	3
Financial	0.177	0.160	0.200	0.075	0.250	0.862	4
Water	0.198	0.160	0.200	0.075	0.200	0.833	5
ICT	0.115	0.120	0.200	0.100	0.250	0.785	6
Food	0.115	0.160	0.200	0.075	0.200	0.750	7
Communications	0.120	0.120	0.200	0.100	0.200	0.740	8
Manufacturing	0.026	0.160	0.200	0.100	0.150	0.636	9
Oil and gas	0.010	0.120	0.200	0.100	0.200	0.630	10
Power	0.005	0.160	0.200	0.100	0.150	0.615	11
Civil admin.	0.042	0.120	0.200	0.100	0.150	0.612	12

Table 12 Ranked CNIs based on multi-criteria decision matrix (continued)

CNI	*Gp*	*Gs*	*Df*	*As*	*Pr*	*Score*	*Rank*
Space and research	0.010	0.120	0.200	0.075	0.200	0.605	13
Defence	0.089	0.120	0.150	0.050	0.150	0.559	14
Info. technology	0.021	0.160	0.100	0.075	0.200	0.556	15
Commercial facilities	0.021	0.160	0.100	0.075	0.200	0.556	15
Industry	0.036	0.120	0.150	0.075	0.150	0.531	16
Pub/legal/others	0.063	0.080	0.200	0.025	0.100	0.468	17
E-government	0.083	0.080	0.100	0.050	0.150	0.463	18
Cybersecurity	0.005	0.040	0.100	0.050	0.250	0.445	19
Safety	0.031	0.120	0.100	0.075	0.100	0.426	20
Chemical	0.031	0.120	0.050	0.075	0.150	0.426	20
Emergency services	0.063	0.120	0.100	0.025	0.100	0.408	21
Nuclear	0.021	0.080	0.050	0.025	0.200	0.376	22
Rescue services	0.016	0.080	0.100	0.050	0.100	0.346	23
Dams	0.010	0.160	0.050	0.025	0.100	0.345	24
Mining and tourism	0.005	0.120	0.100	0.050	0.050	0.325	25
Strategic facilities	0.052	0.040	0.050	0.075	0.100	0.317	26
Information and culture	0.026	0.080	0.100	0.025	0.050	0.281	27
Irrigation	0.010	0.120	0.050	0.050	0.050	0.280	28
Info. and culture	0.031	0.080	0.050	0.025	0.050	0.236	29

6 Discussion

None of the African countries was among the top ten in HDI (UNDP, 2019). This is correlated in this study equally, like most African countries, being demographically large (World Population Maps – Graphs and maps – Ined – Institut national d'études démographiques, 2020) lacked sustainable digital transformation. Conversely, it shows that most of the European and Asian countries have a significant number of recognised CNI, ranging from 6 to 13. The USA topped the global list with 16 CNI, although some countries in the same continent identified as low as 4 CNI.

Another interesting insight is how some countries separated the CNI sectors. For instance, while some countries have separate sectors for communication, telecommunication, IT, and others combined them. On the other hand, Canada classified based on the similarity of functions, such as ICT for communications, telecommunications and IT. Similarly, some countries categorised safety, emergency services and rescue services into a single sector. The foregoing, clearly support the earlier assumption that there is no global consensus or standard for the identification, characterisation and designation of CI. Most countries arbitrarily decide on how to categorise and designate CIs perhaps based on national priorities (Mbanaso et al., 2019). This arbitrariness somehow implies that there is generally no harmonious way or consensus on how to identify and designate CNIs worldwide. Again, the analysis so far suggests that there is no correlation between HDI with the number of critical sectors a country can identify and designate, so HDI does not influence how countries view critical services to society.

Many countries are yet to appreciate the importance of identifying CNI appropriately. As our analysis has shown, out of the 49 countries studied, only about 57% of them identified between 8 and 16 CNI published in the public domain. The implication is that without proper characterisation, CNI protection in the context of cyber threats may be poorly handled due to an incoherent understanding of the potential threats faced. The fact remains that cyber threats have exacerbated CNI or CNII protection as indispensable to modern society as disruption or failure can adversely affect the wellbeing of the society (Iturriza et al., 2018; Rehak et al., 2016). However, in considering the criticality of CI, there are factors such as population size, geographical spread, interdependency, etc. that have to be considered. Interestingly, cybersecurity, space and research were designated by only a country each, while the oil and gas sector is recognised by three countries out of the 47 countries studied. For cybersecurity as an intangible infrastructure but providing essential functions or services, it is still debatable whether it can be considered as a sector.

