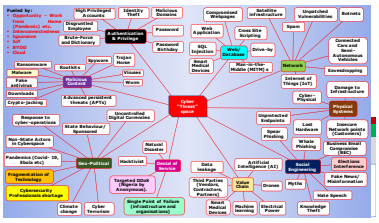
National Cybersecurity Policy and Strategy (NCPS) 2021: FAKENEWS: from Social Media to Social Menace

Body of Computer Cadres in the Unified Local Governments of Lagos State (BCLG) 2021 Public Discourse (Virtual)

On the 23 February 2021, President Buhari launched the Nigeria National Cybersecurity Policy and Strategy (NCPS) 2021[1]. launched by President Buhari on 23 February 2021. It was developed by a multi-stakeholder team that represented the perspectives of Civil Society, Academia, the Private and Public sectors. Significant and detailed work was carried out by the multi-stakeholder Committee, Secretariat and the unsung heroes and heroines who all ensured that this task was completed on time and within budget. The team is grateful for the leadership of the National Security Adviser, Major General Babagana Monguno (retired) for making this happen. Furthermore, the team thanks His Excellency, President Muhammadu Buhari for the confidence entrusted in us and this unique opportunity to serve.



While digital technologies expand the possibilities for people to enjoy freedoms and the right to access information and knowledge, and the opportunity to enhance their well-being, we must appreciate that **Cyber "Threat" space** continues to expand and reacting to emerging threats such as cybercrime and cyber-terrorism has become an imperative of all levels of governments worldwide. Governments around the world, and other stakeholders, have generally understood that addressing cyber malfeasance requires global multi-stakeholder collaboration, as one weak link potentially undermines global value chains. It is thus imperative, that Africa, its nations, organisations, institutions, and peoples are not the weak link. That said, cybersecurity is principally about risk management and it is also about people, especially the next generation and the next one billion, mainly from the global south, including Africa including at the local government level, who are getting connected as we speak.

Cyber-platforms are agnostic in that they can be used positively or negatively. Despite the multiple benefits of cyberspace, we must appreciate that it has weaknesses and provides opportunities good and bad actors. For example, the scourge of Fake News and Hate Speech:

1. **Undermines the individual's right to truth**: Thus, undermines the foundations of the liberal democracy we are building.
2. **Fosters distrust of institutions**: Keep the people from meaningfully engaging.
3. **Increases social polarization**: Thereby exacerbates various social, political, religious and other divides.
4. **Goes against the fundamental religious doctrines**: All Religions abhor rumours and false accusation, and it usually constitutes the SIN of slander.
5. **Maligns and undermines constituted authority**: Leading to breakdown of law and order and subsequently loss of trust by external parties e.g., investors.

The International Technology platforms have become too powerful. They are global sensors of our information, perspectives and opinions thus bypassing traditional government censors and undermining related government institutions and using the doctrines, principles, and standards, of other societies to determine what information can and cannot be shared. In effect we have exchanged government censorship for censorship by foreign companies that are primarily beholden to their shareholders.

It is possible to any Hack the Military using cyberspace, which presents significant national security challenges that require eternal vigilance. However, social media can be used to Hack those who elect the Commander-in-Chief, which is a worse social menace, with more dire consequences, than only hacking the Military.

The mitigating "#FakeNews" and "#HateSpeech" requires that we:

1. Identify sources of "#FakeNews" and "#HateSpeech" through early warning systems that Categorize, monitor, and Legally take down Fake Social Media Accounts.
2. Discrediting, Discouraging, Derailing or Diminishing the Sources by promoting factual narratives from credible sources, reach out to sources, or key propagators and leverage unlikely avenues for refuting rumours.
3. Drowning "#FakeNews" and "#HateSpeech" with positive counter-narratives, encourage citizens to question "Fake News" and "Hate Speech"; Credible validation website e.g., Factcheck.org and Snopes.com plus Rumour Control Webpages e.g., US-FEMA and Sebenarnya.my.
4. As a last resort engage in Offensive Security Operations as needed in addition to society-wide Social Media Coordination/ Responsiveness.

[1] https://cert.gov.ng/ngcert/resources/NATIONAL_CYBERSECURITY_POLICY_AND_STRATEGY_2021.pdf

We must consider, "**Who Else Is Using Cyberspace?**" Players: Boko Haram, ISIS, FARC, Aum Shinrikyo: **Values, Propaganda, Financing and Recruitment**. Even the Pentagon Manipulates Social Media for Propaganda Purposes[2].

