AI for Cybersecurity: The Algorithmic Battlefield

School of Digital Transformation and Innovation in the Caribbean 2025
16-20 June

Dr Craig Ramlal

School of Digital Transformation and Innovation in the Caribbean 2025 16-20 June

Current Landscape of Cyber

Cyber skills gap

The sector is currently lacking up to 4.8 million cybersecurity professionals. Only 14% of organizations say they have the skilled people they need in the current cyber landscape, while the report finds the cyber skills gap increased by 8% during 2024, predominantly in the public sector.

2024 ISC2 Cybersecurity Workforce Study

-67% of organizations report a moderate-to-critical skills gap in cybersecurity
-23% of organizations recruit outside of traditional cybersecurity degrees or credentials

AI adoption and security preparedness

Organizations are rapidly embracing AI tools but often without adequate safeguards. Two-thirds of companies anticipate AI will impact their cybersecurity by 2025, yet only one-third (37%) say they have the tools to assess AI-related security risks. This gap is even wider for smaller entities, nearly 69% lack proper protections for secure AI deployment.

Sentiment of AI replacement

AI will likely replace some of the technical skills needed in cybersecurity. There is speculation on what skills may be automated or streamlined, they cannot yet predict what activities, if any, AI will replace.
As a result of this uncertainty, hiring managers aren't rushing to hire more specialized workers. Instead, they are prioritizing nontechnical skills like problem-solving that will be transferable through the increased use of AI.

2024 ISC2 Cybersecurity Workforce Study

Why is there a talent shortage?

-Layoffs and budget cuts exacerbate security team shortages, which participants have told us are a persistent issue
-Organizations reported the inability to find talent or skills needed.
-More than a quarter (26%) highlighted the challenges of retaining people with in-demand skills, while 22% are struggling with developing and advancing their cybersecurity staff.

AI is exacerbating the issue

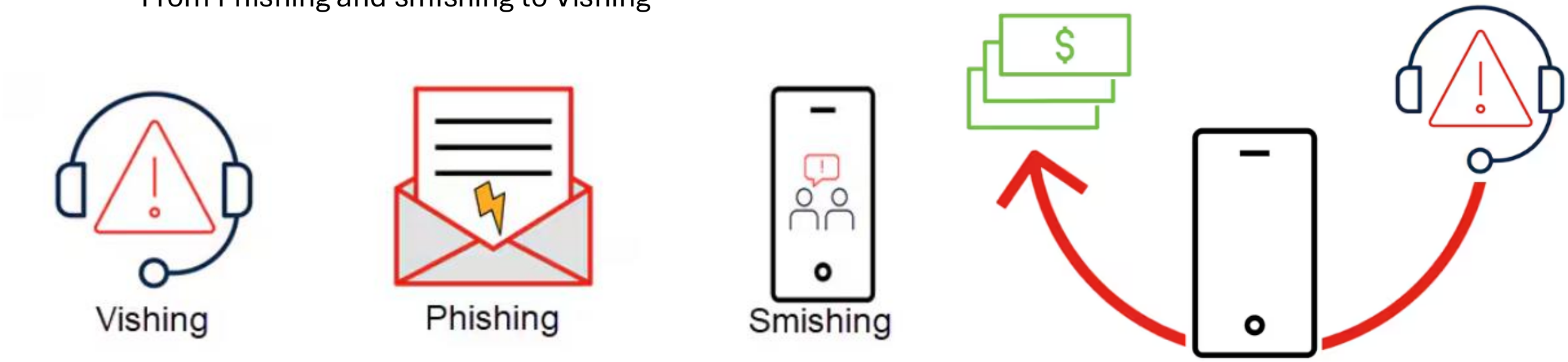
-Increased sophistication and volume of attacks
-Automated attack chains
-Rapid malware development

Attractiveness of Field in the GenAI Era

-Increased workload and pressures
-Disadvantage for Defenders
-Difficulty in Recognizing AI-Generated Threats

