*FUDMA Journal of Sciences (FJS)*
*ISSN online: 2616-1370*
*ISSN print: 2645 - 2944*
*Vol. 8 No. 6, December, 2024, pp 36 - 43*
*DOI: https://doi.org/10.33003/fjs-2024-0806-2906*

# DISRUPTIVE TECHNOLOGIES FOR EDUCATIONAL INNOVATION IN DELTA STATE AND ITS CYBER SECURITY IMPLICATIONS: A POST COVID-19 ASSESSMENT

***[1]Okpako, Abugor Ejaita, [1]Isitor, Nkechi , [2]Ojie, Deborah Voke and [2]Ukadike, Destiny**

[1]Department of Cyber Security, University of Delta, Agbor, Delta State, Nigeria
[2]Department of Software Engineering, University of Delta, Agbor, Delta State, Nigeria

*Corresponding authors' email: ejaita.okpako@unidel.edu.ng

## ABSTRACT

Technology is everywhere and it's changing the way things work, hence it is disruptive depending on its application and context. Disruptive technology introduces new markets and modifies existing ones, providing end users with better access, convenience, empowerment, choice, and value as well as competing with established models and practically transforming products and services. The COVID-19 pandemic necessitated a rapid shift to remote learning and the adoption of disruptive technologies in educational institutions worldwide, including Nigeria. Despite this, there is limited evidence investigating how different disruptive technologies and configurations associate with cyber security within the educational sector. This research work examines the association of disruptive technology and cyber security implications in the Delta State educational system during the post COVID 19 pandemic period. A cross sectional approach was used for data collection through questionnaires where 55 responses out of 80 respondents from some selected schools in Delta State were used. The results confirm some cyber threats on using disruptive technology in e-learning as phishing and identity theft. The respondent's level of online satisfaction, cyber security awareness and performance was significantly associated with various independent variables such as e-learning platforms, online interaction, and privacy concerns. An understanding of these relationships will help educators and other stakeholders to prioritize legislation and regulations that will address such developments. The aim should not to over-regulate and consequently strangle them, but to envisage change, prepare for it, and set up appropriate regulatory frameworks to ensure societal balance.

**Keywords**: Cyber security, Covid 19, Disruptive Technology, Education, E-learning

## INTRODUCTION

The Nigerian society is unfamiliar with the emergence of disruptive technology. Nigerians have experienced some technological disruptions as members of the global community, which have both improved their lives and caused friction between the disrupting technology and the markets. However, these frictions have created emerging market for other products and services. Disruptive technologies embodies technological transitions that create winners and losers while also introducing new forms of interaction that challenge existing social and institutional redistribution mechanisms. These disruptions are seen in almost all fields of human endeavours, from telecommunications, transportation, trade and commerce and more particularly in education

Technology and innovation have continued to shape learning and expanded its frontier within the educational ecosystem. It has enhanced content, delivery quality and depth, as well as the breadth in terms of geographical coverage. For instance, online learning is gaining traction in tertiary institutions worldwide through the introduction of online bookstores and search engines such as Okada Books, Law Pavilion, LegalPedia, and others, traditional bookshops and publishers have seen a decrease in patronage. It is no longer necessary to be physically present in a classroom to be taught. The teacher is also not required to be physically present in order to teach. Virtual knowledge exchange sessions are now possible. The advent of the World Wide Web (www) has created many opportunities. One of such opportunity is electronic learning (e-learning). According to (Timothy etal.,2008),e-learning is the use of electronic technology to deliver education and training applications, monitor learner's performance and report learner's progress. It as an innovative approach for delivering electronically mediated, well-designed, learner-centered and interactive learning environments to anyone, anyplace, anytime by utilizing the internet and digital technologies in concern with instructional design principles. It is all about learning with the use of computers. Information and communication systems, whether networked or not, serve as specific media to implement the learning process. Computing technologies have continued to be gaining traction and applicability in different sectors such as James et al. (2022) developed a hybrid intelligent based information retrieval technique to filter relevant materials for researchers and help them find information over the internet. In medical diagnosis, Akazue et al. (2023) developed a system for prediction of survivability of diabetes mellitus using machine learning

Globally, the novel coronavirus (Covid-19) has undoubtedly made the e-learning revolution more prominent. Krönke (2020) reported that UNESCO puts 1.2 billion students and the youth worldwide at a disadvantage as a result of closure of schools and universities due to Covid-19 pandemic; and in Africa, approaches to adaptations to changes in technology-enhanced learning keep improving, but at a snail's pace. One may assume that this phenomenon would have affected only under-developed and/or developing countries (Daniel et al., 2022). However, Nawaz (2013) stated that it is a global challenge for higher education institutions to effectively implement e-learning solutions. Despite this, Nigeria, a developing nation, was severely affected when the government announced the mass closure of all educational institutions following the outbreak of Covid-19 in March 2020. This made it abundantly clear to key education stakeholders in Nigeria that, regrettably, covid-19 had emerged to disrupt traditional methods, particularly in the area of education.

