INTERNET OF THINGS, 5G AND CYBER SECURITY: IMPLICATIONS FOR NIGERIA

Chikwendu. Stephen Chilaka
Department of Sociology/Anthropology
Nnamdi Azikiwe University, Awka
E-mail: sc.chikwendu@unizik.ng

Emerho. Godstime Emerson
Department of Sociology/Anthropology
Nnamdi Azikiwe University, Awka
E-mail: godstimeemerho@gmail.com

Abstract
This paper examines cyber security issues associated with the development of the Internet of Things (IoT) and the Fifth Generation (5G) wireless technology in Nigeria. Internet of Things refers to a network comprised of physical objects capable of gathering and sharing electronic information while 5G is the wireless technology developed to speed up this process. The Internet of Things is becoming part of daily life activities with an unpredictable speed and unintended risks. The peculiar risks associated with IoT includes the possibility of unauthorized hands like cyber criminals getting hold of items like cars, electronic appliances, power stations and security systems, amongst others and using them to their advantage and against the people. This study looked at IoT, 5G and their capacities for increased cyber security concerns for Nigeria despite the advantages. The risk society theory was adopted as the theoretical orientation for the study. The study found that the risks associated with IoT and 5G as it concerns cyber security are far-reaching. It is recommended that regulations targeted at mitigating the cyber security issues that will continue to arise from IoT as it evolves should be put in place. Also, the rigidity inherent in changing or amending laws in Nigeria should be revisited particularly as it concerns IoT and cyber security

Key Words: *Internet of things, 5G, cyber security, risk society, crime*

Introduction

The Internet of Things (IoT) refers to a network comprised of physical objects capable of gathering and sharing electronic information. The Internet of Things includes a wide variety of smart devices from industrial machines that transmit data about the production process to sensors that track information about the human body (Kenton, 2020). These devices use Internet Protocol (IP), the same protocol that identifies computers over the web and allows them to communicate with one another. The goal behind the Internet of Things is to have devices that self-report in real-time, improving efficiency and bringing important information to the surface more quickly than a system depending on human

intervention. Again, the desire to have physical objects functioning way beyond human capacity informed the development of the IOT technology (Kenton, 2020).

The term Internet of Things is a relatively new concept. But the actual idea of connected devices had been around longer at least since the 1970s. Back then, the idea was often called embedded internet or pervasive computing. But the actual term, Internet of Things was coined by Kevin Ashton in 1999 (Foote, 2016). The Internet of Things consists of any device with an on/off switch connected to the internet. This includes almost anything you can think of, ranging from phones to power plants to the jet engine of an airplane. Medical devices such as heart monitor implant can transfer data over a network and are members of the ever expanding IoT family. If it has an off/on switch, then it can theoretically be part of the system. The IoT consists of a gigantic network of internet connected things and devices.

The connected things and devices require internet speed to effectively and efficiently process information. This has given rise to the development of the fifth generation of wireless technology. Fifth-generation wireless (5G) is the latest iteration of cellular technology engineered to greatly increase the speed and responsiveness of wireless networks. With 5G, data transmitted over wireless broadband connections can travel at multigigabit speeds with potential peak speeds as high as 20 gigabits per second (Gbps) by some estimates. These speeds exceed wire line network speeds and offer latency of 1 millisecond (ms) or lower for uses that require real-time feedback. 5G will also enable a sharp increase in the amount of data transmitted over wireless systems due to more available bandwidth and advanced antenna technology (Rouse, 2015).

From the forgoing, it is clear that fast-tracking of the development of the 5G technology is centered on enhancing efficiency of the IoT technology but this has come with a myriad of cyber security concerns for countries. For instance, the volume of cyber-attacks on UK businesses have increased by over 240%, with IoT devices and file sharing services being the most frequently targeted applications (Borgia, 2014). Cyber attacks on IoT devices are booming, as even though more and more people and organizations are purchasing smart (network-connected and interactive) devices such as routers or DVR security cameras, not everybody considers them worth protecting. Cybercriminals however, are seeing more and more financial opportunities in exploiting such gadgets. They use networks of infected smart devices to conduct attacks or as proxy for other types of malicious actions (Vladimir, Mikhali, Yaroslav, Denis & Igor 2017). The paper takes a more detailed look at these issues as they affect Nigeria.

