Supported by tetfund TERTIARY EDUCATION TRUST FUND

Empirical Findings of the Degree of Dependency of Critical Infrastructures on Information and Communication Technology

Uche Magnus Mbanaso[1] and Victor Emmanuel Kulugh[2]
[1-2]Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria
[2]corresponding author: vkulugh30@gmail.com, 08069811543

Received: December 13, 2021 Accepted: February 20, 2022

Abstract: The increasing adoption of ICT in traditional Critical infrastructure (CI) to improve productivity and efficiency while creating new services and functions is vital for modern society. However, CI driven by ICT is inherently vulnerable to cyberattacks with potentials for cascaded and escalating effects on depending and interconnected CIs. Therefore, the degree of CI dependency on ICT is a cyber risk factor that requires empirical quantification. Consequently, an ICT Dependency Model was developed for this purpose, based on predefined pillars, namely: *Adoption*, *Integration* and *Automation*. These pillars form the basis for computation of the ICT dependency index (IDI). The ICT Dependency Quadrant (IDQ) is introduced to categorise the IDI of CI organisations into four quadrants, viz: Q1, Q2, Q3 and Q4. Twenty-seven CI organisations participated in the pilot test of the model. The Findings showed that 3 of the CI organisations fall in Q4, while 20 fall in Q3. Similarly, 3 and 1 organisations fall into Q2 and Q1 respectively. The combination of IDI and IDQ provide a comparative tool to visualise the various IDI scores in a single view. Thus, it supports the monitoring of the growth of ICT in CI organisations vis-à-vis the potential cyber risk it presents.

Keywords: Nigeria, Critical Sectors, Critical Infrastructure, Critical National Information Infrastructure, ICT Dependency.

Introduction

The fundamental objective of every nation-state is for her economy and security to operate without disruptions. This depends on the effective functioning of her Critical Infrastructure (CI) assets. However, the failure, disruption or degradation of a single CI can have monumental negative consequences on national security, economy and wellbeing of citizens (USA Patriot Act, 2001; Banerjee *et al.*, 2017; Kure, Islam and Razzaque, 2018). According to Izuakor & White, (2017), the growing dependence on information and communications technology (ICT) has continued to influence the increasing interconnectedness of modern critical infrastructure and accelerated integrations. This singularly exacerbates the threat landscape with intriguing cyber risks due to the inherent ICT vulnerabilities. Consequently, these cyber events introduce some elements of surprise and urgency with high risks (Canzani, 2017). Therefore, modern CI dependency on ICT requires proportionate protections against cyber events capable of causing damages of catastrophic or debilitating proportion. Conversely, the proportionate protection of CI, requires that the extent of CI's dependency on ICT be quantified using a scientific and empirical measurement to ascertain this degree of importance. The continuous evaluation of the increasing degree of dependency of CI such as electricity, water, transportation, education, financial services, intelligence, security, etc. on ICT (Mbanaso *et al.*, 2019a), is essential to Critical Information Infrastructure Protection (CIIP).

Emerging technologies like the Internet of Things (IoT), Smart Grids, Industrial Control Systems (ICS), Cloud Computing, 5G and Smart Cities will further exacerbate CI cyber risks as they will potentially amplify CI dependency on ICT. Consequently, the unavailability, disruption or destruction of ICT-enabled systems even for the shortest period has the potentials for catastrophic failures, which may result to cascading and escalating effects (Argonne National Laboratory, 2015; Rehak *et al.*, 2018). In (Dobson *et al.*, 2019), it is argued that critical sectors are sturdily dependent on ICT infrastructure by evolution and opportunism without foresight and adequate planning. As a result, the security and safety of the ICT systems are not usually envisioned *ab initio*. However, a key requirement for CIIP should be to understand the extent of the inherent vulnerability of ICT systems (Petit *et al.*, 2013; Pursiainen, 2020) due to dependency. So, the expectation is that CI should have the ability (resilience) to maintain a reasonably acceptable level of operation in the face of disruptions including deliberate cyberattacks, operational overload, misconfiguration, and equipment failures (Willke, 2007; Pursiainen, 2020). Thus, CI supported by growing ICT interconnections to improve modern society requires the guaranteed operational correctness within the interlace of the underlying ICT system vulnerabilities.

In Nigeria, despite the increasing digitalisation of traditional operations and emergence of critical information infrastructure (CII), empirical study in this area is unduly limited. Basic information regarding CII is unavailable in the public domain. More so, there is no publicly available empirical evidence of growing CI dependency on ICT, in a manner that critical sectors' managers can scientifically gauge the level of their ICT dependence. The implication is that any protection strategy that is not empirically supported is akin to a false sense of security. Critical sector organisations need to continuously estimate the level of ICT dependency to further appreciate the cyber risks they may potentially face. To fill this void, this article presents a quantitative ICT dependency assessment, leveraging a dependency tool developed by our research team (Mbanaso *et al.*, 2019b). Three metrics are implemented i.e. *Adoption*, *Integration* and *Automation* to reflect various maturity levels of ICT provision. Each metric has indicators as units of quantifiable measurements. The survey inputs from the critical sector organisations formed the basis for the computation of various organisational ICT Dependency Index (IDI) based on the mathematical constructs of the model.
The rest of the paper is organised as follows: Section 2 provides background and related works; Section 3 describes the methodological approach, and section 4 describes the computational model; section 5 presents the results. Section 6, presents findings, analyses and discussions; and section 7 concludes the paper.

