DIGITALIZING CAMPUS SECURITY MANAGEMENT IN THE FACE OF RISING SECURITY CHALLENGES IN NIGERIA: PROBLEMS AND PROSPECTS.

[1] Dr. Joyce Chisoma Wodi
wodijoyce@yahoo.com / joyce.wodi@ust.edu.ng

&

[2.] Dr. John Amaoge Wordu john.wordu2@ust.edu.ng

[1 & 2] Department of Educational Management
Faculty of Education
Rivers State University Nkpolu, Oroworukwo, Port Harcourt.

Abstract

The main goal of any higher education institution is to provide students with education in a secure environment. While establishing policies and protocols for ensuring campus safety is crucial, universities must also use digital technology to enhance their efforts. This paper discussed digitalizing campus security management in the face of rising security challenges in Nigeria, problems and prospects. Digitalization of campus security includes adopting digital transformation strategies to modernize campus security architecture. By leveraging innovative digital security systems, including surveillance cameras, access control, emergency notification systems, and data analytics, these institutions can enhance situational awareness, streamline incident response, and foster a safer learning environment. The study enumerated some of the challenges of campus security as cyber threats and vulnerabilities, privacy and data protection concerns and the issue of funding among others. The study suggested that the managers of tertiary education should prioritized the purchase of modern security gadgets, periodic security assessments and regular training and retraining of security personnel. Campus security implies that it will not only enhance teaching and learning but will also improve situational awareness and enhance students' responses.

Keywords: *Digitalizing, Security, Security management.*

Introduction

The safety of students, faculties and staff on the university campuses is of paramount concern to all stakeholders in education. With more and more people entering universities for further education, more attention is paid to campus safety. A foundational aspect of learning is providing a safe and secure learning environment for students. Students and their support groups need to believe that school is a safe and secure place as well. If students perceive they are in a place of violence or bullying, they spend more time worrying than learning. In the past, schools were the safest place to be, because it was considered as a sacred place and highly respected by all and sundry for its role and what it stands for in the society but the recent developments contradict this testimony because school attacks abound in the world today, and they are often conducted without any cogent reason. In most cases, the attacks may not in any way be related to the goals of the school, rather it may be based on mere religious, tribal, political and socioeconomic activities of a State. This recent development has made campus security a persistent concern for administrators, students and the broader community as Nigerian university campuses have continued to grapple with security challenges, ranging from theft, vandalism,

violence, unrest, terrorist attack, gunmen attack, kidnapping, adoption, killings and other clandestine criminal elements (Radda, 2012).

Nigeria is passing through trying times owing to deteriorated security situation in the nation. On a daily basis lives and properties are lost. Citizens of Nigeria live in fear and as a result human activities in some parts of the country are grinding to a halt owing to security concerns. No wonder Abechi (2018) averred that no section of the nation is immune from the spate of insecurity confronting the nation as the subject matter of security pervades every aspect of human endeavour. The general insecurity that affects the nation naturally spreads and affects the educational institutions especially the due to the organic relationship between the country and educational institutions (Radda, 2012). Similarly, Tripathi and Gupta (2014) said that security has always been a prime concern for any institution, with increase in interaction and exposure with the global world this has become contextually more important. This they said accounts for the reason why various organizations are investing significant amount of resources in seeking for more efficient, effective and innovative ways of solving security problems. Hence, digitalization of campus security architecture represents a significant advancement in enhancing safety and security on educational campuses. By integrating digital technologies into security systems, educational institutions can improve their ability to prevent, respond to, and mitigate security threats, ultimately creating a safer and more secure environment for all members of the campus community. A welldesigned physical campus, fully incorporating digital technology, is essential for building the brand of a university -by enhancing the student experience, and delivering the right settings and facilities for teaching, learning and research.

In the literature on educational management, researchers have explored the potential benefits and challenges of digitalizing campus security architecture. Studies have highlighted how technologies such as surveillance cameras, access control systems, biometric identification, and emergency notification systems can improve the monitoring and response capabilities of campus security personnel. By leveraging data analytics and artificial intelligence, these digital tools enable proactive threat detection, real-time incident management, and effective resource allocation (Etannibi, 2015).

Abechi (2022) noted that Nigerian universities have regrettably recorded some incidents in time past. On April 29, 2012 Boko Haram invaded Bayero University, Kano State killing scores of people, professors, non-academic staff and students on the campus. There was also an attack on the University of Maiduguri where several students including lecturers where feared dead through the terrorist activities of the Boko Haram. The Greenfield University, Kaduna was also attacked in April 2021. In the same year College of Forestry in Kaduna State was attacked and students were adopted, killed and some were lucky to be released after handsome amount of ransom were paid on them by their parents (Channel, 2021). Federal university of Agriculture Markurdi was attacked in February, 2023. Ambrose Ali university, Ekpoma was attacked in October 2022, Ahmadu Bello university, Zaria was attacked in July, 2022. Niger State College of education, Minna was attacked In June, 2022, Confluence university of science and technology Osaro Okene Kogi state (CUSTECH) was attacked at night by gunmen who shot sporadically and whisked away nine (9) students from the school (Channel, 2024). Attacks on students, academic staff, and education institutions could have devastating impact. Immediate effects can include death, injuries and the destruction of education facilities as well as disrupted access to education. In the long term, such attacks can lead to diminished education quality, loss of teachers and academics, and weakened education systems. The quality and relevance of higher education can be degraded and research and innovation curtailed. Weakened education adversely affects a country's economic, political and social development, and undermines efforts to reduce poverty. The researchers are worried that these incidents take place in the campuses and the attackers go Scot-free without any trace or apprehension by the law enforcement agents. This development is disturbing, frightening and requires urgent attention from policymakers, stakeholders and the government to adopt measures that will give a dead blow to this gory scenario which is not healthy for our collective political, economic and industrial development.

It is because the traditional security approaches such as manual patrols and outdated surveillance systems have proven inefficient in addressing the evolving nature of threats faced by educational institutions

that this paper delves into the topic of digitalizing campus security management in the face of rising security challenges in Nigeria: problems and prospects, marshalling out digital means through which campuses can be better secured to prevent incidents so that learning, teaching and research can go on smoothly to improve our society without attacks.

