Special Issue
Journal of General Studies ESUT ISSN: 1115-6767, E-ISSN: 2971-6241 **Vol. 7 No. 1, 2025**

REIMAGINING CYBERSECURITY AND DIGITAL JUSTICE IN THE DIGITAL AGE: BRIDGING LAW, ETHICS AND TECHNOLOGY FOR A SECURE FUTURE

Being
The second Guest Paper Delivered at the 1st annual International Conference organized by the General Studies Division, Enugu State University of Science and Technology (ESUT), Agbani, Enugu. March 18-20, 2025

By

His Worship,

Dr. Nnesochi Nweze-Iloekwe

Enugu State Judiciary.

Abstract
The digital revolution has fundamentally altered how societies function, creating immense opportunities while exposing new vulnerabilities. The rapid expansion of the internet, artificial intelligence (AI), and blockchain technology has reshaped governance, commerce, and communication. However, as these technologies evolve, so too do cyber threats, which have become more sophisticated and widespread. In Nigeria, cybercrimes, ranging from financial fraud to AI-driven misinformation, digital election interference, cyberterrorism, and large-scale data breaches, has significantly impacted national security, economic stability, and democratic processes. Cybersecurity is not simply a technological concern; it is a legal, ethical, and societal issue that requires an interdisciplinary approach. Law plays a crucial role in regulating cyber activity, ethics provides guidance on responsible technology use, and science offers tools to combat emerging cyber threats. This paper explores how Nigeria can reimagine its cybersecurity framework by integrating legal, ethical, and scientific perspectives to create a secure and just digital ecosystem. It analyses Nigeria's existing cyber laws and policies in comparison to global frameworks such as the Budapest Convention (2001), Malabo Convention (2014), UN Cybercrime Convention (2024), and the ECOWAS Cybersecurity Strategy. Additionally, it examines the effectiveness of these frameworks in addressing contemporary cyber threats and how Nigeria can adapt them to its unique digital ecosystem. Furthermore, it examines how AI, blockchain, and digital forensics can be utilized to strengthen cybersecurity while protecting digital rights and human freedoms. Through case studies, expert analysis, and global best practices, this paper argues that cybersecurity should not merely be a matter of surveillance and control but should be human-centred, just, and accountable. It provides a roadmap for policymakers, educators, and technology leaders to build a cyber-resilient Nigeria that prioritizes security without compromising democracy, privacy, and human dignity.

Introduction
In today's interconnected world, where digital technologies are embedded into nearly every aspect of life, cybersecurity has become a critical issue for nations, businesses, and individuals alike. A decade ago, cybersecurity concerns revolved mainly around personal data breaches and financial fraud. Today, the landscape has shifted

dramatically, cybercrime now influences elections, economic stability, and even global peace and security. Cybercrime today extends beyond traditional hacking and now encompasses **state-sponsored cyber espionage, AI-generated disinformation, election hacking, and ransomware attacks on national infrastructure (Brynjolfsson & McAfee, 2021)**

Nigeria is experiencing a massive digital expansion, with millions gaining internet access and adopting digital services such as mobile banking, e-governance, and online education **(Nigeria's digital economy policy and strategy 2020- 2030)**. However, this rapid digitalization has also made Nigeria a prime target for cybercriminals. Reports from INTERPOL (2024) indicate that Nigeria is among the top countries in Africa for cyber fraud, with an estimated **₦200 billion** lost annually to cybercrime. Moreover, cyber threats in Nigeria are no longer limited to individual scams but now include AI-generated misinformation, cyberterrorism, and digital espionage targeting critical infrastructure.

A common misconception is that cybersecurity is purely a technical issue, requiring only stronger firewalls, better encryption, and more advanced threat detection systems. While these tools are necessary, they are not sufficient on their own. Cybersecurity is not just about **protecting data and financial assets**; it is about **safeguarding digital justice**, ensuring that every citizen has equal access to security, privacy, and rights in the digital space. However, the question remains: **How can Nigeria protect its digital infrastructure while ensuring that human rights and ethical considerations are upheld?** Cybersecurity is fundamentally about governance, law, ethics, and social responsibility. Digital security measures must not come at the expense of fundamental rights such as privacy, free speech, and democratic participation.

This paper argues that cybersecurity must be approached as a multidisciplinary challenge, where law, ethics, and technology work in harmony to create a safer digital environment. By analysing global cybersecurity conventions, Nigeria's current legal frameworks, and the potential of scientific advancements like AI-driven threat detection and blockchain security, this study outlines a human-centred approach to cybersecurity that ensures both safety and justice.

The Intersection of Cybersecurity, Humanities, and Sciences

Cybersecurity is not an isolated field but a domain where multiple disciplines intersect. Law and ethics shape the rules that govern digital interactions, while science and technology provide the tools to enforce these rules effectively. A failure to integrate these perspectives sometimes results in either overreach (where surveillance and security measures infringe on digital rights) or under reach (where weak cybersecurity frameworks leave citizens vulnerable to cyberattacks). Cybersecurity must be understood as an interdisciplinary field that incorporates law, ethics, social sciences, and international relations alongside technological innovations.

