BOOK CHAPTER | Cyber safety & Sustainable Development

Investigating the Link Between Cyber Security and Sustainable Development: A Conceptual Analysis.

Olanipekun, Wahid Damilola (PhD)
College of Management and Information Technology,
American International University, West Africa, The Gambia
E-mail: w.olanipekun@aiu.edu.gm
Phone: +2207026523

Abstract

This study uses phenomenological approach to examine the link among communication technology, cyber security and sustainable development. The phenomenological approach provides a philosophical and introductory background on the relationship that exists among the concepts. The review of literature through desk research further provides insights on various definitions of conceptualization of cyber security and sustainable development. Automation of processes based on the cooperation of interconnected devices using Internet results in the enhanced exposure to cyber threats that can become the greatest drag chain to ICT's development. Hence, cyber security should be perceived as the indispensable element and should lie at the roots of the ongoing Green Technological Revolution. The study concludes that cyber security, data regulation and sustainability are very germane to the digital transformation processes in the coming years. Hence, the need for improved cybersecurity strategies, policies, and programs are strongly recommended.

Keywords: Cyber security, Globalization, Internet, Sustainable Development, Technology

Introduction

Organizations and business entities are heavily reliant on ICT systems, networks and the Internet for e-business and e-commerce. Companies rely on reliable information for strategic and operational decision making, to improve productivity, and to maintain their competitiveness in the volatile and dynamic cyber world (International Telecommunication Union, 2019). As a result, computers, information systems, and networks that create, process, store and transact information electronically have become important assets of organizations. Impressive leverages of information and communication technologies (ICT) allow efficient exchanges of data, streamlining of operations, virtualization of numerous products and services, and the adoption of diverse electronic payment methods (Vasiu, & Vasiu, 2015).

Citation: Olanipekun, W.D. (2022). Investigating the Link between Cyber Security and Sustainable Development: A Conceptual Analysis. SMART-IEEE-ACity-ICTU-CRACC-ICTU-Foundations Series

One of the most notable risks concerns cybersecurity, which can take numerous forms and can have very significant negative consequences for the victims. This reality makes cybersecurity a major differentiator for organizations and an essential sustainable economic development factor (Vasiu & Vasiu, 2018). The Internet plays an important role in the economic, political, cultural, and social developments of nations. The immense benefits that Internet has on health, education, financial services and agriculture are well documented both in developed and developing countries (Evans, 2011; Internet Society, 2016; Marcus & Wong, 2016). The Internet and related technologies are the foundation of the digital economy (OECD, 2017). The Internet and ICTs have become a "critical national resource for governments, a vital part of national infrastructures, and a key driver of socio-economic growth and development" (Klimburg, 2012).

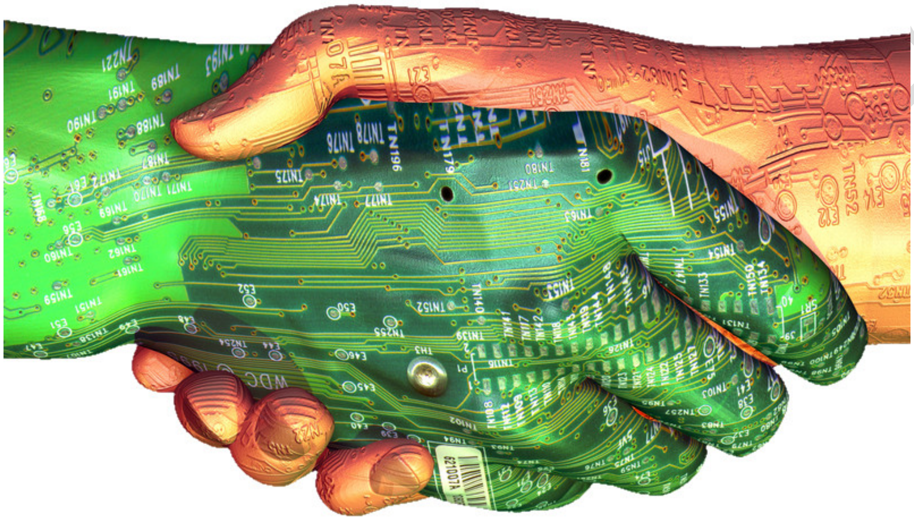

Fig 1: Cyber Security & Sustainable Development Handshake
Source: https://www.linkedin.com/pulse/cybersecurity-sustainable-development-massimiliano-passalacqua