Concept of Campus Security

Campus security is a multifaceted challenge that requires a comprehensive and proactive approach. By understanding the unique vulnerabilities of higher education institutions, leveraging technology as a force multiplier and adopting a holistic security strategy, campus security teams can enhance their security posture and create a safer environment for students, faculty, and staff (SiteOwl, 2024). Spotting the flaws in conventional campus security suggests that traditional campus security isn't enough to secure the members of the campus community hence the need for an upgrade in strategy. Proactive security for the modern campus emphasizes the power of being proactive, integrating tech (digital) solutions and preventative tactics. Technology as a forcemultiplier explores how technology amplifies security efforts, making campuses safe for students and staff. Abechi, Anyegba and Egbuche, 2017; Abechi, 2022) defined security as a state of secured and safe existence from fear, terror, intimidation, harassment, theft, uncertainty, loss of lives and valuables that may result from the activities of thieves, kidnappers, guerrilla fighters like Boko- Haram, tribal militias and agitators. Similarly, Guideline (2001); Alimba (2018); Abechi (2022) conceives security as an all-encompassing condition in which people and communities live in freedom, peace and safety, participate fully in the governance of their countries, enjoy the protection of fundamental rights, have access to resources and basic necessities of life, and inhabit an environment which is not detrimental to their health and well-being. As regards to the university campuses, the purpose for which they are established can only be realized when the campuses are safe, free from attacks, violence, danger and not detrimental to the well-being of members of the campus community.

Campus ssafety and security also encompasses social and emotional well-being of students. Students deserve to feel comfortable and secure at school so they can focus on learning and contribute to the learning environment (Dellenbach, 2016). Student security, according to Marginson, Nyland, Sawir, and Forbes-Mewett (2010) is the social and economic well-being of cross-border students, which includes personal safety, financial issues, work experiences, housing, health and welfare services, language problems, and students' personal and social networks, including family, community, and affinity groups, and experiences with government and university authorities. Similarly, Etannibi (2015) conceives security as protection from danger, violence, fear, and want that impair, or is capable of impairing the full development and existential well-being of citizens. Security implies the absence of fear and want.

Concept of Digitalization

According to Honeywell Forg, (2024) digitalization is a transformation process that involves the integration of digital technologies into all areas of a business, education inclusive, leading to fundamental changes in how the business operates and delivers value to its customers. The dynamic and rapidly evolving digital landscape is driving disruptive change across all industries – including education. The dynamics driving digital transformation includes:

Cloud Computing: The cloud has revolutionized the way businesses store, manage and access data. By moving data and applications to the cloud, companies can improve scalability and increase agility (while also reducing infrastructure costs).

Artificial Intelligence (AI): AI helps transform how businesses operate by automating repetitive tasks, providing insights and improving decision-making. A simple example we can all understand is the AI-powered chatbot or virtual assistant used by many companies for customer service. An industrial-grade example is AI algorithms that help optimize supply chains and improve operational efficiency.

The Internet of Things (IoT): IoT involves the interconnectivity of physical devices and sensors, allowing for the creation of smart systems that can collect and analyze data in real time. The industrial internet of things (IIoT) is a further extension used for industrial purposes such as manufacturing, monitoring, and supply chain management, enabling companies to improve the efficiency of their operations (Honeywell Forge, 2024). Valenduc and Vendramin (2017) opined that the term "digitalization" is not the irruption of a new revolution, but the pervasive synergy of digital innovations in the whole economy and society. Reis, Amorim, Melão, Cohen, and Rodrigues (2020) in corroborating this point said that digitalization is the most significant technological trend that is changing both, society and business. Nowadays, firms are constantly under pressure to use digital technologies and to adapt their business models to this new reality. However, going digital evokes many benefits, it also requires investments and associated costs given the noticeable progress of digital technologies, the question is how digitalization is being employed by practitioners and into what extent this progress is being followed by scholars and academics.

Universities, like all modern businesses, must seek every means to drive efficiency and save cost. There is the saying in business: 'digitally disrupt or be digitally disrupted'. This now applies equally to the ever-more competitive university sector. Hagberg et al (2016) averred that digitalization is one of the most significant ongoing transformations of contemporary society and encompasses many elements of business and everyday life by digitization of everything that can be digitized' Although this general term involves all types of digital technologies, we focus on the integration of Internet- connected digital technologies in particular and on the interface security architecture of university campuses. Digitalization refers both to a transformation from "analogue" to "digital" (e.g. a shift from cash to electronic payments) and to the facilitation of new forms of value creation (e.g. Accessibility, availability, and transparency). Employing the notion of 'digitalization' rather than 'digital' implies that this transformation is on-going and has no clear beginning or end. Thus, we approach the notion of digitalization as something that is emerging and in the making rather than something already achieved. We conceive digitalization as an open and dynamic concept that has not been fully defined; it is an on-going process that should be approached with sensitivity and openness to what it might encompass. Machekhina (2017) asserts that digitalization means transformation of all information types (text, sound, visuals, video and other data from various sources) into the digital language. He further revealed that digitalization of education is a powerful trend in terms of reformation and modernization of global education environment. Discussing the phenomenon of digitalization, it should be noted that various analysts and forecast experts (mostly British, including Tim Berners-Lee - one of the inventors of the World Wide Web (Stuart, 2014)) consider transition of education process into digital stage as the turning point in the history of education. Devereux and Vella (2018) said that Digitalization is the process of spreading of general-purpose technology. The last similar phenomenon was electrification. Digitalization of products and services shortens distances between people and things. It increases mobility. It makes network effects decisive. It allows the use of specific data to such an extent that it permits the satisfaction of individual customer needs – be it consumers or businesses. It opens up ample opportunities for innovation, investment, and the creation of new businesses and jobs. Going forward it will be one of the main drivers of sustainable growth.

The digitalization of campus security management is a concept that has gained increasing attention in the field of educational management in recent time. As educational institutions strive to create safe and secure environments for students, faculty, and staff, the integration of digital technologies into campus security systems has emerged as a promising approach to enhance safety and efficiency. Digital technology plays a significant role in combating insurgences particularly because sophisticated and advanced technologies have greatly replaced older forms of security operations and surveillance gadgets.