The Role of Law and Ethics in Cybersecurity

Laws provide the backbone for cybersecurity by defining what constitutes cybercrime, outlining enforcement mechanisms, and ensuring accountability. Legal frameworks provide the basis for prosecuting cybercriminals, protecting data privacy, and establishing digital rights. Legal framework such as the **General Data Protection Regulation (GDPR) in the EU and the Budapest Convention (2001)** provide **global standards for digital security, privacy rights, and cybercrime prosecution** (Council of Europe, 2022). In Nigeria, the Cybercrimes (Prohibition, Prevention, Etc.) Act (2015) serves as the primary legal framework for addressing cyber threats. However, the Act has notable limitations, as the rapid evolution of technology have outpaced the legislation, leading to gaps in legal protections. It does not adequately address emerging threats such as AI-driven misinformation, digital election interference, cross-border cybercrime, digital justice or the ethical use of surveillance tools and algorithmic discrimination (Okoro, 2022).

Ethics plays a critical role in shaping cybersecurity laws and policies. Who governs the machines? Should AI-driven cybersecurity systems have the authority to make decisions that impact human rights? Cybersecurity ethics encompasses the moral principles guiding the conduct of professionals in protecting data, systems, and networks from unauthorized access and attacks. Key principles include integrity, accountability, privacy, fairness, and societal well-being. Ethical frameworks help address these dilemmas by ensuring that cybersecurity measures align with democratic values and human dignity.

A well-intentioned security measure, such as internet surveillance to prevent terrorism, can quickly become an instrument of mass digital surveillance, infringing on privacy rights if left unchecked. Furthermore, ethical questions arise in areas like AI bias, algorithmic justice, and responsible data collection. A human-centred approach to cybersecurity ensures that policies protect citizens without enabling authoritarian control over digital spaces. Key ethical concerns in cybersecurity include:

- **The balance between security and privacy** (Solove, 2022).
- **Ethical considerations in AI-driven surveillance and hacking**.
- **Algorithmic bias and its impact on digital justice** (O'Neil, 2016).

Scientific and Technological Innovations in Cybersecurity

Scientific and technological advancements are crucial for strengthening cybersecurity. For instance, AI-powered threat detection systems can analyse vast amounts of data to identify cyberattacks before they happen. Blockchain technology, known for its decentralized security model, can be used to protect financial transactions and digital identities. Digital forensics, which involves the investigation of cybercrimes through data analysis, is essential for law enforcement agencies in tracking cybercriminals. Emerging technologies such as AI, machine learning, and blockchain have reshaped cybersecurity:

- **AI-driven cybersecurity** can detect threats in real-time (Johnson, 2023).
- **Blockchain enhances transparency in financial transactions** (Nwankwo, 2023).
- **Digital forensics aids in cybercrime investigations** (Vincent, 2023).

However, technology is a double-edged sword. AI is not only used for cyber defense but also for cybercrime, criminals now leverage AI-generated deep fakes to commit fraud, spread disinformation, and manipulate elections. The proliferation of AI-based cybersecurity solutions raises concerns about potential algorithm biases, ethical implications, and the necessity for robust regulatory frameworks to oversee their deployment. This underscores the need for a balanced approach that regulates technology while fostering innovation. This is why **a balanced approach is needed,** governments and organizations must regulate AI to **prevent misuse,** while still encouraging **innovation in cybersecurity** to stay ahead of cybercriminals.

Bridging the Gap: A Holistic Approach to Cybersecurity Governance

The most effective cybersecurity strategies do not treat law, ethics, and technology as separate domains but rather as complementary elements of a single framework. A robust cybersecurity framework must integrate legal and ethical considerations with technological advancements Governments must ensure that cybersecurity policies align with legal and ethical standards while integrating the best available technology. This means:

1. Crafting cybersecurity laws that protect citizens from cyber threats while safeguarding their digital rights.
2. This requires interdisciplinary education and training programs that equip legal professionals with technical knowledge and cybersecurity experts with an understanding of law and ethics.
3. Encouraging ethical AI development to ensure fairness, accountability, and transparency.
4. Leveraging scientific innovations to improve security measures while preventing misuse of technology. Organisations and governments digitize their activities, they become more susceptible to cyber threats, necessitating advanced AI solutions to analyse extensive data, identify anomalies, and proactively defend against malicious actions. Cybersecurity should not be weaponized against citizens but should serve as a tool for fostering a safer, freer, and more just digital society.

Governments, businesses, and civil society must work together to develop policies that are both technologically sound and legally enforceable.