Disruptive technologies create an entirely new industry or product by displacing conventional technology. Ojoboh &

Okpako (2023) underscore the social media has reinvented how social interactions are carried out and has introduced various forms of modernised and globalized types of communication. However, Ojoboh et al. (2022) also underscore the negative effect of misinformation and disinformation on social media during the covid 19 pandemic. There are five (5) disruptive technologies in education which are online learning (e-Learning), Artificial Intelligence (AI) Guided learning, Chat-Based collaboration, Virtual and Augmented Reality (VR and AR). E-learning is disrupting conventional classroom learning (U-EENI, 2022) as there is no gain saying that Universities rely heavilty on the Internet and Cyberspace to actualize their statutory responsibilities.

Cybercrime has become the world's second-largest man-made risk (Soomro & Hussain, 2019). According to Okpako et al. (2023), the quest for material gains has undermined the essence of societal well-being through misapplication and misuse of the digital landscape for negative endeavours in form of cyber crime. Cybercrimes have had debilitating effects on individuals, governments, organizations, and universities. It has sent many governments, organizations, and individuals into bankruptcy and global shock (De Paoli et al., 2020). Cybercrime has remained a major threat to universities, particularly as it touches that core mandates of teaching, learning, research, community services, and administration and management of staff and student records (Bukhari, 2018). Okpako et al. (2022) opine that crime and criminal activities have been a subjective concept in different parts of Nigeria thereby turning the country into a state of legalized lawlessness there the law is entirely emptied of content.

It is therefore pertinent to have a robust cybersecurity management framework for organizations and educational institutions in Nigeria. It acknowledges the need for actionable knowledge to address cybercrime and related incidents. The Office of the National Security Adviser (NSA) and the National Information and Technology Development Agency (NITDA) in Nigeria, along with Microsoft and the National Institutes of Standards and Technology, recognize the threats and advocate for the implementation of a consolidated cybersecurity framework. While the existing frameworks primarily target sectors like finance, oil and gas, and conglomerates, the statement highlights the significance of developing a specific cybersecurity framework tailored for Nigerian universities. While cybersecurity is essentially the practice of protecting and guarding computers, servers, mobile devices, electronic systems, networks, and data from being compromised by malicious attacks, the practice of cybersecurity is only as effective as how cybersecurity conscious the cyber user is. Thus, awareness and education remain the first line of defense against cybercrimes. One of the major causes for the worldwide increase in internet related crimes and cybersecurity incidents, is the limited security knowledge among cyber users. Cybercriminals take advantage of the ignorance of cyber users to perpetuate their malicious activities and this has been a major challenge to curbing cybercrimes.The rapid adoption of disruptive technologies in the educational sector in Nigeria, particularly in response to the COVID-19 pandemic, has brought about significant changes in teaching and learning. While these technologies offer numerous benefits, they also present cyber security implications that need to be addressed. Some Nigeria's institution have also witnessed the impact on cybercrime activities such as the incidence of Denial of Service (DOS) where an unknown person abused the Network Time Protocol Server in Federal University of Technology, Akure as reported by Mojeed , 2020. In the same vein, Madonna University, a privately owned university also reported that unauthorized individuals accessed and tempered with over 25,000mdata in their database (Egbunike, 2019).

An understanding of cyber security implication of disruptive technologies will help educators and other stakeholders to prioritize legislation and regulations that will address such developments. The goal should not be to stop these disruptions or to over-regulate and thus strangle them, but to anticipate change, prepare for it, and put appropriate regulatory frameworks in place to achieve societal balance.

