

# **Governing AI in the Public Sector: Balancing Innovation, Privacy & Security in the Fifth Industrial Age**

**Dr. May Siksik**

**CEO, Innovation Network Global**

**[May.siksik@innovationnetwork.ca](mailto:May.siksik@innovationnetwork.ca)**

# Innovation Network Global

**ING, the international expression of Innovation Network Canada, is a non-profit dedicated to commercializing and governing responsible tech**

**Builds and drives deep tech holistic innovation by bringing together:**

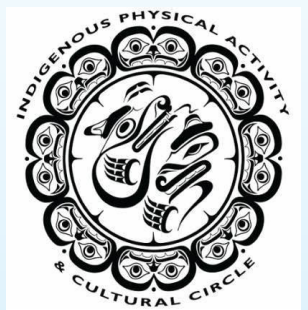
- ✓ Tech Companies**
- ✓ End Users**
- ✓ Commercialization Partners**
- ✓ Funding Organizations**

**Host of Dynamic Coalition on Emerging tech at the United Nations IGF**

**ING: Where Governance Meets Commercialization**



Edwin S.H. Leong Centre for Healthy Aging AP CARDIOLOGY ASSOCIATES



# Imagine a world where AI silently decides:

Who gets access to **healthcare, jobs, and public services**

How governments **monitor and secure citizens**

Which decisions are **automated and irreversible**

**... etc**

**Do we understand how these decisions are made?**

**Can we guarantee that AI is fair, transparent, secure, and accountable?**

**Our choices determine the future of trust in government, privacy rights, and digital sovereignty**

**Without structured governance, AI's influence could lead to a future where privacy rights, digital sovereignty, and public trust are at risk**

# The Need for a New Governance Model

- **Emerging technologies (AI, blockchain, cybersecurity, quantum computing) are deeply interconnected**
- **Existing governance models treat them as silos**
- **We need a governance framework that evolves with technology**

**What happens when an AI financial system, a blockchain-based ID platform, and a cybersecurity framework interact - but no one is ensuring they work together safely?**

# The Public Sector's AI Dilemma

## Key AI Governance Challenges:

- ✓ **Bias & Fairness Risks** – AI can discriminate in hiring, law enforcement, healthcare.
- ✓ **Security Vulnerabilities** – AI-powered cyberattacks, deepfakes, adversarial AI.
- ✓ **Lack of Accountability** – *Who is responsible when AI makes a mistake?*

**Without governance AI in public decision making can create more problems than it solves – Governance is critical to ensuring public trust**

# Smart Cities Example: Risks of AI in Public Infrastructure

## Smart Streetlights

- ✓ AI-powered streetlights track traffic & environmental conditions
- ✓ Connected to emergency response & smart city networks

## Risks:

- Hacking could disable city lighting, creating crime “dark zones”
- Surveillance misuse - citizen tracking without consent
- Security loopholes could expose critical infrastructure

**To prevent these risks, governments rely on AI governance frameworks**



# ISO 42001: Strengths & Gaps

## ISO 42001: What It Covers

- ✓ AI policy & risk management
- ✓ AI transparency & accountability
- ✓ AI alignment with cybersecurity best practices (ISO 27001)

## What's Missing?

- ✗ No bias, fairness, or explainability audits
- ✗ No human rights compliance
- ✗ No sector-specific AI governance
- ✗ No adversarial attack testing

**ISO 42001 is a foundation but lacks AI system certification for ethical and security risks**

# Dynamic Coalition Certification at the United Nations IGF



## What Makes this AI Certification Different?

- ✓ Certifies AI systems, not just governance processes
- ✓ Bias & fairness audits
- ✓ Security & adversarial attack testing
- ✓ Alignment with global governance frameworks (UN SDGs, OECD AI, G20)

**Bridges the gap between policy & real-world AI risks**

### Co-Leads:

1. Dino Cataldo Dell'Accio (CIO, UNJSPF)
2. May Siksik (CEO, ING)

# AI in Healthcare: PHIS Case Study

## Personalized Health Information System (PHIS)

- ✓ Uses AI for diagnostics & patient tracking
- ✓ Integrates wearables & predictive analytics

## Risks:

- Bias in medical AI predictions
- Privacy concerns in patient data sharing
- Cybersecurity vulnerabilities in hospital networks

## How Certification Helps:

- ✓ Bias-free health predictions
- ✓ Quantum-safe encryption for patient records
- ✓ Ongoing security & compliance audits

**AI in healthcare must be safe, secure, and equitable**

# AI Security & Cyber Threats

## AI and quantum computing cybersecurity threats:

-  Deepfake misinformation & AI-powered fraud
-  AI-enhanced phishing & cyberattacks
-  Quantum computing threats to encryption
-  AI/Quantum hybrid threats

## Governance Solutions:

- ✓ AI resilience certification
- ✓ Continuous cybersecurity risk assessments
- ✓ Post-quantum security compliance
- ✓ Multi-technology governance models

**Governments must stay ahead of AI security risks**

# 8 Practical AI Governance Strategies

## Governments must:

- 1 Establish AI governance structures (Chief AI Officer, AI Ethics Board)
- 2 Mandate AI certification before deployment
- 3 Require Privacy Impact Assessments (PIAs)
- 4 Ensure AI transparency & explainability
- 5 Conduct independent AI bias audits
- 6 Align AI with UN SDGs & OECD AI Principles
- 7 Prepare for quantum AI & adversarial risks
- 8 Educate the public on AI governance & security

**Proactive governance is the key to AI's success in the public sector**

**Do we want AI to assist us, or do we want AI to govern us? The choice is ours, but only if we act now**

# Thank you!

## Contact us!

**Innovation Network Global Headquarters: Vancouver, Canada**

**Dr. May Siksik**

[May.Siksik@innovationnetwork.ca](mailto:May.Siksik@innovationnetwork.ca)

[www.innovationnetwork.global](http://www.innovationnetwork.global)

[info@innovationnetwork.global](mailto:info@innovationnetwork.global)

[dellaccio@un.org](mailto:dellaccio@un.org)