Quantitative assessment of critical infrastructures degree of dependency on information and communications technology

Uche M. Mbanaso, Victor Emmanuel Kulugh* and Habiba Musa

Centre for Cyberspace Studies,
Nasarawa State University,
Keffi, Nigeria
Email: uche.magnus@mbanaso.org
Email: vkulugh30@gmail.com
Email: habibahmusa09@gmail.com
*Corresponding author

Gilbert I.O. Aimufua

Department of Computer Science,
Nasarawa State University,
Keffi, Nigeria
Email: aimufuagio@gmail.com

Emmanuel S. Dandaura

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

Abstract: This paper presents a computational model for the quantification of critical infrastructure (CI) degree of dependency on ICT. Traditional CIs that support modern society in providing uninterruptable vital services are increasingly ICT dependent. To build the needed bulwark against cyber threats, there is the need to assess their dependency on ICT since ICT infrastructure comes with vulnerabilities that amplify cyber risk. Consequently, the proposed computational model for the quantification of CI degree of dependency on ICT is a function of ICT metrics and indicators based on mathematical constructs. The outcome is ICT dependency index (IDI), and ICT dependency quadrant (IDQ), which compare, rank, and visualise the IDI of sectors and organisations. The findings show that no one sector can be chosen arbitrarily as the most critical ICT dependent. The model is particularly useful for developing countries to uniformly assess CI's degree of dependency on ICT as opposed to uninformed valuation.

Keywords: critical infrastructure; critical systems; critical national information infrastructure; ICT dependency.

Copyright © 2022 Inderscience Enterprises Ltd.

Reference to this paper should be made as follows: Mbanaso, U.M., Kulugh, V.E., Musa, H., Aimufua, G.I.O. and Dandaura, E.S. (2022) 'Quantitative assessment of critical infrastructures degree of dependency on information and communications technology', *Int. J. Critical Infrastructures*, Vol. 18, No. 1, pp.45–62.

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 TETFund sponsored research on Cybersecurity and Critical National Infrastructure (CNI). He earned his undergraduate qualification in Electronics and Communications Engineering (Bida, 1989), MSc in Information Technology (Bradford, UK, 2003) and PhD Communications and Information Security (Salford, UK, 2009).

Victor Emmanuel 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. His research interest is in the area of critical information infrastructure dependency and resilience. He obtained his BSc from the Enugu State University of Science and Technology, Enugu, Nigeria in 2013 and an MSc in Computer Science (Networking) in 2017 from the Nasarawa State University, Keffi, Nigeria.

Habiba Musa is an investigator on the CNI project and an information and communication technology law expert. She has worked on several cyberlaw and electronics governance projects, legislations and regulation. She received her PhD in Law in the Nasarawa State University, Keffi, Nigeria in 2018. She is currently the Deputy Director in the Centre for Cyberspace Studies and lectures at the Faculty of Law, Nasarawa State University, Keffi, Nigeria. Her research interest is in the area of legal protection for critical infrastructure and data privacy.

Gilbert I.O. Aimufua is an investigator on the CNI project and a Senior Lecturer at the Computer Science Department, Nasarawa State University, Keffi, Nigeria. He specialises in information systems, e-government, big data, artificial intelligence and machine learning. Presently, he lectures computing courses and researching actively on improving business information systems, cybersecurity and CNI study. He received his PhD at the Accra Institute of Technology, Ghana in 2020.

Emmanuel S. Dandaura is an investigator on the CNI project and a Professor of Participatory Communications and Performance Aesthetics who has two post-doctoral certifications in ICT and Knowledge Management Systems. He is an expert in people aspect of cybersecurity, focusing on cyber relations and ethics having conducted and supervised seminal research in the relatively emerging sub-discipline of cyberrelations.

1 Introduction

Critical infrastructure (CI) or critical national infrastructure (CNI) refers to assets that provide uninterrupted essential services or vital functions to the society to run efficiently and productively. Thus, their failure, incapacitation, or degradation can potentially render a nation or society incapable of functioning effectively (Bloomfield et al., 2017). Accordingly, CI services are increasingly dependent on ICT infrastructure to deliver cost-effective services promptly. This has increased the rate of adoption of ICT infrastructure by many nations and organisations that seek to participate effectively in the emerging digital economy. The upshot of the ravaging COVID-19 (Coronavirus) and the campaign for virtual working and collaboration have further accentuated the need for organisations and nations to digitalise more and more of their operations. The 2017 International Telecommunications Union (ITU) ICT Development Index (IDI), and the 2018 United Nations E-Government Development Index (EGDI) indicate increases with regards to ICT adoption globally (ITU, 2018a). Undisputedly, there is a manifest growth in ICT adoption in key critical sectors such as energy, financial services, transport, healthcare, etc. The organisations in these sectors are at various levels of ICT adoption and maturity (WEF, 2016; Zaballos and Jeun, 2016).