With increasing dependency on information systems, networks, and the Internet; securing and protecting cyberspace from malicious attackers and cyber criminals is a serious concern. While the Internet has transformed all aspects of governments, businesses, and societies; the increasing dependency, has heightened the importance of cybersecurity. The high level of inter-connectivity, which characterizes modern society and the international trade, has opened many avenues for cyber attacks, rendering cybersecurity an issue of major concern for all organizations (Baesens *et al*., 2014; Günther, 2017; World Economic Forum, 2018).Through advanced tools, tactics and procedures (TTP), such as SQL injection; malware infection; advertisement click fraud; business e-mail compromise (BEC); and exploitation of zero-day vulnerabilities, used in watering hole attacks, cyber criminals pose major threats to organizations and citizens

Computer data is essential for the proper functioning of organizations. Successful damage or impairment attacks can negatively impact the integrity and availability of data and/or information systems. Whether in the form of impairment, sabotage, subversion, or intrusion, these attacks can inflict direct and proximate harm on a significant scale. This fact is reflected in a recent survey of business continuity professionals from 80 countries, which identified "cyber attacks" as the fourth most significant cause of business disruption, while "data breach" was ranked the ninth most important source of disruption (Business Continuity Institute, 2017).

The proliferation of Information and Communication Technology (ICT) in Sub-Saharan Africa has brought with it tremendous positive changes in socio-economic growth and development within the region. Paradoxically, ICT has also evolved to become a sophisticated tool in the hand of criminal for perpetrating different forms of cyber crime. (Longe, Ngwa, Wada, Mbarika & Kvasny, 2009). Cyber security concerns the "technologies, processes, and policies that help to prevent and/or reduce the negative impact of events in cyberspace that can happen as the result of deliberate actions against information technology by a hostile or malevolent actor" (Clark, Berson, & Lin, 2014).

Literature Review

Conceptual Clarifications

Cyber security and its Implications

Lewis (2006) defined cyber security as the process of safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption. Craigen *et al.,* (2014) opined that cyber security Organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights. It is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets."(ITU, 2009).

It relates to measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means. Information and communication technology, though an indispensable tool for national development can portend very great danger if not well managed (Longe & Chiemeke, 2008). The responsibility of preventing and resolving technological crimes against victims is not merely a federal or local government issue. Events and trends has shown that it is a global responsibility as cyber crime is a borderless crime. Unintended issues such as e-mail scam, identity theft, child pornography, organized crime and solicitation for prostitution are some of the vices that have become recurring indices on the internet

The cyberspace is a complex virtual environment, which is globally distributed and dynamic in nature, the understanding and perspective of cyberspace and cybersecurity varies. The cases of cybersecurity and cybercrime are increasing, but at the same time evolving and are becoming more complex, sophisticated, and resilient. Both developed and developing countries are facing cybersecurity challenges ranging from managing cybersecurity risks to information resources to building cybersecurity awareness to creating an incident response capability team

The causes of cybersecurity incidents are numerous, multifaceted, and, often, intricated. Successful cyber attacks are usually the result of various problems, such as software vulnerabilities, poor authentication, exploitation of trust mechanisms, insufficient awareness of cybersecurity risks, or administrative errors. The most obvious results of cybersecurity incidents are financial losses, however, cyber incidents can also result in costly recovery or remediation and, in certain cases, litigation; serious harm to consumers' privacy, resulting in potential fines, imposed on the basis of regulations,

In 2010, the United Nations' Group of Governmental Experts (UN GGE) recognized cyber capacity building as being of "vital importance to achieve success in ensuring global ICT security, to assist developing countries in their efforts to enhance the security of their critical national information infrastructure, and to bridge the current divide in ICT security" (United Nations 2010). The ability to manage the cybersecurity risk is essential for organizations' success. In order to effectively be part of the solution to cyber risks, it is imperative that organizations make extensive vulnerability or weakness analysis mandatory (Savaglia & Wang, 2017).