In the literature on educational management, researchers have explored the potential benefits and challenges of digitalizing campus security architecture. Studies have highlighted how technologies such as surveillance cameras, access control systems, biometric identification, and emergency notification systems can improve the monitoring and response capabilities of campus security personnel. By leveraging data analytics and artificial

intelligence, these digital tools can enable proactive threat detection, real-time incident management, and effective resource allocation.

Some Digital tools for managing campus security

In light of the recent incidents in schools and universities nationwide, parents, administrators, and even students are requesting for more security presence which requires new and innovative security measures. Auyo, Mato, and Ibrahim, (2020) and Schwartz, Ramchand, Barnes-Proby, Grant, Jackson, Leuschner, Matsuda, and Saunders (2016) agrees that with digital Technology, it is possible to design and implement modern security processes that provides peace of- mind not only to those within the school (educators and students), but those outside. This paper identifies the following digital tools that can enhance campus security management:

3. **Video Surveillance Technology:** According to Sarre & Prenzler, (2011) Close Circuit Television (CCTV) is a device used to transmit a signal containing images that can be viewed remotely by authorized - University personnel or a security personnel views the security camera images in real-time. According to Auyo, Mato, and Ibrahim, (2020) the role of CCTV is to monitor and record public areas for safety and security for all members of the campus community, including faculty, staff, students, visitors, vendors and contractors.Video surveillance technology can be used proactively to prevent incidents by letting perpetrators know that they are being monitored, as well as to creatively follow up on incidents by recording and identifying perpetrators. Common materials for video surveillance technology include cameras, CCTV, video-recording devices, and a video–motion detection system. Cameras are placed in vulnerable or high-risk areas of school property and portable cameras can be

   quickly installed or located. Feeds from cameras are then sent to a monitoring station, either at the school itself or to a district office. Video–motion detection systems provide added support by producing alarm signals or switching to continuous recording when triggered (Addington, 2009; Heather, Rajeev, Dionne, Sean , Brian, Kristin, Mauri & Jessica, 2016). Cameras often need to be concealed, hidden, or hard-to-reach to prevent vandalism, and angled to avoid glare and maintain their ability to function properly (Heather, Rajeev, Dionne, Sean , Brian, Kristin, Mauri & Jessica, 2016). In general, CCTV cameras are intended to serve two main purposes for the university's community:

   Monitoring of Personal Safety – To capture video, in the event an individual is the subject of harm or crime, that provides information or evidence of what occurred and who is responsible, and thereby deter crimes or harmful conduct toward individuals.

   Monitoring of Property Protection – To capture video, in the case of lost, stolen or damaged property, that provides information or evidence of what occurred and who is responsible, and thereby deter property crimes or violations. CCTV cameras can be used to discover wrongdoing and other criminal activities within the campus. The instrument can be made to be available on campus to monitor abnormal behavior. The use of digital technology in uncovering, studying and identification of people's activities, interaction and movement will help in checkmating any security threatening activities and tasks within the camps community.

4. **Global Positioning System (GPS):** the schools can leverage the transformative potential of GPS technology in promoting campus security and safety. GPS-enabled emergency response systems can enable security personnel to track the location of individuals in distress, facilitate rapid intervention during critical incidents, and coordinate emergency services effectively. Geofencing technology allows security departments to establish virtual boundaries around sensitive areas, monitor access control, and detect unauthorized intrusions in real-time. Asset tracking using GPS helps prevent theft, loss, and misuse of valuable resources on campus, thereby enhancing inventory management and security measures. Furthermore, safe walk programs leveraging GPS technology provide students, faculty, and staff with a secure means of requesting escorts, sharing their location, and receiving assistance during

late hours or in unfamiliar surroundings. Mobile safety apps equipped with GPS features empower individuals to communicate with security personnel, trigger emergency alerts, and access safety resources at their fingertips. Incident mapping tools that integrate GPS data enable security teams to visualize security incidents, identify patterns, and allocate resources strategically to address emerging threats effectively**.**

According to (Katina, McNamee, & Michael, 2006) the University security personnel can leverage the potential of the GPS in tracking who goes in out of the campus. The GPS tracking unit can determine the precise location of a vehicle, person, or other asset to which it is attached and to record the position of the asset at regular intervals. The recorded location data can be stored within the tracking unit, or it may be transmitted to a central location database, or internet-connected computer, using a cellular (GPRS), radio, or satellite modem embedded in the unit. This allows the asset's location to be displayed against a map backdrop either in real-time or when analyzing the track later, using customized software. Mba, Abdurraheem, and Abdullahi (2017) identified other uses of the GPS in education to include aiding students to produce the map of their schools, it can be used by students to locate a hiding object i.e. geocaching, GPS can be used by students to locate the position of a new school or a school in an unfamiliar location, it can be used by students to locate examination centers outside or within their state.

GPS can be used by students to map the schools in the neighborhood of their school as geography practical. Bradon, (2003) observed that GPS tracking also reduces response times and enables more efficient utilization of vehicles used by police departments, fire officials, search and rescue missions, and other emergency services. Law enforcement and wireless communications industries are considering placing GPS technology in cellular telephones and other information systems to facilitate apprehension of criminals and the location of cellular telephones in the possession of individuals trapped in collapsed buildings, snow storms, and other catastrophes. This network incorporates a range of satellites that use microwave signals which are transmitted to GPS devices to give information on location, vehicle speed, time and direction. So, a GPS tracking system can potentially give both real-time and historic navigation data on any kind of journey. A GPS tracking system can work in various ways. From a commercial perspective, GPS devices are generally used to record the position of Objects e.g vehicles as they make their journeys.

5. **Access control:** The digitalization of campus security architecture can greatly enhance access control measures through the implementation of advanced technologies and systems. One of the ways in which digitalization promotes access control in campus security is through electronic Access Control Systems: Digitalization allows for the implementation of electronic access control systems, such as keycard readers, biometric scanners, and smart locks. These systems provide a more secure and efficient way to manage access to campus buildings and facilities, as access can be granted or revoked remotely and access logs can be easily monitored. According to SITEOWL (2024) the sprawling grounds, diverse buildings, and open-access ideals of a college campus can create a deceptive sense of security. While campuses strive to foster welcoming environments, this openness often introduces significant gaps in traditional physical security measures. From outdated perimeter control to insufficient monitoring of high-risk areas, these vulnerabilities can leave students, faculty, and valuable assets exposed. The university management can install electronic gates, doors and turnstiles with biometric authentication. These gadgets can help in monitoring who goes in and out of the campus (eg, facial, recognition, fingerprint scanning etc).