It is already publicly known that cyberattacks are indiscriminate, and the effect may differ from one sector to another (Borgman et al., 2015; Microsoft, 2018; Stoddart, 2016; Usman and Shah, 1996). Proper identification and designation can help in characterising vulnerability, threat and risk at the sectorial level since sector organisation may face similar cyber threats; which can be an appropriate approach in cybersecurity management. The other important factors are types of CI dependency and types of failures which can have diverse effects such as cascading or escalating consequences on the other dependent CNI, implying that relationships amongst infrastructure matters. With the Covid-19 pandemic naturally affecting the health sector, directed cyberattacks against core CNI sectors should be anticipated to increase (Sochas et al., 2017; Sohrabi et al., 2020; Wenham et al., 2020). This further buttress the need for adequate classification of CNI for better prioritisation in time of emergency or crisis. Therefore, the characterisation of CNI provides the first step in an attempt to assess CNI dependency on ICT and the criticality of such dependency. The categorisation of CNI should be thoroughly synthesised based on global evaluation and national peculiarities. For instance, if there is a conscious mindset that health is a CI in the true sense, many countries could have approached the covid-19 pandemic differently (Disease Control Priorities, 2017; Sochas et al., 2017). It is insightfully, based on the data from the various countries studied the arbitrary understanding of critical sectors and limited details of subsectors of the core CNI sector in most countries. For example, ICT, IT, and cybersecurity are differently treated by many countries. Similarly, telecommunications and ICT, defence, safety and emergency services are viewed differently by many countries. Thus, the intricacies of characterisation can be linked to insufficient data in the body of knowledge. Take, for instance, the USA and Canada as depicted in Table 13, the disparity of CNI sector categorisation. This complication further strengthens the fact that the uninformed characterisation is due to a lack of research or the poor understanding of the variable factors by policymakers.

However, due to the global effect of cyber risk (Microsoft, 2018), the need for international cooperation and collaboration, the requirement for sector-based handling of critical information infrastructure protection (CIIP), it is imperative to consider consensus on the uniform characterisation of CNI in context. Additionally, the geographical and cross-border effects of cybersecurity breaches reinforce the above argument that global action on the characterisation of CNI has become a necessity. This will help in defining a comprehensive taxonomy and forge a common understanding at the global level to treat global cyber threat with a common understanding.

Table 13 Comparison of USA and Canada CNI sectors

CNI/country	*Energy*	*Nuclear*	*Chemical*	*Water*	*Dam*	*ICT*
USA	Y	Y	Y	Y	Y	
Canada	Y			Y		Y
CNI/country	*IT*	*Communication*	*Safety*	*Defence*	*Emergency services*	
USA	Y	Y		Y	Y	
Canada			Y			

7 Conclusions

In this article, we demonstrate how to evolve the characterisation of critical sectors, especially for the developing world that may be grappling to categorise CIs. Learning from 47 countries studied, we have attempted to compare CI sectors in Nigeria with that of other countries. The gaps in this process as well as the intricacies have been adequately exposed. We have noted some of the discrepancies in the way countries attempt to categorise CI, especially in Africa where there are gross gaps. We have argued the need for universal standardisation of CI categorisation due to the global nature of cybersecurity. The uniform identification and classification of critical sectors will strengthen global cybersecurity and CIIP.

Thus, we derive a methodological approach for proper identification, characterisation and designation of CI as CNI. Our approach can help mostly developing countries in Africa to suitably identify, categorise and designate CI for proportionate investment in the defence against, and anticipatory response to cyber threats. This study adds to current research in critical infrastructure protection (CIP), particularly, as CIIP has become a worldwide concern that requires local, national and international efforts.

