Cybersecurity Risks and Challenges Facing the Adoption of E-Government Framework in Sudan

Abdalhamid Abdalgader Guma[1], Jamaludin Bin Ibrahim[2]

[1,2]Kuliyyah of Information and Communication Technology

[1,2]International Islamic University Malaysia, Kuala Lumpur, Malaysia.

Abstract: **E-government implementation helping improve efficiency and quality of service delivery to their citizens in cost-effective ways. However, this transition process also creates new challenges and cyber risks. Cybersecurity is a crucial factor in transforming e-government into a resilient one. In this paper, the authors aim to review cybersecurity challenges facing the adoption of e-government framework in Sudan. Rising incidents of cyberattacks towards businesses, individuals, and governments and their cost for the economy is an increasing concern worldwide. Therefore, identifying threats and security vulnerabilities that could constitute an obstacle for the e-government in delivering their services is important. This study focuses on the existing literature. While there is a lack of resources that investigating cybersecurity issues in Sudan, thus this study may contribute to Sudanese library. Finally, the paper proposes some recommendations as countermeasures to mitigate the cyber risks.**

Keywords: **E-government, Sudan, Cybersecurity Challenges, Resilient government.**

I. INTRODUCTION

ICTs have been increasingly adopted by the global community as a key enabler for economic development as well as social. Governments from all over the world started to realize the potential of digital transformation to promote their citizens' well-being and growth. But they also realized that cybersecurity needs to be an important and inseparable part of the technological advancement in facilitating this transition (Brahima Sanou ITU-GCI 2017). A modern platform has been built up by E-government that changed the essence of the entire public sector and its engagement with its constituencies. It has impacted the socio-economic and political aspects of society substantially. E-government offers much more efficient and cost-effective delivery of public services, creating significant incentives for enhancing the performance of the public sector. Notwithstanding this transition has made a significant benefits, but it also gives rise to new challenges particularly in developing countries, where multiple initiatives were not successful Sara Abdalla (2012).

The rapid advancement of ICT and ease of access to internet globally, has resulted in a large number of first-time users in developing countries. With everyday cybercrime as reported by Casey Crane (2019) e-government must assure their level of security and apply countermeasures to keep their assets safe. Addressing the cybersecurity issues and their effects on the Sudanese e-government systems is important.

II. PROBLEM STATEMENT

The implementation of e-government not only saves resources, effort and money but it can also increase the service quality levels. E-government security is one of the critical elements for maintaining a well-functioning e-government. With the increased number of services offered to the public sector, a higher level of e-government security is required as mentioned by Jin-fu, Wang. (2009). Therefore addressing the cybersecurity issues that may arise would mitigate the risks of cyberattacks. Some of research studies recommend further investigation in this area, for instance B. M. E. Elnaim (2014). While hackers every day looking for victims to attack, steal or corrupt their data, countermeasures need to be taken by e-government to safeguard people’s data and privacy. In this paper the authors aims to address the cybersecurity risks that may face the Sudanese e-government.