Emerging Cybersecurity Threats and Their Societal Impact

In recent years, Cyber threats are evolving rapidly, and Nigeria must stay ahead of them. As Nigeria's digital economy continues to grow, so does the complexity of its cybersecurity landscape. In 2024 alone, cybercriminals stole over **₦200 billion ($250 million) through digital fraud schemes (Premium Times, 2024).** The year

2024 marked a pivotal shift in the global cybersecurity landscape, as escalating cyber threats pushed organisations to near breaking point. As predicted in the 2024 Nigeria Cybersecurity Outlook, ransomware attacks reached unprecedented levels, phishing scams grew more sophisticated, and insider threats surged amidst economic downturns **(Delliote 2024).** The rapid adoption of AI by both defenders and attackers further intensified this battle, elevating cybercrime to a formidable challenge that demanded constant vigilance and innovation. The increasing sophistication of cybercriminals has left no sector immune, highlighting the urgent need for proactive security measures. Some of the most pressing cyber risks today include:

1. **AI-Powered Cybercrime** – The adoption of Artificial Intelligence (AI) is revolutionizing the cybersecurity landscape, with AI-powered defense tools becoming indispensable in the fight against increasingly complex threats. Organisations are leveraging AI tools to enhance threat detection, automate incident response, and analyse patterns to identify risks early. These AI-driven solutions enable businesses to respond quickly and effectively, improving resilience by detecting anomalies, predicting potential attacks, and mitigating threats before they escalate (Delliote report 2025).

   On the flip side, the same technology is empowering cybercriminals. AI-powered attacks are making cyber threats more sophisticated, automated, and precise. Malicious actors are using AI to automate phishing campaigns, create polymorphic malware that evade detection, and craft hyper-realistic deep fakes.

   This dual-use of AI creates a paradox. While it bolsters defense capabilities, it also amplifies the scale and precision of cyberattacks, moving them closer to pandemic-like proportions. In 2025, the race between AI-powered cyberattacks and AI-driven defense is expected to intensify, highlighting the urgent need for continuous adaptation and innovation. Organisations must embrace AI not only as a defensive measure but as an integral part of their broader cybersecurity strategy to stay ahead of increasingly sophisticated adversaries. Example of AI powered cybercrime is deep fake technology, which is being used to impersonate political leaders, commit fraud, and spread disinformation. (Vincent, 2023)

   Cyberterrorism and Digital Radicalization – Terrorist organizations like Boko Haram, ISWAP use encrypted messaging platforms to recruit and organize attacks online (Onuoha, 2020).

3. **Election Interference, misinformation and disinformation** – Cyber-enabled disinformation campaigns have become a major threat to democratic institutions. A prominent example is the Cambridge Analytica Scandal (2018), where personal data from 87 million Facebook users was misused to influence elections in the U.S. and U.K. (Cadwalladr, 2018). Similarly, the Russian Interference in the 2016 U.S. Elections demonstrated how state-sponsored hackers exploited social media and

email leaks to manipulate voter behaviour (Mueller, 2019). Nigeria is not immune to such threats. In the 2023 Nigerian elections, cybercriminals attempted to breach the Independent National Electoral Commission (INEC) database, raising concerns about electoral integrity (BBC News, 2023). Strengthening digital election laws and implementing anti-disinformation policies is crucial to safeguarding Nigeria's democracy.

4. **Cryptocurrency and Blockchain Attack**- Nowadays, cryptocurrency and blockchain attacks are the primary security threats for those businesses that deal in a high stage compared to average everyday users. Cryptocurrency is associated with high technological companies however; it has not reached the advanced secure stage. That's why it's caught by several cyberattacks such as; Sybil, DDOS, Eclipse, etc. Those organizations associated with this technology must be aware of all the cybersecurity challenges and make sure no gap is left for attackers to exploit your organization's data. There is also **Crypto jacking** where there is unauthorized use of computing resources to mine cryptocurrencies.

5. **Insider Attacks**- Most of the time, cybersecurity challenges are external for a business's firm or organization; still, there can be instances of inside jobs or attacks. Sometimes, employees having bad intuitions and malicious intent for their organization can leak private information about your data or sell it to your competitors or individuals. Thus, an insider can lead your organization to a significant financial and reputational crisis. Thus, monitoring inbound and outbound traffic and centralized servers to limit access based on jobs is quite challenging to minimize cybersecurity risk.

6. **BYOD Policies**- Currently, many organizations follow the BYOD policy (Bring Your Device Policy). This policy demands employees to bring their own devices to perform their jobs. Getting personal devices to a professional firm gives an invitation to hackers for cyber-attacks. Most of the time, these devices are outdated and easily accessible to hackers for accessing the business's confidential information. Through these devices, it is easy for hackers to access a private network, with a lack of cybersecurity. You need to pay special attention to these challenges, leave the BYOD policies behind, and provide secure devices to your organization's employees.