AI-Powered Attacks: Social Engineering

From Phishing and smishing to Vishing



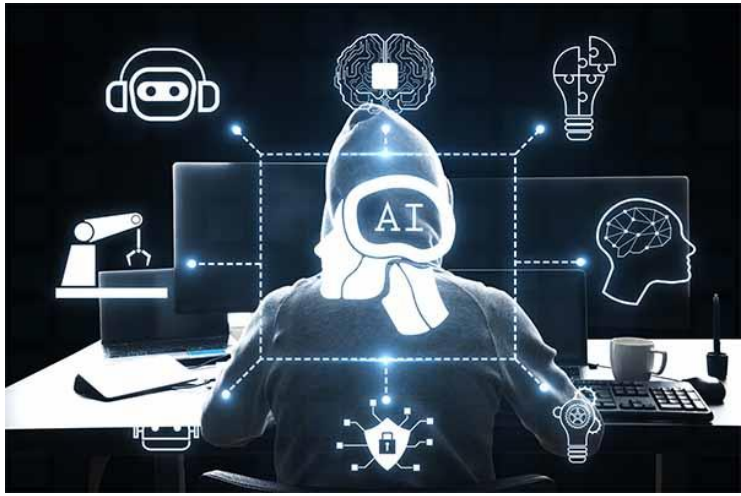
Successful phishing, vishing, deepfake and other social engineering attacks were experienced by 42% of organizations in a 2024 survey

Phishing: Email scams that lure victims into clicking links leading to deceptive websites or malware downloads

Smishing: Text message scams that also prompt victims to click malicious links or visit fake websites

Vishing: Phone call scams that pressure victims to share sensitive information verbally

AI-Powered Attacks: Social Engineering



Hyper-Personalized Social Engineering

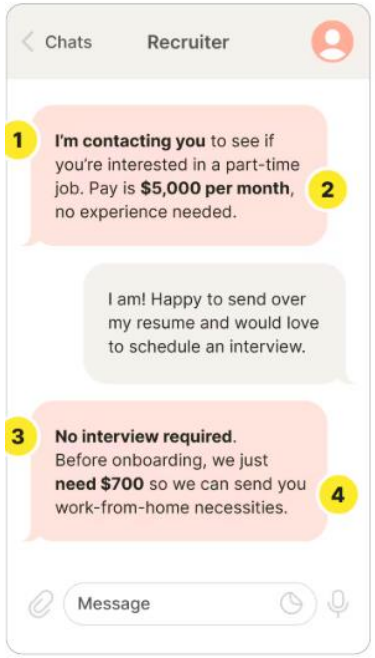
- 1,265% increase in malicious phishing messages since Q4 2022
- On average, 31,000 phishing attacks were sent on a daily basis
- 967% increase in credential phishing
- 68% of all phishing emails are text-based Business Email Compromise (BEC)
- 46% of cybersecurity professionals polled reported receiving a BEC attack
- 77% of cybersecurity professionals polled reported being targets of phishing attacks, and 28% reported receiving those messages via text message
- 39% of all mobile-based attacks were SMS phishing (Smishing)