6. **Intrusion detection system (IDS): i**ntrusion detection system is the kind of software or the application that is basically designed for detecting, blocking and reporting unauthorized activity in the whole network system. Intrusion detection does exactly as the name suggests: they generally detect possible intrusions (Tapan, Hiren & Hardik, 2012). More specifically, IDS main aim is to detect computer attacks and computer misuse, and to alert the proper individuals upon detection. This is the era of web & Cloud based technology and, in this technology, internet plays a very huge role. Internet is a hostile

environment for networked computers. Network Security is the crucial and very important part of information security because it is responsible for securing all the information passed through a Network computer. In this type of environment, we need cyber security that will protect against the different kind of attacks, viruses & heavy inside as well as outside traffic (Tapan, Hiren & Hardik, 2012). In recent years hacking & intrusion incidents are increasing very fast because of technology, without security your data is not safe and secure. Because attackers are everywhere they knows how to exploit vulnerabilities the use of networks and information systems as a tool becomes necessary for the proper functioning and growth of any organizations including educational institutions. The multitude of network usage by unknown or known persons turns the network into potential targets for attackers. Users can exploit the vulnerabilities of network and computer systems to access information or to undermine their good functioning**.** Schools can leverage advanced sensors and alarms for perimeter security, detecting potential security breaches**.** This allows for quick implementation of security policies to detect and react as quickly as possible against attacks occurring in a network. An intrusion detection system can be considered as an application in which individuals and organizations often express the need and objective of protecting their systems against intrusions (Sellami, Sellami &, Tiako, 2019).

Sheetal, Pankaj and Meshram **(**2012) identified that Intruders are of two types, the external intruders who are unauthorized users of the machines they attack, and internal intruders, who have permission to access the system, but not some portions of it. Further internal intruders are divided into intruders who masquerade as another user, those with legitimate access to sensitive data, and the most dangerous type, the clandestine intruders who have the power to turn off audit control for themselves. Different types of threats include:

7. **Explosive Device Detectors:** With the increasing threat of violence and terrorism, the need for effective security measures, including the use of explosive device detectors, has become more critical on college and university campuses. Explosive device detectors play a crucial role in enhancing campus security by providing a means to detect and prevent potential threats posed by explosive devices. These detectors are advanced technological tools that can identify the presence of explosive materials or components within a given area, helping security personnel to respond quickly and effectively to any suspicious activity. According to Riley-Smith & Bate, (2022) the use of explosive device detectors on campus can help to deter potential attackers and provide an added layer of security to protect the campus community.

   By screening individuals, vehicles, bags, and packages for explosive materials, these detectors can help to prevent dangerous incidents and ensure the safety of students, faculty, and staff. Nowadays a lot of attention is being paid to the development of methods and instruments for detecting illegal, dangerous, and explosive devices. Explosives devices could be detected with 100% efficiency, using artificial intelligence (AI) and a new X-ray approach developed by a team led by UCL academics (Riley-Smith & Bate,2022). Some explosives can be difficult to spot using conventional X-ray alone, and the new method could revolutionize how illicit materials such as narcotics, illegal wildlife and explosives are detected. Initiated explosives have already killed thousands of people and injured several tens of thousands worldwide not only in Nigeria. Infrastructural facilities, like railway stations, schools, airports, underground railways, security offices, electricity, water supply, etc. are preferred targets involving up to thousands of people. Artificial intelligence (AI) has the potential to detect explosives early by means of sensors. (Riley-Smith & Bate, 2022).

8. **Automated Personal Data Bank (APDB):** In today's digital age, the security and management of personal data have become paramount concerns for educational institutions, especially on campus where a large amount of sensitive information is stored and accessed regularly. The Automated Personal Data Bank (APDB) offers a comprehensive solution to address these concerns by providing a secure and efficient way to manage personal data within the campus environment. APDB is a sophisticated system that allows educational institutions to centralize and streamline the storage, retrieval, and protection of personal data belonging to students, faculty, and staff. By utilizing advanced encryption and access

control mechanisms, APDB ensures that sensitive information is safeguarded against unauthorized access and data breaches.in the words of Auyo, Mato, and Ibrahim, (2020) it is the use of devoted tools and data bases to receive and keep ironed out data or citizen's information to enable government have easier access to biometric of its citizens. The security department of the university can rely on the APDB to gather data about visitors, students and staff of the university. This data can help in identifying intruders within the campus community. Automated Personal Data Bank (APDB) is the use of dedicative devices and databases to collect and store the detected data and personal information about people that can allow the security personnel to track individual information including suspected terrorist groups or intruders. The APDB records can contain digital images, fingerprints, insurance details, and vehicle registration to assist in monitoring peoples' activities by government security departments and agencies like the (DSSS) and the (SID). Therefore, university security personnel are expected to be vigilant in their duty while the management are expected should ensure their training, equipping them with AI tools to can Counter terrorism/Unrest. The application of AI in the campuses could mitigate terrorism and terrorist attacks.

9. **Entry Control Equipment:** Entry equipment on campus plays a crucial role in ensuring the safety and security of students, staff, and visitors within educational institutions. These tools and systems are designed to control access to campus buildings, parking lots, and other facilities, helping to prevent unauthorized entry and maintain a secure environment. From access control systems and security cameras to gates and turnstiles, entry equipment on campus serves as a first line of defense against potential threats and intrusions. By effectively managing who can enter the campus premises, these devices help to protect valuable assets, prevent incidents of violence or theft, and create a sense of safety for everyone on campus. Ogunode ,Ohibime, Okwelogu, and Musa, (2021) averred that entry control equipment is used across the spectrum of preventing, preparing for, and responding to crises related to school violence and other threats to school safety. They further said that the materials for entry control typically includes electronic door locks, barricades, posted signs, radio frequency identification (RFID) cards, and biometric access control systems. Electronic or electromagnetic locks are remotely controlled to lock or unlock targeted doors as desired. Barricades and posted signs facilitate entry into a school facility at desired access points. Those with access cards can use them to enter facilities without signing in or checking in with school staff as Ibarra-Manzano et al (2008) noted. These technologies are intended to make it easier to limit access to authorized users, reduce crime rates and foster a safer learning environment for student, faculty and staff (Chipley, Lyon, Smilowitz, Williams, Arnold, Blewett, Hazen, & Krimgold, 2012). Hand-held and walkthrough metal detectors, X-ray machines to scan books, bags

often at entrance to school or as students exit school gate. Generally speaking, locks and barricades are standard, low-tech protection technologies. However, electromagnetic locking systems have the potential to mitigate security breaches (Gray, 2014). The university can leverage the electronic or electromagnetic locks for security checks at the entrance and exit points of the school. These equipment enhance response preparedness of campus security personnel.