Background and Related Works

Globally, critical infrastructures face increased risk (Bibao-Osorio, Dutta and Lanvin, 2014; Kure, Islam and Razzaque, 2018). A combination of factors account for the increasing CI-related risk; namely: urbanisation which stresses the utilisation of old infrastructures to their limits; the increasing interwovenness and dependencies of infrastructural services; the desire of the population to have services available anytime, anywhere (Setola, Luiijf and Theocharidou, 2017). Meeting the above goals requires an increased utilisation of ICT to improve efficiency, productivity, and accessibility. Then, provide support for new services and general optimization of the capacity of the CI (Taylor *et al.*, 2015; NITDA, 2019) and to monitor, control and increase CI functionalities (Fekete, 2011). The effect of this is amplified interconnectedness of CI through ICT. However, the increased interconnectedness presents new dimensions of dependencies and interdependencies amongst CI and ICT (Bloomfield *et al.*, 2017). Arguably, it has expanded the dependency and independency of CI (Krepinevich, 2012; Robinson *et al.*, 2018). According to Dobson et al (2019), this has created the cyber organisational layer for CI in a way that the cyber layer is becoming one of the most important sources of interdependencies amidst other organisational layers. Traditionally, the cyber elements are inherently vulnerable to malicious exploitation (Izuakor and White, 2016), making cyberattacks a major threat to CI systems with potentials for cascading failures (Dobson *et al.*, 2019). Consequently, the risk of even a minor disruption in a single CI can lead to catastrophic cascading or escalating failures of other CI networks (Buldyrev *et al.*, 2010). The speed at which ICT systems process data further exacerbate the potential consequences arising from cyberattacks on CI coupled with the fact that cyberattacks, unlike physical attacks can go unnoticed over time, further amplifying the risk of substantial dependency on cyber systems (Kundhavai and Sridevi, 2016).

Over the years, cyber threat actors have taken undue advantage of the inherent cyber vulnerabilities to degrade, abuse or destroy CI to the detriment of the owners, operators and the population (Schreier, 2015; Theohary and Rollins, 2015). For instance, a rogue nation can leverage vulnerabilities in cyber systems to undermine the security of the CI of rival or enemy nations (Saloky and Šeminský, 2017). Invariably, attacks such as advanced persistent attacks (APTs) on CI may go over a long period undetected (Galinec and Steingartner, 2017; Tatar, Gokce and Gheorghe, 2017). Additionally, terrorist organisations do take unfair advantage of cyber weaknesses to carry out nefarious activities against states (Almeida and Técnico, 2008). Similarly, cybercriminal groups can equally exploit a weakness in ICT systems to gain undesired benefits (Baboo and Megalai, 2015); where this vulnerable ICT infrastructure is shared across many CI, a common cause effect may result. Equally, emerging technologies such as the IoT is promising to exponentially increase the integration and interconnectedness of physical infrastructures will further exacerbate security issues in CI. And with 5G technology (WEF, 2015; Dobson *et al.*, 2019), security may worsen exponentially. According to Dobson et al., (2019), these are bringing fresh risks as the cybersecurity maturity of emerging new technologies remains very low. In most cases, security is not thoroughly considered at the initial design and implementations by default. The share expansion of the cyberattack surface created by emerging cyber-physical systems has heightened the risk landscape.

The Ukrainian power grid attack in December 2015 is an example of the cyberattack on CI that had cascading consequences, leading to a total power blackout and impacted other CIs and the population (Lee, Assante and Conway, 2016). Often, the financial sector's cyberinfrastructure across the globe have suffered unprecedented cyberattacks exploiting inherent flaws in cyber systems (Donzelli, Setola and Tucci, 2004). Also, the electricity power blackouts in North America and Canada in 2003, was due to cyberattacks that disrupted the ICT system and failed to provide real-time diagnostic support (Anderson, 2019). The failure cascaded into several geographical regions as well as impacted the operation of other CIs significantly.

Critical Infrastructure Dependence on ICT in Nigeria

In Nigeria, there has been a huge implementation of ICT systems across government and private sector organisations. Notably, the successful implementation of e-Government solutions such as the Treasury Single Account (TSA), Integrated Personnel and Payroll Information System (IPPIS), Government Integrated Financial Management Information System (GIFMIS), Bank Verification Number (BVN), identity management with the National Identity Management Commission (NIMC)'s National Identity Number (NIN) among others (NITDA, 2019). The Nigeria E-Government Master Plan (FMoC, no date) seeks to further deepen the implementation of technology infrastructure in government business. Currently, some aspects of Government to citizen (G2C) model of e-government are been implemented in areas such as immigration services for passport issuance, educational services such as JAMB, health services through the national health insurance scheme, citizenship and voting through the national identity number (NIN) and e-voters' registration. Government to Business (G2B) models are Trademark application, business registration services at the Corporate Affairs Commission, spectrum license application at NCC, NAFDAC export approvals, tax services at the FIRS. There are, however, limited application of the government to government (G2G) models (FMoC, no date). The National E-Government Master Plan and Nigeria E-government interoperability framework seek to further integrate all these processes such that there will be a one-stop-portal for accessing government services by citizens, businesses and government agencies.   One first step in this regard is the implementation of the government portal: www.services.gov.ng. These efforts have heightened ICT utilization within the Nigerian CIs as well as increase their interconnectivity especially post-implementation of the e-governance interoperability framework and the e-government master plan.

Similarly, the National Digital Economy Policy and strategy 2020-2025 (FMoC&DE, 2020a) seek to implement an 8-pillar digital economy strategy thus: developmental regulation, digital literacy, solid infrastructure, service infrastructure, digital services development and promotion, soft infrastructure, digital society and emerging technologies, indigenous content development and adoption. Each of the pillars when fully implemented will aggregate to create a robust and thriving digital economy. In an attempt to begin the implementation of the various pillars of the digital economy plan, the Ministry of Communication and Digital Economy has commenced efforts in the implementation of the physical pillar with the development of the Nigeria National Broadband Plan (NNBP) – 2020-2025 (FMoC&DE, 2020b). The NNBP 2020-2025 will implement strategies that will address the gaps in broadband penetration which is a key driver of the digital economy. The plan addresses infrastructure, policy, demand drivers and funding/incentives (FMoC&DE, 2020b). The goal is to facilitate broadband penetration, improve quality of service, optimize usage and benefits of the spectrum, and promote Information Communication Technologies (ICTs) innovation and investment opportunities across the country (Nigerian Communication Commission, 2015). The World Bank's Nigeria Digital Economy Diagnostics document (World Bank, 2019) suggests that implementation of the 8-pillar digital economy plan will bring shared prosperity and reduce poverty while impacting virtually every aspect of the economy. This will impact digital infrastructure in areas of transportation, energy, health, culture and finance. These, in turn will create the smart city, smart energy, smart agriculture and boost e-commerce activities.

