CENTRE FOR CYBERSPACE STUDIES
NASARAWA STATE UNIVERSITY, KEFFI

NATIONAL WORKSHOP ON ELECTION INFRASTRUCTURE

Vulnerability, Threat and Risk Landscapes

People Process Technology

Enriching the Values of Credible, Fair, Free, Inclusive and Transparent Election

Intellectual, Academic, and Best Practice Dialogue

Credible, free, fair, inclusive and transparent elections are a hallmark of progressive and decent democracies. The confidence and trust of the electorates in the value of their votes is primarily dependent on the security and resilience of the infrastructure that makes the elections possible. Conversely, an electoral process that is both secure and resilient is a vital component of national security that will continue to guarantee equity, justice, inclusiveness and national unity. Accordingly, stakeholders in the Nigerian 2023 elections expect a wholesome implementation of the 2022 Electoral Act as amended to produce a credible, fair, free, inclusive and transparent election. One of the innovations in the Act is the deployment and use of digital election infrastructure to run and deliver a radiant election devoid of manipulation of any sort. Thus, the aim of this Workshop is to technically x-ray the ecosystem of the electoral process, with a view to identify and educate stakeholders on active and passive threats that could undermine the robust infrastructure put in place for the 2023 electoral processes.

In this series of workshops, the Centre for Cyberspace Studies, Nasarawa State University, Keffi has assembled a cream of fine-grained domain experts from local and international platforms to dive into the landscape of vulnerability, threat and risk in the context of people, processes, and technology. The thrust is to keep electoral stakeholders better informed and equipped with the various electoral risks, threat actors and opportunities, and how to mitigate the risks.

The workshops will equip participating stakeholders with the knowledge of vulnerability, threat and risk components capable of undermining the integrity and authenticity of the electoral process. The effect of cybersecurity threats capable of compromising electoral process lifecycle, such as registration and maintenance of voters register database, verification and validation of eligible voters, casting and counting of votes, the transmission of collated votes, computing and aggregation of votes and announcing results are critical for the assurances of free, fair, inclusive and peaceful election.

In addition, the workshop will cover how people, process and technology interact with the broader electoral environment and the digital landscape. The focus is to provide uniform unbiassed lens from which stakeholders can gain balanced knowledge and insights about vulnerability, threat, and risk landscape of the election infrastructures as a whole i.e., how malicious parties can take advantage of an inherent vulnerability in people, process and technology to advance their nefarious activities.

Furthermore, it will help electoral stakeholders manage these risks based on sound engineering principles and international best practices for securing the electoral process as well as garner specific observations and input from critical stakeholders.

Workshop Objectives

- Mastering the goals of Security, Safety and Trust of Election Infrastructure.
- Understanding the landscape of vulnerability in people, processes and technology.
- How to examine and reduce the surface of opportunities offered by such vulnerabilities and threats .
- Understanding the threat landscape, threat actors and their motivations.
- Mastering the risk landscape – impact/severity of security breaches – how it affects electoral chances
- Gain Insightful Knowledge about the Insider-Man Threats in a electoral systems.
- Understanding the weaponization of the electoral process by internal and external forces - use of social media networks (fake news, misinformation, disinformation, propaganda, etc.)

Date

28 - 30th Nov. 2022

Venue

NAF Conference Centre,
Kado, Abuja

Audience

Electoral Management Bodies (EMBs), Political Parties, NGOs, CSOs Security and Intelligence Community, International Observers, Judiciary, Academia, ICT OEMs, Vendors, NBA, etc.

Workshop Fee

N200, 000 (per participant)
N150, 000 (3 & above participant)
$199 (International Participant)

Take Away

Workshop Package
Certificate of participation
e-copy workshop Proceedings

Registration & Payment

+234 8022904983, +234 8144002855, +234 7064984493
wei-2022@cyber.ccs-nsuk.net
https://cyber.ccs-nsuk.net/wei-2022

Association of Telecommunications Companies of Nigeria