7. **IoT (Internet of Things) Attacks**- What is the role of IoT devices? IoT devices are mainly digital or computing devices that are used to transmit data over the network. For example, mobile phones, smart security devices, desktops, laptops, etc. As IoT devices' usage has been increasing day by day, the rate of IoT cybersecurity risk is also increasing. IoT cybersecurity has become one of the biggest challenges that open the door for malicious attacks. With billions of IoT devices connected globally, security risks increase. IoT devices often lack strong security measures, making them targets for cybercriminals **(Weber, 2023).**

8. **Cloud Attacks**-Nowadays, cloud computing or cloud services are highly in demand for both professional and personal use. Many of us love to store our data on cloud storage. Of course, cloud service is effective and beneficial for storing a huge amount of data, along with hacking of cloud platforms is a major cybersecurity challenge.

9. **Quantum Computing and Cybersecurity -** Quantum computing poses a significant risk to cryptographic security. Traditional encryption methods may become obsolete once quantum computers achieve practical capabilities (Shor, 2023).

There are incidences these cyberattacks have played out recently.

- **Genea Fertility Clinic Breach (2025):** Genea, a leading fertility clinic in Australia, suffered a ransomware attack by the Termite group, resulting in the theft and dark web publication of 940GB of sensitive patient data
- **Texas Tech University Health Sciences Center Attack (September 2024):** A ransomware attack compromised personal and health information of over 1.4 million individuals, including Social Security numbers and medical records
- **U.S. Telecommunications Espionage (2024):** Chinese-affiliated threat actors, notably the Salt Typhoon group, infiltrated major U.S. telecommunications providers like AT&T and Verizon. They accessed customer call records and private communications, including those of political figures such as former President Donald Trump and Vice-President-elect J.D. Vance
- **Social media platform X (March 2025)** suffered Multiple outages as a result of a massive cyberattack on March 10th 2025. X formerly known as Twitter get attacked every day, but this was done with a lot of resources. Elon Musk reported via his page on X, that either a large, coordinated group and/or a country is involved, and they suggested that the attack may have been linked to Ukraine. The massive cyber-attack tried to bring down the X system with IP addresses originating in the Ukraine area.
- **Open AI's Generative AI Targeted (2024):** State-sponsored groups from Russia, China, and Iran attempted to exploit Open AI's large language models for malicious purposes, including spear-phishing and malware development
- In the 2023 Lagos Cyber Fraud Crackdown, authorities uncovered a ₦500 million cryptocurrency scam, leading to multiple arrests and policy discussions on crypto regulation.
- The Colonial Pipeline Ransomware Attack 2021, U.S.A. UK was a target of state-sponsored cyber espionage. China has implemented strict cybersecurity laws with heavy state surveillance, whereas Russia has been accused of cyber warfare and election interference. Understanding these case studies provides valuable lessons for developing effective cybersecurity policies. These incidents underscore the evolving nature of cyber threats, emphasizing the need for robust cybersecurity measures across all sectors. These cyber threats

affect more than just individual users; they undermine democracy, national security, and economic stability. Without a strong cybersecurity strategy, Nigeria risks becoming a hub for cybercrime that destabilizes institutions and erodes public trust.

- Cyber-enabled disinformation campaigns have become a major threat to democratic institutions. A prominent example is the Cambridge Analytica Scandal (2018), where personal data from 87 million Facebook users was misused to influence elections in the U.S. and U.K. (Cadwalladr, 2018)[80]. Similarly, the Russian Interference in the 2016 U.S. Elections demonstrated how state-sponsored hackers exploited social media and email leaks to manipulate voter behaviour (Mueller, 2019). Nigeria is not immune to such threats. In the 2023 Nigerian elections, cybercriminals attempted to breach the Independent National Electoral Commission (INEC) database, raising concerns about electoral integrity (BBC News, 2023). Strengthening digital election laws and implementing anti-disinformation policies is crucial to safeguarding Nigeria's democracy.

Global and Regional Cybersecurity Conventions and Nigeria's Position

The rise of cyber threats has pushed nations and regional blocs to develop comprehensive legal frameworks and strategies to combat cybercrime and protect digital rights. Cybersecurity governance requires international cooperation because cyber threats transcend national borders, making unilateral solutions ineffective. Several global and regional treaties shape cybersecurity policies. Nigeria, like many developing nations, has faced challenges in adapting to global cybersecurity trends and aligning its legal and institutional frameworks with international standards. Nigeria must align its cybersecurity strategy with global best practices.

International Treaties and Agreements

Budapest Convention (2001): The **Convention on Cybercrime**, commonly known as the Budapest Convention, is the first and most comprehensive international treaty addressing cybercrime. Drafted by the Council of Europe and open to non-European countries, the convention sets legal standards for defining cybercrimes, harmonizing national laws, improving investigative techniques, improving cross-border cooperation, and ensuring procedural safeguards in digital investigations **(Council of Europe, 2001).** This convention is the first international treaty seeking to address internet and computer crime by and increasing cooperation among nations.