The foregoing has prompted intensified research efforts to understand and address cyber risks as a result of growing CI dependency on ICT in Nigeria. Although there is a rising consensus within the CI research community that the increasing interdependencies of CIs are fuelled by continuous integration of emerging ICT systems (Kure, Islam and Razzaque, 2018; Seppänen *et al.*, 2018; Tweneboah-Koduah and Buchanan, 2018), which is bringing huge complexity. The (FMoC&DE, 2020a) also acknowledge that the viability and sustainability of the gains of the digital economy is a product of complex interconnectedness. However, most research efforts have concentrated on qualitative assessments, which limits the computation and statistical analysis of CIs dependency on ICT. Also, other research efforts geared towards usage measurement of ICT by populations such as the network readiness index (NRI) (WEF, 2016), which assesses the preparedness of nations, and how they continuously leverage emerging technologies to reap the benefits presented by digital revolution and evolution (UNCTAD, 2011). Similarly, the Global Cybersecurity Index (GCI) measures the cybersecurity readiness of member countries (ITU, 2018). These efforts fall short of quantifying the degree of CI dependency on ICT.

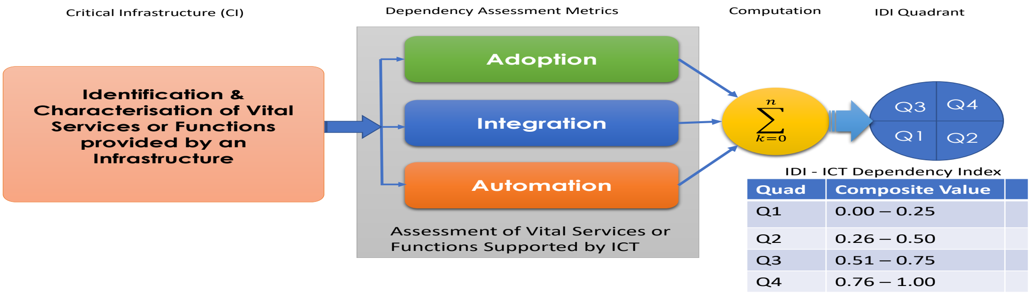
The Nigeria national cybersecurity policy and strategy (Office of the National Security Adviser (ONSA), 2014, 2021) recognised the increased dependency of CI on ICT infrastructure and the risk associated with this dependency. Consequently, the strategy listed thirteen critical infrastructure sectors. However, there is no scientific or empirical approach to measuring the ICT dependency and subsequent cyber risks exposure of the listed critical sectors. Donzelli et al., (2004) proposed a framework that identifies dependencies of an organization on technological infrastructures and to evaluate the business impact of any possible failure without the implementation of scientific metrics to quantify the dependency. Similar work by European Commission (2009) studied Critical Dependencies of Energy, Finance and Transport Infrastructure on ICT Infrastructure but lacked quantitative computational model to use empirical data to quantify the CI level of dependency on ICT. Thus, this paper describes a computational model to assess the CI degree of dependency on ICT quantitatively.

Materials and Methods

This study belongs to the positivist paradigm and experimental using the principles of design and creation research (Oates, 2006). The quantitative measurement is based on computational ICT Dependency tool (Mbanaso *et al.*, 2019b) based on three metrics i.e. *Adoption*, *Integration* and *Automation*. The model has mathematical constructs that influenced the creation of data structures, algorithms and development of software tool itself. An instrument is framed based on the three metrics and indicators that are a granular unit of measure based on a ratio scale. The questionnaires are close-ended and span across the metrics, the indicators are the specific input parameters to the model to enable quantitative measurement. As a result, the questionnaire was administered to 27 organisations from 9 critical sectors with not less than three respondents from each organisation. The justification to use a minimum of 3 respondents from each organisation is to minimise bias that may arise from a single respondent per organisation. The mean of the of three computed scores of the respondents per organisation is taken as the score of that organisation. The real-time data generation tool automatically computes and analyse the Dependency Factor (DF) scores of the metrics, and subsequently compute the IDI scores, dissect and classify IDI scores into constituent quadrants. Additionally, the real-time computation places the sectors and organisations in their respective quads based on the IDI scores.

The ICT Dependency Model

In Figure 1, the ICT Dependency model showing various components, and how they interrelate is presented as adopted from (Mbanaso, Kulugh, Musa, Aimufua, & Dandaura, 2021). There are four principal components, each comprises sub-components designed to provide more in-depth measurements. The dependency assessment metrics define the thematic areas of measurement, the computation component calculates the values derived from the metrics, the variable items of measure reflect the various indicators.


Critical Infrastructure (CI)
Dependency Assessment Metrics
Computation
IDI Quadrant
Identification & Characterisation of Vital Services or Functions provided by an Infrastructure
Adoption
Integration
Automation
Assessment of Vital Services or Functions Supported by ICT
$\sum_{k=0}^{n}$
Q3
Q4
Q1
Q2
IDI - ICT Dependency Index

Quad	Composite Value
Q1	0.00 – 0.25
Q2	0.26 – 0.50
Q3	0.51 – 0.75
Q4	0.76 – 1.00

Figure 1:ICT Dependency Model, Adopted from Mbanaso et al, 2021)

The various components of the ICT dependency model, namely: CI characterisation, dependency assessment metrics, dependency indicator, computational model and ICT dependency quadrant (IDQ) perform different functions towards accurate measurements as described in (Mbanaso and Kulugh, 2021). Table 1 is a further description of the dependency assessment metrics and their respective contributions to the ICT dependency assessment equations based on cyber risk considerations

Table 1: Description of Dependency Assessment Metrics

SN	Dependency Metrics	Abbreviation	Description	Weights (%)	Weight factor (w_f)
1	Adoption	*Ade*	This depicts the organisation's readiness to adopt ICT as a viable operational tool for improved productivity and efficiency but little or none has been implemented.	25	0.25
2	Integration	*Ine*	This portrays that integration of ICT functions and features into the core operations of a particular organisation has been achieved.	35	0.35
3	Automation	*Aue*	This indicates the integration of core operations with full automation of business operations using ICT functions and features.	40	0.40
			Total	**100**	**1.00**

The individual contributions of the dependency assessment metrics is expressed in Table 1 as weights or weight factors. Table 2 describeds the *Dependency Indicator (DI)* as a unit of measure based on a quantitative five-range ratio scale. It captures in quantitative terms the effect of exact dependency attributes, depicting the level of achievement of that particular indicator in context.