The increasing CI dependency on ICT raises concerns due to inherent ICT vulnerabilities, which often have serious negative national effects (Krepinevich, 2012). The fact remains that a single successful attack can have manifold adverse effects including cascading and escalating impacts across sectors of the economy. Schreier (2015) pointed out that cybercriminals do take advantage of the difficulty in attribution and degree of anonymity, especially state actors that can deploy excessive cyber power to advance their missions. Again, this particular factor further exacerbates the threat landscape of CI. Therefore, to effectively provide protection for CI against cyber threats nationally, it is important to characterise and determine the degree of ICT dependency first. Thus, this study is an initial step towards determining the criticality of CI dependency on ICT. Presently, as far as the authors are aware, there is no publicly available scientific quantitative tool to estimate the ICT dependency level of organisations or nations. Therefore, this paper proposes a computational model that can support the estimation of the degree of dependency of the CI on ICT infrastructures. The ICT dependency measurement in quantitative terms is conceptualised from the perception of cyber risk. Thus, the model, which is framed based on measurable metrics and indicators, is a novel tool to quantify the CI degree of dependency on ICT and it is grounded on mathematical constructs. By implication, the insight into the degree of dependency, presumably, indicates potential cyber risks that can be faced by a CI (ITU, 2017; Harašta, 2018).

In testing the model, three metrics (or pillars) were framed. These are *adoption*, *integration*, and *automation*. Each of the metrics has sub-pillars, and then indicators, which form the variable unit item of measure. To aggregate the indicator values, the values are summed and normalised to what is described as the ICT dependency index (IDI). The various IDI scores of organisations are comparatively benchmarked in another construct referred to as the ICT dependency quadrant (IDQ). The IDQ is a four-band quadrant scale that ranks and displays the scores of IDI of organisations in a single view. The novelty is that firstly, the model is adaptable, secondly, it is scientific and empirical, implying that it is based on a repeatable and transparent measurement process. Thirdly, it provides a comparatively single view to gauge diverse organisations' ICT dependency

levels within different sectors in a country. The benefit is that a nation can comparatively gauge the ICT dependency of CIs as part of the national cyber risk management process. The rest of the paper is organised as follows: Section 2 provides background to the study and related works; Section 3 describes the methodological approach; Section 4 presents the ICT dependency model while Section 5 explains the dependency mathematical constructs. Section 6 presents the testing and verification; Section 7 provides insights into the findings and discusses the result, and Section 8 concludes the article.

2 Background and related works

CIs are so prime to modern society, in the sense that their failure or incapacitation will significantly undermine key national interests such as security, economic prosperity, health, and even the safety of citizens (Rinaldi et al., 2001; Government Accountability Office, 2014). As a result of the economic and social benefits arising from the growing digitalization of business, government, and individual operations, the proper functioning of ICT or cyberinfrastructure (Bloomfield et al., 2017) is imperative. According to the WEF (2016), the capacity of ICT to create new services and products at greater efficiency in terms of speed, accuracy, and at minimal cost, is further spurring more innovative ICT features into core functions and services. The United Nations EGDI, and the ITU (2017, 2018b) IDI show that nations are progressively implementing ICT solutions to enhance the efficiency of key services and resources. Zaballos and Jeun (2016) stated the rising investment in ICT and Internet Infrastructure arguing that the expansion of data and voice communications infrastructure is giving rise to high demand for cloud storage and data back-up infrastructure, which forms an important part of critical information infrastructure (CII).

Furthermore, the financial, energy, and transport sectors are witnessing accelerated growth in innovating value ICT solutions. The trends show a growing dependency on ICT infrastructure globally. According to Stergiopoulos et al. (2018), the more dependent the critical services of a nation are on ICT, the higher the cyber risk faced. This assertion implies that inherent vulnerabilities and threats from ICT can have a debilitating effect on CI with a high level of ICT integration. In the same vein, Krepinevich (2012) argued that the severity of the impact of a cyber-attack on CIs can be directly proportional to the level of CI digitalization – dependency of such assets on ICT systems. Another huge concern is infrastructural dependency and interdependency, which can result in cascading or escalating effects among interconnected infrastructures in the event of any form of failure or cyberattack. Thus, the cyberspace is fast becoming a theatre of conflicts and espionage, and further exacerbating cyber risks (Krepinevich, 2012). The effect as argued by Cornish et al. (2010) is that critical asset owners are already paying the cost of the cyber-amplified risks in diverse ways. For example, some are accepting the substantial economic losses inflicted by repeated cyberattacks. Others are working to secure and protect CI at significant costs.

So far, the foregoing views allude to the consensus that a society that is super dependent on ICT, can also anticipate enormous cyber threats, which in effect requires new governance approaches (WEF, 2016; Robinson et al., 2018). Furthermore, the consensus also extends the fact that the higher the CI dependency on ICT systems, the higher the potential cyber risks (Krepinevich, 2012). Nonetheless, many countries have continued to evolve and develop a variety of defensive (NIPP DHS, 2013; ENISA, 2012;