8 Future work

We are currently investigating how to quantitatively measure the criticality of an infrastructure, and provide a comparative indication of criticality of infrastructures in a single view.

Acknowledgements

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

References

Adrian, C. and Co, C. (2020) *A Plan for Transformative Change by 2020.*

Almeida, A. and Técnico, I.S. (2008) *A Multi-criteria Methodology for the Identification & Ranking of Critical Infrastructures*, pp.1–10.

Andersson, G., Donalek, P., Farmer, R., Hatziargyriou, N., Kamwa, I., Kundur, P. and Vittal, V. (2005) 'Causes of the 2003 major grid blackouts in North America Europe, and recommended means to improve system dynamic performance', *IEEE Transactions on Power Systems*, Vol. 20, No. 4, pp.1922–1928, https://doi.org/10.1109/TPWRS.2005.857942.

Bank, W. (2020) *Morocco Infrastructure Review*, December 2019, https://doi.org/10.1596/33965.

Borgman, B., Mubarak, S. and Choo, K.K.R. (2015) 'Cyber security readiness in the South Australian Government', *Computer Standards and Interfaces*, Vol. 37, No. 2015, pp.1–8, https://doi.org/10.1016/j.csi.2014.06.002.

Briceno-Garmendia, C. and Benitez, D.A. (2014) *Cape Verde's Infrastructure A Continental Perspective*, May [online] https://www.researchgate.net/publication/228304222%0ACape (accessed 12 October 2020).

Brown, S.P.A. and Huntington, H.G. (2017) 'OPEC and world oil security', *Energy Policy*, Vol. 108, No. 9, pp.512–523, https://doi.org/10.1016/j.enpol.2017.06.034.

CIPedia (2012) *Critical Infrastructure Sector – CIPedia* [online] https://websites.fraunhofer.de/CIPedia/index.php/Critical_Infrastructure_Sector#Republic_of_Trinidad_.26_Tobago (accessed 14 October 2020).

CIPedia (2015) *Critical Infrastructure Sector – CIPedia* [online] https://websites.fraunhofer.de/CIPedia/index.php/Critical_Infrastructure_Protection (accessed 15 September 2020).

Compared, L. (2017) *National Cybersecurity Policy* [online] https://creativecommons.org/licenses/by-sa/4.0/.

Disease Control Priorities (2017) 'Improving health and reducing poverty', in *Disease Control Priorities*, 3rd ed., Vol. 9, https://doi.org/10.1596/978-1-4648-0527-1.

Dominguez, C. and Briceno-Garmendia, C. (2011) *Botswana's Infrastructure: A Continental Perspective*, World Bank Policy Research Working Paper, No. 5887.

Elgin, B., Myriam, D.C., Jennifer, G. and Manuel, S. (2010) *CRN Focal Report 4* [online] https://css.ethz.ch/en/services/digital-library/publications/publication.html/139032 (accessed 11 August 2020).

Encyclopedia, N.W. (2019) *List of Countries by Continent* [online] https://www.newworldencyclopedia.org/entry/list_of_countries_by_continent (accessed 27 March 2020).

Fu, C., Hou, B., Chang, W., Feng, N. and Yang, S. (2020) 'Comparison of evidential reasoning algorithm with linear combination in decision making', *International Journal of Fuzzy Systems*, Vol. 22, No. 2, pp.686–711, https://doi.org/10.1007/s40815-019-00746-3.

Herrera, L.C. and Maennel, O. (2019) 'A comprehensive instrument for identifying critical information infrastructure services', *International Journal of Critical Infrastructure Protection*, June, Vol. 25, pp.50–61, https://doi.org/10.1016/j.ijcip.2019.02.001.

Human Development Report (2019) *Human Development Indices and Indicators* [online] https://hdr.undp.org/sites/default/files/hdr_2019_overview_-_english.pdf.

Ibrahim, S.M.A.A.M.A.J.B. (2016) 'Critical infrastructure protection of ICT in Muslim world', *International Journal of Science and Research (IJSR)*, Vol. 5, No. 12, pp.325–329.

Infrastructure, C. (2020) *Critical National Infrastructure |CPNI| Public Website*, in Center for the Protection of Critical National Infrastruture [online] https://www.cpni.gov.uk/critical-national-infrastructure-0.