Table 2: Dependency Indicator (DI) Scale

Qualitative	Quantitative	Description
None	0	None existence – complete absence, implying quantitatively a zero attribute of measure.
Low	2	Has little attribute value of measure to the organisational operation, function or service.
Moderate	3	The modest attribute value of measure to the organisational operation, function or service
High	4	Indication of the substantive attribute value of measure to the organisational operation, function or service.
Very High	5	Implies a mission-critical attribute value of measure to the organisational operation, function or service.

Table 3: ICT Dependency Quadrant (IDQ) Description

Quadrant	Composite Values	Note
Q1	0.00 – 0.25	The organisation is considering the use of ICT infrastructure, but efforts are not documented nor organised. This quad connotes lower dependency and lower risk.
Q2	0.26 – 0.50	Some ICT infrastructure is in place, but not consistently and structurally organised; considerably, important elements of ICT are missing. This quad implies high risk with low dependency.
Q3	0.51 – 0.75	ICT infrastructure is structurally implemented and integrated into the core organisation's operations but with fewer elements missing. This quad means high dependency and high risk.
Q4	0,76 – 1.00	Critical operations, services and functions are ICT-enabled and automated. This quad implies high dependency and very high risk.

Computation Model: The computation model calculates the ICT Dependency Index (IDI) based on the summation of measured metrics and indicators. The underlying mathematical constructs described in (Mbanaso and Kulugh, 2021) shows a step-wise mathematical formulae for the various stages of computation to arrive at the IDI.

The ICT Dependency Quadrant (IDQ): The IDQ concept is shown in Figure 2, which offers the mechanism for a single view of IDIs of various organisations. The concept of the quadrant is to provide a four-band range based on proportional dependency and risk in a single assessment. A full description of the quads is provided in Table 3. Figures 2 presents the ICT Dependency Quadrant (IDQ), it depicts that ICT dependency can be directly proportional to cyber risk, i.e., the higher the dependency, the higher the potential cyber risk. Thus, organisations that fall under Q1 are less dependent on ICT, which implies that cyber risk is low. Table 3 is a description of the various quadrants and the ranges of scores that defines them.

The ICT Dependency Mathematical Model

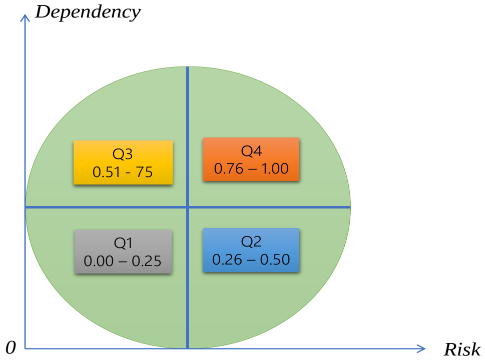


Figure 2: ICT Dependency Quadrant: Adopted from (Mbanaso et al 2021

This section provides formally, the taxonomy of ICT-dependency quantitative measurement, with mathematical and standardised parameters as adopted from (Mbanaso and Kulugh, 2021). This aims to provide a scientific but repeatable and transparent measurement mechanism influenced by common criteria. This provides the basis to calculate the bands of ICT-dependency based on a scale of degree of preference since all CIs cannot have an equal degree of ICT dependency.

$$IDI = 0.25(DF_0Ade) + 0.35(DF_0Ine) + 0.40(DF_0Aue$$

Thus, *IDI* lies between ($0.00 \leq$ IDI ≤ 1.00), which represents the composite ICT Dependency Index (IDI) value of a particular organisation. The equation and its derivation was adopted from (Mbanaso et al., 2021) and applied on the computations that generated the results shown in the next section.

Results and Discussion

Figure 3 presents the data of the survey, showing organisations, their IDI scores and quadrants. Note, the organisations have been masked to protect the identity and privacy of respondents. Based on Figure 3, it can be deduced that 3 organisations scored above 0.75 in IDI and are in Q4; similarly, 20 organisations scored between 0.51 and 0.75 to fall in Q3; and 3 organisations scored between 0.26 and 0.50 while 1 organisation scored below 0.26, thus falling in Q2 and Q1 respectively. The dependency assessments metrics of *Adoption*, *Integration* and *Automation* formed the ground for data collection as presented in Figure 3. These metrics provide the foundations for the measurement of CI dependency on ICT from a cyber risk-based perspective. Thus, data was collected and computed based on these metrics. The computation of the IDI presented in Figure 3 relied on the data and computations of the dependency metrics. Observable trends and insights from the analysis of this data are presented the Findings, Analysis and Discussion section.