Sustainable Development

The transformation of the society and the world’s economy on a sustainable basis is one of the most significant challenges in the 21st century. The sustainability agenda today not only poses challenges, but also opens up significant innovation opportunities, such as new or more sustainable products and services; new or more sustainable processes; new extended markets built on exploiting a growing concern with sustainability issues; and new business models reframing existing arrangements to emphasise sustainability (World Bank, 2019)

Sustainable development has been a focus of international public policy since the Earth Summit in 1992. It identifies three core objectives for human development – economic growth, social inclusion and environmental sustainability (United Nations, 2019). Only by pursuing these together can the world achieve ‘development that meets the needs of the present without compromising the ability of future generations to meet their own needs. In September 2015, the UN summit placed Sustainable Development Goals (SDGs) at the heart of its Post-2015 Development Agenda, which will guide development until 2030 (United Nations, 2015). Sustainable Development is a multi-disciplinary process that involves all issues such as science, innovation, technology, research and development, information technology and e-commerce, economic development, health, FDI and MNCs, international debt and aid, trade, politics, war, natural disasters, population growth, terrorism, etc

When technology is used for good in addressing sustainable development goals, fundamental human rights are adhered to. In the context of technology, we can discuss privacy, data rights and cybersecurity as three areas that are integral in maintaining the freedom and dignity of the individual (Choejey, 2020). It is a holistic mechanism, that provides a means for realizing all the Sustainable Development Goals (SDG) set out by the United Nations (UN). However, technology is often hindered by external factors in facilitation and transference. On the one hand, technology is an enabler if used appropriately, and on the other hand, it may well be perceived as an oppressive instrument if used subversively to topple human rights (Bronitt & Michael, 2012).

Empirical Review

Catota, Morgan and Sicker (2018) conducted a study on Cybersecurity education in a developing nation: the Ecuadorian environment. Based on qualitative analysis of data from 28 semi-structured interviews with educational leaders from thirteen Ecuadorian institutions of higher education, this article explores challenges faced by the higher educational system of Ecuador in advancing cybersecurity education. On the basis of the insights gained, opportunities for enhancing the system are then identified and discussed. Today cybersecurity education is mostly elementary in Ecuador. Nationwide, interviewees at only four of the thirteen universities studied expressed some confidence in their institution’s ability to provide students with reasonable preparation. The challenges that domestic cybersecurity education faces includes cybersecurity skills, structural capabilities, social integration, economic resources, and governance capacity.

Vasiu and Vasiu (2018) conducted a study on Cybersecurity as an Essential Sustainable Economic Development Factor. The paper employed an empirically-informed theoretical approach, and, based on a large corpus of data, consisting essentially of cases brought to courts, cybersecurity reports, and press releases, examines the main cybersecurity risks, grouped in three broad categories: damage, theft of trade secrets, and payment fraud. In each category, the main issues are illustrated with real case examples. The findings of this study underline the need for improved cybersecurity strategies, policies, and programs. The paper proposes a number of measures that must be taken, in order to provide conditions for a safer and better economic development environment.

Michael, Kobran, Abbas and Hamdoun (2019) conducted a study on Privacy, Data Rights and Cybersecurity Technology for Good in the Achievement of Sustainable Development Goals. The researchers opined that when technology is used for good in addressing sustainable development goals, fundamental human rights are adhered to. In a rush to bring developing nations on par with developed nations, the rapid deployment of technology is often seen as the answer to the achievement of all 17 sustainable development goals. The paper emphasized the need for three ethical elements- privacy, data rights and cybersecurity- in the deployment of new technologies and provides examples throughout history that demonstrate positive or negative applications of technology.

Onyango and Ondiek (2021) conducted a study on Digitalization and Integration of Sustainable Development Goals (SGDs) in Public Organizations in Kenya. This study mapped the role of ICT, digital platforms, the internet connectivity and skills of the personnel vis-à-vis implementation processes of SDGs in public organizations in Kenya. Findings show cross-cutting institutionalization and internalization deficits as a result of limited mastery of ICT skills and training of the personnel, insufficient ICT platforms, mainly, computers, poor internet connectivity and poor investment in digital platforms by the government institutions. An organizational culture that predisposes institutions to change resistance also constrained integration of SDG goals in public organizations. The article concludes by providing critical policy recommendations for addressing these problems.