Australian Government, 2010) and offensive strategies (Izuakor and White, 2016; Theohary and Rollins, 2015) to protect CI. The authors consider that the first step towards designating infrastructure as CII is to gauge the infrastructure's degree of dependency on ICT. As far as the authors are aware, there is no publicly available scientific-based quantitative tool to measure the extent of the dependency of CIs on ICT. Research efforts in the past have been directed towards measuring the impacts of ICT on various economies and groups, especially as it relates to improving the country's digital infrastructure (Domínguez and Charles, 2010; Rehak et al., 2016). Notably, the Network Readiness Index (NRI) (WEF, 2016) assesses the preparedness of nations, and how they continuously leverage emerging technologies to reap the benefits presented by digital revolution and opportunities. The NRI assessment is based on metrics such as technological environment, infrastructure, ICT adoption/usage as well as the economic and social impact of technologies. Similarly, the ITU (2018a) IDI focuses on providing a comparative analysis of the performance of countries on the usage of ICT, and how it impacts development and decision making. At the centre of the ITU IDI, the study is the measurement of ICT readiness with an emphasis on the availability of infrastructure and access, ICT usage, ICT capability, and the combined effects of these indicators. Conversely, the various measurement frameworks fail short of addressing the degree of ICT dependency, which is vital for formulating cybersecurity management. Consequently, this study addresses the gap by developing a scientific model for the quantification of ICT dependency. Thus, it can be indicated that the quantification of the degree of ICT dependency is critically important to CII protection and resilience. At the national level, it can help to comparatively gauge the different phases of organisations' digitalization effort and investment in protecting such infrastructures. Consequently, our model provides a transparent and repeatable scientific tool that can present in a single view, the various ICT dependency of critical organisations. This throws fresh insight that there is a strong correlation between the degree of ICT dependency and cyber risks. And of course, protection cannot be provided in a vacuum, it provides the mechanism to view potential cyber risks from the prism of the national dependence on ICT infrastructures. Thus, quantifying the extent of national ICT dependency forms an integral part of our ongoing study on CNI and cybersecurity. The ultimate is a proven scientific and empirical tool that has the property of repeatability to guide in the continuous quantitative assessment of ICT dependency to aid in prioritizing critical information infrastructure protection (CIIP).

3 Design/methodology/approach

The authors conducted an extensive review of ICT frameworks and standards; CIIP frameworks and standards to conceptualise the measurable constructs of ICT dependency. To frame ICT dependency variable factors, parameterised metrics, and indicators form the basis for the measurement and weighting factors. The variable parameters that underpin the degree of ICT dependency were gestated and thoroughly analysed to aid in the development of the ICT dependency model. In testing the model, three metrics – *adoption*, *integration*, and *automation* (also referred to as the three functional pillars of the model) formed the key metrics for the measurement of the IDI. The metrics have sub-pillars and indicators as the granular variable items of measurement. To evaluate quantitatively, a five-point ratio scale of 0–5 was adapted for

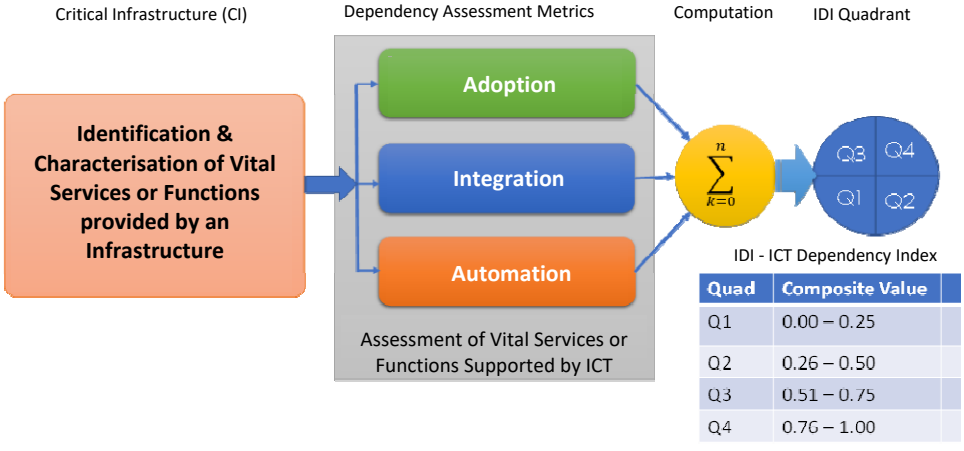
the granular measurement and using a generated hypothetical dataset, the model was tested and verified. In the five-point ratio scale, zero (0) connotes non-existence or absence of specific items of measure, while five depicts the highest quantitative value measurable. The IDI scores of organisations are displayed using IDQ – a four-band quadrant that comparatively visualises the organisation scores.

4 The ICT dependency model

4.1 Conceptual model design

Figure 1 depicts the core ICT Dependency model showing the various components, and how they relate together. There are four primary components, each comprises sub-components designed to provide more in-depth measurements. The dependency assessment metrics (DAMs) define the thematic areas of measurement, the computation component calculates the values derived from the metrics, the variable items of measure reflecting the various indicators. The descriptions of the components are in following subsections.

Figure 1 The ICT dependency model (see online version for colours)



Source: Adopted from Mbanaso et al. (2019)

4.1.1 CI characterisation

The characterisation of CI is an important step towards correct identification of key functions or services the infrastructure provides (European Commission, 2009). In some cases, the required information may be obtained from publicly available sources. The characterisation helps to situate the core mission of the organisation or an asset, which potentially indicates the commitment of an organisation in terms of digital transformation (Voeller et al., 2008). The identification of CI followed a double-fold approach:

1 Identification, analysis, and characterisation of tangible assets, vital services or functions that depend on ICT with emphasis on physical infrastructure.

2 ICT-dependency assessment based on three metrics – *adoption*, *integration*, and *automation*, which provide deep parameterization of the contributory variable attributes of the measurement.

4.1.2 Dependency assessment metric

This is a construct that measures dependency factors (DFs) at various phases of ICT provisioning. Each metric has sub-elements followed by indicators; an indicator is a concrete granular attribute that is measurable, called the *dependency indicator* (*DI*). Similarly, a metric is simply an abstract contributory measurable factor, somewhat, a pillar that aggregates sub-elements and diverse indicators (Robert et al., 2009). The outcome referred to as *DF* is the summation of the sub-elements and their indicators. The following section describes the pillars of the DAMs.