Islam, T. and Moselhi, O. (2012) 'Modeling geospatial interdependence for integrated municipal infrastructure', *Journal of Infrastructure Systems*, Vol. 18, No. 2, pp.68–74, https://doi.org/10.1061/(ASCE)IS.1943-555X.0000065.

ITU (2017) *Global Cybersecurity Index (GCI)*, in International Telecommunication Union.

Iturriza, M. et al. (2018) 'Modelling methodologies for analysing critical infrastructures', *Journal of Simulation*, Vol. 12, No. 2, pp.128–143, doi: 10.1080/17477778.2017.1418640.

Izuakor, C. and White, R. (2016) 'Critical infrastructure asset identification: policy, methodology and gap analysis', *IFIP Advances in Information and Communication Technology*, Vol. 485, pp.27–41, https://doi.org/10.1007/978-3-319-48737-3_2.

Katina, P.F. and Keating, C.B. (2015) 'Critical infrastructures: a perspective from systems of systems', *International Journal of Critical Infrastructures*, Vol. 11, No. 4, pp.316–344, https://doi.org/10.1504/IJCIS.2015.073840.

Kazimieras Zavadskas, E., Antucheviciene, J. and Chatterjee, P. (2018) 'Multiple-criteria decision-making (MCDM) techniques for business processes information management', *Information*, Vol. 10, No. 1, p.4, https://doi.org/10.3390/info10010004.

Khan, S., Ali, M., Sher, N., Asim, Y., Naeem, W. and Kamran, M. (2016) 'Software-defined networks (SDNs) and internet of things (IoTs): a qualitative prediction for 2020', *International Journal of Advanced Computer Science and Applications*, Vol. 7, No. 11, https://doi.org/10.14569/ijacsa.2016.071151.

Kovacevic,M., Assa, J., Bonini, A., Calderon, C., Hsu, Y-C., Lengfelder, C., Mukhopadhyay, T. and Shivani Nayyar, C.R. (2018) *Human Development Indices and Indicators 2018 Statistical Update*.

Lo, H.W., Liou, J.J.H., Huang, C.N., Chuang, Y.C. and Tzeng, G.H. (2020) 'A new soft computing approach for analyzing the influential relationships of critical infrastructures', *International Journal of Critical Infrastructure Protection*, Vol. 28, No. 28, pp.1–16, https://doi.org/10.1016/j.ijcip.2019.100336.

Luiijf, E.A.M. and Klaver, M.H.A. (2004) 'Protecting a nation's critical infrastructure: the first steps', *Conference Proceedings – IEEE International Conference on Systems, Man and Cybernetics*, Vol. 2, pp.1185–1190, https://doi.org/10.1109/ICSMC.2004.1399785.

Mao, Q. and Li, N. (2018) 'Assessment of the impact of interdependencies on the resilience of networked critical infrastructure systems', *Natural Hazards*, Vol. 93, No. 1, pp.315–337, https://doi.org/10.1007/s11069-018-3302-3.

Mbanaso, U.M., Kulugh, V.E. and Makinde, J.A. (2019) 'Characterisation of critical infrastructure organisation in Nigeria', *2019 15th International Conference on Electronics, Computer and Computation (ICECCO)*, pp.1–5, https://doi.org/10.1109/ICECCO48375.2019.9043210.

Mcevoy, W.E. (2008) *Critical Asset Identification Methodology*, Northeast Power Coordinating Council, Inc. (NPCC), New York.

Microsoft (2018) *Navigating the New Cybersecurity Threat Landscape How to Securely Accelerate your Digital Transformation Foreword*, pp.1–16.

Mitrovic, Z. (2018) *Protecting Critical Infrastructure, VM Advisory, Securing Your Cyberspace from VM Advisory Website* [online] https://vmadvisory.com/protecting-critical-infrastructure/ (accessed 28 October 2020).

Mohamed, A.A.A. (2019) 'On the rising interdependency between the power grid, ICT network, and e-mobility: modeling and analysis', *Energies*, Vol. 12, No. 10, pp.1–17, https://doi.org/10.3390/en12101874.

