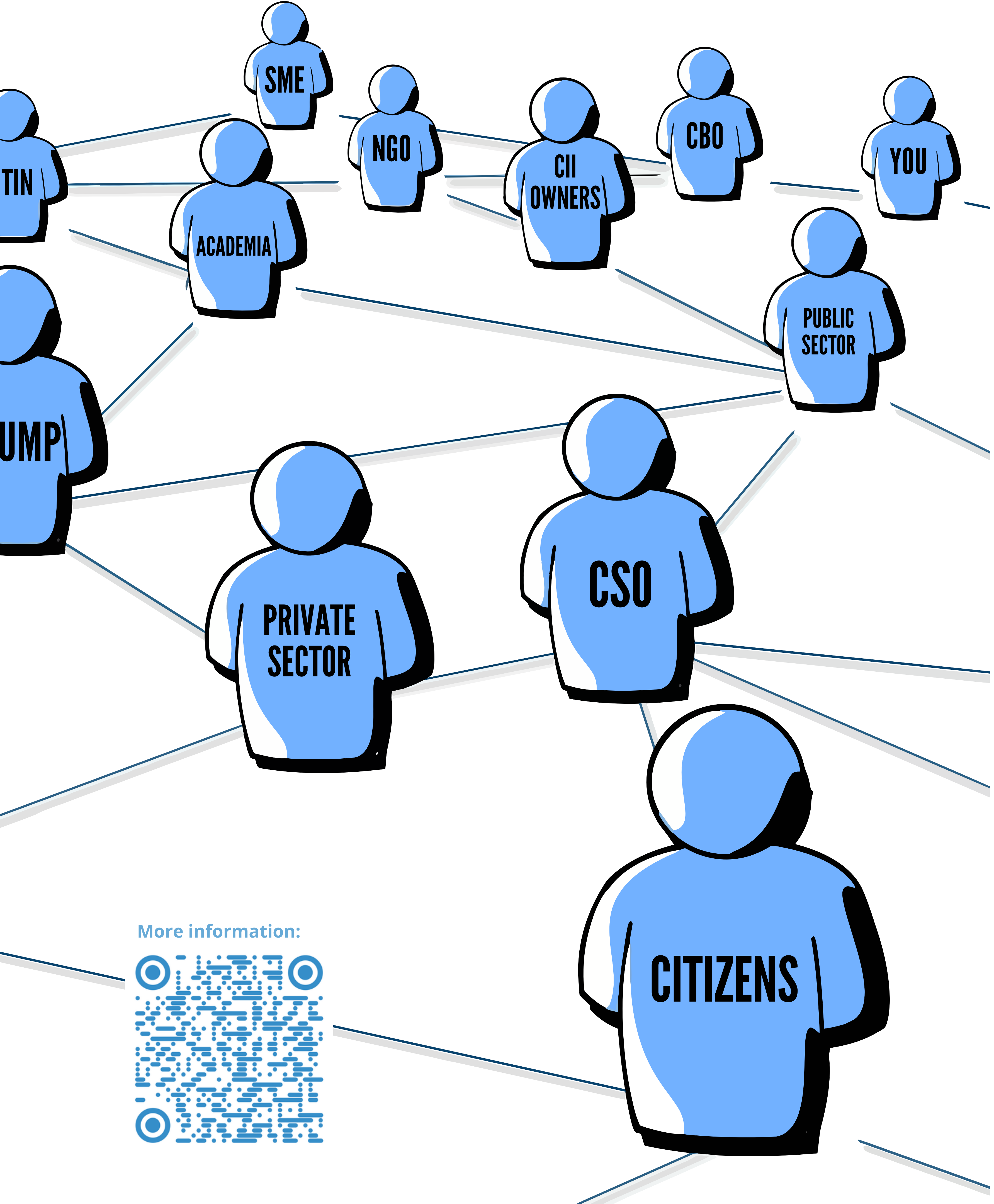
CYBER RESILIENCE AND AWARENESS FOR SOCIETY FOSTERING COLLABORATION WITH ITU

MAMELLO THINYANE
WITH DEBORA CHRISTINE AND CHRISTY UN

CYBERSECURITY POST-FORUM SESSION (DAY 3)
ITU Regional Development Forum Asia-Pacific