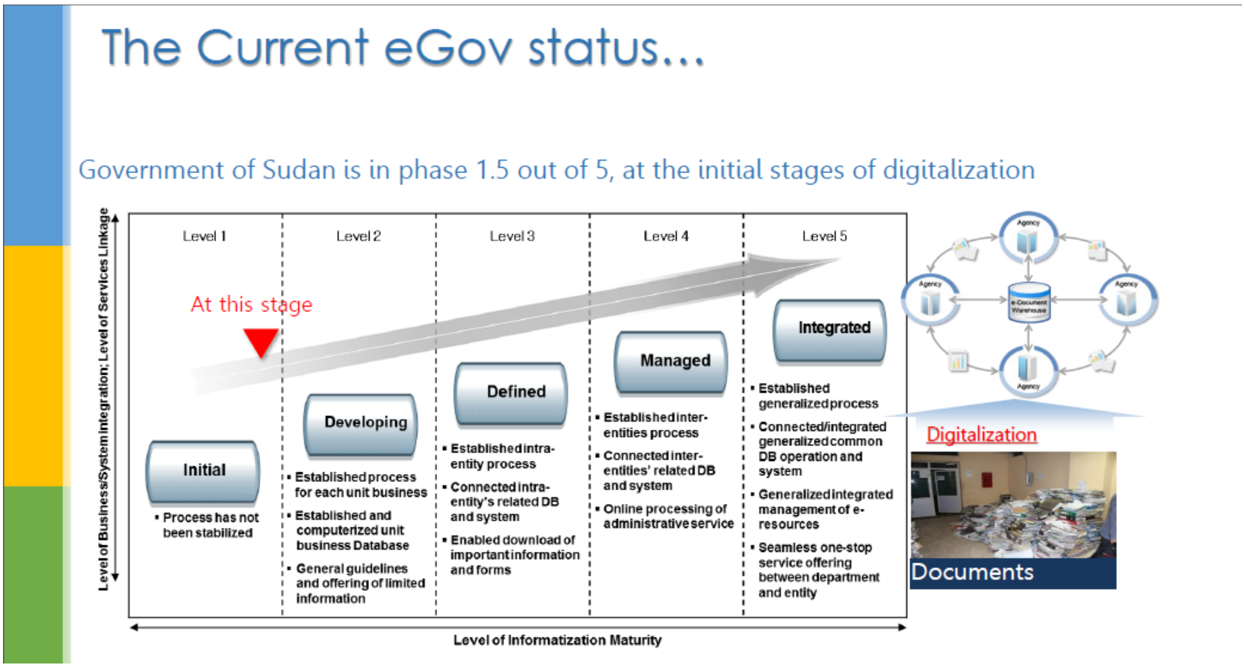
III. LITERATURE REVIEW

A. *E-government Definition*

E-government can be defined as the employment of information and communication technology for delivering government services to the citizens M. M. Saeed (2017). Some studies limited the definition of e-government to the internet-enabled applications only, while e-government focuses on the whole ICT applications to improve the efficiency of public sector organizations according to Q. Li and E. O. Abdalla (2014). In other words, e-government refers to the utilization of ICT technologies to facilitate government services to the citizens and the public sector through internet applications and other communication mediums in efficient and cost-effective ways.

B. *E-government Current Status in Sudan*

In accordance with B. M. E. Elnaim (2014) the implementation of e-government in Sudan has several stages that can be roughly summarized into the Planning, policies and strategies phase, Capacity building & ICT Infrastructure phase, and Promotion of scientific research and digital services phase. In the year 2016, the Sudanese government started to implement the Sudan eGov and transition to SMART Master plan 2016-2020 as reported by the Sudanese National Information Center NIC. The report also mentioned the achievements of the previous phases (phase 1 & phase 2) from enacting a number of laws and legislations to extending fiber-optic to around 30,000Km. In the same year of 2016 the government has moved to implement electronic receipt throughout all ministries for payment collection. By the year 2017, the e-government websites were published and contain information and instructions of 50 government services to the citizens and the public sector. Government of Sudan is in phase 1.5 out of 5, which means is still at the initial stages of digitalization. Notwithstanding communication infrastructure is well developed in Sudan compared to other countries in the region, but due to the sanctions and other external factors resulted in overall the level of Sudan to be rated at level 1.5. The following figure shows the stage of Sudan in the implementation plan.



The Current eGov status…

Government of Sudan is in phase 1.5 out of 5, at the initial stages of digitalization

Level 1 — Initial
- Process has not been stabilized

Level 2 — Developing
- Established process for each unit business
- Established and computerized unit business Database
- General guidelines and offering of limited information

Level 3 — Defined
- Established intra-entity process
- Connected intra-entity's related DB and system
- Enabled download of important information and forms

Level 4 — Managed
- Established inter-entities process
- Connected inter-entities' related DB and system
- Online processing of administrative service

Level 5 — Integrated
- Established generalized process
- Connected/integrated generalized common DB operation and system
- Generalized integrated management of e-resources
- Seamless one-stop service offering between department and entity

At this stage
Level of Business/System integration; Level of Services Linkage
Level of Informatization Maturity
Agency
Agency
Agency
Agency
e-Document Warehouse
Digitalization
Documents

FIGURE 1: THE PROGRESS OF SUDAN IN E-GOVERNMENT IMPLEMENTATION

C. *Challenges Facing the Implementation of E-Government in Sudan*

The main objective of the e-government project in Sudan is to create efficient, systematical, and trustworthy e-government to accomplish proper management and socio-economic development as reported by Y. E. S. Ahmed (2017). There are many challenges facing Sudan in applying electronic government. For example poor communications network infrastructure and incapacity to provide equal efficiency for all users, areas, and cities. M. M. Saeed (2017). It is necessary for E-government to go far beyond technology to adapt to challenges, a new model of leadership and cooperation between public and private sector partnerships is required. Q. Li and E. O. Abdalla (2014).