Annarelli and Palombi, (2021) conducted a study on Digitalization Capabilities for Sustainable Cyber Resilience: A Conceptual Framework. Sustainability. The research article provides a literature analysis on approaches and models for cyber resilience, digitalization capabilities, and a conceptual framework showing how digitalization capabilities drive cyber resilience. Digitalization capabilities are involved in the plan/prepare phase and in the adaptation phase of the cyber resilience process. In particular, the researchers opined that online informational capabilities can drive both these phases. Other capabilities such as the employment of heterogeneous resources and the promotion of continuous learning drive the plan/prepare phase, while the scanning of the evolution of the digital environment and a timely reconfiguration of resources drive the adaptation phase.

Adam, Małgorzata, Agnieszka, Jarosław and Tomasz, (2021) conducted a study on Cybersecurity and Sustainable Development. Hence, the aim of the article was to provide a theoretical discussion and research on the relationships between cybersecurity and sustainable development in the inter-organizational networks. Therefore, the article is an attempt to give an answer to the question about the current state of the implementation of cybersecurity in relation to the EGSS part of the economy in different EU countries. Growing interdependencies between organizations lead them towards the creation of inter-organizational networks where cybersecurity and sustainable development have become one of the most important issues.

The Environmental Goods and Services Sector (EGSS) is one of the fastest developing sectors of economy fueled by the growing relationships between network entities based on the ICT usage. In this sector the Green Cybersecurity is an emerging issue because it secures processes related directly and indirectly to the environmental management and protection. In the future the multidimensional development of the EGSS can help European Union to overcome the upcoming crises. At the same time computer technologies and cybersecurity can contribute to the implementation of the concept of sustainable development.

Conclusion and Recommendations

Recent developments in frontier technologies, including artificial intelligence, robotics and biotechnology, have shown tremendous potential for sustainable development. Technological progress is essential for sustainable development, but can also perpetuate inequalities or create new ones, either by limiting access to more privileged groups and affluent countries, or through built-in biases or unintended consequences. The task for governments is thus to maximise the potential benefits, while mitigating harmful outcomes, and ensuring universal access.

The conceptual exposition above reveals that there is connection between the technology, cybersecurity and sustainable development. Automation of processes based on the cooperation of interconnected devices using Internet results in the enhanced exposure to cyber threats that can become the greatest drag chain to ICT's development. Hence, cyber security should be perceived as the indispensable element and should lie at the roots of the ongoing Green Technological Revolution. It should also be emphasized that cyber attacks are evolving and that is why it is so important to have measures (legal, regulatory and organizational) to control cyber security. In the era of the development of new techniques and technologies, it should be noted that for investors, first of all, security is essential. The development of information and communication technologies has, in practice, transformed every aspect of our lives today. Cybersecurity, data regulation and sustainability are very germane to the digital transformation processes in the coming years

The importance of ICTs and the Internet to development cannot be over emphasized. That value has grown with time because of rapid improvements in technology, increased bandwidth, and new services like social media and cloud computing. It will continue to grow dynamically as ICTs' capabilities and reach extend further during the implementation period for the SDGs. The Internet provides the underpinning platform for the growth of ICTs and for an emerging digital economy, in which production, distribution and consumption depend on broadband networks and services. It will, therefore, be a critical enabler of sustainable development. Governments, business, civil society and individuals have adopted them extensively.

Mobile telephony, Internet access and social media have transformed communications opportunities for individuals, while governments and businesses increasingly rely on the Internet for communications and administration, delivering services and disseminating information. More attention must therefore be paid to the relationship between the Internet and sustainable development to ensure that potential gains are maximized. All stakeholders share responsibility to work together to develop policies, services, tools and applications that will bring the benefits of Internet access and use to everyone, improving access to health and education, spreading information and knowledge, enabling innovation and enterprise, and thereby promoting economic growth, social inclusion and environmental sustainability.