Wednesday 4th November 2020, 14h45 - 15h45 (UTC+7)

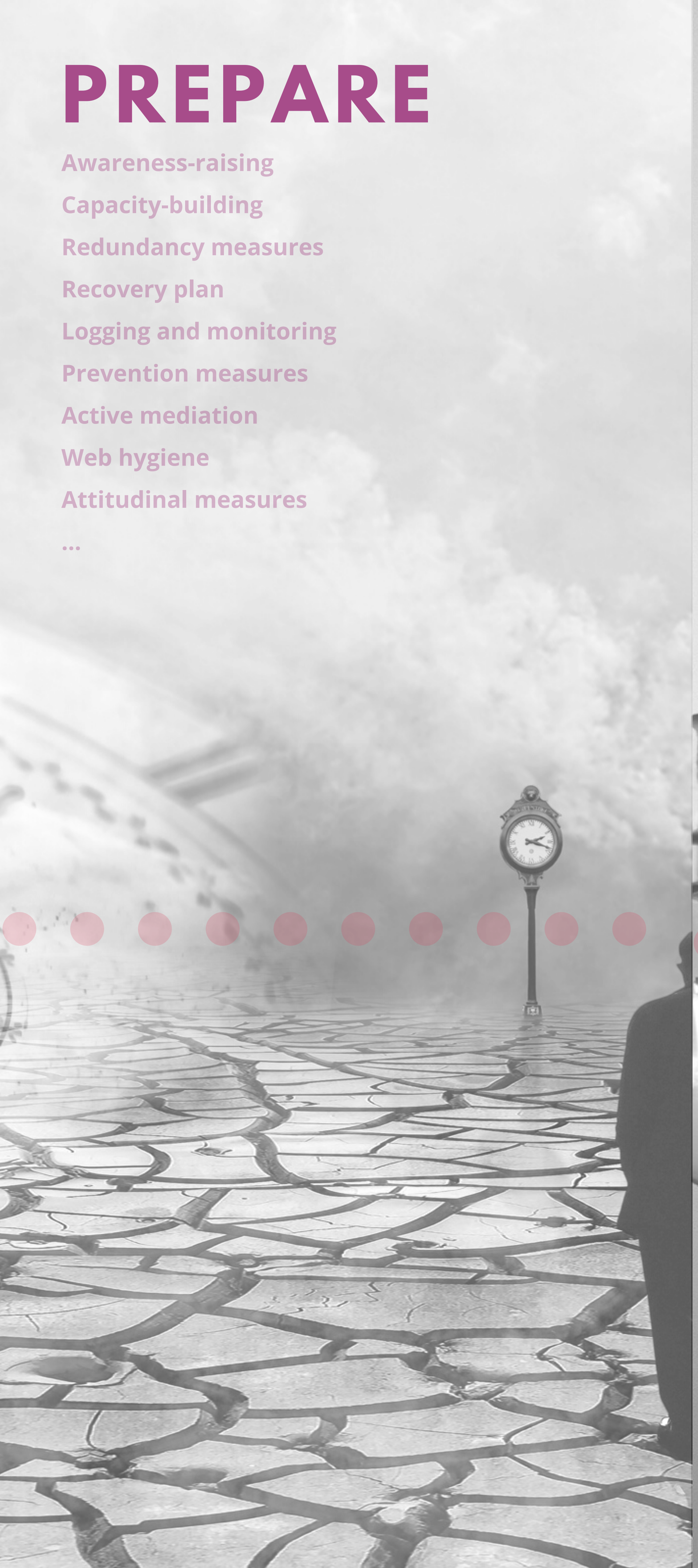
UNITED NATIONS UNIVERSITY
Institute in Macau



More information:

WHY CONSIDER CIVIL SOCIETY FOR NATIONAL CYBER RESILIENCE?

- 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



PREPARE

- Awareness-raising
- Capacity-building
- Redundancy measures
- Recovery plan
- Logging and monitoring
- Prevention measures
- Active mediation
- Web hygiene
- Attitudinal measures
- ...