AI-Powered Attacks: Social Engineering

DeepFaceLab & Face swap

FraudGPT and WormGPT

BlackmailerV3



Telegram FraudBot

Commercial

Open Source

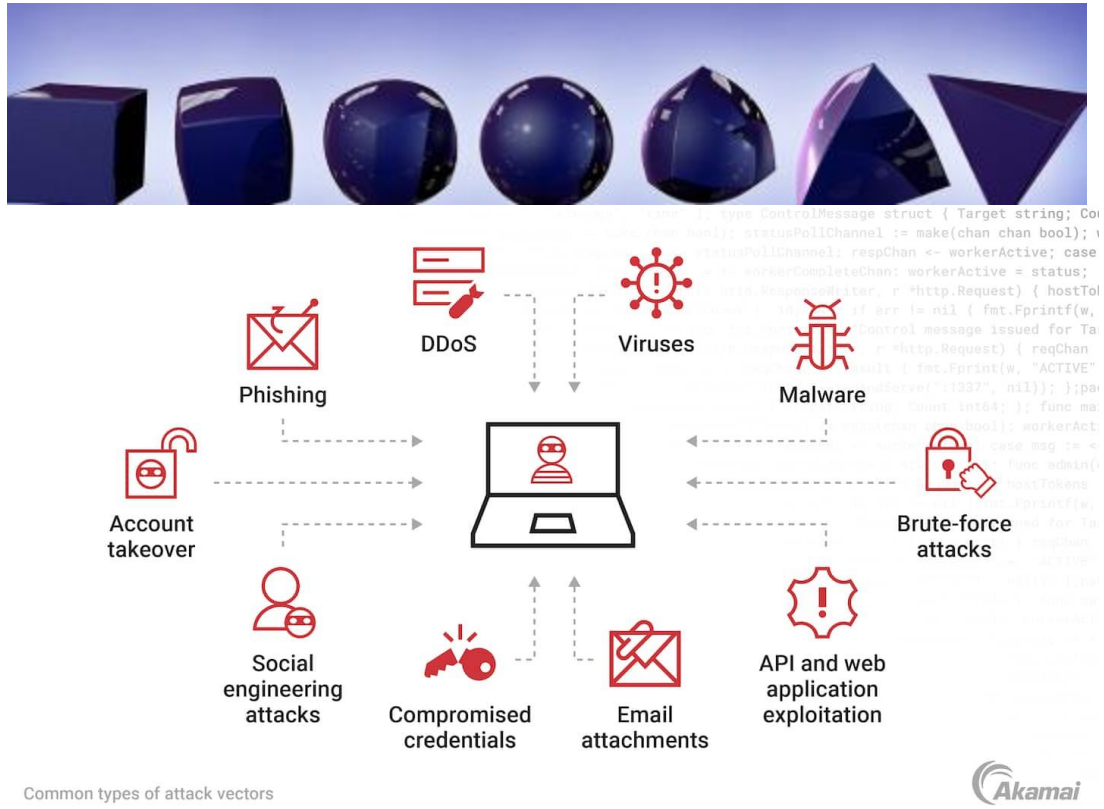
Eleven Labs

deepseek

ZONOS

AI-Powered Attacks: Malware

- Adaptive Malware
- Dynamic Malware Payloads
- Zero-Day and One-Day Attacks
- Content Obfuscation