Understanding Internet of things

The IoT device is a hardware component that allows the entity (psychical object) to be a part of the digital world. It is also referred to as a smart thing which can be a home appliance, healthcare device, vehicle, building, factory and almost anything networked and fitted with sensors providing information about the physical environment (e.g., temperature, humidity, presence detectors and pollution), actuators (e.g., light switches, displays, motor-assisted shutters or any other action that a device can perform) and embedded computers (Strassmann, 2009). An IoT device is capable of communicating with other IoT devices and ICT systems. These devices communicate via different means including the developing 5G technology.

IoT device classification depends on size, i.e., small or normal; mobility, i.e., mobile or fixed; external or internal power source; whether they are connected intermittently or always-on; automated or non-automated; logical or physical objects; and lastly, whether they are IP-enabled objects or non IP objects. The characteristics of IoT devices are their ability to actuate and/or sense the capability of limiting power/energy, connection to the physical world, intermittent connectivity and mobility (Thoma, Meyer, Sperner, Meissner & Braun, 2012). Some must be fast and reliable and provide credible security and privacy while others might not. A number of these devices have physical protection whereas others are unattended. In fact, in IoT environments, devices should be protected against any threats that can affect their functionality. However, most IoT devices are vulnerable to external and internal attacks due to their characteristics (Hongsong, Zhongchuan & Dongyan, 2011). A typical example of how IoT can be manipulated or compromised to endanger the lives of users is the story of how the prescriptions of a patient were altered through a compromise of the device he was being attended to with. According to the Indian Express (2002), an underworld Don in a hospital was to undergo a minor surgery. his rival went ahead to hire a computer expert who altered his prescriptions through hacking the hospital's computer system. He was administered the altered prescription by an innocent nurse, this resulted in the death of the patient. It is challenging to implement and use a strong security mechanism due to resource constraints in terms of IoT computational capabilities, memory and battery power (Mayer, 2009).

IoT services facilitate the easy integration of IoT entities into the Service-Oriented Architecture (SOA) world as well as service science. An IoT service is a transaction between two parties, the service provider and service consumer. It causes a prescribed function, enabling interaction with the physical world by measuring the state of entities or by initiating actions that will initiate a change to the entities. A service provides a well-defined and standardized interface offering all necessary functionalities for interacting with entities and related processes.

In no distant time, every segment of our daily lives will be centered on IoT. Infact, it is projected that by 2025, there will be an estimated 75 billion internet connected devices globally. While most countries are stepping up to the cyber security challenges that will emanate from this, Nigeria appears to be lagging behind. The cyber-security architecture in the country seems to be extremely vulnerable to attackers, coupled with inadequate laws and regulations (Strassmann, 2009).

Theoretical Orientation

The risk society theory forms the theoretical orientation for this paper. The risk society theory is a critical theory of modernization firmly focused on the manner in which modern society organizes in response to risk. It is closely associated with sociologist, Ulrick Beck. The concept of risk society was coined in the 1980s and became popularized in the 1990s as a consequence of its links in thinking about wider modernity, in particular the growing environmental concerns during the period (Beck, 1992). The theory is premised on the existence of less obvious and frequently unanticipated risks. According to Egbue (2015), risk is not the same as catastrophe but the anticipation of the future catastrophe in the present. As a result, risk leads a dubious, insidious, would-be, fictitious elusive existence. In this sense, risk is present and absent, existent and non-existent, doubtful and real. Efe (2005) popularized the concept of manufactured risk. Manufactured risks according to him, are man-made risks. They are marked by a high level of human agency involved in both producing and mitigating such risks.

Internet of Things and 5G are technological innovations designed to make human activity easier, less cumbersome and more efficient. But this comes with a cost; the risks. Internet of Things and 5G are manufactured or man-made risks as they continue to raise cyber security concerns that affect every segment of the society. The financial institutions, hospitals, homes, schools and even religious organizations are faced with the inevitable reality of adapting to the usage of IoT devices powered by the very powerful 5th Generation network. As the risk society theory holds, there are less obvious and frequently unanticipated risks in human actions and even inactions. However, as time progresses, these risks will begin to show up in different ways. The developers of the Internet of Things and 5G technology (expected to give a boost to the IoT and its operations) did not entirely envisage the numerous security concerns associated with their innovations. The risk of cyber security issues like the shutting down of IoT compliant power stations which could put a whole country in blackouts or the alteration of the functioning of medical machines likely may not have been entirely envisaged.