Moteff, J. (2005) 'Risk management and critical infrastructure protection: assessing, integrating, and managing threats, vulnerabilities and consequences', *International Journal of Disaster Risk Science*, Vol. 2, No. 1, pp.15–24, https://doi.org/10.1007/s13753-011-0002-y.

Office of National Security Adviser (2014) *National Cybersecurity Policy* [online] https://www.nacsa.gov.my/ncsp.php (accessed 4 February 2020).

Ousmane, D., John, B., Ntamu, F., Apetey, A., Okoro, R-C., Mohammed, U. and Cheetham, R. (2016) *An Infrastructure Action Plan for Nigeria* [online] https://www.afdb.org/fileadmin/uploads/afdb/Documents/Project-and-Operations/An_Infrastructure_Action_Plan_for_Nigeria_-_Closing_the_Infrastructure_Gap_and_Accelerating_Economic_Transformation.pdf (accessed 11 June 2020).

Pillay, K. (2017) *NCIIPC Newsletter*, National Critical Information Infrastructure Protection Centre, Vol. 1, No. 2, p.40.

Ponemon Institute (2019) *Research Studies: White Papers Archives for October* [online] https://www.ponemon.org/library/archives/2019/10 (accessed 26 January 2020).

Provincial Emergency Program (PEP) (2007) *Critical Infrastructure Rating Workbook,* EMBC [online] https://www.pep.bc.ca/community/CI-RatingsWkbk.pdf.

Rehak, D. et al. (2016) 'Quantitative evaluation of the synergistic effects of failures in a critical infrastructure system', *International Journal of Critical Infrastructure Protection*, Vol. 14, pp.3–17, doi: 10.1016/j.ijcip.2016.06.002.

Reichard, A., Tikos, A., Passeggia, A., Pyznar, M., Wrzosek, M., Konečný, M. and Salamon, Y. (2016) *Stocktaking, Analysis and Recommendations on the Protection of CIIs About ENISA Stocktaking, Analysis and Recommendations on the Protection of CIIs 03 Stocktaking, Analysis and Recommendations on the Protection of CIIs*, https://doi.org/10.2824/534303.

Rinaldi, S.M., Peerenboom, J.P. and Kelly, T.K. (2001) 'Identifying, understanding, and analyzing critical infrastructure interdependencies', *IEEE Control Systems Magazine*, Vol. 21, No. 6, pp.11–25, https://doi.org/10.1109/37.969131.

Rossella Mattioli, D.C.L-B. (2014) *Methodologies for the Identification of Critical Information Infrastructure Assets and Services*, https://doi.org/10.2824/38100.

Serre, D. and Heinzlef, C. (2018) 'Assessing and mapping urban resilience to floods with respect to cascading effects through critical infrastructure networks', *International Journal of Disaster Risk Reduction*, October 2017, Vol. 30, pp.235–243, https://doi.org/10.1016/j.ijdrr.2018.02.018.

Siddiqui, F., Hagan, M. and Sezer, S. (2018) 'Embedded policing and policy enforcement approach for future secure IoT technologies', *IET Conference Publications*, 2018(CP740), pp.1–10, https://doi.org/10.1049/cp.2018.0010.

Singh, A.N., Gupta, M.P. and Ojha, A. (2014) 'Identifying critical infrastructure sectors and their dependencies: an Indian scenario', *International Journal of Critical Infrastructure Protection*, Vol. 7, No. 2, pp.71–85, https://doi.org/10.1016/j.ijcip.2014.04.003.

Sochas, L., Channon, A. and Nam, S. (2017) 'Counting indirect crisis-related deaths in the context of a low-resilience health system: the case of maternal and neonatal health during the Ebola epidemic in Sierra Leone', *Health Policy Plan*, Vol. 32, pp.iii32–iii39.

Sohrabi, C., Alsafi, Z., O'Neill, N., Khan, M., Kerwan, A., Al-Jabir, A. and Agha, R. (2020) 'World Health Organization declares global emergency: a review of the 2019 novel coronavirus (COVID-19)', *International Journal of Surgery*, April, Vol. 76, pp.71–76, https://doi.org/10.1016/j.ijsu.2020.02.034.