The treaty provides guidelines for criminalizing offenses such as hacking, identity theft, child exploitation, and cyber fraud. Although widely adopted, some countries, including China and Russia, have criticized it for being Western-centric and have opted for alternative frameworks. While Nigeria is not a signatory, the convention serves as a benchmark for developing cybercrime legislation.

[80]The Cambridge Analytica case led to a £500,000 fine by the U.K.'s Information Commissioner's Office (ICO) and stricter EU GDPR regulations on data protection (ICO, 2018).

UN Cybercrime Convention (2024): Recognizing the limitations of the Budapest Convention in achieving global consensus, the United Nations initiated the **Cybercrime Convention (2024)**, which aims to provide a more inclusive and universally accepted framework. A more recent effort to address emerging cyber threats with a global consensus. This treaty emphasizes digital sovereignty, recognizing that nations have different legal systems and priorities regarding cybersecurity.

It also expands on newer challenges such as AI-powered cybercrime, data privacy, and digital human rights protections **(United Nations, 2024**). This convention emphasizes global cooperation, capacity building, and respect for human rights in combating cybercrime. Nigeria's involvement underscores its commitment to international cybersecurity norms.

Shanghai Cooperation Organization Cybersecurity Treaty: This treaty focuses on information security and combating the use of information technologies for purposes detrimental to member states' interests. This agreement prioritizes state control over cyberspace, emphasizing cyber sovereignty and national security over individual digital right. Although Nigeria is not a member, understanding this treaty provides insights into alternative approaches to cybersecurity governance. Countries that oppose Western-led cybersecurity governance frameworks, including China and Russia, have supported the **Shanghai Cooperation Organization (SCO) Cybersecurity Treaty**. While criticized for its restrictive approach, it underscores the global divide in cybersecurity governance and the need for Nigeria to navigate these differing legal frameworks strategically (Kaspersky, 2023).

Regional Cybersecurity Strategies in Africa

Malabo Convention (2014): Officially known as the African Union Convention on Cyber Security and Personal Data Protection, it aims to establish a legal framework for cybersecurity, electronic transactions, and personal data protection in Africa. It further aims to harmonize laws across African nations, promoting stronger legal responses to cybercrime, privacy protection, and digital commerce security (African Union, 2014). It is Africa's response to cybersecurity, emphasizing digital sovereignty and data protection. Nigeria has signed but not yet ratified the convention, indicating a need for further legislative action.

ECOWAS Cybersecurity Strategy (2022): The Economic Community of West African States adopted this strategy to strengthen regional cybersecurity measures, promote cooperation among member states, and protect critical infrastructure. They developed a regional cybersecurity strategy to strengthen collaboration among West African nations. This strategy emphasizes cross-border cooperation, intelligence sharing, and capacity building for law enforcement agencies in tackling cyber threats (ECOWAS, 2022). Nigeria's active participation aligns with its regional leadership role. Nigeria, as the largest economy in West Africa, plays a critical role in

implementing this strategy, yet significant gaps remain in enforcement and policy execution.

African Union's Digital Transformation Strategy (2020–2030): This strategy envisions an integrated and inclusive digital society and economy in Africa, driven by harmonized policies and regulations, digital infrastructure, and skilled human capacity. It seeks to integrate cybersecurity within the broader agenda of Africa's digital economic growth. The strategy promotes investments in digital infrastructure, cybersecurity skills development, and ethical AI governance. African Union, (2020). Cybersecurity is a foundational pillar, emphasizing the need for robust legal and regulatory frameworks. Nigeria's alignment with this strategy can help bolster its cybersecurity resilience while fostering digital economic expansion.

Challenges in Current Legal Systems in Nigeria

As discussed earlier, in Nigeria, the Cybercrimes (Prohibition, Prevention, Etc.) Act (2015) serves as the primary legal framework for addressing cyber threats. There are gaps in legislation concerning emerging technologies. While this law criminalizes cyber offenses such as hacking, identity theft, and cyberstalking, it has several shortcomings:

- It does not adequately address emerging threats such as AI-generated deep-fakes, election interference, and state-sponsored cyber espionage.
- There are concerns about its misuse to suppress digital freedoms, as seen in cases where authorities have used cyber laws to arrest journalists and activists.

In **UBA v Sunday Ogeh (2018)**, a Nigerian cyber fraudster was prosecuted for using phishing techniques to steal customer's banking details, defrauding them of millions of naira. The defendant, Sunday Ogeh, was arrested by the Economic and Financial Crimes Commission (EFCC) for operating a phishing scheme. He impersonated UBA bank officials, sending fraudulent emails and SMS messages to customers requesting their banking details. Many unsuspecting victims provided their PINs, BVNs, and passwords, allowing the fraudster to siphon millions of naira. The EFCC prosecuted him under Section 14(2) of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, which criminalizes online fraud.