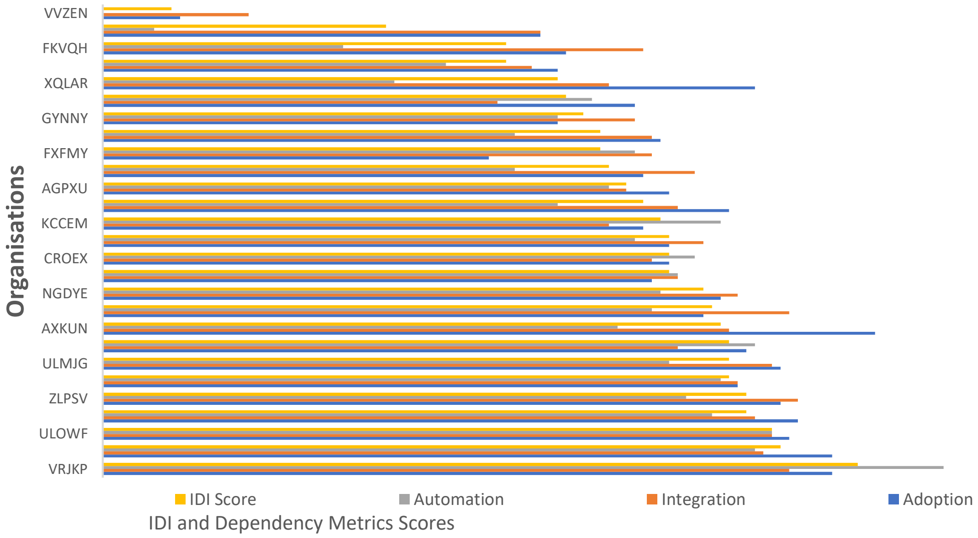


Figure 3: Comparism of IDI and Dependency Metrics

Findings, Analysis and Discussions

Figure 3 presents organisations according to their ICT dependency Index (IDI), adoption, integration and automation scores, the distribtuion in the Figure further shows that 3 organisations are in Q4, 20 in Q3 indicating a high level of dependency on ICT and a corresponding high cyber risk, 3 and 1 organisation fall in Q2 and Q1 respectively. It equally showed that dependency can cut across sectors, this can be viewed in Q3 where 20 organisations' IDI cut across 8 out of the 9 sectors. More so, the IDI scores in Q4 and Q2 span across sectors. Figure 3 depicts the scores based on ID and the dependency metrics of *Adoption*, *Integration* and *Automation*. The results as further analysed in Figure 4 showed that 59.26% of the organisations fall in Q3 of adoption and automation metrics respectively. 66.67% of the organisations fall in Q3 of the integration metrics. This is in contrast with the overall IDI of the organisations as shown in Figure 3, where 74.07% of the organisations fall in the Q3 band. *Note that the IDI score is a normalised aggregation of the scores of the dependency metrics (i.e adoption, integration and automation).* Consequently, it can be inferred that low scores in some metrics were compensated for with high scores in other metrics for the same organisation to generate high IDI scores in these organisations. This accounts for more organisations with high IDI scores when compared to the individual dependency metrics. The implication is that organisations should attempt to understand how the various metrics affect their overall scores and potentially the high risk areas.

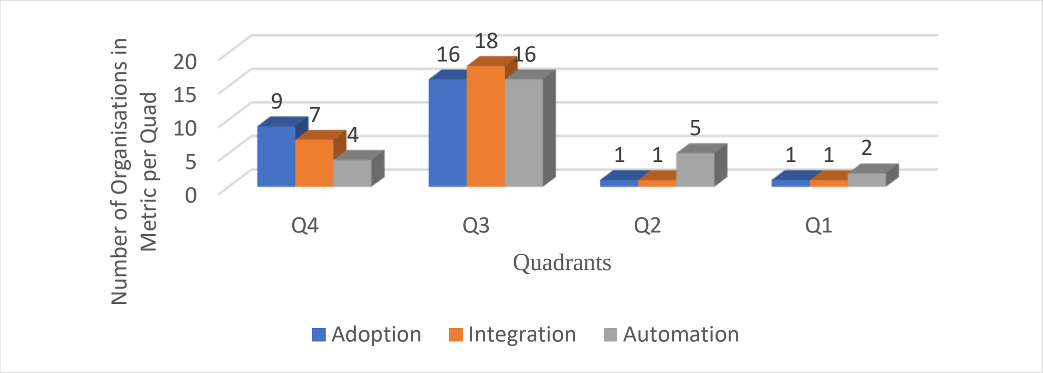


Figure 4: Number of Organisations Per Quad of Dependency Metrics

Organisations in Quadrants of the Dependency Metrics

Figure 4 is an extrapolation of the number of organisations per quadrant of the dependency metrics (DM). Thus, Figure 4 shows that in the adoption metric, 9 organisations are in Q4, 16 in Q3 while Q2 and Q1 have 1 organisation each. The integration DM showed that 7 organisations are in Q4, 18 in Q3 while Q2 and Q1 have 1 organisation each. The automation DM, on the other hand, has 4 Organisations in Q4, 16 in Q3, 5 and 2 in Q2 and Q1 respectively. The implication is that the 4 organisations with a Q4 dependency on the automation metric are highly dependent and as well as being at extreme risk level. Their risk is further compounded if they have a poor adoption metric performance. It can also be observed in Figure 4 that the bars in Q4 showed a normal trajectory with the highest number of organisations in adoption, followed by integration and automation in that other, however, Q3 bars showed an uneven distribution of organisations with an equal number of organisations

in *Adoption* and *Automation* metrics, while the highest number of organisations appeared in

Integration. Q2 and Q1 show an opposite trajectory when compared to Q4. Both Q2 and Q1displayed the opposite of the Q4 distribution, having the highest number of organisations at the automation metric. The implication is that a greater number of organisations as shown in Figures 6 and 7 have distribution patterns of ICT implementation that show an increase in their vulnerability to cyber risk.

Figure 5 is the distribution of the participating organisations and sectors according to the ICT Dependency Quadrant (IDQ); thus, it can be shown that 3 organisations are in Q4, 20 organisations representing 74.07% of the total number of participating organisations are in Q3, another 3 and 1 organisations are in Q2 and Q1 respectively. The organisations in Q4 indicate the highest level of dependency followed by those in Q3, Q2 and Q1 in that order, this represents a corresponding level of cyber risk as well. Similarly, the sectoral distribution showed the majority of the sectors are in Q3 while the remaining sectors are distributed among the other three quadrants. This indicates that ICT distribution and risk cut across sectors.