Srinivasu, B. and Islamia, J.M. (2013) 'Infrastructure development and economic growth : prospects and perspective', *Journal Of Business Management & Social Sciences Research*, Vol. 2, No. 1, pp.81–91.

Stéphane, H., Gergana, P. and Salash, N. (2018) *The First Cybersecurity Law in Luxembourg is Coming Introducing Security and Incident Notification Requirements for Operators of Essential Services and Digital Service Providers* [online] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (accessed 16 March 2021).

Stoddart, K. (2016) 'UK cyber security and critical national infrastructure protection', *International Affairs*, Vol. 92, No. 5, pp.1079–1105, https://doi.org/10.1111/1468-2346.12706.

Theron, P. and Bologna, S. (2013) *Critical Information Infrastructure Protection and Resilience in the ICT Sector*, IGI Global, Hershey, PA 17033, USA, doi: 10.4018/978-1-4666-2964-6.

United Nations Development Programme (UNDP) (2019) *2019 Human Development Index Ranking | Human Development Reports* [online] https://hdr.undp.org/en/content/2019-human-development-index-ranking (accessed 21 April 2020).

UNOPS Lucia, S. (2020) *National Infrastructure Assessment Infrastructure*, August.

Usman, A.K. and Shah, M.H. (1996) 'Critical success factors for preventing e-banking fraud', *Journal of Internet Banking and Commerce*, Vol. 18 [online] https://www.icommercecentral.com/open-access/critical-success-factors-for-preventing-ebanking-fraud-1-14.php?aid=38196 (accessed 14 November 2020).

Wenham, C., Smith, J. and Morgan, R. (2020) 'COVID-19: the gendered impacts of the outbreak', *The Lancet*, Vol. 395, No. 10227, pp.846–848, https://doi.org/10.1016/S0140-6736(20)30526-2.

West, D.M. and Lansang, C. (2018) *Global Manufacturing Scorecard: How the US Compares to 18 Other Nations from Governance Studies Main Line Website* [online] https://www.brookings.edu/research/global-manufacturing-scorecard-how-the-us-compares-to-18-other-nations/ (accessed 27 March 2020).

World Population Maps – Graphs and maps – Ined – Institut national d'études démographiques (2020) [online] https://www.ined.fr/en/everything_about_population/graphs-maps/world-maps-interactiv/ (accessed 8 March 2021).

World, C. (2020) *7 Continents of the World and their Countries* [online] https://www.countries-ofthe-world.com/continents-of-the-world.html (accessed 27 March 2020).

Worldatlas (2020) *Countries Listed by Continents* [online] https://www.worldatlas.com/cntycont.htm (accessed 26 April 2020).