1 *Adoption:* The concept of adoption is used here to connote the corporate decision of an organisation to implement ICT systems for operational efficiency and high productivity (Atkin et al., 2017). Due to the complexity of ICT provisioning, planning for digital transformations should be considered methodically such as the technology acceptance model (TAM), which can be the basis to conceptualise the anticipated utility of the technology (Taylor et al., 2015). Thus, an organisation needs to articulate the business value such transformation will bring to bear on the mission and core objectives of the organisation (United Nations, 2011). Consequently, the *adoption* metric incorporates the indicators that quantify the earlier measurable variable parameters that will lay the foundation, and drive the digital transformation benefits more sustainably. To this extent, the study considered elements such as ICT roadmap, ICT policy, ICT Security policy, awareness, training, and ICT usage (Izuakor and White, 2016).

2 *Integration:* ICT integration refers to the degree or extent to which ICT systems have been embedded into an organisation's processes and operations (United Nations, 2005). The level of integration is determined by the interplay between users and the technology infrastructure across the enterprise ecosystem. Integration can be measured in an organisational context by the availability of ICT infrastructure, accessibility, and the skill set to effectively utilize them to realise organisational objectives or benefits. It implies that at the organisational level, integration can be measured based on the overall operational use of ICT for greater efficiency and productivity (Taylor et al., 2015). Such parameters that can be considered include the availability of network (LAN) concerning the number of devices or nodes connected to the LAN, access to the public network (Chew et al., 2008), web presence, availability of assets, and identity management systems. The thrust is that the interconnectedness of an organisation, its services, and functions to the public can raise the organisation's profile beneficially.

3 *Automation:* Today the ubiquitous influence of the internet has brought about the notion of the fourth utility revolution, making the internet, the most indispensable technology of modern society. It is that core services and functions requiring seamless integration, in which both people and physical objects are increasingly

being interlinked to enhance the modern-day digital experience. Consequently, ICT automation is becoming a functional requirement for most organisations as the NITDA (2019) interoperability framework indicates. *Automation* in this context is a measure of how an organisation improved operational workflow to reduce human interventions by pre-setting many of the operational processes to self-drive. Taylor et al. (2015) opine that functions such as *enterprise resource planning* (*ERP*), *decision support systems* (*DSS*), *electronic inventory management systems* (*EIMS*), *participatory project management* (*PPM*), and *knowledge management systems* (*KMS*) are all elements of ICT automation. Besides, the deployment of modern technologies such as the internet of things (IoT), radio frequency identification (RFID) and near field communication (NFC), which can raise the level of automation can be considered.

In the sections that follow, we conceptualise the features that support the framing of the mathematical and computational constructs.

Table 1 provides a brief description of DAM and the contributory weighted factors.

Table 1 Brief description of DAMs

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 not 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 criteria for the arbitrary assignments of weights are based on the fact that the effect of cyber risk is unlikely to have the same impact on the metrics. Presumably, from a cybersecurity risk perspective, and the degree of ICT dependency, the impact of failure cannot be distributed equally across the tiers of the metrics. This assumption strengthens the argument that an organisation with a high level of *automation* is likely to be more susceptible to cyber threats than an organisation with a high level of *integration* but a low level of *automation*. A similar argument holds for *adoption* in comparison to *integration*; implying that an organisation with a high level of *integration*, is likely to have a higher cyber risk than an organisation with a high level of *adoption* but low level of *integration*. Thus, it can be argued that there is a correlation between the degree of dependency and the impact of failure concerning contributory factors of the metrics. Therefore, it implies

that potential cyber risk factors influence the weighting of the metrics, which emphasizes the commensurate potential impact invariance of the metric causative factors.

4.1.3 Dependency indicator

The DI is the unit of measure based on a quantitative five-range ratio scale. It captures in quantitative terms the effect of exact dependency attributes that depicts the level of achievement of that particular indicator within the context. This concept adapted from (Chew et al., 2008), the guidance for performance measurement of information security metrics, is based on the goals and objectives of the cogency of the quantification. This should easily be obtainable and feasible to measure. Consequently, this provides a repeatable process, and relevant performance trends over time within a contextual environment. The quantitative scale in consideration of DI is shown in Table 2.

Table 2 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.

4.1.4 Computation model

The computation model calculates the IDI based on the summation of assessment metrics and indicators. The underlying mathematical constructs described in Section 4 shows step by step mathematical formulae for the various stages of computation to arrive at the IDI. The IDI provides a composite value of the degree of an organisational dependence on ICT. The selection of the *DI* follows a ratio scale of 0, 2–5, where 0 implies the none existence or absences of an indicator, and 5 is the possible highest value of a measure. The IDI provides the basis for the comparative analysis of the quantification of ICT dependency of organisations. Again, interpreting the *DI* scale in terms of cybersecurity risks, implies that 0 value connotes zero dependencies and zero risks, while 5 connotes potentially high risk and high dependency.

4.1.5 The IDQ

The IDQ is shown in Figure 2, which presents the mechanism for a single view of IDIs of various organisations. The concept of the quadrant is to provide a four-range band based on proportional dependency and risk. It simplifies a way to rank and benchmark various organisation's ICT dependency in a comparative and repeatable model. In this way, the IDI of organisations from different sectors can be compared in a risk-view manner. That is, the IDQ exposes the ICT dependency of an organisation concerning other

organisations, even though the organisations may unlikely belong to the same sector. More so, national, the IDQ can offer the advantage of comparative analysis of sectors and organisations in a single assessment. The full explanation of the quads is provided in Table 3.