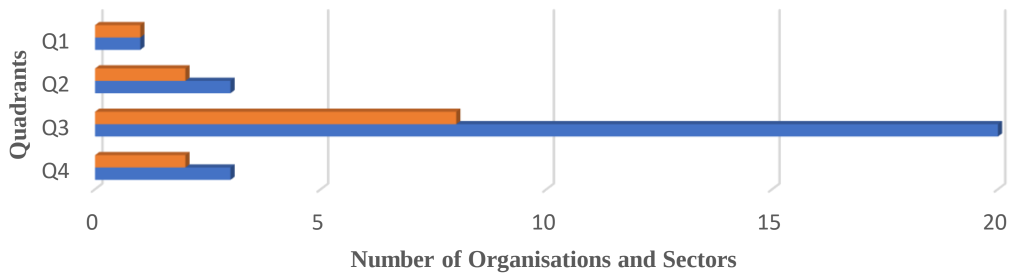


Figure 5: Number of Organisations and Sectors per Quadrant

Cyber Risk Distribution Pattern (CRDP)

In Table 4, data were presented according to the dependency metrics (DMs) of adoption, integration and automation. The adoption metric or phase is the preparatory stage for ICT implementation at national or organisational levels (Taylor et al., 2015). However, contrary to expectations that surveyed CI organisations will show their highest performances at the adoption phase, followed by integration and automation to minimise risk in the CI dependence on ICT relationship, not all surveyed CIs displayed this pattern. CI organisations ought to have a robust ICT adoption with all preparatory elements such as; ICT roadmap, ICT policy, ICT security policy, etc in place before delving into the integration of CI processes and machines with ICT; preparing the ground for moving onto to higher levels of processes integration which is automation. An analysis of the data in Table 4 was further examined and presented in Figure 7 showed that 12 out of the 27 organisations surveyed presented a *normal dependency* pattern such that organisations scored higher in adoption, followed by integration and automation in that order. This suggests that

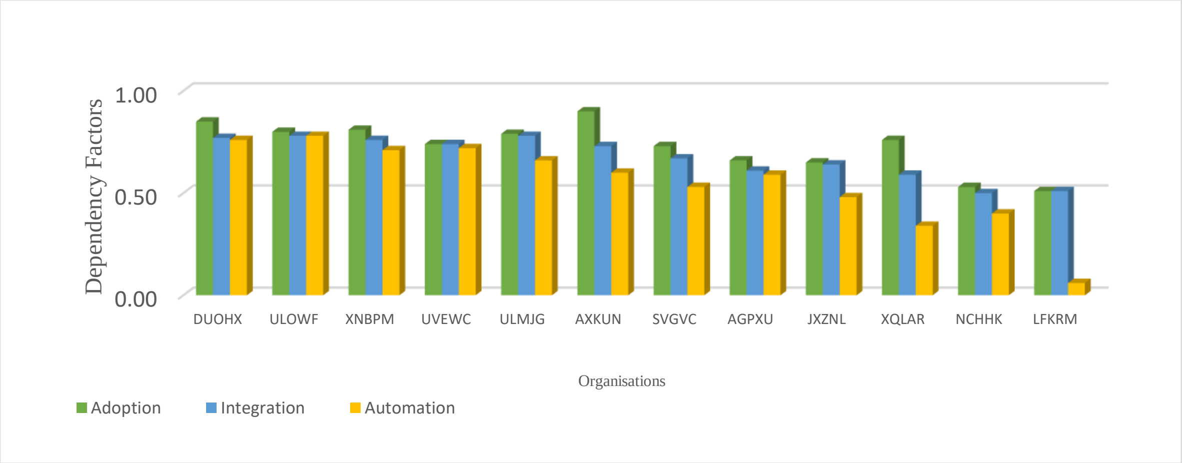


Figure 6: Normal Dependency Metrics Patterns

preparatory processes are taken into account before moving to higher levels of ICT implementation. This phased implementation trajectory potentially eliminates vulnerabilities thus minimizing the cyber risk that depending CIs in these organisations will be exposed to. This dependency pattern is presented in Figure 6.

Table 4: Survey Dataset showing Dependency Metrics and Dependency Factor (DF) Scores

#	Organisation Code	Sector	Adoption	Integration	Automation
1	VRJKP	Communications & Media	0.85	0.80	0.98
2	DUOHX	MDAs	0.85	0.77	0.76
3	ULOWF	MDAs	0.80	0.78	0.78
4	XNBPM	MDAs	0.81	0.76	0.71
5	ZLPSV	MDAs	0.79	0.81	0.68
6	UVEWC	Info. Technology	0.74	0.74	0.72
7	ULMJG	MDAs	0.79	0.78	0.66
8	THZDG	Security & Safety	0.75	0.67	0.76
9	AXKUN	MDAs	0.90	0.73	0.60
10	PPJIW	MDAs	0.70	0.80	0.64
11	NGDYE	Energy	0.72	0.74	0.65
12	ZREMB	Education	0.64	0.67	0.67
13	CROEX	Education	0.66	0.64	0.69
14	DDVPK	MDAs	0.66	0.70	0.62
15	KCCEM	Energy	0.63	0.59	0.72
16	SVGVC	MDAs	0.73	0.67	0.53
17	AGPXU	Education	0.66	0.61	0.59
18	FXBQV	Education	0.63	0.69	0.48
19	FXFMY	Energy	0.45	0.64	0.62
20	JXZNL	Health	0.65	0.64	0.48
21	GYNNY	Auxiliary Sectors	0.53	0.62	0.53
22	WVLGY	State	0.62	0.46	0.57
23	XQLAR	Security & Safety	0.76	0.59	0.34
24	NCHHK	MDAs	0.53	0.50	0.40
25	FKVQH	Energy	0.54	0.63	0.28
26	LFKRM	MDAs	0.51	0.51	0.06
27	VVZEN	MDAs	0.09	0.17	0.00

In Figure 7 on the other hand, 4 organisations presented what is describe here as Risky Dependency Patterns (RDP), a trend that is a reverse of that observed in Figure 6 such that they recorded their highest scores in automation, followed by integration and adoption in that order. This is suggestive of the fact that these organisations have poor preparatory processes, thus, are potentially vulnerable and exposed to higher cyber risks. For organisations in this group that fall within Q4 and Q3 where there is a high dependency on ICT and a corresponding high cyber risk, their cyber risk is further compounded by this uneven implementation of ICT in the CI operations.

In Figure 8 where 11 organisations are presented, there is no definitive pattern in the movement of the DMs scores. The lack of patterning in these organisations may depict near-total lack of planning in the ICT implementation process, this is equally a recipe for high cyber risk in the ICT infrastructure underpinning these entities' CIs.