Appendix

Table A1a Identified CNI per country selected

		Sectors *Countries*	*Chemical*	*Civil administration*	*Communications*	*Comm. facilities*	*Cybersecurity*	*Dams*	*Defence*	*E-government*	*Emergency services*	*Energy*	*Financial*	*Food*	*Health*	*ICT*	*Info. technology*	*Info and culture*	*Industry*	*Irrigation*	*Manufacturing*	*Mining and tourism*	*Nuclear*	*Oil and gas*	*Power*	*Pub/ legal order*	*Rescue services*	*Safety*	*Space and research*	*Strategic facilities*	*Transportation*	*Water*	*Total*
Africa	1	South Africa		Y					Y			Y	Y		Y		Y				Y	Y				Y					Y	Y	11
	2	Cape Verde										Y				Y															Y	Y	4
	3	Morocco										Y			Y	Y															Y	Y	5
	4	Egypt										Y				Y		Y													Y		4
	5	Botswana														Y				Y											Y	Y	4
	6	Libya			Y							Y	Y	Y	Y						Y	Y		Y	Y		Y				Y		11
	7	Ghana							Y	Y	Y	Y	Y	Y	Y	Y															Y	Y	10
	8	Kenya										Y				Y				Y											Y	Y	5
	9	Nigeria	Y		Y	Y		Y	Y	Y	Y	Y	Y	Y	Y		Y				Y										Y	Y	15
Asia	1	Rep. of Korea			Y	Y				Y		Y	Y		Y								Y								Y	Y	9
	2	Japan	Y	Y								Y	Y		Y	Y															Y	Y	8
	3	Singapore		Y							Y	Y	Y		Y	Y		Y													Y	Y	9
	4	Qatar								Y		Y	Y		Y	Y															Y		6
	5	UAE								Y	Y	Y	Y	Y	Y	Y															Y	Y	9
	6	Malaysia							Y	Y	Y	Y	Y	Y	Y	Y															Y	Y	10
	7	Turkey			Y							Y	Y																	Y	Y	Y	6
	8	Kuwait							Y			Y	Y		Y	Y								Y		Y					Y		8
	9	China										Y		Y	Y	Y				Y											Y	Y	7
	10	Philippines			Y	Y				Y	Y	Y	Y		Y			Y														Y	9
Europe	1	Iceland			Y						Y	Y	Y	Y	Y																Y		7
	2	Switzerland							Y			Y	Y	Y	Y	Y			Y											Y	Y	Y	10
	3	Denmark							Y			Y	Y	Y	Y	Y										Y	Y				Y	Y	10
	4	United Kingdom	Y		Y				Y	Y	Y	Y	Y	Y	Y								Y							Y	Y	Y	13
	5	Netherlands	Y						Y		Y	Y	Y	Y	Y			Y				Y			Y		Y			Y			12
	6	Norway			Y							Y												Y						Y	Y	Y	6
	7	Luxembourg										Y	Y		Y	Y															Y	Y	6
	8	Sweden							Y	Y		Y	Y	Y	Y	Y			Y							Y				Y	Y		11
	9	Germany										Y	Y	Y	Y	Y		Y								Y					Y	Y	9
	10	France		Y					Y			Y	Y	Y	Y	Y			Y							Y			Y		Y	Y	12
		Total	4	4	8	3	0	1	11	9	9	28	22	14	23	19	2	5	3	3	3	3	2	3	2	6	3	0	1	6	27	22	

Table A1b Identified CNI per country selected

		Sectors Countries	*Chemical*	*Civil administration*	*Communications*	*Comm. facilities*	*Cybersecurity*	*Dams*	*Defence*	*E-Government*	*Emergency services*	*Energy*	*Financial*	*Food*	*Health*	*ICT*	*Info. technology*	*Info and culture*	*Industry*	*Irrigation*	*Manufacturing*	*Mining and tourism*	*Nuclear*	*Oil and gas*	*Power*	*Pub/ legal order*	*Rescue services*	*Safety*	*Space and research*	*Strategic facilities*	*Transportation*	*Water*	*Total*
N. America	1	United States	Y	Y	Y	Y		Y	Y		Y	Y	Y	Y	Y		Y				Y		Y								Y	Y	16
	2	Canada		Y								Y	Y	Y	Y	Y					Y							Y			Y	Y	10
	3	Barbados										Y	Y			Y															Y	Y	5
	4	Bahamas			Y							Y																			Y	Y	4
	5	Mexico			Y		Y					Y		Y																Y	Y	Y	7
	6	St. Lucia										Y	Y	Y	Y						Y	Y				Y	Y		Y		Y	Y	11
	7	El Salvador			Y							Y																			Y	Y	4
S. America	1	Argentina			Y							Y																			Y	Y	4
	2	Chile			Y				Y	Y		Y	Y		Y												Y	Y			Y	Y	10
	3	Brazil			Y							Y																			Y	Y	4
	4	Trinidad and Tobago											Y		Y	Y												Y			Y		5
	5	Colombia			Y							Y			Y																	Y	4
	6	Venezuela										Y			Y																Y		3
	7	Peru			Y							Y																				Y	3
Oceania	1	New Zealand			Y					Y	Y	Y			Y																Y		6
	2	Australia			Y							Y	Y	Y	Y																Y	Y	7
	3	Fiji										Y					Y														Y	Y	4
	4	Solomon Islands										Y																Y			Y	Y	4
		Total	1	2	11	1	1	1	2	2	2	17	7	5	9	3	2	0	0	0	3	1	1	0	0	1	2	4	1	1	16	15	