Cybersecurity
CENTRE OF EXCELLENCE

CYBERSECURITY
CENTRE OF EXCELLENCE

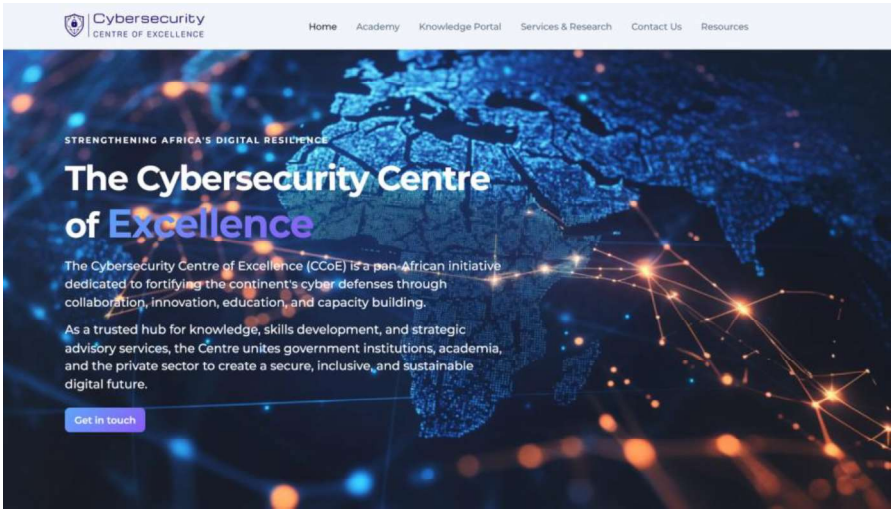
Company Profile

INTRODUCTION: CYBERSECURITY CENTRE OF EXCELLENCE

Rapid advances in connectivity, digital trade, and innovation are unlocking unprecedented opportunities for growth, inclusion, and prosperity. Yet, this transformation is accompanied by escalating cybersecurity risks that threaten national security, economic stability, and public trust. Many African nations face significant gaps in resilience due to limited resources, fragmented capacity, and rising costs of expertise [1].

The **Cybersecurity Centre of Excellence (CCoE)** responds directly to this challenge. It is designed as a collaborative ecosystem that cultivates a robust cybersecurity foundation for Africa. The Centre seeks not only to defend against cyber threats but also to act as a knowledge hub, skills incubator, and catalyst for policy innovation.

The Cybersecurity Centre of Excellence draws its strength from a multidisciplinary team of cybersecurity professionals, researchers, and policy experts with experience spanning technology, academia, and public service. Our expertise bridges organisations and nation-states, combining advanced technologies, strategic policymaking, and national capacity-building to strengthen Africa's cybersecurity landscape



The Cybersecurity Centre of Excellence (CCoE) is built on three strategic pillars:

A **Training Academy** is a comprehensive capacity-building platform offering programs from end-user awareness to advanced technical, executive, and policy-level training, supported by certifications and practical simulations. It is meant to train and certify a new generation of cybersecurity professionals, executives, and policymakers while raising awareness among citizens and SMEs.

Services and Research that guide institutions and governments in building strategies, frameworks, and responses in various sectors including the critical infrastructure and critical information infrastructure. It has a dedicated research capacity producing localised studies, policy briefs, and research papers that generate context-specific insights.

A **Knowledge Portal** that democratizes access to curated, repository of policies, strategies, best practices, research, and case studies, enhanced with advanced indexing, and AI-powered search capabilities.

Our **Resources** page contains our Document Repository, where we have curated and classified a wide array of open-source cybersecurity documents, which is freely available as a dynamic and comprehensive repository of knowledge. It also contains our interactive GIS-enables Map that provides comprehensive

[1] https://www.weforum.org/publications/global-risks-report-2024/

information across various categories. This freely available and updated on a continuous basis to ensure that the information we provide is accurate and current

TRAINING ACADEMY

Training in cybersecurity encompasses a wide spectrum, catering to various skill levels and professional needs. The Academy is designed to equip individuals, organisations, and national institutions with the cybersecurity knowledge and skills necessary to thrive in an increasingly digital world.

Accredited Training Programs: A portfolio of accredited cybersecurity courses designed to build technical and managerial skills. These programs cover core areas of the cybersecurity domain - ensuring participants gain recognised qualifications aligned with global standards.

Master Classes & Seminars: Specialised masterclasses delivered by leading experts, covering both foundational and advanced topics in cybersecurity, the intersection of cybersecurity and AI, cyber law, digital forensics and incident response (DFIR), and digital diplomacy.

Tailored executive programs equip board members and senior leaders with the insights needed for strategic decision-making. Interactive workshops and webinars provide practical skills, hands-on learning, and exposure to real-world case studies.