Common types of attack vectors

AI-Powered Attacks: Malware

Forest Blizzard

Emerald Sleet

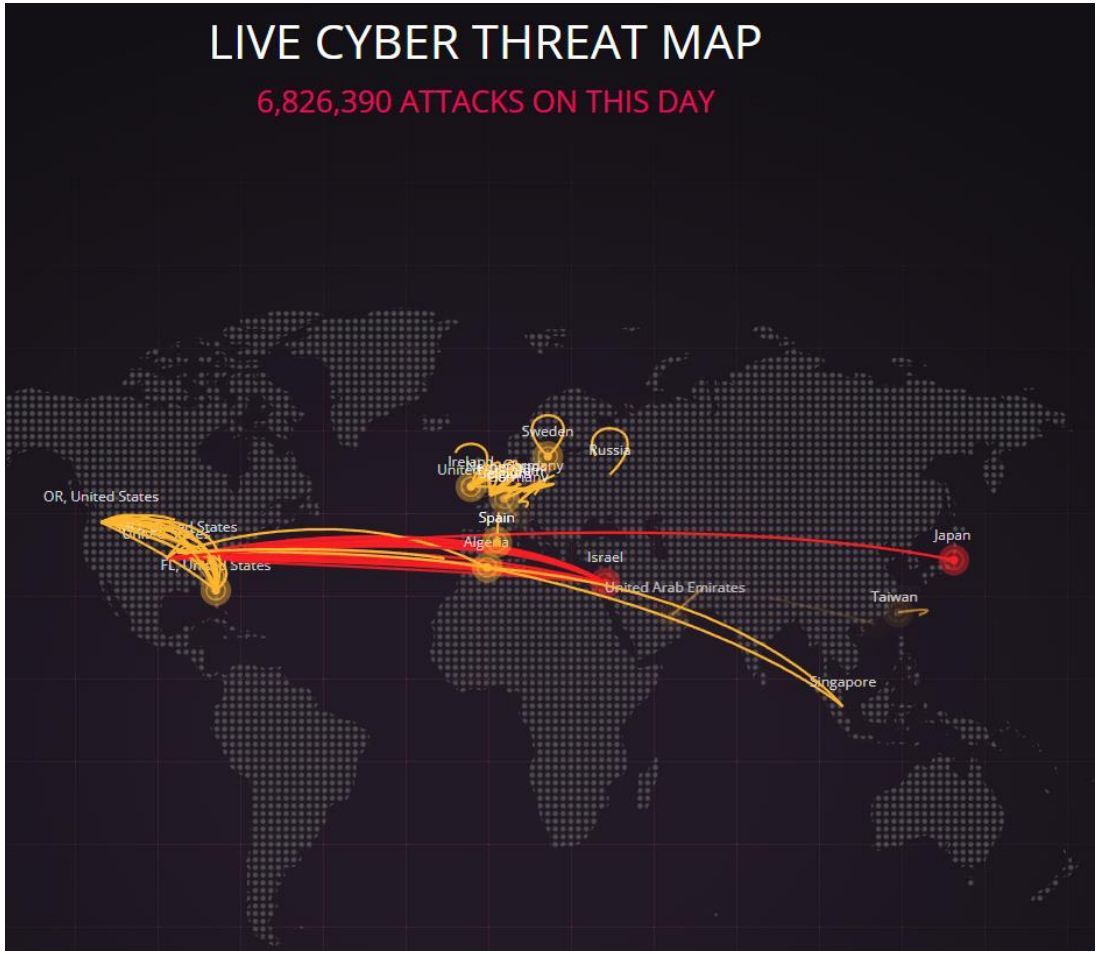
Crimson Sandstorm

Cybercrime as a Service: Era of the democratization of hacking

1. Ransomware as a Service (RaaS)
2. Malware as a Service (MaaS)
3. Exploit as a Service
4. Initial-Access Brokers

Moving away from a detect only strategy

Nation vs Nation



Ransomware-as-a-Service (RaaS) becomes geopolitical. Critical infrastructure targeted. AI-based attacks appear.

School of Digital Transformation and Innovation in the Caribbean 2025
16-20 June

Caribbean, Cyber Security and AI

Caribbean Cyber Threats: A Growing Concern

- Ransomware: The Apex Predator
- Phishing & Cyber Fraud: Constant Threats
- Critical Infrastructure & Government Agencies Under Siege

The Way Forward: Urgent Need for Cyber Resilience

- **Mirrors Global Patterns**

The Caribbean's cyber threat landscape mirrors global patterns, with ransomware, phishing, and sophisticated malware campaigns leading the list of threats.

- **Key Challenges**

Persistent infrastructure vulnerabilities and a shortage of cybersecurity skills.

- **National Security Priority**

Regional leaders are now treating cybersecurity as a **national security priority** to protect economies, critical services, and public trust in the digital age.

School of Digital Transformation and Innovation in the Caribbean 2025
16-20 June

Building Governance and Capacity in AI & Cyber

Caribbean's Major Opportunities/Challenges for AI Adoption/Development

BIG 6

School of Digital Transformation and Innovation in the Caribbean 2025 16-20 June

1. Equitable Access to AI resources and development of capable low-compute systems (& tensor processors)

2. Frameworks for mitigating AI-driven economic disruptions

3. Capacity development, maintaining cultural identity & Brain drain

4. Access to funding pools for research & developing sustainable ecosystems given current infrastructure and economic challenges