Figure 2 ICT dependency quadrant (see online version for colours)

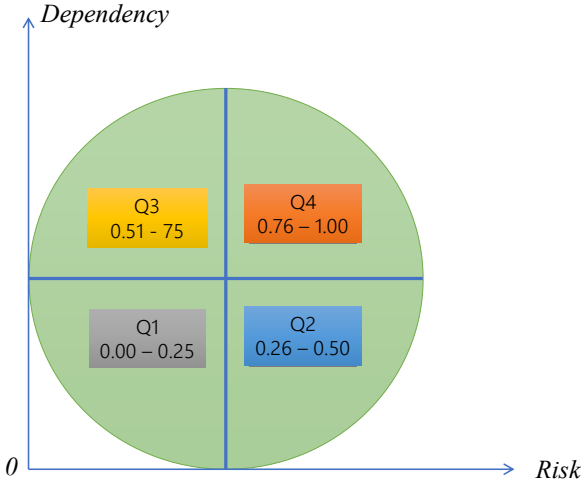


Table 3 IDQ description

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.

The IDQ 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. In contrast, Q4 depicts an organisation with a high degree of ICT dependency, the concomitant potential high cyber risks. The novelty of IDQ draws from the fact that it is a comparative risk-view tool that can help a country to be more proactive in its cybersecurity plan by providing incentives for high-risk organisations. Again, infrastructure may be vital but may have potentially low cybersecurity exposure. Thus, prioritization can be given to highly ICT-dependent entities in terms of resources for proportionate protection.

5 The mathematical model for ICT dependency

This section provides formally, the taxonomy of ICT-dependency quantitative measurement, with mathematical and standardized parameters. 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.

5.1 Formal definitions

The following variables are defined to help formulate the mathematical equations:

1 *DI: DI* is the quantitative evaluation of the degree of dependency of a particular indicator, in the scale of 0, 2–5, which is the granular unit of measure.

2 *DF: DF* is the summation of the various *DIs* – the indicators of a particular dependency metric (*DM*). The *DF* is usually normalized to give a composite value which lies between 0.00 and 1.00.

3 *IDI:* This is the weighted summation of the *DMs* (or the main pillars) – the computational summation based on *DFs* and weighted factors assigned to the *DMs*. The scores of IDI lies between 0.00 and 1.00.

5.1.1 Dependency factor

The *DF* is the summation of the *DIs* of a particular DM and can be represented mathematically as shown in equation (1).

$$DF = \sum_{i=1}^{n} DI_i \tag{1}$$

where $i = 1$ to n, and n is the number of DI being measured.

To normalise *DF* to a composite value, equation (1) can be modified such that:

$$Df_0 = \frac{DF}{Z} \tag{2}$$

where Df_0 is the optimised composite value, and Z is the number of indicators multiplied by the highest quantitative scale ratio Q. As shown in Table 2 Q is 5, it follows that Z can then be derived thus:

$$Z = 5N \tag{3}$$

Therefore, substituting Z in equation (2), DF_0 thus becomes:

$$DF_0 = \frac{DF}{5N} \tag{4}$$

where N is the number of indicators of a particular metric being measured, and N can be said to be a derivable variable constant.

5.1.2 The IDI

The *IDI* is the sum of the *DFs*, which is the summation of the contributing effects of the *DFs*. Thus:

$$IDI = w_i \sum_{i=1}^{n} DF_0 i \tag{5}$$

where i = 1 to n and n is the number of DFs, in this case n = 3, i.e., adoption (*Ade*), integration (*Ine*) and automation (*Aue*), and w_i is the weight factor of each metrics as shown in Table 1. Therefore, equation (5) becomes:

$$IDI = \left[(DF_{0\,Ads}) - (w_{Ads})\right] + \left[(DF_{0\,Ine})(w_{Ine})\right] + \left[(DF_{0\,Aue})(w_{Aue})\right] \tag{6}$$

The weights factors of the DMs are assigned as stated in Table 1, the w_i can be substituted in equation (6) as follows:

$$IDI = 0.25(DF_{0\,Ade}) + 0.35(DF_{0\,Ine}) + 0.40(DF_{0\,Aue}) \tag{7}$$

Thus, *IDI* lies between ($0.00 \leq IDI \leq 1.00$), which represents the IDI of a particular organisation.

6 Testing and verification

To test and verify the ICT Dependency model, the derived mathematical model was implemented as a software tool based on algorithms and data structures that evolved. Then, a dataset was randomly generated to simulate data input from 30 organisations based on 60 sample questions with 20 allotted to each of the DMs (*adoption*, *integration*, and *automation*). The organisations were categorized and grouped into 6 critical sectors in a manner that each sector has five organisations. The testing was distributed for maximum IDI, i.e., 1.0 and minimum IDI, i.e., 0.0 to verify the upper and lower limits of the IDI scores. The test result is shown in Table 4. The chart shown in Figure 3 depicts that six organisations fall in the Q4 band, implying an IDI score of above 0.75, and 12 organisations scored that scored within 0.5 to 0.75 fall in Q3 quad. Similarly, eight organisations within 0.26 to 0.50, and are in the Q2 quad and four organisations that scored below 0.26 and are in Q1 quad. Thus, the IDI score shows the spread of ICT dependency across sectors. The IDQ provides a single view of the degree of ICT dependency in comparison with other sectors.