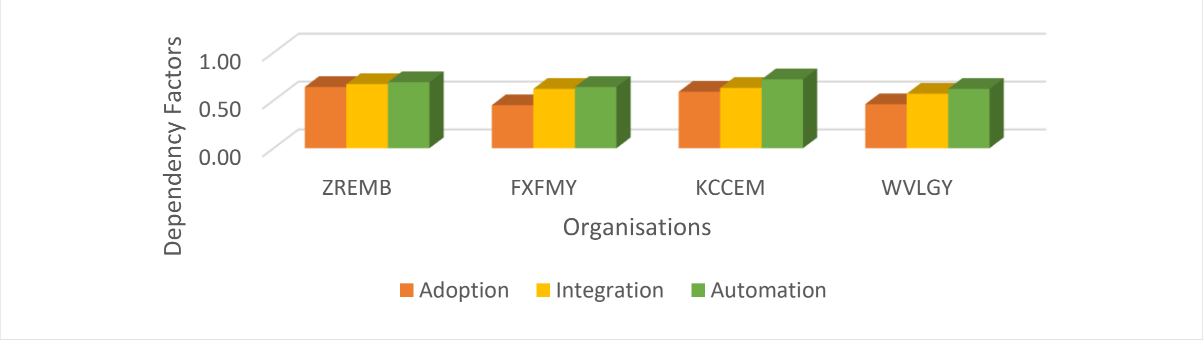


Figure 7:Risky Dependency Patterns (RDP)

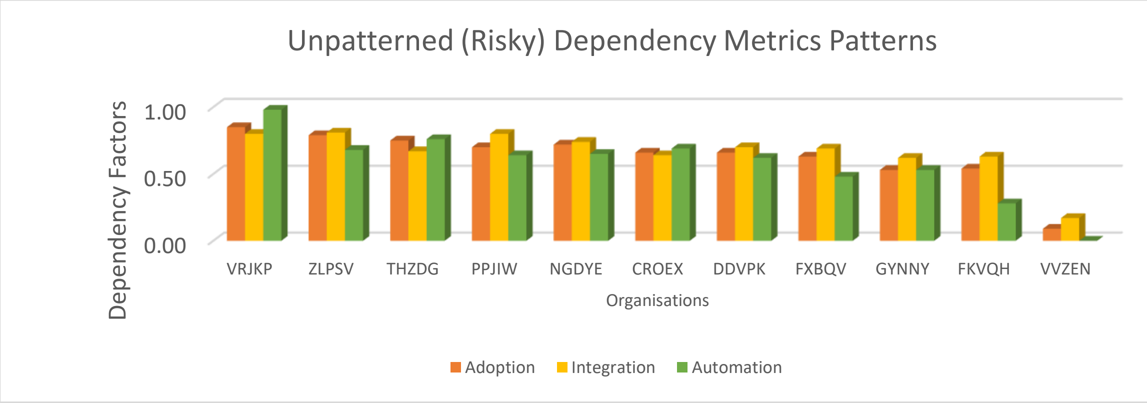


Figure 8: Uneven (Risky) Dependency Metrics Patterns

Conclusion

This article describes the computational and mathematical constructs, data collection and analysis of the resulting data from the assessment of the degree of CI dependence on ICT. Based on the model computation of quantitative variables resulting from the data collected from organisations. Consequently, the results show that the cyber risk organisations face is directly proportional to the level of dependency on ICT systems. The analysis showed that 3 organisations scored above 0.75 of the IDI and fall into the Q4 quad. This implies that these organisations are highly dependent on ICT, suggesting the highest level of exposure to cyber risk. Also, 20 organisations are in Q3 based on their IDI scores, their dependency and risk are lower compared to those in Q4 but higher than the 3 and 1 organisations in Q2 and Q1 respectively. Another key fact is that a high IDI score may not necessarily mean that the CI has performed optimally in all the metrics. The measurement of the extent of a CI's dependency on ICT, and in contrast, with other CIs is vitally important to how a nation can prioritise her CIIP since all CIs are unlikely to have the same characteristics and equal criticality. The quantitative model for computing CI degree of dependency on ICT is part of cybersecurity requirements. In sum, a scientific and empirical model in the comparative quantification of CIs' dependency on ICT allows for universal and repeatable processes continuously.

Acknowledgement

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

References

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

Anderson, R. N. (2019) 'U . S . -Canada Power System

Outage Task Force Final Report on the August 14 , 2003 Blackout in the United States and Canada : Causes and Recommendations', (August 2004).

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

Baboo, S. S. and Megalai, S. M. (2015) 'Cyber Forensic Investigation and Exploration on CloudComputing Environment', *Global Journal of Computer Science and Technology: B Cloud and Distributed*, 15(1).

Banerjee, J. *et al.* (2017) 'A Survey of Interdependency Models for Critical Infrastructure Networks', *Physics.soc-ph*. doi: DOI:3233/978-1-61499-391-9-1.

Bibao-Osorio, B., Dutta, S. and Lanvin, B. (2014) *Global Information Technology Report 2014: Rewards and Risks of Big Data*, *Wef*. Available at: http://reports.weforum.org/global-information-technology-report-2014/.

Bloomfield, R. E. *et al.* (2017) 'Preliminary interdependency analysis: An approach to support critical-infrastructure risk-assessment', *Reliability Engineering and System Safety*. Elsevier Ltd, 167(July 2015), pp. 198–217. doi: 10.1016/j.ress.2017.05.030.

Buldyrev, S. V *et al.* (2010) 'Catastrophic cascade of failures in interdependent networks', *Nature*. Nature Publishing Group, 464(7291), pp. 1025–1028. doi: 10.1038/nature08932.

Canzani, E. (2017) *Dynamic Interdependency Models for Cybersecurity of Critical Infrastructures*. Univestit¨at der Bundeswehr M¨unchen.

Dobson, S. *et al.* (2019) 'Self-Organization and Resilience for Networked Systems : Design Principles and Open Research Issues', pp. 1–16. doi: 10.1109/JPROC.2019.2894512.

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

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*.

Fekete, A. (2011) 'Common Criteria for the Assessment of Critical Infrastructures', *International of Disaster and Risk Science*, 2(1), pp. 15–24. doi: 10.1007/s13753-011-0002-y.

FMoC&DE (2020a) *National Digital Economy Policy and Strategy (2020-2030)*. Abuja, Nigeria. Available at: https://www.commtech.gov.ng/Doc/National_Digital_Economy.pdf.