5. Identifying & resourcing niche industries that can greatly benefit from AI and earn foreign exchange

6. Regional agreements to AI development, including data sharing, standardization and legal frameworks


United Nations
AI Advisory Body


OMORROW:
H ENGAGEMENT
GUARDING
LEGACIES


Craig Ramlal

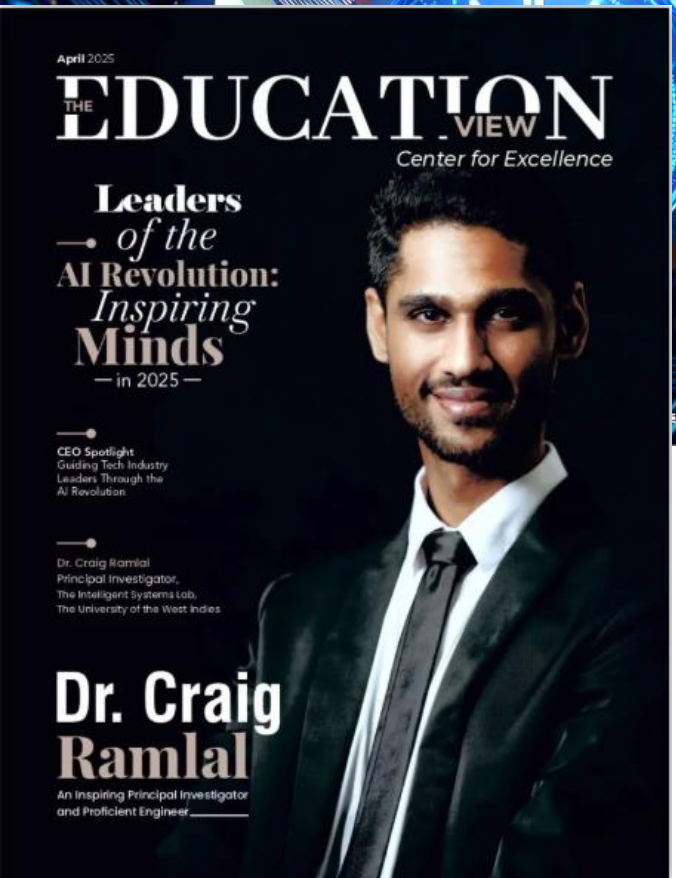

DAY TWO
SESSION FIVE
THE FIFTH INDUSTRIAL REVOLUTION, ROBOTICS AND AI PARTNERSHIPS -
The rise of AI and Robotics
BIG DATA FORUM
JOINT SDG FUND


AI SEOUL SUMMIT
21 - 22 MAY 2024
AI GLOBAL FORU
22 MAY 2024
Seoul AI Night


MINISTRY OF EDUCATION


Craig Ramlal
United Nations
Office of the Secretary-General's Envoy on Technology
AI Advisory Body


GLOBAL FORUM
THE ETHICS OF
ARTIFICIAL
INTELLIGENCE
esco
REPUBLIC OF SLOVENIA
MINISTRY OF DIGITAL TRANSFORMATION



Ensure AI serves institutions, not the other way around

We'd all prefer that AI tools helped us to do research and grade papers rather than take over campuses. Here's how to develop AI tools for your institution responsibly

Artificial intelligence | Digital strategy | Feature article | North America

Craig J. Ramlal
The University of the West Indies

24 Mar 2025

0

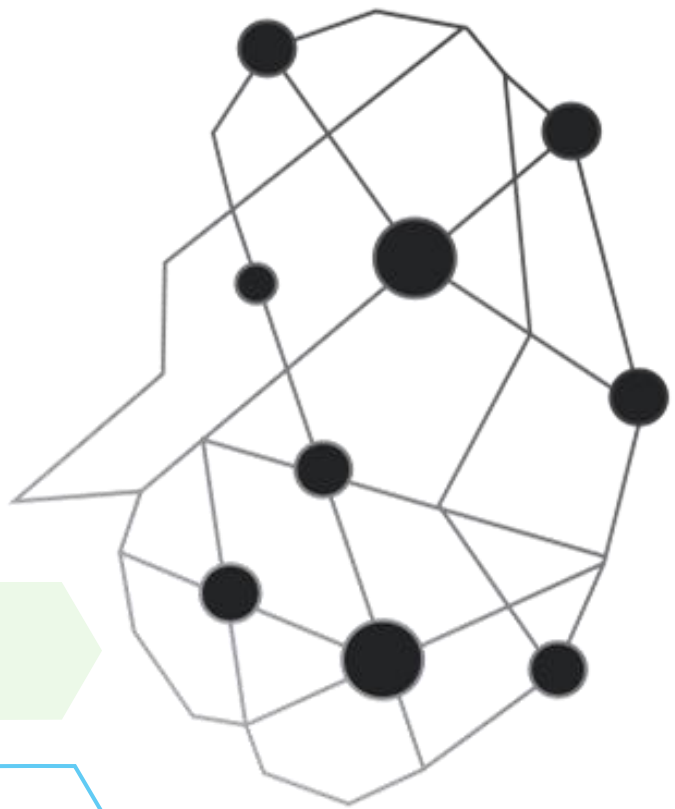
BROOKINGS U.S. Trade Policy | International Affairs | U.S. Government

COMMENTARY

Integrating Caribbean realities into global AI safety policies

Craig Ramlal
February 21, 2025

- Global AI safety frameworks often overlook the unique needs of smaller regions like the Caribbean and fail to accommodate these regions' cultural and linguistic diversity.
- The absence of representative datasets and the dominance of external entities in data collection can impact local sovereignty and cultural preservation.
- To ensure inclusivity, multilateral agreements should prioritize the inclusion of historically marginalized regions in decision-making.