10. **Autonomous robots and drones for surveillance and monitoring**: one of the security challenges faced by the tertiary institutions is how to develop a robust and efficient surveillance system that can constantly monitor and detect any suspicious activities in real-time within the campus (Rizwan, Nurul, Muhammad, Rafaqut, 2021). Firstly, autonomous robotsanddrones have the potential to operate 24/7 without fatigue, unlike human security personnel. Secondly, it can patrol a large area in a relatively short amount of time, providing comprehensive surveillance coverage. Thirdly, it can reduce the risk to security personnel by allowing threats to be evaluated and prepared for. Overall, an autonomous mobile surveillance robot can be a valuable tool for enhancing security of both public and private property (Dickens, Maweni**,** Setati**,** & Suddoo**,** 2023**).** Drones can be deployed quickly in areas considered to be too unsafe for humans and are used to guide rescuers, collect data, deliver essential supplies or provide communication service. Security robots are commonly used to protect and safeguard a location, some valuable assets, or personal against danger, damage, loss, and crime (Gregoriades, Obadan, Michael, Papadopoulou, Despina, 2010).

Drones are the best solution nowadays when it comes to assessing damage and spotting people in distress. In future drones will take on an increasingly important role in natural disaster response, search and rescue, firefighting and other disaster management activities, reducing the risk to human life during operations, and limiting damage to assets by enabling first responders to work proactively. Drones can perform critical tasks as disasters unfold, including spotting people in need of urgent help. Evidence suggests drones may have certain advantages over traditional search-and- rescue efforts, including speed, as well as they can provide help in the aftermath of disasters to assess damage to buildings, roads and bridges, power lines. (Velev, Zlateva , Steshina , & Petukhov, 2019).

The Problems of Digitalization of Campus Security Management

1. **Cyber threats and vulnerabilities:** One of the primary concerns with the digitalization of campus security management is the potential for cyber threats and vulnerabilities. According to Mamoona, Mahmood, Noor, Mohammad, and Sajjad (2020) these are the flaws in a system or its design that allows an attacker to execute malicious commands, access data in an unauthorized way, and /or conduct various denial-of service attacks. As security systems become more interconnected and reliant on digital platforms, they also become more susceptible to the following attacks as identified by Mamoona, et al (2020):

Data Breaches, Disruption of Services, Malware and Ransom ware, Phishing and Social Engineering, IoT Security Risks etc**.**

2. **Privacy and data protection concerns:** Another challenge of digitalization is the issue of privacy and data protection. As security systems collect and store vast amounts of data including biometric information, surveillance footage, access logs, and other sensitive information, there is a risk that this information could be misused or compromised. It is crucial for institutions to implement robust data protection measures and adhere to strict privacy regulations to safeguard the personal information of individuals on campus to avoid unauthorized access, misuse, or theft, leading to privacy violations and potential harm to individuals.

3. **Funding issues:** the implementation of digital security systems can be costly and resource intensive. Educational institutions must allocate sufficient funds and resources to invest in the necessary technology and infrastructure to support digital security measures. This can be a significant financial burden for many institutions, particularly those with limited budgets. Funding is a major challenge because it has negatively affected many areas of security in Nigeria. Money is required to procure and maintain security gadgets and software packages; money is required to train and retrain security personnel. The universities lack funds needed to pursue the security challenges in the country (Gbadamosi,2006**;** Auyo, Mato, & Ibrahim, 2020).

4. **Power Supply**: Modern societies critically depend on secure supply of high-quality electrical energy (Hatziargiriou, 2009; Marko, Jelena, Slobodan, Octavio, & Vanco, 2013). Most of campuses experience epileptic power supply. Power outage is a great and concurrent problem affecting usage of digital tools for campus security. Most of the digital tools require adequate and constant power supply before they can function. (Ohiwerei, 2013**;** Auyo, Mato, & Ibrahim, 2020) argued that Nigeria being a developing nation cannot boast of a twenty-four-hour electricity supply to its citizens. Most of the schools are directly connected to Power Holding Company of Nigeria; it is a sad to note that some of the schools cannot afford a generating set that can power the entire campus community. This in itself makes the campus vulnerable. Prospects of Digitalization of Campus Security Architecture

11. **Improved campus safety:** The combination of preventive measures such as access control and proactive interventions can contribute to reduce crime rates and foster a safer learning environment for students,

faculty and staff. In a world where technology is king, leveraging it to improve campus safety is key (Transact, 2024).

12. **Enhanced Security Measures:** Automated systems are often safer and more reliable than manual systems, helping organizations reduce the risk of accidents and improve safety. Digital security systems offer advanced features such as real-time monitoring, facial recognition, and biometric access control, which can significantly enhance the effectiveness of campus security measures. These technologies can help to identify and respond to security threats more quickly and efficiently, improving overall safety on campus (Editorial, 2023)

13. **Improved situational awareness and enhanced incident Response:** the real-time monitoring and analysis of campus activities through the surveillance system can enable security teams to detect and respond to incidents more effectively. Digital security systems can streamline the process of reporting and responding to security incidents. With features such as automated alerts and notifications, security personnel can be promptly informed of any potential threats, allowing them to take immediate action to mitigate risks and ensure the safety of individuals on campus.

14. **Enhanced Security Awareness:** Threat intelligence software provides businesses with insights into the latest threats and vulnerabilities, helping them to stay up-to-date with the evolving threat landscape (Editorial, 2023).