FMoC&DE (2020b) *Nigerian National Broadband Plan 2020-2025*.

FMoC (no date) *Nigeria E-Government Master Plan*. Available at: https://www.commtech.gov.ng/component/k2/item/61-nigeria-e-government-master-plan.html.

Galinec, D. and Steingartner, W. (2017) 'Combining Cybersecurity and Cyber Defense to achieve Cyber Resilience', in *2017 IEEE 14th International Scientific Conference on Informatics Combining*, pp. 87–93.

ITU (2018) *Global Cybersecurity Index (GCI) 2018*. Available at: D-STR-GCI.01-2018-PDF-E.pdf.

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

Izuakor, C. and White, R. (2017) 'Critical Infrastructure Protection XI', 512, pp. 27–41. doi: 10.1007/978-3-319-70395-4.

Krepinevich, A. F. (2012) 'CYBER WARFARE A "NUCLEAR OPTION"?', *Centre for Strategic and Budgetary Assessments*.

Kundhavai, K. R. and Sridevi, S. (2016) 'International Journal of Computer Science and Mobile Computing IoT and Big Data-The Current and Future Technologies: A Review', *International Journal of Computer Science and Mobile Computing*, 5(1), pp. 10–14. Available at: www.ijcsmc.com.

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

Lee, R. M., Assante, M. J. and Conway, T. (2016) *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Washington DC. Available at: www.eisac.com.

Mbanaso, U. *et al.* (2019a) 'Conceptual Framework for the Assessment of the Degree of Dependency of Critical National Infrastructure on ICT in Nigeria', in *15th International Conference on Electronic Computers and Computations*. Abuja, Nigeria: IEEE Xplore. doi: 10.1109/ICECCO48375.2019.9043230.

Mbanaso, U. *et al.* (2019b) 'Conceptual Framework for the Assessment of the Degree of Dependency of Critical National Infrastructure on ICT in Nigeria', in *Proceedings of 15th International Conference on Electronics, Computer and Computation (ICECCO)*. Abuja, Nigeria: IEEE Xplore. doi: 10.1109/ICECCO48375.2019.9043230.

Mbanaso, U. M. *et al.* (2021) 'Quantitative Assessment of Critical Infrastructures Degree of Dependency on Information and Communications Technology', *International Journal of Critical Infrastructures*, 17(2).

Mbanaso, U. M. and Kulugh, V. E. (2021) 'Empirical Findings of Assessment of Critical Infrastructure Degree of Dependency on ICT', in Agrawal, R. et al. (eds) *International Conference on Cybersecurity in Emerging Digital Era*. Greater Noida: Springer Communications in Computer and Information Science. doi: https://doi.org/10.1007/978-3-030-84842-2.

NITDA (2019) *Nigeria e-Government Interoperability Framework (Ne-GIF) National Information Technology Development Agency (NITDA)*. Available at: http://nitda.gov.ng/wp-content/uploads/2018/05/data-interoperability-standards.pdf.

Office of the National Security Adviser (ONSA) (2014) *National Cybersecurity Policy*. Available at: https://cert.gov.ng/ngcert/resources/NATIONAL_CYBESECURITY_STRATEGY.pdf.

Petit, F. *et al.* (2013) 'Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience', (April), p. 70. Available at: www.osti.gov/bridge.

Pursiainen, C. (2020) 'Critical infrastructure resilience : A Nordic model in the making ? ☆', *International Journal of Disaster Risk Reduction*. Elsevier Ltd, (July 2017), pp. 0–1. doi: 10.1016/j.ijdrr.2017.08.006.

Rehak, D. *et al.* (2018) 'PT US CR', *International Journal of Critical Infrastructure Protection*. Elsevier B.V. doi: 10.1016/j.ijcip.2018.06.004.

Robinson, M. *et al.* (2018) 'An introduction to cyber peacekeeping', *Journal of Network and Computer Applications*, 114. doi: 10.1016/j.jnca.2018.04.010.

Saloky, T. and Šeminský, J. (2017) 'Artificial Intelligence and Machine Learning Applied to Cybersecurity', *IEEE Confluence*, pp. 1–18. Available at: http://uni-obuda.hu/conferences/SAMI2005/SALOKY.pdf.

Schreier, F. (2015) 'On Cyberwarfare', *DCAF Horizon 2015 working paper, No7*, (7).

Seppänen, H. *et al.* (2018) 'Critical infrastructure vulnerability—a method for identifying the infrastructure service failure interdependencies Hannes', *International Journal of Critical Infrastructure Protection*. Elsevier B.V. doi: 10.1016/j.ijcip.2018.05.002.

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

Tatar, U., Gokce, Y. and Gheorghe, A. (2017) 'Strategic Cyber Defense: A Multidisciplinary Perspective', in *NATO Advanced Research Workshop on A Framework for a Military Cyber Defense Strategy*.

Taylor, P. *et al.* (2015) 'A Role-based Typology of Information Technology : Model Development and Assessment A Role-based Typology of Information Technology ':, (June), pp. 37–41. doi: 10.1080/10580530.2015.1018770.

Theohary, C. A. and Rollins, J. W. (2015) 'Cyberwarfare and Cyberterrorism : In Brief', *Congressional Research Services*. Available at: www.crs.gov.

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

UNCTAD (2011) *Measuring the Impacts of Information and Communication Technology for Development, New York.*

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

WEF (2015) 'Industrial Internet of Things : Unleashing the Potential of Connected Products and Services', *World Economic Forum*, (January), p. 40. doi: 10.1111/hcre.12119.

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

Willke, B. J. (2007) 'A Critical Information Infrastructure Protection Approach to Multinational Cyber Security Events', *Carnegie Mellon University*, (September). Available at: http://www.enisa.europa.eu/activities/cert/events/files/ENISA_best_practices_for_ciip_Willke.pdf.

World Bank (2019) *Niegria Digital Economy Diagnostic Report*. Available at: http://documents1.worldbank.org/curated/en/387871574812599817/pdf/Nigeria-Digital-Economy-Diagnostic-Report.pdf.