Intelligent Systems Lab

Impact through Systems Learning

Members

Advisory Board / Steering Committee

Dr Craig Ramlal
Principal Investigator
Chair, Advisory Board

Prof Bhesham Ramlal
Co-Investigator

Dr Arvind Singh
Co-Investigator

Prof Chris Maharaj
Co-Investigator

The AIIC Team

Prof Jako Kilter
Co-Investigator

Dr Yohan Seepersad
Co-Investigator

Dr Henri Manninen
Co-Investigator

Dr Sharad Maharaj
Co-Investigator

Amanda Zilla
Co-Investigator

Kyle Hunte
Co-Investigator

Azim Abdool
Co-Investigator

Dr Ken Sooknanan
Co-Investigator

Ravi Deonarine
Project Manager

Kevon Andrews
Project Manager

Amir Mohammed
Researcher

Lincoln Marine
Researcher

Lee Bissessar
Researcher

Jonathan Nancoo
Researcher

Derron Phagoo
Researcher

Sabrina Mohammed
Researcher

Cade Coker
Researcher

Samantha Deonarine
Researcher

Nathan Ragoobar
Researcher

Stephen Allong
Researcher

Chane Gomes
Researcher

Kyle Lochan
Researcher

Daniel Goitia
Technical Officer

Building AI Capacity in a Nation/Region

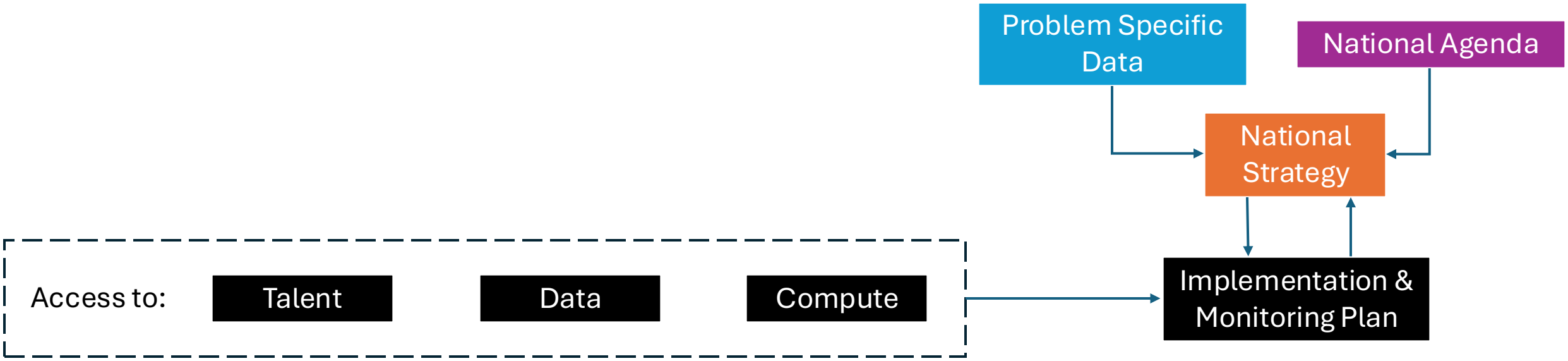
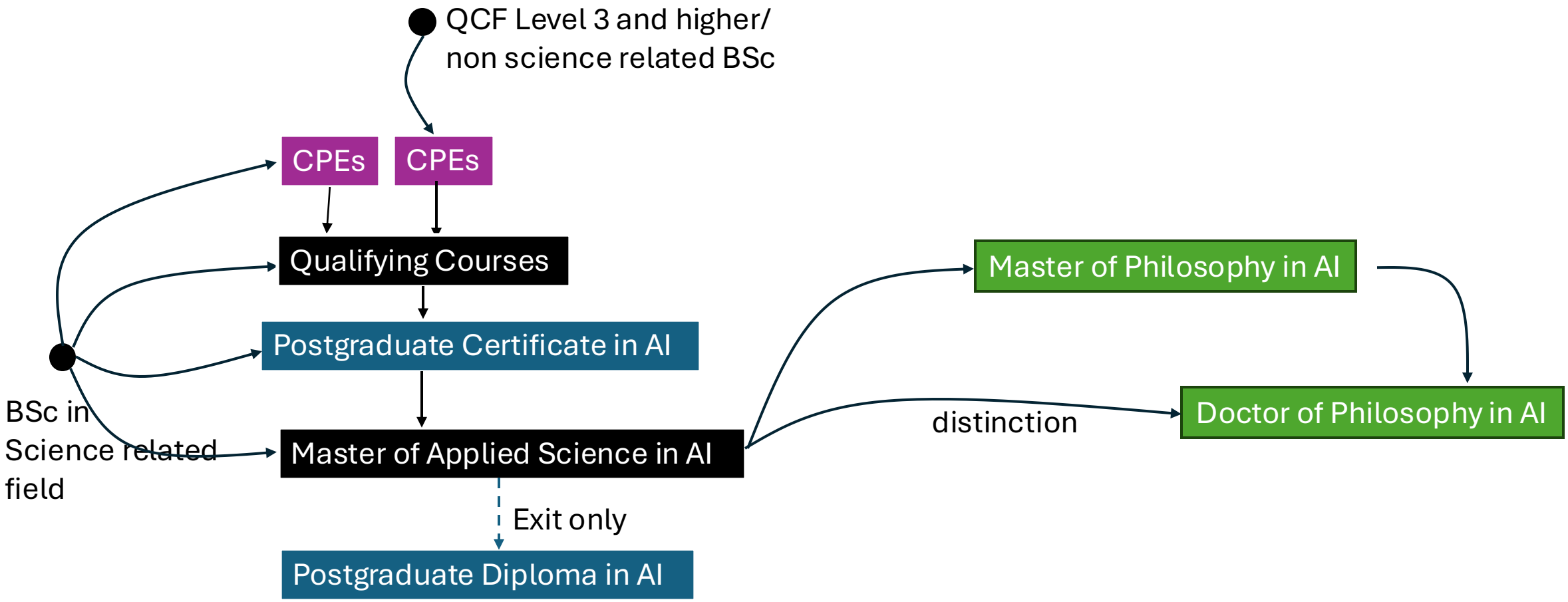
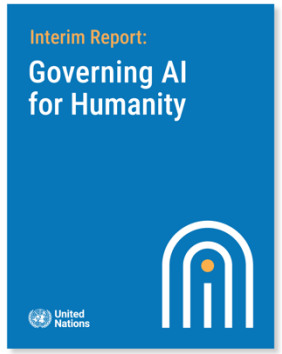