## MATERIALS AND METHODS

The method and procedure that was applied in this study as arranged as Research design, Population of the study , Sample size, Sampling techniques, Research instrument , Validity of the instrument, Method of data collection and Method of data analysis

### Research Design.

This study uses questionnaires which employ a quantitative approach to learn more about people's knowledge, attitudes, and behaviour around the impact of Covid-19 pandemic on the educational sector in Nigeria and its effectiveness of the e-learning strategy adopted by its various stakeholders and the level of cyber security awareness on cyber users. The descriptive approach was used because it facilitates comprehension of the "what" of the research as well as the assessment, description, and evaluation of the issue being studied.

### Research Population

The population in this research comprises of people from University of Delta (Government), Edwin Clark University (Private), some selected secondary schools (Government and Private) in Delta State, Delta State Polytechnic (Government), Oghara and those who have access to the cyberspace in Delta State. We have total population comprises of 80 students and educators majorly from computer science departments, engineering and accounting.

### Sample size

The target sample size used for this study was 80. However, only 55 responses were recovered which is sufficient and adequate for this research as determined using the Krejcie and Morgan Table at a confidence level of 95% and a margin error of 5% (Krejcie and Morgan, 1970). This sample size was to ensure that the population of the study was adequately represented.

### Sampling Techniques

This study used probability sampling, where the specific sampling technique used was simple random sampling. This technique was chosen because each member of the study population has a non-zero chance of participating in the study; every member of the population has an equal chance of being chosen to be examined, judged, and evaluated. This technique also provides an unbiased and better estimate of data analysis for a homogeneous population.

### Research Instrument

The research instrument of this study is a customized self-structured questionnaire. Appropriate questions describing the research goals were formulated in the questionnaires to extract relevant information from the respondents. The questionnaire was designed in a close-ended format to accommodate questions such that the essence of the study can be realized.

The format of the questionnaire was close-ended and divided into sections A through D. Section A was used to gather socio-demographic data about the respondents, and sections B to D used a 4-point Likert scale to gather responses from research participants on their level of the impact of digital technologies on the educational sector, cyber awareness, the precautions they take to prevent cyber security incidents, its implications on educational stakeholders and the influence of ongoing governmental initiatives on cyber security awareness and education.

**Validity of the Instrument**

The research instrument was accessed by expert educationists to determine its appropriateness. The instrument was subjected to both Face and Content validity. Face validity was conducted to evaluate the appearance of the questionnaire in terms of feasibility, readability, consistency of style and formatting, and clarity of language used. Content validity involves detailed and concise examination of the test contents (items in the questionnaire) to determine if they give a good coverage of the domain to be measured. To ensure the reliability of the instrument, the questionnaire was pilot tested with Five (5) participants randomly selected from the sample. They provided clarity and understanding on some items. Their responses were used to refine the instrument before administering to the rest of the sample

**Method of Data Collection**

Survey questionnaires were delivered to respondents in person and online via emails and WhatsApp groups to collect information from respondents on the implication of cyber awareness and education related to cyber security when accessing and using cyberspace. The inclusion of online administration of survey questions allowed the research to cover a broader and more random population sample for the study.

**Method of Data Analysis**

Data collected for this study was analyzed using the SPSS software and the python jupyter notebook respectively. Question and/or statement items used in assessing respondents when answering a particular research question were ranked on a Likert scale as follows:

**Table 1: Likert Scale Rank**

| **Scale** | **Score($x$)** | **Scale** | **Score($x$)** |
|---|---|---|---|
| Not aware | 0 | Strongly disagree | 1 |
| Slightly aware | 1 | Disagree | 2 |
| Very aware | 2 | Agree | 3 |
| Extremely aware | 3 | Strongly agree | 4 |
| **Mean mark** | **1.5** | **Mean mark** | **2.5** |

**RESULTS AND DISCUSSION**

This research work was embarked to assess the level of cyber awareness and education of Nigerians. To facilitate this assessment, survey questions were distributed and administered to a target population of 80 respondents. However, a total of 55 responses were recovered from both distributed questionnaires and online responses. Therefore, the data presentation of the research is based on the number of submitted responses which were analyzed as explained below.

For clarity and understanding, data gathered is presented in a tabular form in frequencies and percentages.

**Table 2: Gender Distribution of Respondents**

| | **Frequency** | **Percentage** |
|---|---|---|
| **Male** | 38 | 69.1 |
| **Female** | 17 | 30.9 |
| Total | **55** | **100.0** |

Source: Primary (Questionnaire). Feb, 2024

Table 2 shows the gender distribution of study respondents. The data gathered reveals that 38 respondents representing 69.1% were males while 17 representing 30.9% were females. Generally, more males participated in the survey compared to their female counterparts.

