Empirical study of the impact of e-government services on cybersecurity Development

Aristotle Onumo*, Andrea Cullen†, Irfan Ullah-Awan‡,
School of Electrical Engineering and Computer Science, University of Bradford
Email: A.O.Onumo@student.bradford.ac.uk* , A.J.Cullen@bradford.ac.uk†, I.U.Awan@bradford.ac.uk‡

***Abstract*—This study seeks to investigate how the development of e-government services impacts on cybersecurity. The study uses the methods of correlation and multiple regression to analyse two sets of global data, the e-government development index of the 2015 United Nations e-government survey and the 2015 International Telecommunication Union global cybersecurity development index (GCI 2015). After analysing the various contextual factors affecting e-government development , the study found that, various composite measures of e-government development are significantly correlated with cybersecurity development. The therefore study contributes to the understanding of the relationship between e-government and cybersecurity development. The authors developed a model to highlight this relationship and have validated the model using empirical data. This is expected to provide guidance on specific dimensions of e-government services that will stimulate the development of cybersecurity. The study provided the basis for understanding the patterns in cybersecurity development and has implication for policy makers in developing trust and confidence for the adoption e-government services.**

Keywords: Cybersecurity development, E-government development, Regression analysis, Online service index, cybersecurity policy

I. Introduction

The development of cybersecurity can be predicated by the need to protect Information and Communication Technology infrastructure and information objects including interests of persons, societies or nations from risk relating, arising through or from their interactions with cyberspace. [12]. The global transition from the traditional economy to the digital economy based on digital technologies and the rapid and sustained spread of Internet dependent technologies coupled with the impact of the broad penetration of both web 1.0 and 2.0 technologies has also resulted in opening new opportunities for interaction between government, the economy, and people. [8]. The evolution of these technologies has also provided the government the platform to digitize the service delivery and processes of governance to ensure transparency and achieve administrative efficiency [15], in making information publicly available [4], minimising cost and maximizing the usefulness of government information [10] which is the main essence of electronic government. Unfortunately, the development of cybersecurity has not kept pace with its counterpart in e-government despite the fact that guaranteed protection is provide by the former. This reassures confidence in the use of the later. One way of ensuring collaborative development is by understanding how the different indicators that shapen the development of e-government impact on cybersecurity development. This study, therefore, aims to investigate how e-government development impacts on the development of cybersecurity. The study is further divided into the following sections Section 2 review related works while section 3 highlights the hypothesis and the research model for the study. Section 4 discusses the methodology, results and discussion are presented in section 5. We present limitations and future work in section 6 and conclusion in section 7.

II. Review of Related Works

A. E-Government and Cybersecurity Development

The World Bank defined e-government as the use by government agencies of Information technologies (such as wide area network, the internet and mobile computing) that have the ability to transform relations with the citizen, business and other arms of the government [17]. Technologies, user behaviour and adoption including socioeconomic issues has often dominated researches in the field of e-government [10], [4]. Also recently, empirical studies on cultural dimension and influence on e-government have beginning to emerge [18], [2]) and also multidimensional studies integrating digital divide and national economies with e-government [2], [3]. Other studies investigated the effect of information security policy on e-government. One of such studies conducted in Nigeria showed that information security particular threat to identity and privacy of information as risk to successful e-government development [1]. [15] investigated the influence of some global indicators such as corruption, national income, innovation and cybersecurity on e-government. By using correlation and regression analysis of worldwide readiness indexes elicited from the United Nation Global E-government Survey 2014, corruption perception index obtained from Transparency international and other World Bank data for 49 countries of Sub-Saharan Africa, the study found out that all the indicators have the positive influence on e-government development. [15] study used sub-regional data as a total of 49 countries that were included in the sample were from the Sub-Saharan Africa. While we acknowledge the contribution of the study to e-government and cybersecurity literature, we wish to clarify the difference between their study and ours. First, our study considers e-government development as a precursor to cybersecurity development, unlike De Wet and Verkijika that considers e-government adoption and use which is enhanced by adequate cybersecurity measure [6], hence e-government becomes our independent variable. Secondly, [15]

fail to consider the multicollinearity of the independent factors in their analysis which we incorporated in our study to have a better outcome of model prediction when considering the contributing factors and thirdly, the variables we considered in our study were elicited from the 2016 global survey of e-government developmental factors. However, research has shown that information security have become important influence factor for successful adoption of e-government systems [7]. Available data from UN survey also shows the progressive development of e-government services among various nations.[16]. The development of cybersecurity in therefore to ensure that e-government services deliver on its objective of improving citizen access to government services [5], [9]. We, therefore, argue that cybersecurity development will be high in countries with high e-government services.