1. Using Cyberspace as:
   a. **Tool**: Develop and disseminate propaganda
   b. **Medium**: Illicit activities financial, mobilization planning and coordination
   c. **Target**: Take down infrastructure, Finance systems, Government services
2. Who is addressing the threat actors:
   a. **National**: E.g., Nigeria collaboration lead by the NSA with sectoral CERTs/CSIRTs.
   b. **Sub-Regional**: E.g., Economic Community of West African States (ECOWAS) Organised Crime: West African Response on Cyber security and fight against Cybercrime' (OCWAR-C) project
   c. **Continental**: E.g., African Union Cybersecurity Experts Group (AUCSEG).
   d. **Multilateral**: E.g., Forum of Incident Responders Security Teams (FIRST).
   e. **Global**: E.G., United Nations.

However, the good actors need a direction, plan and means of getting the right things done at the right time, hence the need for comprehensive policies and robust strategies such as the National Cybersecurity Policy and Strategy (NCPS) 2021.

The goal of the NCPS 2021 is to protect the "**Digital Nigerian**" and "**Digital Nigeria**" by evolving a cybersecurity ecosystem in Nigeria that engenders **trust, opportunity, and agency**.

The team took a whole of society approach with the understanding that Cybersecurity is a collective responsibility and thus the committee endeavoured to cater for the cybersecurity needs of:

1. All socio-economic strata including street vendors like Malam Mai Shai (tea seller), Mama Okpa (purveyor Bambara-nut Curd), Mama Al-Akara (cook of fried cowpeas or black-eyed Beans) and the roadside vulcaniser who now rely increasingly on digital services.
2. Young innovators, technocrats, and ultra-high decision makers.
3. Countering imminent digital threats to our sovereignty, economy, governance and security like digital assets, abuse of social media, disruptive outer-space platforms and evolving global cyber-norms amongst others.

At all stages, the Committee did its best to factor the underserved, unserved and unborn because the team understood that they must live with the consequences of the Policy and Strategy. Through its 8 Pillars + 1 cross cutting topic, the new policy and strategy focuses on:

1. Leveraging jobs creation opportunities in the estimated $4.5 billion African Cybersecurity market by 2023-2025.
2. Enhancing Federal Government anticorruption capacity by addressing new virtual assets that aid money laundering.
3. Deploying new tools that deny terrorists propaganda platforms and improve the capacity of security agencies to bring criminals to justice.

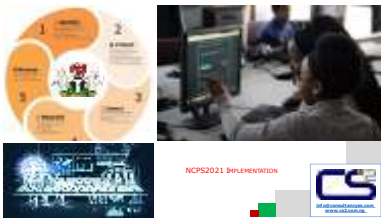
The following broadly outlines the eight plus pillars and one cross cutting topic:

1. Pillar 1, address issues of **Governance** and Coordination and the establishment of institutional mechanism called the **National Cybersecurity Coordination Centre (NCCC)**, pronounced N triple C, to **coordinate** cybersecurity at all levels Federal, State, Local Government, Private Sector, Academic and so on so that multiple initiatives that complement each other for a successful outcome are embarked on. Noting that Cybersecurity is a shared responsibility of all of us.
2. Next, to be addressed is **Critical National Information Infrastructure** (CNII) which are **physical, cyber-based and institutional mechanisms essential to the minimum operations of the society, economy**

[2] Source http://www.globalresearch.ca/pentagon-seeks-to-manipulate-social-media-for-propaganda-purposes/25719

and government." Like Banking, Finance and Pension system, Electrical Power Systems, Information and Communication etc.

3. Pillar 3 addresses **Incident Management and Establishment of Sectoral and other Computer Emergency Response Teams** which are like **CyberSpace teaching hospitals** (treatment, research, teaching, public health, cancer etc).
4. The committee sought to strengthen our **Legal and Regulatory** Frameworks for issues like **Internet Safety and Child Online Protection and Gender Rights Online as well improving the capacity of** Law Enforcement and Judiciary.
5. Pillar 5, addresses enhancing Nigeria Cyber **Defence** Capability and **National Cyber Defence Coordination**
6. Next, are issues related to the Digital **Economy** including virtual assets and ensuring that Nigerians operate in a **Safe and Trusted Online Environment with a commensurate** Cybersecurity Workforce.
7. Pillar 7, address **Assurance** Monitoring and Evaluation as well as **Indigenous Cybersecurity Technology**.
8. The final pillar looks at enhancing International **Cooperation**.
9. The cross-cutting issues were **Funding and Sustainability**.



The team is aware that IMPLIMENTATION is often a challenge that must be improved upon by ALL, and thus the focus in the NCPS2021 is on three key aspects namely:

1. **People** (Awareness, Teaching, Learning, Research, Development, and Innovation).
2. **Process** (Governance, institutions, collaboration, and Assurance).
3. **Technology** (products, services, equipment).