**Table 3: Age Distribution of Respondents**

| | **Frequency** | **Percentage** |
|---|---|---|
| **16 – 20** | 14 | 25.5 |
| **21 – 25** | 3 | 5.5 |
| **26 – 30** | 21 | 38.2 |
| **31 – 35** | 6 | 10.9 |
| **36 – 40** | 7 | 12.8 |
| **41 – above** | 4 | 7.3 |
| Total | **55** | **100.0** |

Source: Primary (Questionnaire). Feb, 2024

Table 3 shows the age distribution of respondents used for his study. Data collected showed that ages 16 – 20yrs were 14 in number representing 25.5%; 21 – 25yrs were 3 representing 5.5%; 26 – 30yrs were 21 representing 38.2%; 31 – 35yrs were 6 in all representing 10.9%; while 36 – 40yrs and 41yrs – above were 7 and 4 representing 12.8% and 7.3% respectively.

**Table 4: Educational Level of Respondents**

| | Frequency | Percentage |
|---|---|---|
| **Post - graduate** | 16 | 29.1 |
| **Secondary** | 12 | 21.8 |
| **Tertiary** | 27 | 49.1 |
| Total | **55** | **100.0** |

Source: Primary (Questionnaire). Feb, 2024

Table 4 shows the educational level of respondents. Data gathered reveals that most respondents had tertiary education (OND and higher) and were a total of 27 representing 49.1% of the study population. Those with secondary education were 12 representing 21.8%; while 16 (29.1%) are post-graduate.

**Table 5: Designation Status of Respondents**

| | Frequency | Percentage |
|---|---|---|
| **Educator** | 4 | 7.3 |
| **Others** | 4 | 7.3 |
| **Student** | 47 | 85.5 |
| Total | **55** | **100.0** |

Source: Primary (Questionnaire). Feb, 2024

Table 5 shows the designation status of study respondents. Collected data showed that 47 respondents representing 85.5% were students; 4 representing 7.3% were educators; and 4 representing 7.3% of the respondents indicated that they were neither students nor educators.

**Table 6: How Do You Access the Cyberspace?**

| | Frequency | Percentage |
|---|---|---|
| **Laptop** | 25 | 45.5 |
| **Smart Phone** | 30 | 54.5 |
| Total | **55** | **100.0** |

Source: Primary (Questionnaire). Feb, 2024

Table 4.5 presents the different devices respondents use to access the cyberspace. Data shows that 30 respondents representing 54.5% indicated that they use smart phones, while 25 (45.5%) respondents indicated also accessing the cyberspace through the laptop.

**Table 7: What Is Your Preferred Device for Accessing the Cyberspace?**

| | Frequency | Percentage |
|---|---|---|
| **Laptop** | 24 | 43.6 |
| **Smart Phone** | 31 | 56.4 |
| Total | **55** | **100.0** |

Source: Primary (Questionnaire). Feb, 2024

Table 7 above shows respondents' preferred device when accessing the cyberspace. Data gathered reveals that the smart phone is the most preferred device with 31 respondents representing 56.4%. This is followed by the laptop with 24 representing 43.6%. As students and teachers use personal devices for remote learning, it is important to emphasize device security. Encouraging the use of up-to-date antivirus software, strong passwords, and regular software updates can mitigate the risk of malware infections and unauthorized access.

**Table 8: What is your source of e-learning services?**

| | Frequency | Percentage |
|---|---|---|
| **Personal gadgets** | 41 | 74.5 |
| **School lab** | 14 | 25.5 |
| Total | **55** | **100.0** |

Source: Primary (Questionnaire). Feb, 2024

Table 8 above shows respondents' source of e-learning when accessing the cyberspace. Data gathered reveals that personal gadgets are the most preferred with 41 respondents representing 74.5%. This is followed by the school laboratory with 14 representing 25.5%.

**Table 9: What Do You Use The Cyberspace For?**

| | Frequency | Percentage |
|---|---|---|
| **Communication** | 6 | 10.9 |
| **E-learning** | 12 | 21.8 |
| **Online examination** | 3 | 5.5 |
| **Others** | 3 | 5.5 |
| **Research** | 19 | 34.5 |
| **Social media** | 12 | 21.8 |
| Total | **55** | **100.0** |

Source: Primary (Questionnaire). Feb, 2024

Table 9 shows what respondents use the cyberspace for. Collected data shows that 19 (34.5%) representing highest proportion of respondents, spend most of their cyberspace access on research. This is followed by e-learning at 12 representing 21.8% and social media at 12 (21.8%). Six respondents representing 10.9% indicated they also use the cyberspace for communication; 3 (5.5%) for online examination and others respectively.