15. **Data Analytics and Predictive Modeling**: By leveraging data analytics and predictive modeling, institutions of learning can proactively identify potential security risks and implement preventive measures to mitigate them before they escalate. Digital security systems can collect and analyze vast amounts of data to identify patterns and trends in security incidents. Rustagi, & Goel, (2022) posits that in identifying fraud, a combination of several analytical methods can refine pattern detection and prevent criminal behavior. As cyber security becomes an issue, high performance behavioral analytic monitors all activities on a network in hard-real time to detect an abnormal feature that may reflect a sign of threat.

16. **Remote Monitoring and Management:** Digital security systems enables remote monitoring and management, allowing security personnel to oversee campus security operations from anywhere at any time. This flexibility can improve the efficiency of security operations and enable a more agile response to security incidents on campus (Faridullah , Jahan , & Khair,.2023).

Conclusion

Campus security is not reacting to incidents but preventing them through a combination of technology, Community engagement and strategic planning. Security is a fundamental and necessary condition for the attainment of institutional goals and must not be compromised. To ignore the need for campus security management, will terribly cripple meaningful activities of the institution. While the digitalization of campus security architecture offers many advantages, it also presents a range of challenges that must be carefully managed. Educational institutions must be proactive in addressing issues such as cyber threats, system obsolescence, privacy concerns, and financial constraints to ensure the safety and security of their campus community. By taking a strategic and holistic approach to digital security, institutions can effectively navigate these challenges and create a secure environment for learning and growth.

Suggestions:

University management has not been able to effectively curb campus security challenges and other social evils within its environment due to mainly endemic problems which makes some Universities in Nigeria though centers of knowledge in principle to develop into environments of violence, barbarism, rape and other forms of crudity. Therefore, to redeem the good image of the University through digitalizing the campus security architectures the following measures should be observed:

1 Government should invest money in procuring modern security gadgets to equip campus security personnel and maintain modern and functional security gadgets/equipment.

2 Government should allocate enough funds to universities to enable them recruit and equip security personnel

3 Regular training should be organized for university security personnel to make them abreast with digital technology that can enhance the safety of both students and staff on campus.

4 Vice Chancellors of Universities should give proper and regular orientation on Security issue to members of the campus Community.

5 The University management should endeavour to carry out periodic security threat assessment to ascertain the level of insecurity, its possible causes in the campuses and strive to minimize/eradicate the existence of such factors.

6 Governments should develop smart innovation strategies for education with the right policy mix to give meaning and purpose to innovation, including creating an innovation-friendly culture.

References

Abdulkadir, A. Shatimah, H. A. & Abdulrahman, A. M. (2016). Effective Use of ICT Tools Menace in Nigeria. *International Journal of modern Trends in Engineering and Research (IJMTER)*. 3(5) 357-360

Abechi, A. (2022). Calls for intensification of security in educational institutions. Retrieved from Academia.edu *https://www.academia.edu › CALLS_FOR_INTESIFIC...*

Auyo, S.G., Idris A., Mato, I., Ibrahim, A. A. (2020). A Review on the Use of ICT as a means of

Security within Tertiary Institutions in Nigeria. *Dutse Journal of Pure and Applied Sciences (DUJOPAS)*, 6 (4) 76-81,

Brandon, J. M.(2003). The global positioning system: global developments and opportunities office of industries. United States International Trade Commission, Office of Industries. DOI: 10.22004/ag.econ.15877

Bratton, W. J. & Burch, J.H. (2009). Campus Security Guidelines Recommended Operational

Policies for Local and Campus Law Enforcement Agencies Campus Security Guidelines

BJA (Bureau of Justice Assistance) U.S. Department of Justice

https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/MCC_CampusSecurity

Chipley, M., Lyon, W., Smilowitz, R., Williams, P., Arnold C., Blewett, W., Hazen, L., & Krimgold, F. (2012). Primer to Design Safe School Projects in Case of Terrorist Attacks and School Shootings. Buildings and

Infrastructure Protection Series. Washington, D.C.: U.S. Department of Homeland Security, FEMA-

428/BIPS07/January. Retrieved from https://www.dhs.gov/xlibrary/assets/st/bips07_428_schools.pdf

Dellenbach, D. (2016). How perceptions of safety and security affect student learning. *Linkedin* https://www.google.com/search?client=firefox-b-d&q=Dellenbach%252C+D.+(2016)

Devereux, M.P. & Vella, J. (2018). Implications of Digitalization for International Corporate Tax

Reform. *Intertax*. 46(6/7), 550 – 559. https://doi.org/10.54648/taxi2018056

Dickens, J., Maweni, T, Setati, T. & Suddoo, Z. (2023). Design of HERMES: A mobile autonomous surveillance robot for security patrol. *MATEC Web of Conferences* 388, 04005 https://doi.org/10.1051/matecconf/202338804005

Editorial. (2023). Protecting Your Data: Enhanced Security Measures For Increased Threats. https://www.techcompanynews.com/protecting-your-data-enhanced-security

Etannibi, E.O.A (2015). Security Challenges and University Systems in Nigeria. University of Jos International Repository. https://uniios.edu.ng>safercampusbexperience

Faridullah, L., Jahan, G., & Khair, M. (2023). Digital Monitoring and its Effects on

Organizational Performance. *Integrated Journal for Research in Arts and Humanities* 3(5):240-247. DOI:10.55544/ijrah.3.5.22

Gary, A. & Norris, C. (2020). The maximum surveillance society: the rise of CCTV. Taylo and

Francis ebooks . https://doi.org/10.4324/9781003136439

Gray, D.E (2014). Doing Research in the Real World, 3rd edition, Sage

https://www.researchgate.net/publication/239938424_Doing_Research_in_the

Gregoriades, A., Obadan, S., Michail, H. E., Papadopoulou, V. & Despina, M. (2010). A Robotic System for Home Security Enhancement. Paper presented at the 8th

International Conference on Smart Homes and Health Telematics, ICOST 2010, Seoul, Korea, June 22-24, 2010. DOI:10.1007/978-3-642-13778-5_6

Hagberg, J., Sundstrom, M. & Egels-zanden, N.(2016). The digitalization of retailing: An exploratory framework. *International journal of retail and distribution manement*,*44* (7) 694-712. DIO10.1108/IJROM-09-2015-0140

Heather, L. S, Rajeev, R., Dionne, B., Sean G., Brian, A. J., Kristin, J. L., Mauri, M. & Jessica, S. (2016).