7 Findings, analysis, and discussion

Table 4 shows IDI scores of 30 organisations and respective IDQ quad bands. As indicated in extrapolated data in Table 5, the top-ranked organisations in Q4 are not necessarily from a particular sector. Traditionally, countries may arbitrarily declare a particular sector highly critical than others but in actual fact, not all organisations in one sector can have equal DF (or criticality). The results similarly demonstrate that an organisation's DF may be higher in one metric and lower in another metric. One of the

benefits of using metrics to quantify the ICT dependency is that it can further help organisations to granularly identify gaps in specific areas of the ICT implementation and address the gaps appropriately and proportionately.

Table 4 Test result of 30 organisations showing metric scores, IDI scores, and achieved quads

#	*Organisations*	*Sector*	*Adoption*	*Integration*	*Automation*	*IDI*	*Quadrant*
1	M78R85	Financial	1.000	1.000	1.000	1.00	Q4
2	I78C76	Energy	0.740	0.750	0.880	0.80	
3	L86J74	Financial	0.770	0.730	0.870	0.80	
4	D80O73	Energy	0.660	0.710	0.910	0.78	
5	T86S67	Communication and media	0.810	0.740	0.780	0.77	
6	R73S82	Communication and media	0.660	0.710	0.870	0.76	
7	O75Q69	Communication and media	0.660	0.710	0.840	0.75	Q3
8	A83Z86	Communication and media	0.580	0.660	0.820	0.70	
9	V84E66	Health	0.660	0.660	0.660	0.66	
10	Z88G71	Transport	0.660	0.660	0.660	0.66	
11	Y70N69	Transport	0.660	0.660	0.660	0.66	
12	C73O76	Security and safety	0.580	0.580	0.580	0.58	
13	H71L75	Energy	0.580	0.580	0.580	0.58	
14	I73I75	Energy	0.580	0.580	0.580	0.58	
15	O72W66	Transport	0.580	0.580	0.580	0.58	
16	O85V67	Energy	0.540	0.540	0.540	0.54	
17	E83W83	Communication and media	0.360	0.380	0.780	0.54	
18	H75Y83	Financial	0.380	0.340	0.780	0.53	
19	N83G85	Communication and media	0.200	0.280	0.750	0.45	Q2
20	C73F68	Energy	0.480	0.440	0.430	0.45	
21	X65T84	Transport	0.360	0.420	0.420	0.41	
22	H79C85	Health	0.400	0.380	0.420	0.40	
23	E78K78	Transport	0.370	0.360	0.450	0.40	
24	E72O66	Financial	0.300	0.320	0.390	0.34	
25	N74S78	Communication and media	0.340	0.330	0.330	0.33	
26	O88Z68	Security and safety	0.300	0.260	0.320	0.29	
27	S68C78	Financial	0.240	0.310	0.280	0.28	
28	K81M69	Energy	0.260	0.300	0.200	0.25	Q1
29	B86Q79	Financial	0.240	0.220	0.230	0.23	
30	R68S87	Communication and media	0.000	0.000	0.000	0.00	

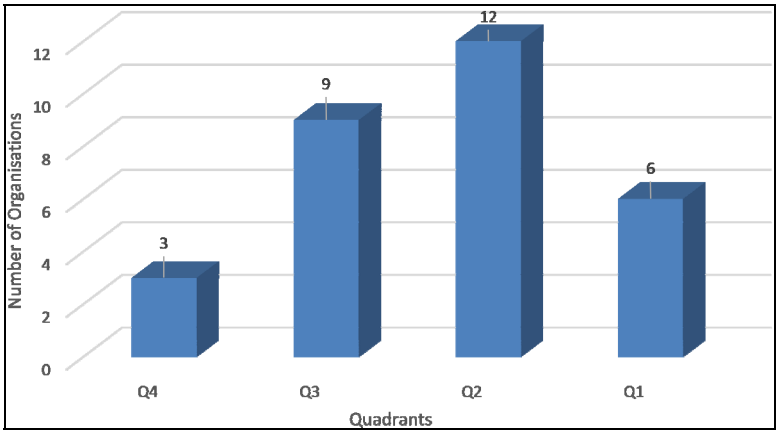
Table 5 Extrapolated dataset showing organisations, sectors, IDI scores and quadrants

#	*Organisations*	*Sector*	*IDI*	*Quadrant*
1	M78R85	Financial	1.00	Q4
2	I78C76	Energy	0.80	Q4
3	L86J74	Financial	0.80	Q4
4	D80O73	Energy	0.78	Q4
5	T86S67	Communication and media	0.77	Q4
6	R73S82	Communication and media	0.76	Q4
7	O75Q69	Communication and media	0.75	Q3
8	A83Z86	Communication and media	0.70	Q3
9	V84E66	Health	0.66	Q3
10	Z88G71	Transport	0.66	Q3
11	Y70N69	Transport	0.66	Q3
12	C73O76	Security and safety	0.58	Q3
13	H71L75	Energy	0.58	Q3
14	I73I75	Energy	0.58	Q3
15	O72W66	Transport	0.58	Q3
16	O85V67	Energy	0.54	Q3
17	E83W83	Communication and media	0.54	Q3
18	H75Y83	Financial	0.53	Q3
19	N83G85	Communication and media	0.45	Q2
20	C73F68	Energy	0.45	Q2
21	X65T84	Transport	0.41	Q2
22	H79C85	Health	0.40	Q2
23	E78K78	Transport	0.40	Q2
24	E72O66	Financial	0.34	Q2
25	N74S78	Communication and media	0.33	Q2
26	O88Z68	Security and safety	0.29	Q2
27	S68C78	Financial	0.28	Q2
28	K81M69	Energy	0.25	Q1
29	B86Q79	Financial	0.23	Q1
30	R68S87	Communication and media	0.00	Q1