*Diagram shows high-level blocks and is not detailed

AI postgraduate Programmes Pathway

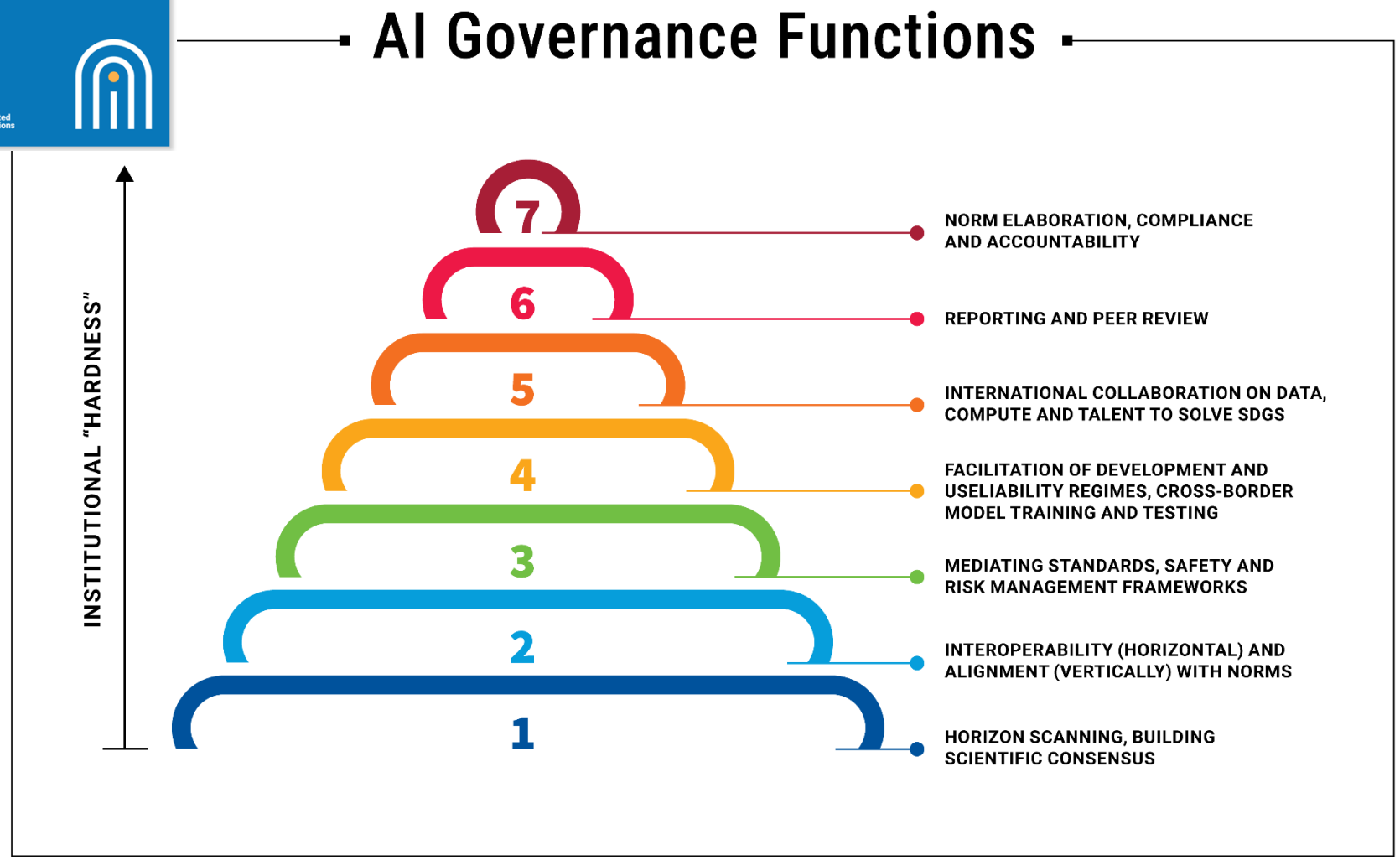


AI Governance Functions proposed in Interim Report



- To properly govern AI for humanity, Interim Report proposes that an international governance regime for AI should **carry out at least these functions**

- Could be carried out by **individual institution(s)** or a **network** of institutions



GOVERNING AI

Technical Infrastructure & Standards

Risk & Safety Governance

Institutional & Human Capacity

Law, Regulation & Enforcement

Ethical Principles & Societal Impact

Data Governance & Sovereignty

Public Engagement & Transparency

Global Cooperation & Diplomacy

AI Governance

Dimension	Key Focus Areas	Challenges	Recommended Strategies / Actions	Outcome / Goal
Technical Infrastructure & Standards	Data architectures, interoperability, lifecycle tools, compute resources	Legacy system integration; scalability constraints; cybersecurity vulnerabilities	Modernize IT infrastructure; ensure interoperability; adopt secure, scalable, and modular systems	Robust, secure, and future-ready AI infrastructure
Law, Regulation & Enforcement	Adaptive legislation, compliance, liability, IP rights, data protection	Technological pace outstripping lawmaking; legal ambiguity	Develop flexible legal frameworks; engage stakeholders; institutionalize regular legal reviews	Clear, enforceable, and future-responsive AI laws
Ethical Principles & Societal Impact	Fairness, transparency, accountability, bias mitigation, privacy	Embedded bias; opaque systems; low public trust	Create national ethical AI guidelines; require algorithmic audits; mandate inclusive design processes	AI systems that are ethical, accountable, and publicly trusted