The modern society is a risky society. With technology controlling every part of our life, the risks become more and more unavoidable. Mobile phones, footwears, wristwatches, cars, everything one can think of are now being controlled by the IoT technology. With a

very weak cyber security architecture, Nigerians are exposed to bigger risks than their counterparts in countries with strong cyber security framework. Whether one is rich or poor is not particularly important as far as risks are concerned. Risks abound everywhere with varying degree and magnitude. Years before the advent of IoT and the 5G technology, such risks were not visible. Indeed, Beck envisaged the unending risks in the modern society especially as man continues to attempt to explore his world further.

Currently, there is a concerted effort by developers to introduce the 5G technology that promises what some have refered to as speed of light capacity in data transmission. While advantageous, the technology will only enhance the activities of fraudsters and further compound the cyber security concerns of people. This is because the speed at which criminals will operate over the internet will be doubled. With an approximately 75 billion connected devices on the IoT technology in 2025, manufactured risks will continue to rise and there is no abating in sight.

The risk society theory has been criticized by Conrad (2013) for its inability to present itself as realist or constructionist as Beck never substantiated on whether the world has become riskier or that risk merely intervenes between really existing risks and our response to them.

Cyber Security and Internet of Things in Nigeria

Ndubueze (2017) observes that cyber-related threats are increasingly becoming ubiquitous in this tech-driven age. Makeri (2017) agrees that prior to the year 2001, the phenomenon of cyber-crime was not globally associated with Nigeria. This resonates with the fact that in Nigeria, we came into realization of the full potential of the internet right about that time. Since then, however, the country has acquired a world-wide notoriety in criminal activities especially financial scams facilitated through the use of the internet.

Nigerian cyber criminals are daily devising new ways of perpetrating this form of crime and the existing methods of tracking these criminals are no longer suitable to deal with their new tricks. The victims as well show increasing naivety and gullibility at the prospects incited by these fraudsters. While the advancement in IoT will expose victims to more vicious attacks, it will most likely open up new vistas for cyber criminals as they will go on to exploit the loopholes in IoT devices and cyber security regulations in Nigeria.

Cyber security 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 (Makeri, 2017). Cyber security strives to ensure the attainment and maintenance of

the security properties of the organization and user's assets against relevant security risks in the cyber environment.

Without equivocation, IoT technology will increase the cyber-security issues in Nigeria for three reasons. One is that the technology is relatively new and hence will require time to learn and understand both by users and regulators. The issue of speed in law making and regulations is another factor. In Nigeria, law making is expected to pass through several stages, each stage comes with its own unique bottlenecks that delay the final passage of the law. In some other countries like the USA and UK, law making is swift and precautionary. However, lawmaking in Nigeria seems to be more reactive than precautionary and when it is precautionary, it sometimes seems to be incomprehensive or inefficient to tackle the marauding cyber-security issues. This is closely followed by the lack of finance that is required to invest in cyber-security in the country. Cyber security involves a lot of high-end calibrations which costs a lot of money to establish and maintain. It is the responsibility of both users and government to purchase security features that will ensure that IoT devices are reasonably safe and secure from attackers. But the reality remains that Nigerians seem to see no need to invest money in cyber security thereby leaving their devices open for attack. On the other hand, government has been foot-dragging in making funds available to focus on protecting IoT devices (Makeri, 2017).

Evidently, IoT devices will become part of everyday life in Nigeria and will present peculiar cyber security challenges. There is little being done to hammer on this impending reality despite its implications for government and individuals in the country. From possible manipulations of IoT devices in the media sector to the possibility of cyber criminals taking over the control of household IoT-enabled devices in the homes, the risks associated with IoT and cyber security in Nigeria will overwhelm the nation if concrete measures are not taken to mitigate same (Zorzi, Gluhak, Lange & Bassi, 2010)

Conclusion

Unintended consequences are the outcomes of a purposeful action that are not intended or foreseen as explained by Robert Merton, a popular American Sociologist. While cyber security concerns have been around for several decades with the invention of the computers and internet, there is an urgent need to begin to do things differently in tackling cyber criminality due to the emerging usefulness of the internet. More precisely, the Internet of Things and 5G network will have the lives of everyone firmly controlled by the IoT technology. The reality is that, as the IoT technology continues to emerge, there is little possibility that anyone can avoid using any of the IoT devices. In essence, cyber security will now affect even rural dwellers and poor people as much as it affects those in the cities and the rich.