Table 5, indicates that among the 30 organisations, two organisations from the financial sector, two organisations from the energy, and communications and media sectors fall in the Q4 quad. Similarly, organisations from different sectors fall into the Q3 quad, just as Q2 and Q1 bands share similar patterns. Figure 3 depicts the number of organisations per quad, showing that Q3 has the highest number of organisations. The IDQ based on Figure 3, shows a normal distribution pattern, depicting that the highest number of organisations are in the Q3 quad. The normal distribution can attest to the veracity of the model and prediction of dependency (or criticality), which suggests that the increasing level of ICT implementation in CI, has the potential to exacerbate high cyber risks profile

amongst CIs. It further validates our earlier assumption that high ICT dependency is directly proportional to potential cyber risks. So, it indicates that the more organisations move towards total digitalization, the more their potential cyber risk exposure increases. Consequently, the Q3 quad-band infers a high degree of ICT dependency and a corresponding potential high cyber risk. While the Q4 depicts very high use of ICT, meaning that core functions and services integrated and automated imply potential very high cyber risks. On the other hand, organisations Q1 quad-band represents low ICT usage, and subsequently, potentially low cyber risks. This way, the result is insightful in the sense that a particular IDQ (or quad) can cut across sectors as exemplified in Q4, Additionally, it can be deduced that organisations in Q3 and Q4 quads demand prioritisation of investment in protecting the organisations since they are highly exposed to cyber risks.

Figure 3 Number of organisations per quad (see online version for colours)



Moreover, using the concept of IDQ, the DF values of the metrics grouped in the quadrant can be comparatively analysed to throw useful insight into the growth of ICT in a particular sector or all sectors. This individual metric index can be viewed in the IDQ to give insights into the performance of each metrics. It can as well give further understanding of the correlation between the IDI scores and DF scores since the scores are normalised composite value derived from the computational constructs. This feature, in particular, allows for further drilling of the individual metrics to deepen the understanding of the various metric effects. Notwithstanding this, the insight can help determine the economic impact of the various metrics and the overall IDI in the event of incidents that can affect the CI dependency on ICT. The perception of an organisation's IDQ depicted by the interpretation of the quads Q1, Q2, Q3, and Q4 can reveal the economic impact since the degree of ICT dependency is proportional to the cyber risks. Thus, Q1 represents a very low economic impact, and Q4 represents very high economic impact.

The novelty of this approach is that a country can classify its ICT critical organisations into four bands depicting potentially the degree of cyber risk exposure. With this national view and ICT Dependency software tool, a country can repeatedly and repetitively quantify CI dependency on ICT, and subsequently, manage the cybersecurity exposure of critical cyber dependent organisations consistently and transparently. Also,

identifying the predominant services or functions provided by these organisations, including physical assets, and configurations are as well core operational cybersecurity objectives. Also, assets whose failure or degradation could have catastrophic consequences of national magnitude can be deduced from the IDQ view based on the metrics of measurement. Also, the fact that the computation of IDI is based on mathematical and computational constructs allows for the extensibility of the metrics, and expansion of the indicators to further fine-tune the quality of measurements.

Figure 4 Number of sectors per quad (see online version for colours)

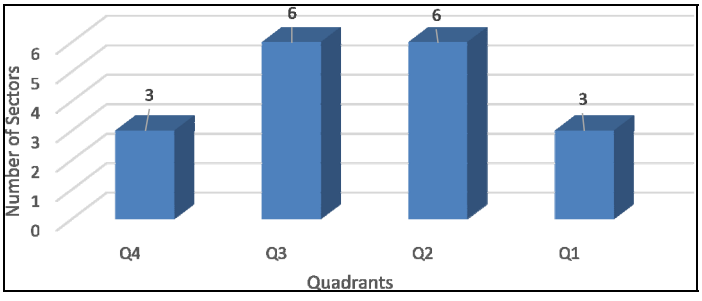


Figure 4 depicts the number of sectors per quad, again, showing that Q3 has the highest number of sectors. The pattern shows a normal distribution, and following the results, it is evident that the ICT Dependency model described in the article is ground-breaking, and its application can throw useful insights into CI dependency of ICT and potentially, associated cyber risks. Furthermore, the findings are an indication that the degree of ICT dependency is directly proportional to cyber risk, which provides the basis for informed prioritisation of a national CIIP in terms of cybersecurity investments.

8 Conclusions

The article has presented a novel computational model for the quantitative assessment of CI organisation's degree of ICT dependency using scientific and empirical methods. The study is vital for nations at both advanced levels of ICT adoption and developing nations, whose digital transformation growth is increasing at a considerable speed. The quantitative approach provides the mechanism to classify and group CI organisations' dependency into four bands based on the level of dependency, which is also proportional to potential cyber risks. The development of the software tool (to be presented in another article) followed sound engineering principles, derived mathematical constructs, which fundamentally influenced data structures and algorithms for the computation of IDI and IDQ. The test results show the veracity of the model, significance, and benefits from both organisational and national perspectives.