B. ITU Global Cybersecurity Index (GCI)

The International Telecommunication union conducted and caused to be published a research/survey on cybersecurity development of in its member nation state. The 2015 survey which is the first of its kind is aimed at effectively measuring each nation states level compliance and commitment to Global Cybersecurity Agenda (GCA)[5]. The development of cybersecurity, due to its integration with nations overall security strategy coupled with its domain of activity is often hampered by constrain in the public sector as well as the level of awareness amongst its citizen, ICT infrastructural development, and the existence of the required policies, strategies and legal frameworks which are key indicators of cybersecurity capabilities. The GCI is a composite of the level of national commitment to the development of cybersecurity. The index is largely based on ITU survey of compliance to GCA of 193 member states which were conducted in 2015. The index measures each nation states commitment to cybersecurity. It is the weighted average of five normalise scores on five most important dimension of cybersecurity which is critical to measuring national cybersecurity capabilities [5]; Legal measure, Technical measure, Organisational measure, capacity building measure and international cooperation.

C. Explainatory Variables

1) E-government Development Index (EGDI): More than a decade now, the United Nations Department of Economic and Social Affairs has been conducting and publishing surveys on e-government development of its member states. The 2016 survey is very significant in that it anchors its analysis to reflect the potential of e-government to support the implementation of 2030 agenda for sustainable development. The index is the composite measure of the level of countries advancement on the development of online service and bridging the digital divide. According to [16], the index is a weighted average of the normalised scores of the three most important dimensions of e-government; the Online Service Index (OSI), the state of the development of Telecommunication Infrastructure i.e Telecommunication Infrastructure Index (TII). We shall examine these dimensions independently to evaluate their influence in cybersecurity development.

2) Online Service Index (OSI): Digital technologies are now the potent tool of government in an attempt to deliver advanced electronic and mobile services with sole aim of bringing in transparency and credibility in overall governance and service delivery. It signifies the presence of networks, e-service portals, e-participation portals as well as websites of Ministries and Agencies of government [16]. It therefore reasonable to suggest that as these services are migrated to the digital space, it follows the imperative of digital protection, hence there exist a positive correlation between online service and cybersecurity development. We therefore argue that countries with established online services and presence will have high cybersecurity development.

3) Telecommunication Infrastructure Index (TII): The index is derived primarily from the 2016 E-government survey. It is a composite indicator measuring; the number of fixed telephone line per 100 persons, the number of mobile subscription per hundred persons, the number of wireless broad band subscription, and the number of fixed broad band subscription per hundred persons [16]. The telecommunication infrastructure is the vehicle that transport digital objects within and around the cyberspace and therefore a potential target that deserves adequate security. However the same infrastructure offers a credible platform to those who take advantage of the developed infrastructure for criminal exploitation. We therefore argue that cybersecurity development will be high in countries with high telecommunication infrastructural development.

4) Human Capital Index (HCI): The Human Capital Index indicates the aggregate level of a countrys education and cost of four components [16] namely adult literacy rate, combine primary, secondary and tertiary gross enrolment ratio, expected years of schooling and average year of schooling. The Data source of the HCI is the United Nations Economic Scientific Cultural Organisations (UNESCO). Cybercrime is technologically and skill intensive, hence a knowledge crime [19], which will require even more knowledge to secure the society. We therefore argue that there exist a strong positive between Human Capital Index and Cybersecurity development, hence cybersecurity development will be high in countries with high human capital development.