ABSORB

- Alternative resources
- Withstand measures
- Incident reporting
- Threat removal measures
- Sandboxing and isolation
- Engage measures
- ...

RECOVER

- System recovery
- Account recover
- Data recovery
- Professional support
- Social support
- ...

ADAPT

- Evolve measures
- System upgrades
- Resource swapout
- Bounce forward
- Enhanced capacity
- ...

More information:

TO WHAT EXTENT DO NATIONAL CYBER SECURITY STRATEGIES INCORPORATE CIVIL SOCIETY CYBER RESILIENCE?

IN 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

INCLUSION OF CYBER RESILIENCE THINKING IN THE STRATEGIES

USE OF "RESILIENCE" TERMINOLOGY

- Most countries use the term resilience in the strategies, but few elaborate on operationalization of resilience
- Others do not use the term "resilience" but include strategies for building resilient systems and ensuring business continuity

RESILIENCE AS A GOAL

- Some countries identify secure and resilience environment as a strategic goal in the NCS

SPECIFIC CASES

- Singapore and Philippines have very elaborate incorporation of cyber resilience into the NCS
- They define resilient state of cyberspace, and the norms, procedures, processes and practices that it comprises

WHOLE-OF-SOCIETY POSTURING IN THE STRATEGIES

CYBER RISKS IDENTIFIED

- All countries identify not only state-level and entity-level cyber risks, they also note individual-level risks (e.g., identify theft)
- People are identified as one of the important attack surfaces

ROLES AND RESPONSIBILITIES

- Several countries identify the role of community-level stakeholders
- Third-sector organizations encouraged to participate in:
  - information sharing,
  - outreach activities,
  - evaluating cybercrime law (e.g., Bangladesh)
  - joining national CERT (e.g., New Zealand)
  - joining national cybersecurity steering committee (e.g., Vanuatu)

WHOLE-OF-SOCIETY POSTURING IN THE STRATEGIES

PUBLIC COMMUNICATION

- All countries use diverse programs and materials to raise awareness on cybersecurity risks
- Singapore adopts an advanced public outreach approach and draws on behavioral insights to nudge good cyber hygiene practice in the general public

CAPACITY BUILDING

- Countries adopt a variety of approaches for building cyber capacity in citizens:
  - professional training programs including sector-specific training
  - educational programs run in schools, colleges and universities
  - certification and accreditation for professionals

WHOLE-OF-SOCIETY POSTURING IN THE STRATEGIES

CITIZEN CO-PRODUCTION OF CYBERSECURITY

- Few countries mention specific tools or platforms to facilitate citizen's participation in cybersecurity
- Australia, New Zealand and Singapore have "hotlines" for reporting adverse cyber events

PROTECTION OF VULNERABLE GROUPS

- Several countries identify specific population groups and sectors that are vulnerable to cyber attacks
  - children and young people
  - women
  - tourism sector (e.g., Samoa)
  - elderly (e.g., Sri Lanka)
  - rural communities
- Specific mechanisms to empower the vulnerable
  - child online protection (e.g., Afghanistan, Samoa, Vanuatu, China)
  - outreach programs

KEY FINDINGS:

