WHOLE-OF-SOCIETY CYBER RESILIENCE FOR INCLUSIVE AND SUSTAINABLE INNOVATION

MAMELLO THINYANE
SENIOR RESEARCH ADVISOR, UNU

SESSION 4 – INDUSTRY, INNOVATION, AND INFRASTRUCTURE (SDG 9)
6th North-East Asia Multistakeholder Forum on Sustainable Development Goals

Wednesday 7th September 2022, 15h30 - 17h00 (UTC+8)
The World Economic Forum recognizes that the risks, rewards and governance of the networked economy are core issues of the global agenda and fundamental for sustainable growth and stability. Additionally, it recognizes that only a coordinated approach will ensure that new opportunities for growth are fully leveraged, and risks managed.
Focus on information systems, ICT infrastructure, technology tools and platforms

Due to the high impact of failure of critical information infrastructure / SCADA systems

Focus on government and private sector; Better interaction between governments and business
Resilience is a systemic attribute and requires whole-of-society approach.

Multi-dimensionality of cyber resilience

Important responsibility of civil society as active cybersecurity agents

Increasing cyber risks to individuals and communities

People are the key attack surface and vector

Current cybersecurity frameworks are difficult to operationalize for civil society
TO WHAT EXTENT DO NATIONAL CYBER SECURITY STRATEGIES INCORPORATE CIVIL SOCIETY CYBER RESILIENCE?

IN (North-East) ASIA AND THE PACIFIC
GLOBAL CYBERSECURITY INDEX

HIGH
- Singapore,
- Malaysia, Australia,
- Japan, South
- Korea, China, New
- Zealand, India

MEDIUM
- Philippines,
- Bangladesh, Sri
- Lanka, Samoa

LOW
- Afghanistan,
- Vanuatu

HUMAN DEVELOPMENT INDEX

VERY HIGH
- Singapore, Malaysia,
- Australia, Japan,
- South Korea, New
- Zealand

HIGH
- Philippines,
- Samoa, China,
- Sri Lanka

MEDIUM
- Vanuatu, India,
- Bangladesh

LOW
- Afghanistan
• Several countries include resilience thinking in their strategies
• Few countries give elaborate framing and operationalization of cyber resilience
• All countries acknowledge cyber security as a shared duty of all stakeholders
• However, there are limited avenues for citizen co-production of cyber security
• Citizens largely framed as recipients of cyber security
• There is better engagement between certain sectors e.g., government and private sector
CYBER RESILIENCE POSTURE OF CIVIL SOCIETY ORGANIZATIONS IN MACAU SAR
Digital technologies can be a double-edged sword for CSOs, linked to the benefits of digital transformation and the exposure to cybersecurity risks.

CSOs operate in a context of limited resources and capacity for cyber resilience, increasingly complex regulatory and compliance environment, as well as an evolving cybersecurity risk environment.

There’s a need to strengthen local cybersecurity ecosystems with specific support and focus on CSOs.

Cyber resilience capacity-building is critical for CSOs.
Capacity-building with Civil Society Organizations
Recommendations

For government

• Prioritize cyber resilience resourcing and capacity building for civil society stakeholders
• Making allowances for cyber security in funding instruments
• Strengthening local CERTs
• Support for local compliance
• Facilitate engagement of civil society in coproduction of cyber resilience

For civil society organizations

• Put in place an organizational cyber resilience plan operationalized through policies, guidelines, programs and control activities
• Identify cost-effective controls including capacity-building, asset, and access management

For citizens

• Enhance your cyber resilience posture through capacity-building activities
• Actively manage your cyber resilience
THANK YOU

UNITED NATIONS UNIVERSITY
INSTITUTE IN MACAU
Estrada do Engenheiro Trigo No 4, Macau SAR

CONTACT
cyber-resilience@unu.edu

Acknowledgement:
This work is supported by the Science and Technology Development Fund of Macau (FDCT) under Grant No. 0016/2019/A