III. Hypothesis

Based on our understanding of the casual link between the endogenous and exogenous variables arising from our exploratory study, hypotheses were formed and a research model aimed at investigating how e-government services will impact on cybersecurity development was established. Our hypotheses are formerly presented from the argument identified from supporting and relevant literatures. We therefore present as follows:

H1: Cybersecurity development is high in countries with high e-government services

H1b: Provision of online services is positively associated with cybersecurity development

H1c: The development of Telecommunication infrastructure has a positive influence on the development of cybersecurity

H1d: Human Capital development has a positively associated

on cybersecurity development
The hypotheses are summarised in our initial conceptual model

$$GCI = f(OSI, TII, HCI) \tag{1}$$

$$GCI = (\beta_0 + \beta_1 OSI + \beta_2 TII + \beta_3 HCI) + \xi_0 \tag{2}$$

IV. Methodology

We have used large global data sets to empirically test our research model and generate findings that are likely to have implications. Collecting primary data source to test our hypotheses was not considered in view of time and resource constraint. How ever primary data couldn't have given a better result in view of the fact that the global data sets used for our analysis were collected from primary sources by some of the world's most reputable institutions and researchers in the filed of study[3]. Our team therefore opted for the collection of archival data compiled and held by credible and competent international institutions such as the International Telecommunication Union (ITU) and United Nations (UN). The summary is presented in Table I

A. Framework for result Analysis

The study used IBM SPSS 23 for the analysis. The tool is well suited in analysing influence factors and determining the direction of influence using predictive models. The study also conducted statistics such as correlation and regression analysis including multiple regression to determine how various variables in the research contribute in predicting the outcome of our model and the direction of the association. Equations 3-11 captures the theoretical framework for the analysis in this research.

$$r = \frac{C_x y}{\sqrt{C_x x C_y y}} = \frac{C_x x}{\sigma_x \sigma_y} \tag{3}$$

For set of N two dimensional data points $x_1, x_2, x_3 ... x_N$ and $y_1, y_2, y_3 ... y_N$ we have;

$$\overline{x} = \frac{1}{N} \sum_i x_i \tag{4}$$

$$\overline{y} = \frac{1}{N} \sum_i y_i \tag{5}$$

$$C_{xy} = \frac{1}{N-1} \sum_i (x_i - \overline{x})(y_i - \overline{y}) \tag{6}$$

$$C_{yy} = \sigma_y^2 = \frac{1}{N-1} \sum_i (y_i - \overline{y})^2 \tag{7}$$

The relationship to be tested is a linear one. In this case the outcome follows the equations as highlighted below;

$$y_i = Ax_i + B, \overline{y} = A\overline{x} + B \tag{8}$$

$$\begin{aligned} C_{xy} &= \frac{1}{N-1} \sum_i (x_i - \overline{x})(y_i - \overline{y}) \\ &= \frac{1}{N-1} \sum_i (x_i - \overline{x})(Ax_i + B - A\overline{x} - B \\ &= \frac{A}{N-1} \sum_i (x_i - \overline{x})^2 \end{aligned} \tag{9}$$

$$C_{xx} = \sigma_x^2 = \frac{1}{N-1} \sum_i (x_i - \overline{x})^2 \tag{10}$$

$$C_{yy} = \sigma_y^2 = \frac{A^2}{N-1} \sum_i (x_i - \overline{x})^2 \tag{11}$$

$$r = \frac{C_{xy}}{\sqrt{C_{xx} C^{yy}}} = \frac{A}{|A|} = \pm 1 \tag{12}$$

Hence if x and y are exactly linearly related, $r = 1$; depending on whether the slope is positive or negative. In real application, there will be a spread in the values of x and y, in which case the correlation will be less than maximal $|r| < 1$.

V. Results

The results show that all the explanatory variables are significantly correlated with development cybersecurity as shown in Table II and (11), while e-government development demonstrates a higher significant correlation with cybersecurity development. The positive influence of e-government on cybersecurity development has earlier been posited by other studies [7]. However among the three composite measures of e-government, online service appears to be more significantly correlated with cybersecurity development than the others (OSI, r = .752**) followed by Telecommunication Infrastructure (TII, r = .570**) and Human Capital Development (HCI, r = .507**) as shown in Table II. The strength of the correlation also suggests that all the explanatory variables are positively associated with cybersecurity development. All our hypotheses are therefore supported. As the primary focus of this study is to examine empirically how e-government impacts on cybersecurity development, we went further and conducted multiple regression analysis so that we could enter variable on the basis of our theoretical understanding and the result of our correlation statistics. We entered OSI first because it has a stronger correlation with cybersecurity development as indicated in Table II. We then entered other variables HCI and TII into the second step of the model. We examined the Variance Influence factor to address the problem of multi-collinearity. We found that collinearity is not an issue as none of the Variance influence factors are greater greater 5. A variance influence factor less than 5 indicates acceptable shared variance. [20] By carrying out multiple regression analysis we found that the three composite measure of e-government accounted for 56.6 percent of the variation in cybersecurity development (R squared =0.566 Table III model 2 summary). From Model 1 summary of Table III, we also