D. Cybercrimes in Africa Region

In pursuant to ACTIR report (2018) there is lack of awareness and uncoordinated regulations in African countries have increased the continent cyber vulnerability. Cybercrime threats such as fraudulent emails, ransomware, denial-of-service attacks are growing every day, yet African nations remain unprotected and should actively deal with the implications. Cybercrime costs Africa an estimated amount of $3.7 billion in 2017. The report also mention that more than 90% of African organizations and businesses are operating below cybersecurity countermeasures. The matter becomes even worse when the government agencies were unaware of the cyber risks they are facing. In addition, the Kenyan and Nigerian governments have been hacked and lost millions of dollars by hackers and leaving the internal-revenue authorities getting hit the most. The report also stated that attacks were not promoted by financial motivations only, but a presence of diplomatic-sponsored hacking occurs as well.

E. Challenges Facing the Implementation of E-Government in Sudan

During the period from January to October 2016, more than 200 million of government data records were compromised as reported by IBM X-Force Security Incident Data. As well the government sector ranks second among all industries in terms of records compromised in the same year. Cyber protection is an important needs for the Sudanese e-government. The key security challenges for the e-government in Sudan are described as following:

E.1 Cybercrime Legislation: Cyber-crime legislation defines appropriate conduct requirements for users of the ICT and sets socio-legal cyberattacks penalties, as well as safeguards ICT users. Moreover, reduce or block harm to people’s data or systems, as well to authorize the prosecution of online committed crimes. UNODC (2013). The expanding landscape of cybercrime is an important challenge for law enforcement authorities and investigators. The National Information Center NIC is one of the existing legal institutions dealing with cybersecurity and cybercrime. NIC had released several laws that govern and regulate the ICT in Sudan for example the E-crimes law for the year 2007 in relation to cybersecurity as reported by NIC (2016). Cybercrime has a dynamic nature that makes it difficult for law enforcement to get control of it. As cybercrimes are growing new rules and regulations need to take place all the time.

E.2 National Cybersecurity Strategies: The digital divide is considered one of the big challenges for e-government in Sudan. Digital divide refers to the gap that exist between people who have access and those who do not B. M. E. Elnaim (2014). According to IWS 2020 only 29.9% of the total population have access to the internet, which means not all the Sudanese have equal access to the internet whether for limited IT skills or any other reasons. Not to mention the high percentage of computer literacy which will lead them to become an easy victims of online threats. As investigated by Dodel & Mesch (2018) quality of access to the internet and education level of users are correlated with their level of digital security awareness. ICT infrastructure is coming under increased attacks and the ways that this is happening is going to be facilitated through 5G technologies. With the emergence of 5G technologies such as Artificial Intelligence (AI) and the Internet of Things (IoT), there is a need to leverage the academic community (lack of cybersecurity courses in the universities in Sudan) and get prepared to get advantage of these technologies.

E.3 Computer emergency response teams (CERTs): The Sudan Computer Emergency Response Team (Sudan CERT) is responsible for leveraging awareness about networks and information security among businesses and users of ICT systems. The team is also responsible for safeguarding them from Cyber threats. Furthermore, the team plays the first responder when an incident occurs. In a step to provide a secure and stable environment, the Sudanese government has lunched the national data center for hosting applications and the databases of all government institutions pursuant to NIC (2016). The continued growth of compliance obligations and enforcement for security measures, increase the demand for professional staffs. According to B. M. E. Elnaim (2014) there is lack of high qualified officers and ICT skills, also improper human resources training.