As a risk-based influencing tool, it has demonstrated how it can complement CIIP management using metrics and indicators to assess the level of ICT maturity of an organisation at sectoral, and national levels. The implication is that a government can potentially appreciate the anticipated impact of failures or cyberattacks against critical organisations. Therefore, it can be concluded that the model has addressed the ICT dependency measurement in a risk-based and empirical-backed scientific approach. This

can be beneficial to organisations as well as a nation to derive informed decisions using the tools on how to protect critical national information infrastructures in a more knowledgeable and coordinated fashion.

Acknowledgements

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

References

Atkin, D. et al. (2017) 'Organizational barriers to technology adoption: evidence from soccer-ball producers in Pakistan', *Quarterly Journal of Economics*, Vol. 132, No. 3, pp.1101–1164, DOI: 10.1093/qje/qjx010.

Australian Government (2010) *Critical Infrastructure Resilience Strategy*, *Report* [online] papers2://publication/uuid/C8ECF2E8-3ED2-4881-86E2-39F8F0581282%5Cnhttp://www.tisn.gov.au/documents/australian+government+s+critical+infrastructure+resilience+strategy.pdf (accessed 20 February 2020).

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

Chew, E. et al. (2008) *Performance Measurement Guide for Information Security*, NIST Special Publication 800-55 Revision 1, July.

Cornish, P. et al. (2010) *On Cyber Warfare*, The Royal Institute of International Affairs Chatham House [online] http://www.chathamhouse.org.uk (accessed 113 January 2020).

Domínguez, N. and Charles, R. (2010) *Introduction to E-Government ICT-Driven Change Management, Project Management and Process Management*, April [online] http://www.ads.gov.ba/v2/attachments/710_01_Introduction_to_eGov_Sarajevo_2010.pdf (accessed 20 February 2020).

ENISA (2012) *National Cyber Security Strategies: Setting the Course for National Efforts to Strengthen Security in Cyberspace*, DOI: 10.2824/3903.

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.

Government Accountability Office (2014) 'DHS action needed to enhance integration and coordination of vulnerability assessment efforts', *Critical Infrastructure Protection*, GAO-14-507.

Harašta, J. (2018) 'Legally critical: defining critical infrastructure in an interconnected world', *IJCIP*, pp.1–10, DOI: 10.1016/j.ijcip.2018.05.007.

ITU (2017) *Measuring the Information Society Report 2017*, International Telecommunications Union, Switzerland.

ITU (2018a) *Measuring the Information Society Report*, International Telecommunications Union, Geneva.

ITU (2018b) *Measuring the Information Society Report*, International Telecommunications Union, Switzerland.

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, DOI: 10.1007/978-3-319-48737-3_2.

Krepinevich, A.F. (2012) *Cyber Warfare A 'Nuclear Option'?*, Centre for Strategic and Budgetary Assessments.

Mbanaso, U.M., Kulugh, V.E., Musa, H. and Aimufua, G. (2019) 'Conceptual framework for the assessment of the degree of dependency of critical national infrastructure on ICT in Nigeria', *Proceedings of 15th International Conference on Electronics, Computer and Computation (ICECCO)*, Abuja, 10–12 December 2019.

National Information Technology Development Agency (NITDA) (2019) *Nigeria e-Government Interoperability Framework (Ne-GIF)*, National Information Technology Development Agency (NITDA).

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

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, Elsevier, DOI: 10.1016/j.ijcip.2016.06.002.

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, DOI: 10.1109/37.969131.

Robert, G. et al. (2009) *Organisational Factors Influencing Technology Adoption and Assimilation in the NHS: A Systematic Literature Review*, Report for the National Institute for Health Research Service Delivery and Organisation Programme.

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

Schreier, F. (2015) 'On cyberwarfare', *DCAF Horizon 2015 Working Paper*, No. 7, p.7.

Stergiopoulos, G. et al. (2018) 'Common criteria for the assessment of critical infrastructures', *International Journal of Disaster Risk Science*, Vol. 2, No. 1, pp.15–24, Elsevier Ltd., DOI: 10.1007/s13753-011-0002-y.

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 [online] http://www.crs.gov (accessed 17 April 2020).

United Nations (2005) *Core ICT Indicators: Partnership on Measuring ICT for Development* [online] http://www.itu.int/ITU-D/ict/partnership/material/CoreICTIndicators.pdf (accessed 20 February 2020).

United Nations (2011) 'Measuring the impacts of information and communication technology for development', *United Nations Conference on Trade and Development*.

Voeller, J.G. et al. (2008) 'Cyber security metrics and measures', *Wiley Handbook of Science and Technology for Homeland Security*, November, DOI: 10.1002/9780470087923.hhs440.

World Economic Forum (WEF) (2016) *The Global Information Technology Report 2016*, Insight Report [online] http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf%0Ahttps://www.weforum.org/reports/the-global-information-technology-report-2016 (accessed 21 May 2020).

Zaballos, A.G. and Jeun, I. (2016) *Best Practices for Critical Information Infrastructure Protection (CIIP)*, 1st ed., Inter-American Development Bank, Washington.

Notes

1 CI is a generic term that refers to a variety of systems, networks, and assets that are so vital to a given society, the economy, and the public's health and/or safety, of which their continued operation is highly desirable. CNI on the other hand can refer to CI officially designated by a country. CI and CNI are used interchangeably in this article.