Efe (2005) amplified the issue of manufactured risks as mentioned earlier. What this means is that the society has manufactured risks for itself though unintended. The advantages of the advancement in technology cannot be overemphasized so also can the risks not be downplayed.

Recommendations

There is a lot that could be done to better mitigate the cyber security challenges associated with the Internet of Things and the 5G technology.

1. The Nigerian Cyber Security law is not comprehensive enough and does not cover the peculiarities of the IoT technology. This has to be immediately reviewed by the lawmakers. Again, the long process involved in law making could hamper proactive measures that could reduce cyber security attacks in the context of IoT technology. Criminals are swift and smart, lawmaking should be swifter and smarter.
2. There is need to see the cyber space as one that must be adequately secured. If this is not done, the IoT technology will be counterproductive in Nigeria as the security concerns that will emanate from it will be too disastrous. One can only imagine the fatalities that hacked moving cars, home appliances and office equipment will have on the people. The government is therefore expected to prioritize funding for security fortification of the cyber space in the country.
3. Members of the public should take responsibility by also spending money in securing their devices because the cost of salvaging a situation is usually higher than the cost of preventing same. Cyber security issues could be prevented or minimized if people follow security measures as stipulated on the devices they use.
4. Finally, this paper is not exhaustive. There is need for increased studies on the security implications of IoT and 5G in developing countries like Nigeria. Doing so will place such countries on the right pedestal to tackle emerging cyber security concerns.

References

Beck, U. (1992). *Risk Society: Towards a New Modernity*. New Delhi: Sage

Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications*, 54, pp.1-31.

Egbue, N.G. (2015). Poverty Dimensions of Environmental Exploitation and Degradation: Implications for Poverty Reduction and Sustainable Development in Nigeria. In: *Development issues in Nigerian Society*. Enugu: Oktek Nig. Ltd.

Foote, K. D. (2016). A brief history of the internet of things https://www.dataversity.net/brief-history-internet-things/#.Accessed 20th May, 2020

Hongsong, C., Zhongchuan, F. & Dongyan, Z (2011). Security and trust research in m2m system,". In: *Vehicular Electronics and Safety* (ICVES). IEEE International Conference on. IEEE, 2011, pp. 286–290.

Kenton, W. (2020). *The Internet of Things.* https://www.investopedia.com/terms/i/internet-things.asp. Accessed 20th May, 2020.

Koien, G. M. & Oleshchuk, V. A. (2011). *Aspects of Personal Privacy in Communications Problems, Technology and Solutions.* London: River Publishers.

Makeri, Y. A. (2017). Cyber Security Issues in Nigeria and Challenges. *International Journal of. Advanced Research in Computer Science and. Software,* 3 (439-445).

Mayer, C. P. (2009). Security and privacy challenges in the internet of things. *Electronic Communications of the EAST*, 17(66-79),

Ndubueze, N. P. (2017). *Cyber Criminology and Technology-Assisted Crime Control: A reader.* Kaduna: Ahmadu Bello University Press.

Strassmann, P. A. (2009). *Cyber Security for the Department of Defense,* Accessed May 10, 2020 from http://www.strassmann.com/pubs/dod/cybersecurity-draft-v1.pdf.

Thoma, M., Meyer, S., Sperner, K., Meissner, S. & Braun, T. (2012). On IoT services: Survey, classification and enterprise integration. In: *Green Computing and Communications.* IEEE International Conference on. IEEE, 2012, pp. 257–260.

Zorzi, M., Gluhak, A., Lange, S. & Bassi, A (2010). From today's intranet of things to a future internet of things: A wireless-and mobility-related view. *Wireless Communications, IEEE,* 17 (44–51).