E.4 The Capacity of Implementing Strategies and Awareness Rise: Almost all industries are covered by cybersecurity applications. A lot of efforts need to be done by economic, social and political authorities for the seek of national capabilities development and skills. There are a variety of ways for these authorities to implement strategies and raise awareness among the stakeholders. This can be done through law enforcement and justice departments for the compliance aspect, as well as educational institutions, private sector organizations, and developers of technology to raise awareness ITU-GCI (2018). The main objective of awareness is to mitigate or prevent cyber-attacks, it requires engaging users on an enduring basis to keep them a post of any new threats, and adapt to new behaviors that keep them safe online. According to Symantec report ISTR during the year 2018 they block an average of 10,573 malicious mobile apps per day. Where 39% of tools apps were malicious, 15% lifestyle and 7% of Entertainment apps.

F. Threats and Security vulnerabilities

E-government offers information delivery and service delivery. In the information section: users interact with the interface of browsing. In the service section, the user is given access to the e-government management information system MIS to get various services such as filling forms, pay online, etc. The rapid advancement of technologies is making a surpassing gap comparing to the slow pace of regulations and law-making. All effective governance systems should be robust against malicious attacks and viruses. Various of cybercrimes are motivated through unauthorized access or even a state-sponsored cyber war. These kinds of threats can be critical to the whole community especially if the socially active user is infected. E-government systems are increasingly interconnected which means when one piece is hit it has the potential to cascade to the rest of the other systems as well. Whether using laptop, tablet or smart phone users are vulnerable to ever evolving cyber threats from viruses or other types of malwares.

V. DISCUSSION

Cybersecurity is a crucial factor in transforming e-government into a resilient one. Security measures must be integrated strategically from the beginning of the project, during the planning stage.The findings from the literature review highlighted that around half of the world is now online for the first time ever. In agreement with ITU-GCI (2018) despite that it is a huge opportunity and step to a more progressive digital economy. But the vital assets and systems that underpinning people's daily lives is under increased attacks and exposing users to ever-evolving cyber threats. Therefore, governments need to take countermeasures to safeguard themselves and their citizens from cyberattacks. Unfortunately, still there is a recognized gap between a lot of countries in terms of knowledge in maintaining development in cybercrime legislation, national cybersecurity strategies (NCS), computer emergency response teams (CERTs), awareness and capacity to spread out the strategies, and capabilities and programmes in the field of cybersecurity. ITU News 2019.

A. Recommendations

In consonance with ITU-GCI (2018) outdated programs must be updated specially for banks and businesses, promote qualified staff in charge of systems administration, hire trusted security partners, and audit regularly. Provide training on a regular basis for staff to be aware of the evolving cyber threats. The following suggestions is adopted from A. Wakama 2018 article

- **Develop clear frameworks and policies:** a clear rules and instructions has to be planning the evaluation of cybersecurity. Implementation of technology, personnel management, and training should be accompanied by consistent instructions that are regulated across departments and accepted as best practice.

- **Central vs federated?:** the complexity of cybersecurity and data integrity is increasing dramatically in cloud-based architectures. Storing data like logos from different departments of government centrally and facilitate reporting and data administration. It might be more suitable to store sensitive data into a separate servers that maintained by its own department, and highly protected by best security defense teams.

- **Make the most of advanced security tools:** new defense technologies are emerging all the time to block attackers. taking advantage of these technologies helps in mitigating the cyber risks.

- **Take a balanced approach:** Disruptive technologies change the cyber risk exposure of an organization. Every new wave of innovation seems to broaden the threat in new and different ways. Nevertheless, the concern of security risks will never lead to creativity being ignored, and emerging technology being shunned. The best approach is to carefully analyze all emerging developments from a risk and safety perspective, consider deeply how they can impact the environment of the threat, and then implement them wisely.