The Role of Technology in Improving K–12 School Safety.

https://www.rand.org/pubs/research_reports/RR1488.html. Also available in print form.

Honeywellforge. (2024). What Is Digitalization? And Why Is It Important? https://www.honeywellforge.ai/us/en/learn/blog/what-is-digitalization-and-wh

Ibarra-Manzano, O. G., Morales-Mendoza, L. J., Shmaliy, Y., Arceo-Miquel, L. J. & MontielRodriguez, M. (2008). Moving Average Hybrid FIR Filter in Ultrasound Image Processing. *8th International Conference on Electronics, Communications and Computers (conielecomp)* Puebla, Mexico: 03-05 March 2008. DOI: 10.1109/CONIELECOMP.2008.13

Kaiko, M.(2021). Understanding school safety and security: Conceptualization and definitions. *Journal of Lexicography and terminology*, 5(1), 76-86.

https://www.reseachgate.net/publicaion/353702474_understanding_school_safet...

Katina, M. McNamee, A., Michael, M. G. & Tootell, H. (2006). Location-Based Intelligence – Modeling Behavior in Humans using GPS. *University of Wollongong Research online* https://ro.uow.edu.au/infopapers/386

Machekhina, O.N. (2017). Digitalization of education as a trend of its modernization and reforming. *Revista Espacious. 38* (40) 26

Mamoona, H., Mahmood, N. i., Noor, Z. J., Mohammad, A. & Sajjad, M. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arabian Journal for Science and Engineering, 45*(2), DOI:10.1007/s13369-019-04319-2

Marko, D., Jelena, M., Slobodan, B., Octavio, N. & Vanco, L. (2013). ICT and power: New challenges and solutions. *International Journal of Reasoning-based Intelligent Systems* 5(1). 32 – 41. DOI:10.1504/IJRIS.2013.055125

Mba, T. W, Abdurraheem, M. I . & Abdullahi, A. (2017). Application of GPS Technology in Education. *International Journal of Trend in Research and Development*, 4(3), 338-339. www.ijtrd.com

NIOSH. National institute for occupational safety and health (2024) Prevention through Design. Retrieved from https://www.cdc.gov/niosh/ptd/about/index.html

Ogunode, N.S J., Ohibime, E. O. Okwelogu, I. S & Musa, A. (2021). Deployment of Information

Communication Technology (ICT) for Effective Security Management in Nigerian Educational System. *Middle European Scientific Bulletin, vol 19 https://www.researchgate.net/publication/358221469_Deployment_of_Information.*

Tripathi, P. & Gupta, S. (2012). Security Metrics: Relevance in Securing Educational Institutions. *Signal processing and information technology (SPIT) conference paper*. 215= 221 RETRIEVED FROM https://link.springer.com>chapter

Radda, S. I. (2012, July 25). The role and importance of security awareness in the enhancement of security on university campuses in Nigeria: An imperative for countering terrorism on university campuses. *Paper presented at training workshop on security awareness and orientation against terrorist threats /attacks for officers of Nigerian universities held at Nigeria university commission auditorium, Abuja on*

Reis, J., Amorim, M., Melão, M., Cohen,Y., & Rodrigues, M. (2020) Digitalization: A Literature Review and Research Agenda. In book: Proceedings on 25th International Joint Conference on Industrial

Engineering and Operations Management – IJCIEOM. 443456 DOI:10.1007/978-3-030-43616-2_47
Riley-Smith & Bate (2022). Explosives detection improved by new X-ray technique, *UCL NEWS*. https://www.ucl.ac.uk/news/2022/sep/explosives-detection-improved-new-x-r

Rizwan, M., Nurul, A. A., Muhammad, F. M. & Rafaqut, K. (2021). Drone Security: Issues and Challenges. *IJACSA) International Journal of Advanced Computer Science and Applications*, 12, (5). 720-723.

Rustagi, M. & Goel, N. (2022). Predictive Analytics: A study of its Advantages and Applications. *IARS'*

International Research Journal, vol. 12, (1), https://www.redalyc.org/articulo.oa?id=663872727008

Sarre, R. & Prenzler, T. (2011). Private security and public interest: Exploring private security trends and directions for reform in the new era of plural policing. Sydney: Australian Security Industry Association Limited. https://www.semanticscholar.org/paper/PrivateSecurity-and-Public-Interest%253A-E.

Schwartz, H.L. Ramchand, R., Barnes-Proby, D., Grant, S., Jackson, B. A. , Leuschner, K. J. , Matsuda, M. & Saunders, J. (2016). The Role of Technology in Improving K–12 School Safety. *Santa Monica, CA: RAND Corporation.*

https://www.rand.org/pubs/research_reports/RR1488.html.

Sellami, L, Sellami, K., & Tiako, P. (2019). Efficient Management of security for supporting Intrusion Detection in Ubiquitous and pervasive environments. *Poceddia computer science*. 155. 402-409. https://doi.org/10.1016/j.proc.2019.08.056

Sheetal, T., Pankaj, I., Meshram, B.B. (2012). IDS: Intrusion Detection System the Survey of Information Security. *International Journal of Emerging Technology and Advanced Engineering* Website. www.ijetae.com (ISSN 2250-2459, Volume 2, (31).86-87.

https://www.academia.edu/97539525/IDS_Intrusion_Detection_System_the_Survey

Siteowl. (2024) campus security made simple: Strategies and insights for a safer campus experience. 1-8. Retrieved from https://getsiteowl.com/wpcontent/uploads/2024/03/campus-securitymade-simple-ebook.pdf.

Stuart, K.O. (2014). Activity theory as a reflective and analytic tool for action research on multi-professionalcoolaborative practice. Reflective practice. 15(3).347-362. http://insight.cumbria.ac.uk/id/eprint/1716/

Tapan, P. G., Hiren, D. J., Hardik, J. J. (2012) Different Tools and Types of Intrusion Detection System with Network Attacks "T&T-IDSys" - A Review. 2nd international conference on multidisciplinary research

& practice. retrieved from https://www.academia.edu/19956613/Different_Toolsand_Types_of_Intrusion3(1)

Transact, (2024, July 17). The Future is Now: Technology For Transforming Your Campus. https://www.transactcampus.com/home

Velev, D., Zlateva, P., Steshina, L. & Petukhov, I. (2019). Challenges of using drones and virtual/augmented reality for disaster risk management. The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Volume XLII3/W8, 337-339 Geoinformation for Disaster Management, Prague, Czech Republic.