Workshops, Cyber Drills & Simulations: Immersive, practice-oriented sessions that prepare participants for real-world challenges. These include hands-on labs, capture-the-flag (CTF) exercises, tabletop exercises, cyber drills, and live simulations - all designed to test readiness, build teamwork, and strengthen incident response capabilities.

Program Name	Description
Artificial Intelligence for Government Officials	designed to equip government officials with a foundational and practical understanding of Artificial Intelligence (AI), enabling them to make informed policy decisions, drive responsible innovation, and enhance public service delivery. The 5 module program begins with an accessible introduction to AI fundamentals, ensuring participants gain clarity on key concepts and their implications. It then delves into critical debates around AI ethics, transparency, and fairness, before exploring the emerging legislative and regulatory landscape globally and within developing country contexts.
Masterclass for Business Leaders: The Governance of Artificial Intelligence	This program is designed to help organizational leaders navigate the intricate landscape of AI. It begins by highlighting the urgent need for AI governance, given the vast opportunities and risks associated with this technology, and the current lack of adequate oversight.
Digital Diplomacy in a Multi-Polar World: Navigating Technology, Power and Governance	This program builds the capacity of government officials to understand and influence international digital governance. It recognizes that diplomacy now extends beyond traditional negotiations to include cyber norms, AI ethics, data flows, and standards-setting processes. Participants will gain the knowledge and tools needed to align national interests with global digital policy developments and engage confidently in key multilateral forums—such as the UN, WTO, ILO, AU, and IGF.
Cybersecurity Leadership Masterclass: Leading Organisational Resilience	The Cybersecurity Leadership Masterclass is designed as an interdisciplinary course, focusing on management strategies, organisational governance, the technical elements that underpin the Cybersecurity discipline, security technologies, national policy and legislation, and standards, The course incorporates elements relevant to creating a culture of cybersecurity awareness and resilience and focuses on the developing relevant strategic responses to the security challenges posed to organisations in an increasingly complex digitally transforming environment.
Strengthening Cyber Resilience Through Real-World Practice	In today's rapidly evolving digital landscape, cyber threats are not a matter of if but when. Organizations need more than policies and frameworks - they need teams that can act decisively under pressure. Practical, scenario-based exercises are vital to closing the gap between theory and practice, ensuring that cybersecurity professionals are prepared to respond to real incidents with confidence and precision Our immersive, practice-oriented training goes beyond theory to prepare participants for the realities of today's threat landscape. Through hands-on labs, capture-the-flag (CTF) challenges, tabletop exercises, cyber drills, and live simulations, participants gain the skills to detect, respond, and recover from incidents under real-world pressure. Designed to test readiness, sharpen teamwork, and

Training Portfolio extract

ADVISORY SERVICES

The Cybersecurity Centre of Excellence (CCoE) provides specialized advisory services to help governments, organizations, and institutions navigate the complex cybersecurity landscape. Our team of experts works across policy, technical, and strategic domains to enhance cyber resilience, mitigate risks, and build a secure digital ecosystem for Africa.

Key offerings within the Advisory Services include:

Strategic Guidance, Technical Expertise, and National Cybersecurity Maturity

Trusted advisory services to governments, businesses, and institutions, helping them navigate the complex and fast-evolving cyber landscape. We work at the intersection of strategy, technology, and policy to deliver guidance that is practical and forward-looking. It includes developing cybersecurity strategies, frameworks, and governance models that are compliant with global standards and regulatory requirements, strengthening organisational and national readiness through capacity building, incident response planning, crisis management, and business continuity.

Specialized Cybersecurity Consulting

Our niche consulting services focus on national-level cyber resilience initiatives, providing expert guidance on the establishment, operationalization and maturity (e.g. FIRST Membership) of national CERT/CSIRTs and SOCs**,** and the development of legislative and regulatory frameworks, national cybersecurity strategies, and the establishment of industry specific sector-CERTs.

Current Project

Lead consultants on the Design phase of a SOC for a leading African telco service provider. The design includes the integration of a Digital Forensics lab to provide DFIR capabilities and the establishment of a telco sector-CERT. The design phase adheres to various global standards (ISO/IEC 27001, NIST Cybersecurity Framework and ENISA's SOC Guidelines) and also emphasises standards for the Build-Operate phases (ISO/IEC 22301 for Business Continuity Management, NIST SP 800-160 – Systems Security Engineering, and CIS Controls v8).

Previous Projects

Individually our members have extensive experience in the establishment and maturing of national CERTs, drafting of national legislation and regulations, development of national cybersecurity strategies, establishment of sector-CERTs, and other national initiatives including skills, training, curriculum development and awareness strategies.

Research

We offer bespoke research services that blends academic excellence with real-world application. Our research is conducted by a multidisciplinary team of professional academics and experienced business practitioners, ensuring a balance between theoretical rigour, academic due diligence and practical insights. Our research team have collectively published over two hundred peer-reviewed journal articles in leading international journals.