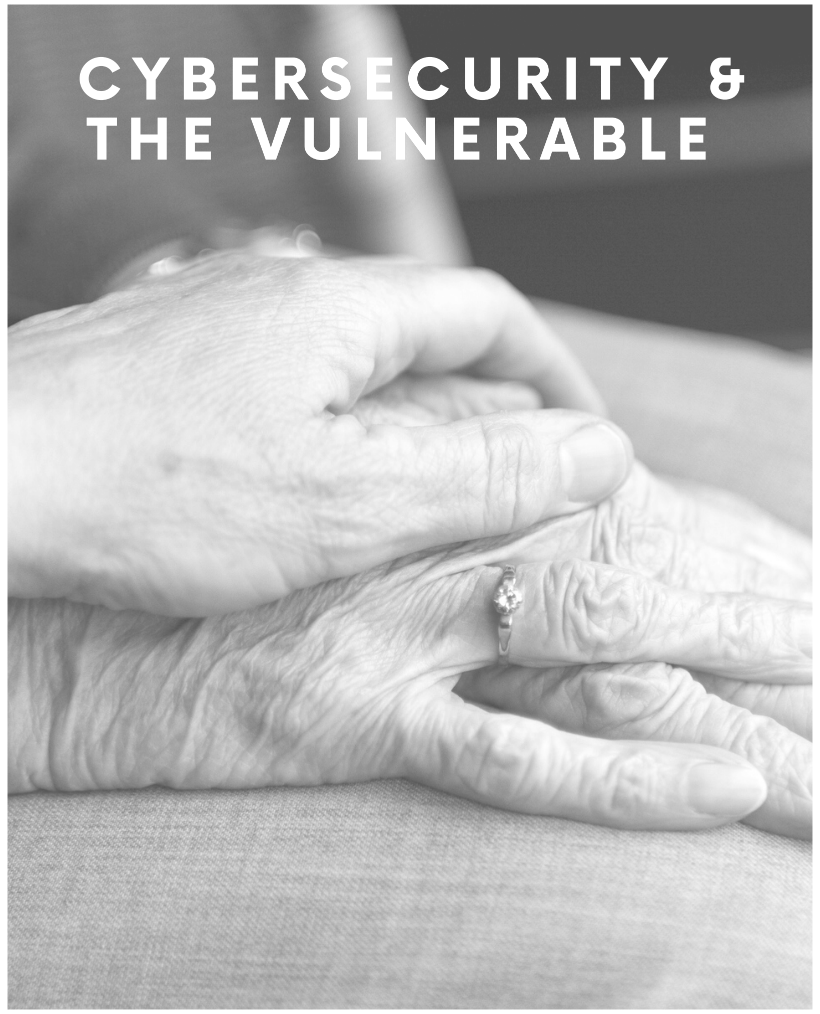
The full report available at
https://collections.unu.edu/view/UNU:7760

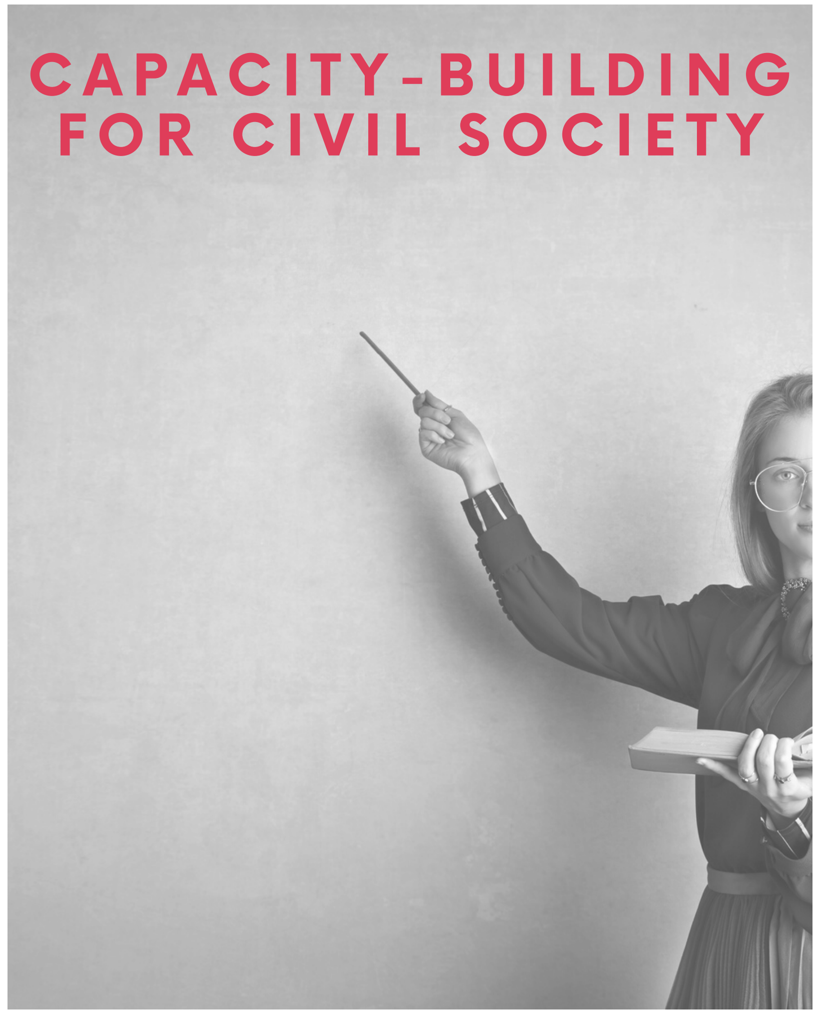
- Several countries include resilience thinking in their strategies
- Few countries give elaborate framing and operationalization of cyber resilience
- All countries acknowledge cyber security as a shared duty of all stakeholders
- However there are limited avenues for citizen co-production of cyber security
- Citizens largely framed as recipients of cyber security
- There is better engagement between certain sectors e.g., government and private sector