**Table 10: Relevant materials are delivered electronically?**

| | Frequency | Percentage |
|---|---|---|
| **Most times** | 6 | 10.9 |
| **No** | 14 | 25.5 |
| **Sometimes** | 20 | 36.4 |
| **Yes** | 15 | 27.3 |
| Total | **55** | **100.0** |

Source: Primary (Questionnaire). Feb, 2024

Table 10 shows the rate at which educational materials are delivered online. Collected data shows that 20 (36.4%) representing highest proportion of respondents, confirmed that sometimes materials are uploaded on their online platforms. While 20(36.4%) agreed that sometimes materials are scarcely available, however, 14(25.5%) respondents disagreed that no material is uploaded at all while other respondents 6(10.9%) confirmed that most times materials are readily available. With increased reliance on digital platforms, educational institutions must prioritize data privacy and protection. They need to implement robust security measures to safeguard student and staff data from unauthorized access, breaches, and cyber-attacks (Kronke , 2020).

**Table 11: Virtual platform used by my institution**

| | Frequency | Percentage |
|---|---|---|
| **Google meet** | 6 | 10.9 |
| **Others** | 5 | 9.1 |
| **Website** | 7 | 12.7 |
| **WhatsApp** | 12 | 21.8 |
| **Zoom** | 25 | 45.5 |
| Total | **55** | **100.0** |

Source: Primary (Questionnaire). Feb, 2024

Table 11 represents data for the various online platforms created by the various institutions. Collected data shows that 25 (45.5%) representing highest proportion of respondents used zoom as created by their school. This is followed by WhatsApp at 12 representing 21.8% and google meet at 6 (10.9%).

**Table 12: Awareness of Cybercrime**

| Question Item | Extremely aware (EA) | Very aware (VA) | Slightly aware (SA) | Not aware (NA) | Mean Score | Standard deviation |
|---|---|---|---|---|---|---|
| **To what extent are you aware of the cybercrime?** | 15 (27.3%) | 23 (41.8%) | 17 (30.9%) | - | 1.96 | .769 |
| **To what extent are you aware about phishing?** | 5 (9.1%) | 9 (16.4%) | 17 (30.9%) | 24 (43.6%) | .91 | .986 |
| **To what extent are you aware about cyberbullying?** | 14 (25.5%) | 15 (27.3%) | 13 (23.6%) | 13 (23.6%) | 1.55 | 1.119 |
| **To what extent are you aware of anti-malware or antivirus?** | 13 (23.6%) | 38 (69.1%) | 4 (7.3%) | - | 2.16 | .536 |
| **To what extent are you aware about identity theft?** | 6 (10.9%) | 21 (38.2%) | 11 (20.0%) | 17 (30.9%) | 1.29 | 1.031 |
| **To what extent are you aware that you are a likely cybercrime target?** | 8 (14.5%) | 19 (34.5%) | 18 (32.7%) | 10 (18.2%) | 1.45 | .959 |

Source: Questionnaire, 2024. Frequencies (percentages) of responses are shown in the table

Table 12 shows respondents' awareness of cybercrime. Data depicts majority of the respondents to be very aware of cybercrime (41.8%), cyber bullying (23.7%), malware/viruses (69.1) %, and identity theft (38.2%) and that they are likely cybercrime targets (34.5%) and slightly aware about phishing (30.9%). Respondents generally showed a poor awareness particularly on phishing and identity theft. According to Adanikun et al. (2020) proper training and awareness programs for teachers and staff members are crucial to help them identify potential security risks and follow best practices. This can include training on password hygiene, recognizing phishing attempts, and handling sensitive information securely.