TABLE I
GLOBAL DATA SOURCE

Variable	Measure	Data Source
Cybersecurity Development	Legal	GCI[5]
	Organisation	
	Organisation	
	Capacity Building	
	International Corperation	
	Technical Measure	
E-government Development	Composite measure of	UN[16]
	Online Service	
	Telecomm Infrastructure	
	Human capital Development	
Online Service Development	Online Presence	UN[16]
Telecomm. Infrastructure	Fixed and mobile	ITU, [16]
	Wireless and Broadband	
Human Capital Development	Adult Literacy	UNESCO in [16]
	School enrolment	
	Year of Schooling	

observed that OSI explains 56.5 percent of this variation. This is resented in the scatter plot as shown in Fig 1 which and indicates the goodness of fit of our model. Less than 1 percent of the variation was explained by other variables in the model.

Based on our statistical analysis using Pearson Correlation Matrix, all our hypotheses are sustained. However using regression analysis to evaluate how each of the factors contributes to the development of cybersecurity, we observed that the development of cybersecurity is strongly predicted by online service deployment as this explains 56.5 percent variation in the model at p value of 0.01 as shown in Table IV which is highly significant. We therefore refined our model as follows;

$$GCI = (\beta_0 + \beta_1 OSI+) + \xi_0 \tag{13}$$

and based on (13), H1c is rejected; The development of telecommunication infrastructure has a positive influence on the development of cybersecurity

TABLE II
CORRELATION MATRIX

Variables	GCI	EGDI	OSI	TII	HCI
GCI	1	.680**	.752**	.570**	507**
EGDI	.680**	1	.908**	.936**	.889**
OSI	.752**	.908**	1	.760**	.674**
TII	.570**	.936**	.760**	1	.808**
HCI	.507**	.889**	.674**	.808**	1

**. Correlation is significant at the 0.01 level (2-tailed).

Discussion

Our study is aimed at examining how e-government service development could explain the level of cybersecurity development in a country. The result shows that all the composite factors of e-government development have a positive influence on cybersecurity development while online service alone explains 56.5 percent of the variance in cybersecurity development. This therefore explains the reason why most countries with a high level of development of e-government service rank very high on cybersecurity development. Countries like Canada, Unites States of America, United Kingdom, South Korea, Japan and other developed countries fall into this category.[5] Countries that intend to increase their ranking in the global cybersecurity index as a show of commitment to the various dimension of cybersecurity development should give priority to online service development. Our study further suggest that while cybersecurity development leads to increased confidence in the adoption of e-government service, it does not necessarily lead to e-government development. It also revealed that the outcome of cybersecurity development is determined by how much government organisations endorse digital technology as exemplified in the various e-government service measures.
It is noteworthy from the results of our correlation analysis that the contextual and composite factors of e-government are significantly correlated with cybersecurity, however only OSI (onlione Service Index) could significantly predict cybersecurity development from our regression analysis. This though may not be surprising as online services are gateway to the cyberspace, what is however surprising is that TII (Telecommunication Infrastructure Index) did not significantly contribute to predicting cybersecurity development. One possible explanation for this is the over concentration on the development of online service without the corresponding development of cyber-infrastructure which has implication for privacy and protection of digital objects.