Desimone, L. M. (2009). Improving impact studies of teachers' professional development: Toward better conceptualizations and measures. *Educational researcher, 38*(3), 181-199.

Dillenbourg, P. (2006). *Collaborative-learning: Cognitive and computational approaches*. Francis Printing Press.

Downes, S. (2007). Models for sustainable open educational resources. *Interdisciplinary Journal of Knowledge and Learning Objects, 3*(1), 29-44.

Dziuban, C., &Moskal, P. D. (2017). Evaluating the impact of course delivery strategy on student outcomes.*EDUCAUSE Center for Applied Research Bulletin, 3*(4), 1-11.

Edyburn, D. L. (2010). Would you recognize universal design for learning if you saw it? Ten propositions for new directions for the second decade of UDL.*Learning Disability Quarterly, 33*(1), 33-41.

Ertmer, P. A., Ottenbreit-Leftwich, A., Sadik, O., Sendurur, E., &Sendurur, P. (2012). Teacher beliefs and technology integration practices: A critical relationship. *Computers & Education, 59*(2), 423-435.

Fishman, B. J., Penuel, W. R., Allen, A. R., Cheng, B. H., &Sabelli, N. (2013). Design-based implementation research: An emerging model for transforming the relationship of research and practice. *Yearbook of the National Society for the Study of Education, 112*(2), 136-156.

Fullan, M., &Langworthy, M. (2014). *A rich seam: How new pedagogies find deep learning*. Pearson.

Garrison, D. R., &Kanuka, H. (2016). Blended learning: Uncovering its transformative potential in higher education. *The Internet and Higher Education, 7*(2), 95-105.

Garrison, D. R., & Vaughan, N. D. (2008). *Blended learning in higher education: Framework, principles, and guidelines.* John Wiley & Sons.

Garrison, D. R., Anderson, T., & Archer, W. (2018). Critical inquiry in a text-based environment: Computer conferencing in higher education. *The Internet and Higher Education, 2*(2-3), 87-105.

Gee, J. P. (2019). What video games have to teach us about learning and literacy? *Computers in Entertainment (CIE), 1*(1), 20-20.

Graham, C. R. (2018). Blended learning systems: Definition, current trends, and future directions. *Global Perspectives, 12*(3), 3-21.

Greenhow, C., Robelia, B., & Hughes, J. E. (2013). Learning, teaching, and scholarship in a digital age: Web 2.0 and classroom research: What path should we take now? *Educational Researcher, 38*(4), 246-259.

Guskey, T. R. (2010). What makes professional development effective? *Phi Delta Kappan, 84*(10), 748-750.

Hattie, J. (2009). *Visible learning: A synthesis of over 800 meta-analyses relating to achievement*. Routledge.

Hattie, J., &Timperley, H. (2007). The power of feedback. *Review of Educational Research, 77*(1), 81-112.

Hrastinski, S. (2008). Asynchronous and synchronous e-learning. *EDUCAUSE Quarterly, 31*(4), 51-55.

Jenkins, H. (2006). *Convergence Culture: Where old and new media collide.*NYU Press.

Kay, R., &Knaack, L. (2008). Evaluating the learning in learning objects. *Educational Technology, 48*(5), 3239.

Lankshear, C., &Knobel, M. (2006). *New literacies: Everyday practices and social learning*. Open University Press.

Laurillard, D. (2012). *Teaching as a design science: Building pedagogical patterns for learning and technology*. Routledge.

Means, B., Toyama, Y., Murphy, R., Bakia, M., & Jones, K. (2014). *Evaluation of evidence-based practices in online learning: A meta-analysis and review of online learning studies*. US Department of Education.

Oliver, M., & Herrington, J. (2015). Exploring technology-mediated learning from a pedagogical perspective. *Interactive Learning Environments, 11*(2), 111-126.

Picciano, A. G. (2017). Blending with purpose: The multimodal model. *Journal of Asynchronous Learning Networks, 13*(1), 7-18.

Picciano, A. G., &Dziuban, C. (2014). *Blended learning: Research perspectives*. The Sloan Consortium.

Reeves, D. B. (2016). *Bold school: Old school wisdom + new school technologies = blended learning that works*. Solution Tree Press.

Rheingold, H. (2014). *Net smart: How to thrive online.*MIT Press.

Richardson, W., & Dixon, B. (2017). *The global achievement gap: Why even our best schools don't teach the new survival skills our children need—and what we can do about it.* Hachette UK.

Rose, R. F., & Meyer, A. (2006).*A practical reader in universal design for learning*. Harvard Education Press.
Schleicher, A. (2018). *World class: How to build a 21st-century school system*. Jossey-Bass.

Selwyn, N. (2010). Apart from technology: Understanding people's non-use of information and communication technologies in everyday life. *Technology in Society, 25*(1), 99-116.

Sharples, M., Adams, A., Ferguson, R., Gaved, M., McAndrew, P., Rienties, B., & Whitelock, D. (2014). Innovating pedagogy 2014: Open university innovation report 3. Open University Innovation Report.

Trust, T., Krutka, D. G., & Carpenter, J. P. (2016). Together we are better: Professional learning networks for teachers. *Computers & Education, 102*(2), 15-34.

Turkle, S. (2011). *Alone together: Why we expect more from technology and less from each other.* Basic Books.

UNESCO. (2008). *Policy guidelines on inclusion in education*. United Nations Educational, Scientific and Cultural Organization.

Van den Heuvel, J., & van Bruggen, J. (2017). Toward personalized learning environments: Needs, infrastructure, and implementation. *TechTrends, 61*(5), 441-450.

Voogt, J., Knezek, G., Christensen, R., & Lai, K. W. (2017). Research on TPACK: Looking back and looking forward. *TechTrends, 61*(3), 260-267.

Vygotsky, L. S. (1978). *Mind in society: The development of higher psychological processes*. Harvard University Press.

Warschauer, M. (2007). *Technology and social Inclusion: Rethinking the digital divide.*MIT Press. Wiliam,
D. (2011). *Embedded formative assessment.* Solution Tree Press.