**Table 13: Awareness of Cyber security**

| Question Item | Extremely aware (EA) | Very aware (VA) | Slightly aware (SA) | Not aware (NA) | Mean Score | Standard deviation |
|---|---|---|---|---|---|---|
| **To what extent are you aware of the importance of cybersecurity?** | 9 (16.4%) | 13 (23.6%) | 15 (27.3%) | 18 (32.7%) | 1.24 | 1.088 |
| **To what extent are you aware of the risks with using the cyberspace?** | 15 (27.3%) | 27 (49.1%) | 13 (23.6%) | 0 | 2.04 | .719 |
| **To what extent are you aware of system security updates?** | 13 (23.6%) | 15 (27.3%) | 21 (38.2%) | 6 (10.9%) | 1.64 | .969 |
| **To what extent are you aware of anti-malware or antivirus?** | 22 (40.0%) | 25 (45.5%) | 8 (14.5%) | 0 | 2.25 | .700 |
| **To what extent are you aware of the use of a VPN?** | 6 (16.4%) | 13 (23.6%) | 15 (27.3%) | 18 (32.7%) | 1.24 | 1.088 |

Source: Questionnaire, 2024. Frequencies (percentages) of responses are shown in the table

Table 13 shows the levels of awareness of study respondents on cybersecurity. Across all items used to assess respondents' awareness, most of the respondents were not aware of the importance of cybersecurity (32.7%) and the importance of VPN (32.7%). Respondents representing (38.2%) are slightly aware of system security update, while respondents representing (49.1%) are very aware of risk of with using the cyberspace and anti-malware protection.According to Egbunike (2019) Cybercriminals often exploit vulnerabilities by using phishing emails, deceptive websites, or social engineering techniques to gain unauthorized access. Educating students, teachers, and staff about these threats and implementing security awareness programs is crucial.

**Table 14: Behavioural Measures Taken by Nigerian Cyber-users to Forestall Cyber security Incidents**

| Statement Item | Strongly agree (SA) | Agree (A) | Disagree (D) | Strongly disagree (SD) | Mean score | Standard deviation |
|---|---|---|---|---|---|---|
| **I always perform security updates whenever I see them** | 1 (1.8%) | 22 (40.0%) | 32 (58.2%) | - | 3.56 | .536 |
| **I always perform anti-virus updates whenever I see them** | 31 (56.4%) | 22 (40.0%) | 2 (3.6%) | - | 3.53 | .537 |
| **Changing passwords regularly is necessary** | 4 (7.3%) | 16 (29.1%) | 27 (49.1%) | 8 (14.5%) | 2.29 | .809 |
| **Sharing my password with family and close friends is okay** | 1 (1.8%) | 6 (10.9%) | 28 (50.9%) | 20 (36.4%) | 1.78 | .712 |
| **I download free files from the cyberspace no matter the source** | 1 (1.8%) | 26 (47.3%) | 6 (10.9%) | 22 (40.0%) | 1.75 | .726 |
| **I always use a free Wi-Fi connection when I notice one** | 28 (50.9%) | 20 (36.9%) | 1 (1.8%) | 6 (10.9%) | 1.78 | .712 |

Source: Questionnaire, 2024. Frequencies (percentages) of responses are shown in the table

Table 14 shows behavioural measures taken by Nigerian cyber-users to forestall cybersecurity incidents. Data reveals that a higher percentage of study respondents disagreed that they always perform security updates whenever they see them (58.2%) while31 respondents (56.4%) strongly agreed that they always perform anti-virus updates whenever they see them, however (49.1%) believed that changing passwords regularly is necessary. Respondents disagreed to sharing their password with family and close friends (50.9%); while downloading free files from the cyberspace no matter the source (47.3%) and most respondents strongly agreed they always use a free WI-FI connection when they notice one (50.9%). According to Tabassan & Baker (2020) having an effective incident response plan in place is essential to minimize the impact of cyber-attacks. Regularly backing up data, maintaining off-site backups, and testing the restoration process can help in the event of a security incident.

## CONCLUSION

The introduction of new technologies will result in the formation of a new economy, including the development of new principles and approaches for organizing digital industrial production. When an unprecedented decentralized industrial production system is achieved, it will be possible to create a new "interface" economy based on the use of additive technologies on an industrial scale. And if this occurs, the entire economic system, as well as the social structure of society, will change. Though disruptive technologies have provided opportunities for the educational sector in Nigeria to adapt and continue learning during and after the COVID-19 pandemic, they also bring cyber security risks. Educational institutions must prioritize cyber security measures to protect sensitive data, ensure network and device security, and train staff and students to be vigilant against cyber threats. By adopting a holistic approach to cyber security, the educational