VI. LIMITATIONS AND SUGGESTIONS FOR FUTURE WORKS

There is an apparent lack of empirical studies into the determinants of cybersecurity development as the Global

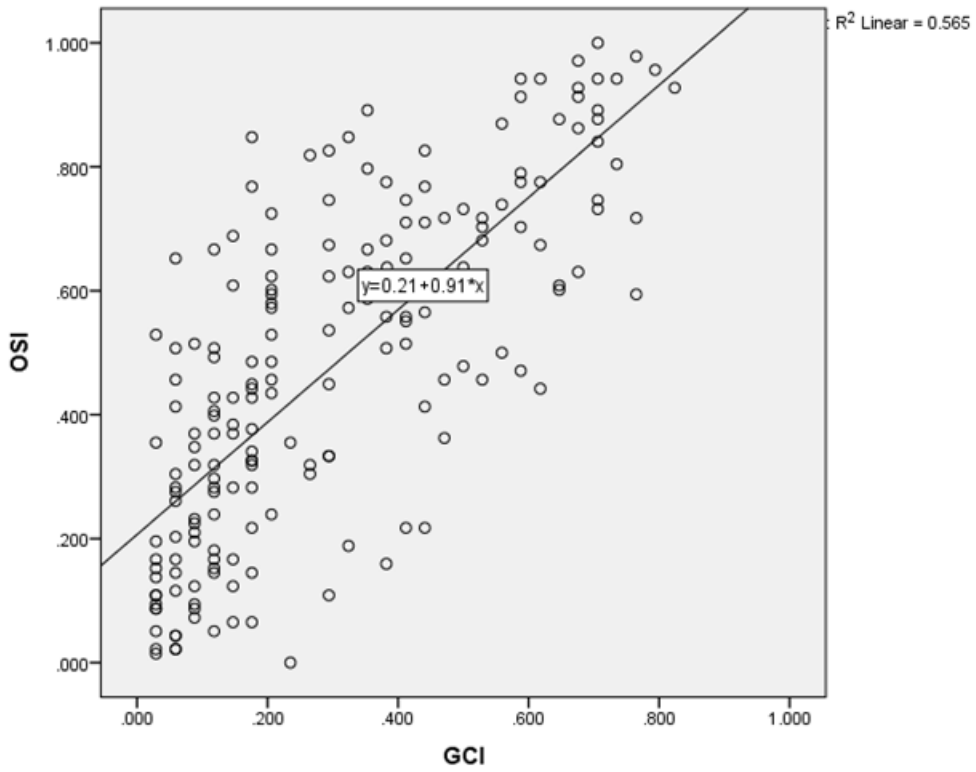

Fig. 1. Scatter Plot

TABLE III
MODEL SUMMARY

Model	R	R Sq.	Adj. R Sq	R Sq. Change	Sg. F. Change
1	.752a	.565	.562	.565	.000
2	.752b	.566	.558	.001	.860

TABLE IV
COEFFICIENTS

Model	Coeff B	Coeff.Beta	Sig.	VIF
1 Constant	.001			
OSI	.623	.752	.000	1.000
2 Constant	0.18			
OSI	.621	.749	.000	2.371
HCI	-.050	-.045	.606	3.206
TII	.043	.046	.637	3.853

Cybersecurity Index is just evolving [5]. We used global data sets which have limitations. As some have argued that the composite indices and score tends to be simplistic and may over look a deeper cause of a phenomena [11]. As this may be partly responsible for the inability of TII in our model to predict Cybersceurity development. Furthermore, with secondary data, it is almost impossible to detect errors during data collection [14], which is another pitfall. Therefore caution should be taken when making generalisation from our findings. However, these limitations may be addressed in future research and our model validated by using primary data and possibly combining both qualitative and quantitative data which may lead to further theoretical development. We believe that the approach and arguments presented in the study have provided a valuable starting point for further discussion and empirical research.

VII. CONCLUSION

The goal of the global cybersecurity index (cyber wellness profile) is to evaluate the commitment countries have to the various dimension of cybersecurity development and in effect provides protection and assurance to the digital environment through legislation, technical support, capacity development, organisation and international cooperation. This study addresses this influence by examining how e-government services influence the development of cybersecurity as cybersecurity development is an emerging phenomena.

The result suggests that the development of e-government services drives the cybersecurity development. The study further provides the basis for understanding the patterns in cybersecurity development far beyond what has been established in the ITU Global Cybersecurity survey. The positive influence of e-government on cybersecurity development underscores the importance of collaborative approach towards cybersecurity development as posited in prior studies [7],[6] This then means that the key actors, such as the policy makers and other institutional arrangements such the the government agencies and the academia are critical to the outcome of cybersecurity development. This study has implication for both policy and decision makers in government organisations as discussed in this paper especially in predicting a balanced investment in development cybersecurity.