The **Cybercrimes Act (2015)** was sufficient to convict Ogeh, but it does **not explicitly address AI-generated phishing scams**. This case highlighted the limitations of Nigeria's cybercrimes Act (2015), which lacks specific provisions for advanced cyber fraud techniques such as deep-fake enabled scams and AI- driven financial fraud. The case exposed banking sector vulnerabilities, as customers were not educated about phishing risks. Unlike the EU's PSD2 (Payment Services Directive 2), which mandates strong customer authentication (SCA), Nigeria lacks strict financial cybersecurity regulations.

Furthermore, Ogeh reportedly worked with an international cybercrime syndicate, but Nigeria's extradition and cybercrime cooperation mechanisms remain weak. Nigeria has not ratified the Budapest Convention (2001), which facilitates international cooperation on cybercrime investigations.

The rapid pace of technological innovation often outstrips existing legal frameworks, leading to regulatory gaps. As discussed above, the rise of AI technologies has introduced new challenges in data privacy and security that current laws may not adequately address. Legal professionals must adapt by acquiring technological competence to effectively navigate the complexities of the digital landscape. This includes understanding cybersecurity measures and their implications for legal practices.

Reimagining Cybersecurity and Digital Justice in Nigeria – Bridging Law, Ethics, and Technology for a more digital future.

Nigeria's growing digital economy and increasing cyber dependency necessitate a reimagination of its cybersecurity approach. Cyber threats in Nigeria have evolved from financial fraud (e.g., "Yahoo Yahoo" cyber scams) to sophisticated attacks targeting critical infrastructure, government systems, and businesses. Addressing these challenges requires a strategic integration of law, ethics, and technology. To effectively address cybersecurity challenges, Nigeria must adopt a multidisciplinary approach that integrates legal reforms, ethical considerations, and scientific advancements.

AI and Ethics: Who Governs the Machines?

The proliferation of artificial intelligence in various sectors necessitates ethical guidelines to prevent misuse. AI-driven cybersecurity tools, such as predictive threat analysis and automated response systems, are powerful for threat detection but may also pose risks related to bias, privacy violations, and ethical misuse. For instance, facial recognition technology used for security surveillance has been found to disproportionately misidentify individuals from minority groups, leading to wrongful accusations **Buolamwini & Gebru, (2018).**

A critical question in Nigeria's cybersecurity strategy is: who governs AI? **Who ensures they are used ethically?** If AI-driven systems make decisions that impact fundamental rights, such as online surveillance or censorship, who ensures accountability? Establishing AI ethics committees and developing national AI ethics guidelines can ensure responsible AI development and deployment. There is need for **AI ethics guidelines** to prevent bias in cybercrime investigations and surveillance. Nigeria must establish a national AI Ethics Board that oversees the responsible use of AI in cybersecurity, ensuring that automated decision-making aligns with human rights principles. Clear guidelines are needed for the ethical use of AI in cybersecurity, ensuring that automated systems do not perpetuate bias or infringe on digital rights.

Reimagining legal reforms and Digital Justice

There is need in updating existing laws to address new cyber threats. The proliferation of AI-generated deep-fakes has posed significant legal challenges, with existing laws struggling to address issues of consent and defamation effectively. This is highly pivotal and crucial. This includes enacting comprehensive data protection laws, aligning national legislation with international conventions, and ensuring that laws protect citizens' digital rights without stifling innovation. For instance, **updating Nigeria's Cybercrimes Act** to reflect modern challenges/emerging threats (AI driven fraud, digital privacy, misinformation and algorithmic bias), **strengthening data protection laws** to align with the **General Data Protection Regulation (GDPR)** and **Malabo Convention, ensuring accountability in digital forensics**, protecting citizen rights while investigating cybercrimes. Furthermore, legal professionals must adapt by acquiring technological competence. This includes understanding e-discovery technologies to preserve relevant digital information and protect privileged data, thereby aligning legal practices with ethical standards.

Furthermore**,** enhancing access to Justice is essential in promoting digital justice. This can be achieved through-

- Online Dispute Resolution (ODR): Implementing platforms that allow individuals to resolve disputes without physical court appearances can make justice more accessible, especially for those in remote areas.
- Digital Legal Assistance: Deploying AI-powered chatbots and virtual assistants can provide immediate legal information and guidance, helping users understand their rights and navigate legal procedures.
- Mobile Justice Apps: Developing applications that offer legal resources, document templates, and court information can empower individuals to handle minor legal matters independently.

Another pertinent issue that must be addressed is the issue of **Challenges in Cybercrime prosecution.** The rapid evolution of cyber threats has outpaced legal frameworks and made it challenging in cybercrime prosecution. Some key legal challenges include:

- **Jurisdiction Issues**: Cybercrimes often cross-national borders, making law enforcement difficult UNODC (2023). The borderless nature of the internet means that cybercrimes can affect multiple countries simultaneously, leading to complexities in determining which nation has the authority to prosecute. This often results in delays and difficulties in bringing offenders to justice.
- **Regulatory Gaps**: Emerging threats like AI-driven cyber-attacks lack comprehensive legal oversight Zuboff, (2022).
- **Issue of identity of cybercriminals:** Cybercriminals often use sophisticated methods to conceal their identities, such as VPNs, proxy servers, and encryption, making it difficult for law enforcement to trace and identify perpetrators.