Current Project

A qualitative, incident-focused study of major cybersecurity breaches in South Africa since 2020 for a global OEM. It catalogues and analyses real-world incidents using available threat intelligence, public disclosures, press reports, Auditor-General of South Africa (AGSA) reports, Information Regulator reports, and key interviews. The broader objective relates to policy context, data privacy, and institutional preparedness.

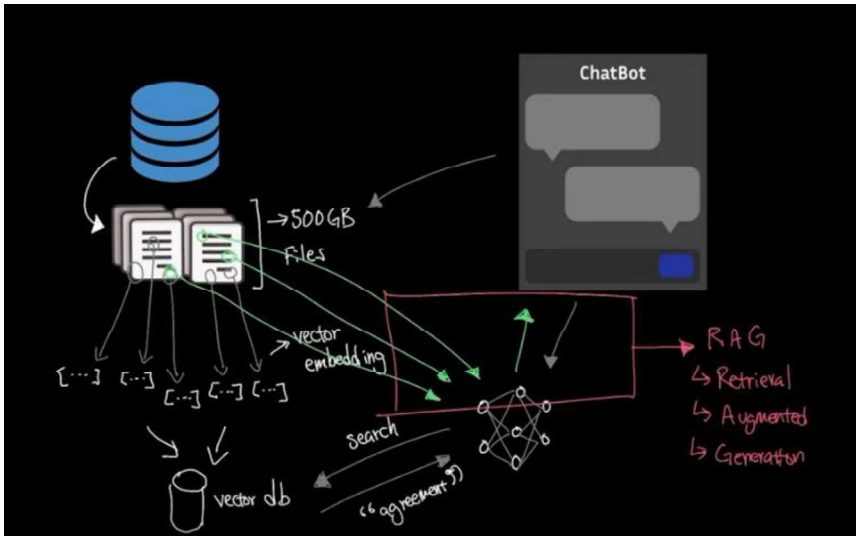
Previous Projects

A series of four in-depth research articles for a leading South African bank ranging from emerging risk frameworks, analysis of cybersecurity and cybercrime legislation in jurisdictions where the bank operates, impact of the metaverse on financial institutions, and understanding the impact of human trafficking on the bank's operations

KNOWLEDGE PORTAL

The Knowledge Portal is designed to democratize access to authoritative cybersecurity resources across Africa. It acts as a one-stop repository that curates, indexes, and classifies a wide range of open-source materials, including national and regional cybersecurity strategies, research papers, academic articles, and policy documents, industry reports and best practice guidelines, case studies and threat intelligence reports.

This platform is specifically designed to accelerate policy framework development and enhance decision-making processes across organizations, by providing instant access to institutional knowledge, regulatory documents, research papers, and historical precedents, that enables policy makers and decision makers.



Our implementation consists of two main components: a document processing pipeline (Python-based) that prepares and indexes documents, and a query interface (SvelteKit web application) that enables intelligent search and retrieval.

From RAG to Agentic Intelligence

We are currently enhancing our baseline RAG model, and the deployment model will of an Agentic Orchestration Layer, whose neural core consists of specialized AI agents coordinated through N8N workflow automation and Model Context Protocol (MCP) integration. This architecture enables:

- Document Curator Agent: Automatically organizes and categorizes incoming documents across domains
- Research Analyst Agent: Conducts autonomous literature reviews and competitive intelligence
- Compliance Monitor Agent: Continuously validates content against regulatory requirements
- Geographic Intelligence Agent: Provides location-aware insights for policy and planning decisions
- Decision Support Agent: Synthesizes multi-source information for strategic recommendations

This platform represents the evolution from traditional RAG systems to fully autonomous, multi-agent knowledge orchestration. Built upon our proven foundation of sophisticated document processing, intelligent metadata generation, and geographic integration, the future system integrates cutting-edge agentic capabilities with open-source orchestration tools to create a comprehensive enterprise AI platform that autonomously manages knowledge, drives decisions, and executes complex workflows across multiple business domains.

Impact of the Knowledge Portal

- Democratization of knowledge: Free and equal access to resources that are often fragmented or difficult to obtain.
- Empowerment of stakeholders: From government officials drafting policies to SMEs improving resilience, users can rely on a credible and constantly updated platform.
- Capacity building: Provides educators and trainers with curated content to enrich curricula.
- Thought leadership: Positions Africa not only as a consumer of cybersecurity knowledge but as an active contributor to global discussions.

OUR RESOURCES PAGE

Under our Document Repository we have curated and classified a wide array of open-source cybersecurity documents, which is freely available as a dynamic and comprehensive repository of knowledge. The document repository facilitates informed decision-making, strategy formulation, and the development of best practices tailored to the unique needs and challenges faced by African nations and organizations.

We have also developed an interactive GIS-enables Map that provides comprehensive information across various categories. This freely available and updated on a continuous basis to ensure that the information we provide is accurate and current