VI. CONCLUSION

Governments across the world started to use ICT technologies to improve the quality of life of their citizens. Despite that delivering e-government information and services online to users at a reduced cost is a significant benefit, but also securing these assets over the cyber is challenging. The Sudanese government started to implement the Sudan eGov and transition to smart government. The government of Sudan is progressing in the implementation of the eGov plan at overall stage of 1.5 out of 5. Cybersecurity is a crucial factor for the e-government to transform into resilient e-government. There are four key security chellenges that addressed in this study a) Cybercrime legislation: cybercrime has a dynamic nature that makes it difficult for law enforcement to get control of it. As cybercrimes are growing new rules and regulations need to take place all the time. b) National cybersecurity strategies: with the emergence of 5G technologies such as Artificial Intelligence and the Internet of Things, there is a need to leverage the academic community (lack of cybersecurity courses in the universities in Sudan) and get prepared to get advantage of these technologies. c) Computer emergency response teams (CERTs): the continued growth of compliance obligations and enforcement for security measures, increase the demand for professional staffs. According to x there is lack of high qualified officers and ICT skills, also improper human resources training. d) The Capacity of implementing strategies and awareness rise: the main objective of awareness is to mitigate or prevent cyber-attacks, it requires engaging users on an enduring basis to keep them a post of any new threats, and adapt to new behaviors that keep them safe online. According to ITU-GCI (2018) still, there is a recognized gap between a lot of countries in terms of knowledge in maintaining development in these key security challenges. Although, there is a lack of resources and statistics shows data breach, vulnerabilities, cyberattacks incidents, cybercrime damage, or costs in Sudan. This paper contributes to the open literature in general and to the Sudanese ICT library. This is a very topical issue in the present digital world, which still needs to be widely addressed.

REFERENCES

[1] ACTIR report (2018). Executive Summary: 2018 Africa Cyber Threat Intelligence Report (ACTIR).

[2] A. WAKAMA (2018). Cyber-security Essential in realising our e-Government ambitions. Retreaved from https://www.itnewsafrica.com/2018/02/cyber-security-essential-in-realising-our-e-government-ambitions/

[3] Brahima Sanou ITU-GCI (2017). Global Cybersecurity Index. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx

[4] B. M. E. Elnaim (2014). An Overview of E-Government Strategy in Sudan. European Journal of Computer Science and Information Technology, 2(2), 1–9.

[5] Casey Crane (2019). 33 Alarming Cybercrime Statistics You Should Know in 2019. Retreaved from https://www.thesslstore.com/blog/33-alarming-cybercrime-statistics-you-should-know/

[6] IBM X-Force (2016). IBM X-Force Security Incident Data. Retrieved from https://www.ibm.com/downloads/cas/5V1Y0ARZ?mhsrc=ibmsearch_a&mhq=cyber%20security%20threats%20to%20e-government

[7] IWS (2020). Sudan Internet Usage and Marketing Report retreaved from https://www.internetworldstats.com/af/sd.htm

[8] ITU-GCI (2018). Global Cybersecurity Index 2018

[9] ITU News 2019 https://news.itu.int/cgi-2019-released/

[10] Jin-fu, Wang. (2009). E-government security management: Key factors and countermeasure. 5th International Conference on Information Assurance and Security, IAS 2009, 2, 483–486. https://doi.org/10.1109/IAS.2009.146

[11] M. M. Saeed (2017). E-Government in Sudan : Challenges and Future Prospects. International Journal of Computer Science Trends and Technology (IJCST), 5(1), 38–42.

[12] NIC Sudan (2016). National Information Center. Sudan eGov and transition to SAMRT Masterplan 2016-2020.

[13] Q. Li and E. O. Abdalla (2014). The E-Government in Sudan: Challenges, Barriers and Prospects. International Conference on Global Economy, Commerce and Service Science (GECSS), (Gecss), 236–240. https://doi.org/10.2991/gecss-14.2014.60

[14] Sara Abdalla (2012). Phd Thesis. An E-Government Adoption Framework for Developing Countries: A Case Study from Sudan. Cranfield University

[15] Dodel, M., & Mesch, G. (2018). Inequality in digital skills and the adoption of online safety behaviors. Information Communication and Society, 21(5), 712–728. https://doi.org/10.1080/1369118X.2018.1428652

[16] Sudan (CERT). Computer Emeregency Response Team. Retreaved from http://www.cert.sd/

[17] Symantec ISTR (2018). Internet Security Threat Report Volume 24. Retrieved from https://docs.broadcom.com/doc/istr-24-2019-en

[18] Y. E. S. Ahmed. (2017). Sudan e-Government Master Plan and Transition to Smart Government 2016-2020 Comparison of Current Approaches. International Journal of Science and Research (IJSR), 6(1), 82–96. https://doi.org/10.21275/art20163955

[19] UNODC (2013). The role of cybercrime law. Retrieved from https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-roleofcybercrimelaw.html#:~:text=Cybercrime%20law%20identifies%20standards%20 of,infrastructure%2C%20in%20particular%3B%20protects%20human