- **Extradition Challenges**: Extraditing cybercriminals is complicated by varying legal standards, lack of treaties between countries, and differing penalties for cybercrimes. These factors can hinder the ability to bring offenders to justice across borders.

To ensure digital justice, Nigeria needs legal reforms that:

- Establish clearer guidelines on digital rights, including data protection and freedom of expression online.
- Strengthen penalties for cyber offenses while ensuring due process protections.
- Align with international treaties such as the **Malabo Convention** to facilitate global cooperation.

Capacity Building for Cybersecurity Resilience

For Nigeria to effectively combat cyber threats, it must invest in **human capital, institutional development, and technical training** across multiple sectors.

Strengthening Law Enforcement and Judicial Capacity

Training for law enforcement agencies on cybercrime investigation, AI forensics, and ethical hacking. **Judicial capacity building**, ensuring that judges and legal professionals understand digital evidence and international cyber laws. **Establishment of specialized Cybercrime Units** in the **Nigeria Police Force, EFCC (Economic and Financial Crimes Commission), and DSS (Department of State Services).**

Integrating cybersecurity into university curricula across law, computer science, and public **policy** programs**.** Educational institutions also play a vital role by incorporating cyber law courses that cover real-time threat assessment, response strategies, and the ethical implications of emerging technologies. This equips future professionals with the necessary skills to navigate the complex landscape of digital ethics and cybersecurity. A skilled workforce is essential for national cybersecurity resilience. Universities and technical institutes must incorporate interdisciplinary cybersecurity training. **Public-private partnerships** to create internship programs and cybersecurity certifications**. Collaboration with international cybersecurity institutions** (For instance**, Interpol, the European Union Agency for Cybersecurity (ENISA), and the U.S. Cybersecurity and Infrastructure Security Agency (CISA**) for training and best practices.

Furthermore, educating the public about digital tools and platforms ensures that technological advancements in justice are accessible to all, preventing a new form of digital divide. Also developing legal technologies with input from diverse communities ensures they meet varied needs and do not inadvertently exclude or disadvantage certain groups. Additionally, involving communities in the development

and implementation of digital justice initiatives fosters trust and ensures the solutions are culturally and contextually appropriate.

Raising Public Awareness on Cyber Threats

There is need for nationwide cybersecurity awareness campaigns to educate citizens on phishing, financial fraud, and data protection. **Cyber hygiene programs for government agencies and businesses** to reduce vulnerabilities. Also **creating local-language cybersecurity content** for better outreach in rural areas will help.

Public-Private Partnerships and Global Cooperation in Cybersecurity

Cybersecurity is not solely the responsibility of governments; private sector actors, including banks, telecom companies, and tech startups, play a crucial role**.** Nigeria must foster public-private partnerships where companies collaborate with government agencies to share threat intelligence and best practices. **Encouraging collaboration between government agencies, banks, and tech companies** to build robust security frameworks, and enhance Nigeria's cybersecurity capabilities. Also **Signing international cybersecurity cooperation agreements** for intelligence sharing and cyber defense, will help. Also Involving diverse stakeholders, including technologists, legal experts, and ethicists, in policy-making ensures that multiple perspectives are considered, leading to more comprehensive and effective regulations.

Nigeria must strengthen global cooperation by engaging in cybersecurity diplomacy. This includes:

- Strengthening ties with INTERPOL and regional cybersecurity organizations to combat transnational cybercrime.
- Participating actively in global cybersecurity forums to shape digital policies that reflect Nigeria's interests.
- Encouraging bilateral agreements with nations that have advanced cybersecurity frameworks, such as the United States, the UK, and China.

Conclusion and Policy Recommendations

From our discussion, we have been able to ascertain that Cybersecurity is not just a technical issue; it is a legal, ethical, and human rights issue. The future of cybersecurity in Nigeria depends on its ability to strike a balance between security, technological innovation, and human rights. The government must strengthen cybersecurity laws, invest in ethical AI development, and promote international collaboration, enhance capacity building for ensuring that law enforcement, judiciary, businesses, and the public can combat cyber threats effectively. Nigeria must align with global cybersecurity standards while tailoring solutions to local challenges. Nigeria must update its Cybercrimes Act to include AI and digital privacy protections. By embracing a multidisciplinary approach, Nigeria can secure its digital future without compromising justice, ethics, and human rights. By bridging the worlds of law, ethics, and technology, Nigeria can create a digital ecosystem that is both secure

and just, ensuring that its citizens remain protected without sacrificing their fundamental freedoms.