sector in Delta State, and generally in Nigeria can make the most of disruptive technologies while maintaining a secure learning environment. Our study provides empirical evidence addressing the association and patterns between various factors for students and other respondents learning in digital ecosystem. However, for the sake of order, it is critical that legislation and regulations be put in place to address such developments. The goal should not be to stop these disruptions or to over-regulate and thus strangle them, but to anticipate change, prepare for it, and put appropriate regulatory frameworks in place to achieve societal balance. Society will continue to evolve, and we must adapt as well. These new technologies will become 'old' at some point in the future, having been surpassed by newer and/or more advanced ones. That is the circle of life, as every emerging technology has inherent advantages and disadvantages. Additionally, a case study approach could be utilized to identify unique difficulties and advancements of Nigerian education institutions. The research further suggest that this would list the difficulties that a variety of higher education institutions face in order to provide institution-specific solutions that take into account the peculiarities of geographical locations as well as infrastructure issues.

## RECOMMENDATIONS

The influencing factors and impact of innovation vary over time, from one technological ecosystem to the next, and are dependent on chance and self-reinforcing mechanisms. Nonetheless, the arguments for innovation policy are compelling, and we have identified some patterns in technological development that can be used in designing policies. The following are some key technological characteristics that will aid in the management of disruptive technologies at the societal level.

**Dependence on infrastructure**

Each technological revolution is linked to a network of infrastructure. Infrastructure, on the other hand, is mostly local, technologies that depend on infrastructures which will have a more limited impact. Though there is the "digital divide" in broadband access remains significant, disruptive technologies in energy and transportation appears to be infrastructure-intensive compared to digital technologies. Policy intervention is generally difficult to change a technology's reliance on an infrastructure.

**Need for adapting locally**

Certain technologies may not function in the same way everywhere. Technologies used in Agriculture have historically been a chief example, with ploughs, horse breeds, and plant varieties requiring significant adaptation to suit local conditions. Transportation and energy technologies are also included in this category to some extent. Aside from language and cultural factors, digital technologies require little adaptation. In general, the need for adapting locally is unlikely to be a feature of technology that can be policy-influenced.

**The life cycle stage**

when a new technology is disruptive, it means that is a threat to incumbents, and consequently, opens up new opportunities for others. Latecomers must have a reasonable productive capacity, human resources, and a geographic advantage to enter the opportunity. As the industry changes in knowledge and technology, demand, institutions, and public policy, windows of opportunity emerge throughout the life cycle of a technology. Product innovation occurs in a variety of cities before being moved to specialised locations for mass production and process innovation. Threats and opportunities are determined by this spatial life cycle.

**Labour and skill intensity**

Some technologies necessitate a small number of workers or workers with limited qualifications, whereas others necessitate a high level of skill or labour. Many industries are affected by technological upskilling or de-skilling. One of the most difficult challenges for inclusive innovation policy is automation in manufacturing, transportation, and less expected occupations. Regional governments should try to predict not only what jobs will be lost, but also what jobs will be created and whether or not the local labour force will be able to transition.

**Product, processes or services**

Not all disruptive technologies involve physical technological products. Many disruptive technologies can take the form of innovative services with a strong local dimension, such as those being disinter mediated by digital platforms and the "sharing" economy.

**Cities systems**

Through agglomeration economies, cities are increasingly seen as the engine of growth and technological development. Large cities have a higher concentration of managerial and technical professionals, making them less vulnerable to automation. Beyond the size of a region's cities, it is their organisation that is important.

**Population structure and cultural factors**

Entrepreneurship and innovation capabilities differ across regions based on population age structure. Cultural and institutional factors are frequently identified as major drivers of city and regional success.

## REFERENCES

Adanikin, Adeoye, Itunuoluwa Adanikin, Ayobami &Ariyo. (2020). COVID-19 and E-Learning: Nigeria Tertiary Education System Experience. 5. 28-31.

Adesina, R, & Ingirige, B (2019). Dismantling barriers to effective disaster management in Nigeria. 14th International Postraduate research conference 2019: Contemporary and Future Directions in the Built Environment.

Akazue I. Maureen, Geofrey A. Nwokolo, Okpako A. Ejaita, Ogeh Emmanuel Ufiofio(2023). Machine Learning Survival Analysis Model for Diabetes Mellitus. International Journal of Innovative Science and Research Technology. Vol. 8(4).

Bukhari, B. (2018). Effects of Security Protocols on Cybercrime in Ahmadu Bello University, Zaria [Academic Masters, University of KwaZulu Natal, South Africa].