REFERENCES

[1] Ashaye O. R. and Irani Z., "e-Government Implementation Benefits, Risks and Barriers in Developing Countries: Evidence from Nigeria," International Journal of Information Technology and Computer Science (IJITCS), pp. 92-105

[2] Fang Zhao (2013) An empirical study of cultural dimensions and e-government development: implications of the findings and strategies, Behaviour and Information Technology, 32:3,294-306, DOI: 10.1080/0144929X.2011.644580

[3] Fang Zhao, Joseph Wallis, Mohini Singh, (2015) "E-government development and the digital economy: a reciprocal relationship", Internet Research, Vol. 25 Issue: 5, pp.734-766, doi: 10.1108/IntR-02-2014-0055 DOI:http://dx.doi.org/10.1108/IntR-02-2014-0055

[4] Heeks, R., Ed. (1999). Reinventing government in the information age: International practice in ITenabled public sector reform. London, Routledge.

[5] ITU (2015) Global Cybersecurity Index and Cyber wellness Profile, [online] https://www.itu.int Accessed May 5 2017

[6] Jacobi, A., Jensen, M., Kool, L., Munnichs, G. and Weber, A. (2013). Security of E-goernment Systems. European Parliament. Retrieved from: http://www.europarl.europa.eu/RegData/ etudes/etudes /join/2013/513510/$IPOL-JOIN_ET(2013)513510(ANN02)_EN.pdf$

[7] Khanyaako, E., and Maiga, G. (2013). An information security model for e-government services adoption in Uganda. IST-Africa Conference and Exhibition (IST-Africa),(pp. 1-11)

[8] Kneuer M. Harnisch S. (2016) Diffusion of e-government and e-participation in Democracies and Autocracies Global Policy Volume 7 . Issue 4 . November 2016

[9] Lfstedt, R. E. (2005) Risk Management in Post-Trust Societies. Palgrave MacMillan, Basingstoke, Hampshire, UK and New York

[10] OMB (2000). OMB Circular A-130: Management of Federal Information Resources. O. o. M. a. Budget. Washington, D.C.

[11] OECD(2008), Handbook on Constructing Composite Indicators: Methodology and User Guide, Organization for Economic Cooperation and Development, Paris

[12] ISO/IEC 27032. Information technology - Security techniques - Guidelines for cybersecurity, 2012.

[13] Rayne R. Van Niekerk J (2014) From Information Security to Cyber Security Cultures Organizations to Societies IEEE

[14] Shultz, K.S., Hoffman, C.C. and Reiter-Palmon, R. (2005), Using archival data for IO research: advantages, pitfalls, sources, and examples, The Industrial-Organizational Psychologist, Vol. 42 No. 3, pp. 31

[15] Verkijika S. F. , De Wet L (2016) e-Government Development in Sub-Saharan Africa (SSA): Relationship with Macro Level Indices and Possible Implications, IST-Africa 2016 Conference Proceedings Paul Cunningham and Miriam Cunningham (Eds) IIMC International Information Management Corporation, 2016

[16] United Nations (2016) e-Government Development Survey Report [online] http://workspace.unpan.org/sites/Internet/Documents/UNPAN96407.pdf Accessed May 10 2017

[17] World Bank (2016) E-government [online]. Available from: http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/EXTEGOVERNMENT/0,, menuPK:702592 pagePK:149018 piPK:149093 theSitePK:702586,00. html Accessed May 15 2017

[18] Kovacic, Z., 2005. The impact of national culture on worldwide eGovernment readiness. Informing Science,8, 143158.

[19] Kshetri N (2006) The Simple Economics of Cybercrime *The EEE Security and Privacy* Vol. 4, No. 1 Pages 33 39

[20] Joe F. Hair and Christian M. Ringle and Marko Sarstedt (2011) PLS-SEM: Indeed a Silver Bullet Journal of Marketing Theory and Practice, 19 (2) pages 139-152, doi:10.2753/MTP1069-6679190202,

ACKNOWLEDGMENT

The authors would like to thank the National Information Technology Development Agency, Nigeria for sponsoring this programme.