Ladies and Gentlemen, **Getting Women and youth into IT Security and evolving them into Power Players is a critical societal security issue**.

1. **No Society/ Economy can make significant headway if it does not leverage 50% of its population** (Women) and stifles another 47% (Male Youth) of its population.
2. According to the World Economic Forum "For every dollar invested into girls' rights and education, developing nations could see a return of $2.80, ….[3]
3. It is in our strategic self-interest to encourage our ladies, wives, sisters, and daughters to become cybersecurity power players.
4. **Cyber activities provide flexibility for people to work from home within the boundaries of our traditional values systems**.
5. There are Women who play strategic roles in IT Security like:
   a. Favour Femi-Oyewole, Group Chief Information Security Officer at Access Bank Plc.
   b. Rakiya Shuaibu-Mohammed, Chief Information Security Officer (CISO), CBN.
   c. Chineye Chizea, Chief Information Security Officer (CISO), NIMC.

   Note: Middle aged ladies are more stable and thus more likely be retained as Chief Information Security officers (CISO's).
6. **Ladies know your pioneers, it can be done, and you can do it, God willing**.

It is imperative that Nigeria appreciates the responsibilities of all levels, strata, and arms of government to increase productivity, efficiency, reduce costs, block corruption, and improve the well-being of all members of our society by safely digitising operations. Thus, we must:

1. Establish a cadre of ICT savvy knowledge workers in all government agencies and departments and encourage state and local governments to follow the lead of the Federal Government in line with global good practice.
2. Encourage cities and local governments to create a cross cutting ICT cadre because all aspects of contemporary Smart Cities and Local government activities like Public works, Agriculture, health, education, maintenance of public infrastructure will be knowledge based, information driven and digitised. Furthermore,

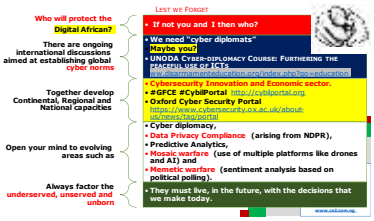
[3] https://www.weforum.org/agenda/2020/10/girls-school-africa-developing-nations-gdp/

each local government should consider how best to maximise such innovations and gain developmental advantage.

3. Urgently amend the Public Service Rules and the Local Government Service Commissions enabling acts across all our states to embed an ICT cadre and stand-alone department with a strong cyber security component.

4. Evolve Local Government staff into 21st Century Knowledge Workers.

Lest we Forget: As we move forward, please consider the following carefully.



1. **Who will protect the Digital African: If not you and I then who?**

2. There are ongoing international discussions aimed at establishing global cyber norms:

   a. **We need "cyber diplomats" Maybe you?**

   b. Look into **UNODA Cyber-diplomacy Course**: Furthering the peaceful use of ICTs ww.disarmamenteducation.org/index.php?go=education

3. Together develop Continental, Regional, and national capacities – **Sustainable Cybersecurity Innovation and Economic sector**. Research via #GFCE #CybilPortal http://cybilportal.org

4. Open your mind to evolving areas such as:

   a. **Cyber diplomacy,**

   b. Data Privacy Compliance arising from Data Protection legislation and regulations like the Nigeria Data Protection Regulation (NDPR).

   c. **Predictive Analytics**,

   d. **Mosaic warfare (use of multiple platforms like drones and AI) and**

   e. **Memetic warfare (sentiment analysis based on political polling).**

5. **Please always factor the underserved, unserved and unborn in our policies and plans as they must live, in the future, with the decisions that we make today.**

Colleagues, ladies, and gentlemen. **The Cyber Threat Landscape is dynamic and continues to evolve - Our survival demands that we must continually improve.**

Please download a copy of the NCPS2021 from: https://cert.gov.ng. Read it, digest it, and implement it.

We must all continually ask ourselves, who will protect the "**Digital Nigerian**" and "**Digital Nigeria**", if not you and I, then who?

The Nigeria National Cybersecurity Policy and Strategy (NCPS) 2021 provides the policies, strategies, and frameworks to protect ourselves and our progeny in collaboration with our friends and partners across the globe.

Thank you, for your attention.

May the Almighty ease all our matters.

God bless the Federal Republic of Nigeria.

Abdul-Hakeem Ajijola (AhA)

info@consultancyss.com | www.cs2.com.ng

https://www.linkedin.com/in/aha01/ | www.facebook.com/CS2Nigeria |twitter.com/cs2Nigeria