Cyber Resilience in Asia-Pacific: A Review of National Cybersecurity Strategies

URL:

https://collections.unu.edu/view/UNU:7760

QR-Code:

Abstract:

Cyber resilience, the ability for positive adaptation in the face of adverse cyber events, is seen as an evolution in the cybersecurity posture of organizations and countries. It represents a mindset shift from protection and avoidance of adverse cyber events and the development of fail-safe systems to anticipation and planning for adverse cyber events, including the development of systems that are safe-to-fail. At the national level, the adoption and incorporation of resilience thinking in the national cybersecurity strategies is given impetus by several factors, including the inevitability of both known and unknown cyber risks, as well as the demands for holistic resilience from multilateral frameworks, including the United Nations 2030 Sustainable Development agenda, the New Urban Agenda, and the Sendai framework. This report presents findings from a review of the national cybersecurity strategies of several countries in the Asia-Pacific region. The review is framed along several lines of inquiry that explore the extent to which the countries incorporate whole-of-society cyber resilience in their national cybersecurity strategies. While most countries give recognition of the importance of cyber resilience, few countries provide a detailed operationalization of cyber resilience in their strategies. Not surprisingly, the pattern, that countries with higher cybersecurity maturity have a more nuanced articulation of cyber resilience, is noted from the review. However, some countries with lower cybersecurity maturity are noted to provide more apparent avenues for the engagement of civil society stakeholders, including third-sector organizations, in the cybersecurity strategies. The report advances the importance of considering cyber resilience at the individual, community, national and global levels, and makes recommendations on how countries could operationalize whole-of-society cyber resilience.

Summary:

Cyber resilience effort and strategy has traditionally been considered from the position of enabling governments and business to deliver the intended outcomes despite disruptions to information and communication systems. There has also been a general focus on the security and resilience of critical information infrastructures, such as operational technology, industrial control systems, supervisory control and data acquisition systems, and also on vital sectors, such as telecommunications, banking, transportation, and health services.

However, there is a growing global recognition of the need for cyber resilience to be framed from the broad cyber ecosystem perspective, beyond the narrow technical and operational domains. Further, there is a recognition of the need for multi-stakeholder partnerships and engagement towards achieving cyber resilience. For example, the World Economic Forum underscored this need in their 2012 report titled "Partnering for Cyber Resilience." The UN Sustainable Development Goals (SDGs) advance the goal of "making cities and human settlements inclusive, resilient, and sustainable" under SDG11[1]. The Sendai Framework for Disaster Risk Reduction also places a key focus on strengthening resilience against disasters, which are broadly defined as "man-made hazards and related environmental, technological, and biological hazards and risks." Lastly, the New Urban Agenda, which was adopted at the Habitat III conference in 2016, emphasizes the need for "strengthening resilience in cities to reduce risk and impact of disasters."

Civil society is increasingly becoming a key stakeholder in the cyber ecosystem for several reasons: they represent one of the significant cyber-attack surfaces and vectors (e.g., through social engineering); they suffer an immense loss due to adverse cyber events including identity theft, data leakages and breaches, and dis/misinformation; and they have an essential role of play in the coproduction of cyber resilience at the individual, community, national, and global levels.

This research investigated the co-production of cyber resilience in Asia and the Pacific by reviewing the national cybersecurity strategies of 14 nation-states in the region to explore the following:

- The involvement of civil society stakeholders in the development of the cybersecurity strategies
- The extent to which resilience is incorporated into the cybersecurity strategies
- The extent to which whole-of-society perspectives are adopted in the strategies
- The roles, responsibilities, and mechanisms for participation ascribed to the civil society stakeholders (i.e., individual citizens, communities, and third sector organisations) in the strategies

The following are the main findings from the review:

[1] https://sdgs.un.org/goals/goal11

Use of “resilience” terminology

- Most countries use the term resilience in the national cybersecurity strategies, but few elaborate on the operationalization of resilience.
- While some countries do not use the term "resilience," they do include strategies for building resilient systems and ensuring business continuity (e.g., Malaysia, Japan, and South Korea).

Resilience as a goal

- Some countries identify a secure and resilient environment as one of the overarching goals of the national cybersecurity strategy i.e., beyond resilience just being a component of the national cybersecurity strategy.

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 critical attack surfaces, through social engineering, in the strategies.

Roles and responsibilities

- Several countries identify the role of community-level stakeholders in the strategy.
- Third-sector organisations are encouraged to participate in:
    - Information sharing.
    - Outreach activities.
    - Evaluating cybercrime law (e.g., Bangladesh).

Public communication

- All countries use diverse programs and materials to raise awareness of cybersecurity risks.
- Some countries adopt advanced public outreach approaches and draw on behavioural insights to nudge good cyber hygiene practices in the general public (e.g., Singapore).

Capacity-building

- Countries adopt a variety of approaches for building cyber capacity in citizens, such as:
    - Professional training programs – including sector-specific training.
    - Educational programmes for schools, colleges, and universities.
    - Certification and accreditation for professionals.

Protection of Vulnerable groups

- Several countries identify population groups and sectors that are vulnerable to specific cyber threats:
    - Children and young people,
    - Women,

    - Tourism sector (e.g., Samoa),
    - Elderly (e.g., New Zealand, Sri Lanka),
    - Rural communities.
- Specific mechanisms to empower the vulnerable are also identified:
    - Child online protection (e.g., Afghanistan, China, Samoa, Vanuatu).
    - Outreach programs.

Overall, countries recognize the importance and need for resilience towards preparing for, absorbing, recovering from, and adapting to the imminent global risks, including the cyber risks. According to the 2020 Global Risks Report, technological risks associated with cyberattacks, data fraud and theft, and infrastructure breakdown, are among the top ten most likely and most impactful global risks[2]. The report advances the importance of considering cyber resilience at the individual, community, national and global levels, and makes recommendations on how countries could operationalize whole-of-society cyber resilience.

Key messages:

- It is necessary and important for countries to frame cyber resilience at the whole-of-society level and from a holistic perspective. Countries are as resilient as their weakest sector within the cyber ecosystem.
- Cyber resilience has to be considered as a critical element of the overall resilience posture of countries.
- While most countries make a reference to “resilience” in their strategies, there remains a need for countries to clearly define cyber resilience and to articulate the goals, metrics, and pathways (including policies, programs, and tools) towards increased resilience.
- Partnerships at the local, national, and international levels are essential towards the achievement for cyber resilience.

[2] https://www.weforum.org/reports/the-global-risks-report-2020