OFFICIAL RESEARCH DIRECTIVE

To: All Appointed Group Leaders and Members
From: Research Coordination Committee
Date: 4th October 2025
Subject: Directive on Specific Research Foci and Project Assignments

1.0 PURPOSE

This directive officially assigns specific research and development projects to all appointed groups. The purpose is to provide clear, actionable objectives for each team, ensuring focused efforts, preventing overlap, and maximizing the collective contribution to the field of cybersecurity.

2.0 ASSIGNED RESEARCH FOCI

The following assignments are effective immediately and shall form the basis of each group's project work.

2.1 RESEARCH THEME: Attribution Techniques in Cyberwarfare

- **Group 1 (Leader: Oluwademilade Samuel Aladewolu)**
  - **Assigned Project:** *Development of a Unified Attribution Framework Integrating the Diamond Model and Cyber Kill Chain*.
  - **Objective:** To research, design, and document a procedural framework that enhances the accuracy and standardization of attributing cyber-attacks to specific threat actors by synthesizing the Diamond Model of Intrusion Analysis with the stages of the Cyber Kill Chain.
- **Group 2 (Leader: Manmeet Kaur)**
  - **Assigned Project:** *Cataloguing and Analysis of Technical Indicators of Compromise (IoCs) for Major State-Sponsored APT Groups*.
  - **Objective:** To conduct a technical analysis of known Advanced Persistent Threat (APT) groups, creating a detailed repository of their unique malware signatures, infrastructure, and Tactics, Techniques, and Procedures (TTPs) to aid in faster and more reliable attribution.

2.2 RESEARCH THEME: Capture The Flag (CTF) for Cybersecurity Training

- **Group 1 (Leader: Tolulope Duru)**
  - **Assigned Project:** *Specialized Preparation for Global CTF Competitions: Web Exploitation and Cryptography Tracks*.

- **Objective:** To achieve operational readiness for global CTF challenges by developing advanced practical skills in identifying and exploiting web application vulnerabilities (e.g., SQLi, XSS) and breaking cryptographic implementations.

2.3 RESEARCH THEME: Cybersecurity Virtual Lab for Hands-On Learning

- **Group 1 (Leader: Daniel Zibom Duniya)**
  - **Assigned Project:** *Design and Implementation of a Modular Network Security Lab for Firewall and IDS/IPS Configuration*.
  - **Objective:** To architect and build a virtualized lab environment that enables the practical configuration and testing of open-source firewall rules and Intrusion Detection/Prevention Systems (e.g., pfSense, Snort) within a segmented network topology.
- **Group 2 (Leader: David Ajuzie)**
  - **Assigned Project:** *Construction of an Isolated Sandbox Environment for Advanced Malware Analysis and Digital Forensics*.
  - **Objective:** To establish a secure, contained lab using tools like Cuckoo Sandbox and REMnux for the dynamic analysis of malicious software and the practice of digital forensics techniques on memory and disk images.
- **Group 3 (Leader: Kamaludeen Aminu)**
  - **Assigned Project:** *Curation and Development of a Multi-Stage Penetration Testing Lab with Real-World Scenarios*.
  - **Objective:** To assemble a comprehensive library of vulnerable virtual machines and design complex, multi-step penetration testing scenarios that simulate realistic enterprise networks, complete with documented attack paths and mitigation strategies.

2.4 RESEARCH THEME: Cyberwarfare & Protection of Critical Infrastructure

- **Group 1 (Leader: Madusonde Emmanuella)**
  - **Assigned Project:** *Vulnerability Assessment and Threat Modeling Framework for Smart Grid Electrical Systems*.
  - **Objective:** To research the architecture of smart grid technologies and develop a comprehensive threat model identifying critical vulnerabilities and proposing a structured assessment methodology for energy sector infrastructure.
- **Group 2 (Leader: Lehlogonolo)**
  - **Assigned Project:** *Development of a Sector-Specific Incident Response Plan for Ransomware Attacks on Healthcare Critical Infrastructure*.

- **Objective:** To create a detailed and actionable Incident Response (IR) plan tailored to a healthcare setting, focusing on containment, communication, and continuity of life-critical services during a severe ransomware incident.

- **Group 3 (Leader: MUGHE GODLOVE BUH)**
  - **Assigned Project:** *Securing Industrial Control Systems (ICS): Strategies for Mitigating Cyber-Physical Attacks on PLCs*.
  - **Objective:** To investigate the security posture of Programmable Logic Controllers (PLCs) and other ICS components and propose a defense-in-depth strategy to protect against attacks capable of causing kinetic damage.

2.5 RESEARCH THEME: Malware Analysis Using AI and Machine Learning

- **Group 1 (Leader: Juliana Kivuva)**
  - **Assigned Project:** *Building a Static Malware Classification Engine using Machine Learning*.
  - **Objective:** To engineer a machine learning model capable of classifying malware families based on static features extracted from Portable Executable (PE) files, such as headers, imports, and section characteristics.
- **Group 2 (Leader: Jamilu Ibrahim Richifa)**
  - **Assigned Project:** *AI-Driven Dynamic Malware Behavioral Analysis and Novel Threat Detection System*.
  - **Objective:** To research and develop a system that uses artificial intelligence to analyze the runtime behavior of malware in a sandbox, aiming to cluster malware into families and identify novel, zero-day threats based on anomalous behavior patterns.

3.0 REPORTING AND DELIVERABLES

Group Leaders are responsible for coordinating their members and driving progress toward the assigned objective. Preliminary project proposals outlining scope, methodology, and projected timelines are to be submitted to the Research Coordination Committee

4.0 AUTHORIZATION

Approved by,

Aminu Idris, AMCPN

Research Coordination Committee