References

1. Adam, S., Małgorzata, R., Agnieszka, K., Jarosław, J., & Tomasz, Z. (2021). Cybersecurity and Sustainable Development. 25th International Conference on Knowledge-Based and Intelligent Information & Engineering Published by Elsevier B.V
2. Annarelli, A.; & Palombi, G. (2021). Digitalization Capabilities for Sustainable Cyber Resilience: A Conceptual Framework. Sustainability 13, 13065. https://doi.org/ 10.3390/su132313065
3. Baesens, B., Bapna, R., Marsden, J.R., Vanthienen, J., & Zhao, J.L. (2014). Transformational issues of big data and analytics in networked business. MIS Quarterly, 38 (2), 629–632. Bharadwaj
4. Bronitt, S. & Michael, K. (2012). Human Rights, Regulation, and National Security, *IEEE Technology and Society Magazine,* vol. 31, no. 1, pp. 15-16, 2012
5. Business Continuity Institute (2017). Horizon Scan Report 2017.
6. Catota, F., Morgan, M. &Sicker, D (2018). Cybersecurity education in a developing nation: the Ecuadorian environment. *Journal of Cybersecurity*, 2019, 1–19 doi: 10.1093/cybsec/tyz001
7. Choejey, P., (2020).Cybersecurity Challenges and Practices: A Case Study of Bhutan. School of Engineering and Information Technology. Murdoch University, Perth, Western Australia
8. Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. Technology *Innovation Management Review*, 4(10).
9. Evans, D. (2011). The internet of things: How the next evolution of the internet is changing everything. CISCO white paper, 1.
10. Günther, W.A. (2017). Debating big data: A literature review on realizing value from big data. Journal of Strategic Information Systems, 26, 191–209.
11. Hilty, L.M., & Hercheui, M.D. (2010). ICT and sustainable development. In What kind of information society? Governance, virtuality, surveillance, sustainability, resilience (pp. 227-235). Springer, Berlin, Heidelberg
12. Internet Society. (2016). Global Internet Report. Retrieved from https://www.internetsociety.org/globalinternetreport/2016/wpcontent/uploads/2016/11/IS OC_GIR_2016-v1.pdf
13. ITU. (2019). Global Cybersecurity Index. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/globalcybersecurity-index.aspx
14. International Telecommunication Union. (2007) ITU Cybersecurity Work Programme to Assist Developing Countries, 2007. Geneva, Switzerland: International Telecommunication Union.
15. Klimburg, A. (2012). National cyber security framework manual: NATO Cooperative Cyber Defense Center of Excellence.
16. Lewis, J. A. (2006). Cybersecurity and critical infrastructure protection. Center for Strategic and International Studies (Washington, DC).
17. Longe, O., Ngwa, O., Wada, F., Mbarika, V Kvasny, L. (2009). Criminal Uses of Information & Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspective. *Journal of Information Technology Impact* 9(3):155-172,
18. Longe, O. B., & Chiemeke, S. C. (2007). Information and communication technology penetration in Nigeria: Prospects, challenges and metrics. *Asian Journal of Information Technology*, 6(3), 280–287.
19. Marcus, A., & Wong, A. (2016). Internet for All: A Framework for Accelerating Internet Access and Adoption. Paper presented at the WORLD ECONOMIC FORUM.
20. Michael, K., Kobran, S., Abbas, R., Hamdoun, S. (2019). Privacy, Data Rights and Cybersecurity Technology for Good in the Achievement of Sustainable Development Goals. 2019 IEEE International Symposium on Technology in Society (ISTAS) Proceedings Miriam Cunningham and Paul Cunningham (Eds)

21. OECD/WTO (2017). Aid for Trade at a Glance 2017: Promoting Trade, Inclusiveness and Connectivity for Sustainable Development, WTO, Geneva/OECD Publishing, Paris.
22. Onyango, G. & Ondiek, J. (2021). Digitalization and Integration of Sustainable Development Goals (SGDs) in Public Organizations in Kenya
23. Savaglia, J. & Wang, P. (2017). Cybersecurity vulnerability analysis via virtualization. Issues in Information Systems 18(4), 91-98.
24. United Nations. (2019). Sustainable Development Goals: Knowledge Platform - Technology. Available: https://sustainabledevelopment.un.org/topics/technology
25. U.N. General Assembly (2015). Transforming our world: the 2030 Agenda for Sustainable Development, A/RES/70/1.
26. Vasiu, I. & Vasiu, L. (2018). Cybersecurity as an Essential Sustainable Economic Development Factor. European Journal of Sustainable Development (2018), 7, 4, 171-178
27. Vasiu, I. & Vasiu, L. (2015). Riders on the Storm: An Analysis of Credit Card Fraud Cases. Suffolk Journal of Trial & Appellate Advocacy, 20, 185-218.
28. World Economic Forum (2018). The Global Risks Report 2018. Retrieved from http://www3.weforum.org/docs/WEF_GRR18_Report.pdf.
29. World Bank (2019) Global cybersecurity capacity program – lessons learned and recommendations towards strengthening the program. The World Bank, Washington, DC