IS 336 Project Three

Deliverables Due: 16 July 2025

Title: **Innovative Cybersecurity Solutions for Protecting Tanzania's 2025 Electoral Process**

Background

Elections and campaigns in Tanzania are increasingly influenced by digital technologies—from social media messaging, voter registration systems, electronic result transmission, to political mobile apps. However, this digital transformation has introduced critical vulnerabilities including misinformation, image tampering, network intrusion, phishing via SMS, and infrastructure-level cyberattacks targeting electoral stakeholders such as NEC, MNOs, TCRA, the ICT Commission, political party systems, data centers, and financial institutions managing election funds.

Amid growing national concern, this project challenges students to explore the threat landscape around elections and develop innovative cybersecurity solutions that can be tested and piloted. The use of AI in the solutions will be an added advantage.

Project Objectives

This project aims to:

- Analyze the electoral ecosystem in Tanzania and identify its stakeholders, cyber assets and attack surfaces.
- Conduct a comprehensive threat modeling exercise tailored to the Tanzanian election lifecycle.
- Develop a cybersecurity solution (preferably AI-driven) that addresses one or more election-related vulnerabilities.
- Propose a realistic stakeholder (e.g., TCRA, NEC, a telco, ICT Commission, or a data center) where the solution could be piloted or deployed.

Tasks

Part 1: Threat Modeling and Impact Assessment

- Select a relevant **election-related stakeholder** (e.g., NEC, Vodacom, TCRA, Banks handling campaign funds).
- Map the **election journey**: from pre-campaign, campaign, voting, to results and post-election.
- Identify critical **assets**, possible **threat agents**, and **attack surfaces** (e.g., voter databases, SMS platforms, result transmission servers).
- Use threat modeling frameworks like **STRIDE**, **attack trees**, or **kill chains** to identify threats.

- Describe **realistic attack scenarios** and assess potential **impact on the integrity, availability, or confidentiality** of the election process.

Deliverable: A report presenting a complete threat model with stakeholder context, annotated journey map, and impact evaluation.

Part 2: Development of an AI-Driven Cybersecurity Solution

Design and develop a working prototype that:

- Uses **AI or ML/NLP/computer vision** to detect, mitigate, or respond to threats. Examples:
  - Deepfake or image forgery detection on campaign materials.
  - Real-time monitoring of misinformation on social media.
  - AI-based phishing/SMS campaign detection.
  - Intelligent firewall/IDS tuned for election-period traffic anomalies.
- Clearly defines **hosting options** (cloud/on-premises) and/or provides a **public GitHub link or demo URL**.
- Shows how the solution integrates with or supports your chosen stakeholder's operations.

Deliverable: A prototype with documentation explaining technical design, AI components, hosting setup, and deployment scope.

Part 3: Pilot Strategy and Stakeholder Engagement Plan

- Identify **where and how your solution can be piloted**—whether within a telco's infrastructure, government regulatory body, media houses, or political parties.
- Outline a **realistic adoption roadmap**: required infrastructure, data flows, training, and testing during elections.
- Propose **metrics for evaluating impact** (e.g., time to detect misinformation, number of forged images blocked, SMS phishing detection rate).

Deliverable: A strategy brief describing pilot scope, partner organization, rollout plan, and KPIs.

Submission Requirements

Each student will submit:

- **Threat Modeling Report** (Part 1)
- **Working Prototype + Documentation** (Part 2)
- **Pilot and Stakeholder Engagement Brief** (Part 3)
- All work must be submitted via LMS.

Evaluation Criteria

Criteria
Quality and depth of threat modeling
Innovation and functionality of solution
Practicality of stakeholder engagement & pilot plan
Technical clarity and completeness
Use of AI/NLP/computer vision

Important Notes

- Projects must address the **Tanzanian electoral context** with local relevance.
- Students are encouraged to draw from Social media and WhatsApp discussions and current events.
- Projects may be used to demonstrate feasibility to real government or MNO partners.
- Academic integrity must be upheld—plagiarism will not be tolerated.

Note:
This project will serve as a make-up for the missed/underperformed test and will contribute significantly to the course grade. It must reflect original work and academic integrity will be strictly enforced.

It has been reported that the previous project on assessing VulnGuard is facing many challenges. So that project will still count for those that were able to complete it. The deadline for that project remains to be 3rd July 2025. Tomorrow I will download all submissions, but in case you wish to switch to this new project then that is totally fine and acceptable.

The deadline for this project is 16th July 2025. Have fun. Remember, the objective is to come up with working solutions rather than get a grade.