Policy and Legislative Recommendations for Nigeria

1. Institutional Reforms

Expand Cybersecurity Training for Law Enforcement and Judiciary

- Introduce mandatory digital forensics and cybercrime cour**ses** for law enforcement agencies and judicial officers.
- Create a National Cybercrime Academy to train security agencies and policymakers.
- Establishing cybercrime -specific court divisions like in the US.
- **Establish a National AI Ethics Board** to regulate the ethical use of AI in cybersecurity operations.

Incorporate Cybersecurity Education in Universities and Technical Institutes

- Establish cybersecurity research labs in leading Nigerian universities.
- Partner with global institutions for joint cybersecurity degree programs and certifications.

Develop a National Cybersecurity Awareness Campaign

- Implement nationwide cyber hygiene programs for citizens.
- Encourage banks, fintech companies, and telecom providers to run cybersecurity awareness programs for customers

2 **Legal and Policy Reforms**

- **Revise the Cybercrimes Act (2015)** to address emerging cyber threats and ensure digital rights protections.
- Pass a Cryptocurrency Regulation Bill to address digital fraud.
- Strengthen penalties for cyber offenses while ensuring human rights protections.

3 **Strengthen Public-Private Partnerships**

- Establish Cybersecurity Innovation Hubs where government, industry, and academia can collaborate on security solutions.
- Develop cyber risk frameworks for financial institutions to prevent large-scale fraud.

4. Enhance International Cybersecurity Cooperation

- Sign bilateral agreements with countries leading in cybersecurity (e.g., U.S., UK, EU, Israel, South Korea).
- Ratification of global cybersecurity treaties, which will strengthen cybercrime prosecution, close legal gaps on emerging treats, boast Nigeria's digital economy and global credibility.
- Join Interpol's Cybercrime Task Force to improve intelligence sharing and cross-border cybercrime prosecution.

Final Thoughts on the Future of Cybersecurity and Digital Justice in Nigeria

To build a secure digital future, Nigeria must invest in human capital development**,** international cooperation, and legal reforms. Cybersecurity is not just about preventing cyberattacks, it is about creating a fair, just**,** and resilient digital society where security, privacy, and human rights are upheld. Nigeria must take proactive steps in fostering a cyber-resilient society, ensuring that security measures do not infringe upon digital rights and freedoms.

References

African Union. (2014). *Malabo Convention on Cyber Security and Data Protection.*

Benjamin, R. (2021). *Race after technology: Abolitionist tools for the new Jim Code.* Polity.

Buolamwini, J., & Gebru, T. (2018). *Gender shades: Intersectional accuracy disparities in commercial gender classification.* MIT Media Lab.

Buolamwini, J., & Gebru, T. (2020). *Gender shades: Intersectional accuracy disparities in commercial gender classification.* MIT Media Lab.

Chesney, R., & Citron, D. K. (2023). *Deepfakes and the new disinformation war: The coming age of AI-powered misinformation. Foreign Affairs.*

Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention).*

Council of Europe. (2023). *Budapest Convention on Cybercrime.* Retrieved from www.coe.int

ECOWAS. (2022). *Regional Cybersecurity Strategy Report.*

European Commission. (2024). *General Data Protection Regulation (GDPR).* Retrieved from www.europa.eu

How data strategy and sophisticated training are integral to the future of GenAI in the legal industry. (2025, February 26). Retrieved from Reuters.com

Kirchschläger, P. (2024). *Digital ethics: How technology shapes society and values.* Springer.

Menlo Report. (n.d.). Retrieved from en.wikipedia.org

Moor, J. H. (2023). *The ethics of privacy and data protection in the digital age.* Oxford University Press.

More spyware, fewer rules: What Trump's return means for US cybersecurity. (2024, December 1). Retrieved from Wired.com

Nissenbaum, H. (2023). *Privacy in context: Technology, policy, and the integrity of social life.* Stanford University Press.

Ojedokun, U. (2023). *Cybercrimes Act of Nigeria: Challenges and prospects. Nigerian Law Review.*

Peter Kirchschläger: "Big Tech firms have consistently shown little concern about harming people and violating their rights." (2024, September 24). Retrieved from Lemonde.fr

Practical cybersecurity ethics: Mapping CyBOK to ethical concerns. (n.d.). Retrieved from dl.acm.org

Solove, D. J. (2022). *Nothing to hide: The false tradeoff between privacy and security.* Yale University Press.

UNODC. (2023). *International cooperation on cybersecurity matters.* United Nations Office on Drugs and Crime.

United Nations. (2024). *Cybercrime Convention.*

Weber, R. H. (2023). *Internet of Things: Legal challenges and cybersecurity risks.* Routledge.

Zuboff, S. (2022). *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* Public Affairs.

Cybersecurity ethics: Everything you need to know. (n.d.). Retrieved from ollusa.edu
AI, growing data risks expand the role of chief privacy officer. (2024, October 1). Retrieved from WSJ.com