Demers, G, Harrington, S, Cianci, M., & Green ,N.(2017). Protecting Colleges & Universities Against Losses in a Virtual World.. The John Marshall Journal of Information Technology & Privacy Law., 33(2),3

De Paoli, S., Johnstone, J., Coull, N., Ferguson, I., Sinclair, G., Tomkins, P., Brown, M., & Martin, R. (2020). A Qualitative Exploratory Study of the Knowledge, Forensic, and Legal Challenges from the Perspective of Police Cybercrime Specialists. Policing: A Journal of Policy and Practice.

Egbunike, N(2019). Nigerian Students face cybercrime charges for criticising their university online. https://globalvoices.org/2019/07/11/nigerian-students-face-cybercrime-charges-for-criticising-their-university-online/

G.G James, A.E Okpako, C. Ituma & J.E. Asuquo.(2022). Development of hybrid intelligent based information retrieval technique. Int J. Comput. Appl, 184(2022), 13. https://doi.org/10.5120/ijca2022922401

Hedge and Hayword (2004). The Status Information and Communication Technology (ICT) in Secondary Schools in Ondo State. (unpublished M.Ed. Thesis.).

Howard, W.R.(2009), "Schneier on Security",*Kybernetes*, Vol. 38 No. 9, pp. 16361637. https://doi.org/10.1108/03684920910991603

Hunton, P. (2011). A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment. Digital investigation, 7(3-4), 105-113.

Krejcie, R.V., & Morgan, D.W., (1970). Determining Sample Size for Research Activities. Educational and Psychological Measurement.

Krönke, Matthias. (2020). Africa's_digital_divide_and_the_promise_of_e-learning/citations https://www.researchgate.net/publication/342165040

Li, F., Li, Z., Han, W., Wu, T., Chen, L., Guo, Y., & Chen, J. (2018). Cyberspace-oriented access control: A cyberspace characteristics-based model and its policies. IEEE Internet of Things Journal, 6(2), 1471-1483.

Mary , L.(2016). IT Security and Privacy

Mojeed, M.(2020). How Nigeria University Launched Massive Cyber attacks Against Premium Times. https://allafric.COM/STORIES/202007280025.html

Morgan, S. (2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025 Cybercrime Magazine. In. Lucky

Ojobo Ogheneruemu & Okpako Abugor Ejaita(2023). An evaluation of smartphone usage and social interaction of Delta State University Students, Abraka. Journal of Information Engineering and Applications. Vol. 13(1)

Ojobo, O. L, Okpako ,A.E, Ivwighren ,H.E(2022). Covid-19 Pandemic Misinformation and Disinformation on Social Media: A study of Abraka Metropolis. Innovations, Number 70

Okpako A.E, Oghoodi D & Ako, R.E (2020). The triadic interplay of culture, globalization and cybercrime trajectory in Nigeria through a sociological lens. Researchjournali's Journal of Computer Science.(5).4

Okpako Abugor Ejaita, Bridget O. Malasowe, F.O Mormah, & Stella C. Chiemeke (2023). Analysis of emerging Cybercrime Entrepreneurship and its implication in Nigeria. Covenant Journal of Entrepreneurship. Vol. 7(1)

Osuji Catherine U. Nwoke, Bright Ihechukwu (2019), Pre-service teachers' perception towards role of e-learning in science education in teacher training institutions | International Journal of Science and Technology . Vol. 8(1). 40-49,2019

Sanoo, J. (2018). Cyber Security Tutorials. Retrieved 26/06/2020 from https://www.javatpoint.com/cyber-security-introduction

Soomro , T.R, & Hussain , M. (2019). Social Media-related cybercrimes and techniques for their prevention. Applied Computer Systems, 24(1), 9-17

Tabassum, L and Baker, S. (2020). Cybersecurity and Safety Measures. International Research Journal of Modernization in Engineering Technology and Science. Vol 02, Issue:06. June2020. Available at SSRN: https://ssrn.com/abstract=3641388

Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. Big Data & Society, 4(2), 2053951717736335.

U-EENI, (2022). E-learning as a disruptive innovation. U-EENI. Retrieved from http://www.u-eeni.edu.es.com

©2024 This is an Open Access article distributed under the terms of the Creative Commons Attribution 4.0 International license viewed via https://creativecommons.org/licenses/by/4.0/ which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is cited appropriately.