Data Governance & Sovereignty	Data quality, ownership, sharing protocols, privacy, and access control	Fragmented standards; unclear ownership; cross-border data issues	Establish unified data standards; enforce data access governance; ensure compliance with privacy laws	Trusted, high-quality, and sovereign data ecosystems
Institutional & Human Capacity	AI talent pipelines, interagency collaboration, policy execution capacity	Workforce skills gaps; institutional silos; lack of execution capabilities	Invest in education & training; build multidisciplinary teams; improve coordination mechanisms	Skilled institutions able to design and manage AI policies
Risk & Safety Governance	Systemic risk identification, real-time monitoring, mitigation protocols	Unknown risks; adversarial attacks; safety assurance in critical sectors	Conduct continuous risk assessments; implement fail-safes and red teaming; certify safety protocols	Safe, resilient, and fail-secure AI deployment
Public Engagement & Transparency	Public education, civic feedback, digital inclusion, algorithmic transparency	Low awareness; digital divide; exclusion from AI decision-making	Host participatory forums; deploy plain-language communication; support access and equity initiatives	An informed, empowered, and digitally included public
Global Cooperation & Diplomacy	International standards, cross-border data governance, AI peace and security	Policy fragmentation; competitive tensions; interoperability challenges	Engage in multilateral forums; align with global AI principles (e.g. OECD, UNESCO); share best	Globally aligned AI systems and cooperative diplomatic posture

School of Digital Transformation and Innovation in the Caribbean 2025 16-20 June

THANK YOU