Going forward?

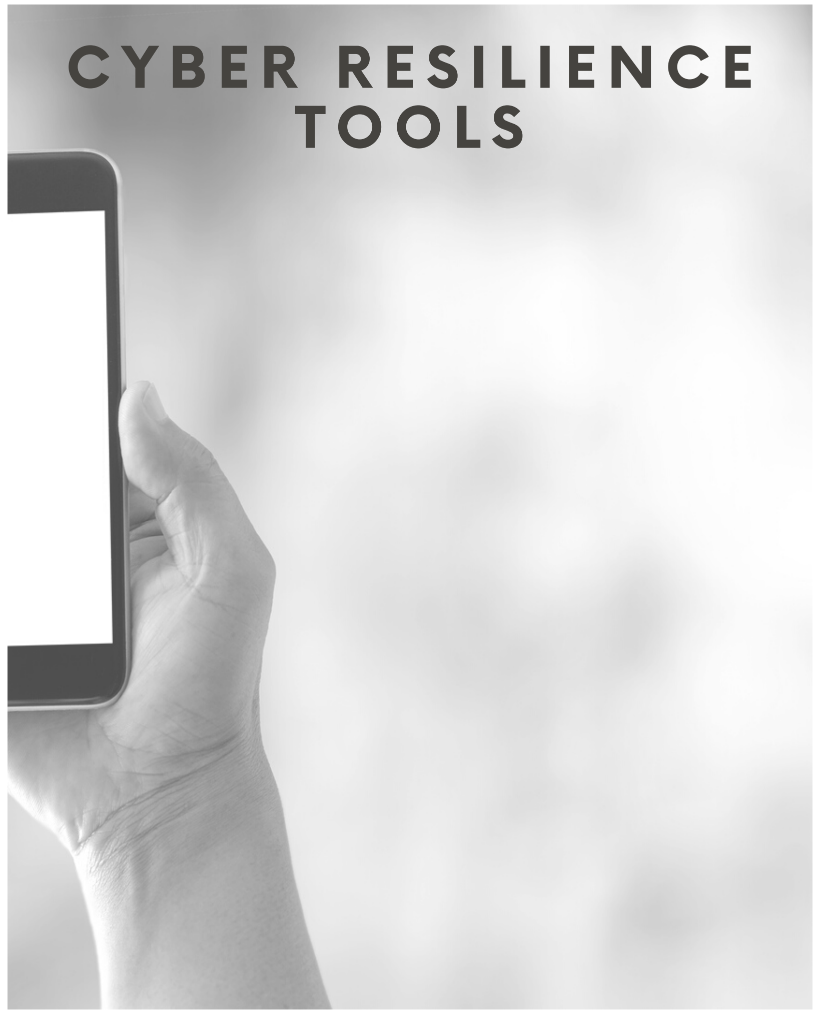
ITU STRATEGIC FRAMEWORK 2020 - 2023 GOAL 3 "SUSTAINABILITY"

"... manage emerging risks, challenges and opportunities resulting from the rapid growth of telecommunications / information and communication technologies ..."


CYBERSECURITY & THE VULNERABLE


CAPACITY-BUILDING FOR CIVIL SOCIETY

NATIONAL CYBERSECURITY STRATEGIES


CYBER RESILIENCE TOOLS

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