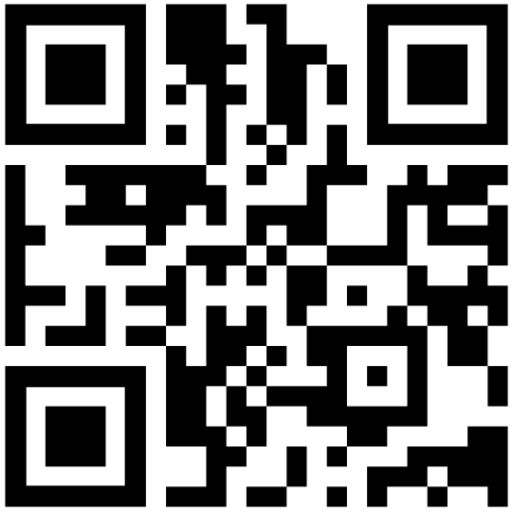
Civil Society Organizations' Cyber Resilience

Leaving No Civil Society Organization behind in Cyber Resilience

URL:

- Access the report at - https://go.unu.edu/3NN1O

QR-Code:



Abstract:

Civil society organisations (CSOs) play a critical role in society towards sustainable development - providing social services and promoting citizen participation. Increasingly, CSOs are relying on digital technologies for their operations. However, despite their increasing reliance on digital technology, especially during the ongoing pandemic, CSOs continue to lack the resources, expertise, capability, and influence to manage their cybersecurity effectively. Further, worldwide, CSOs remain marginalised in the dominant cybersecurity narratives, discussions on cybersecurity, and strategies on cyberspace.

The report presents findings from a study of the cyber resilience posture of CSOs in Macau SAR – China and the region's cybersecurity landscape. Following the pattern of CSOs worldwide, local CSOs occupy a precarious and vulnerable position within the local cybersecurity landscape, where their cyber resilience posture is shaped by their limited resources and limited participation in the local cybersecurity ecosystem. Further, the absence of cyber resilience management solutions tailored for the specific needs, practices, and context of CSOs limits their ability to benefit from existing tools, instruments, and services.

Given the systemic effect of adverse cyber incidents, the report echoes the call for building societal cyber resilience through addressing unequal distribution of cybersecurity resources between different sectors of society, improving cross-sectoral cooperation and coordination in cybersecurity

strategy formulation, capacity-building, and incident handling, and developing contextually informed cybersecurity solutions. It advances specific recommendations for the CSOs management, private service providers, and the government to contribute towards CSOs' cyber resilience.

Executive Summary:

Digital technologies have become increasingly integral to the effective functioning of societies worldwide. These technologies provide the critical infrastructure that supports operations across different domains at different levels. Digital technologies also support the resilience of societies to deal with stresses, shocks, and disasters, as has been evidenced during the COVID-19 pandemic. For example, despite the lockdown measures worldwide, schools continued providing lessons online, businesses and organisations shifted to virtual operations, and governments digitised their services.

As far as Civil Society Organisations (CSOs) are concerned, studies show an increasing reliance on digital technology for their mission and operations. For CSOs, the COVID-19 pandemic catalysed new forms of civic mobilisation, which has seen organisations shifting to digital organising and increasing their collaboration with various stakeholders in emergency relief and informal activism. However, digital technologies can also have constraining and adverse effects on the CSOs, for example, by increasing CSOs' exposure to new and advanced cyber risks, such as disinformation campaigns and advanced persistent threats (APT) attacks. Under this evolving threat landscape, CSOs remain ill-positioned and under-resourced, making them more susceptible to risks from adverse cyber incidents relative to the public and private sectors.

This situation underscores the need of cyber resilience, the capability to prepare for, absorb, recover from, and adapt to significant cyber threats which are multi-dimensional, emanating from the social, technological, environmental or personal environments. Cyber resilience needs to be considered at the systemic level in terms of the ability of different sectors of society, including citizens and civil society organisations, to cooperate and interact to deal with adverse cyber incidents.

This report observes how CSOs worldwide operate in a context of limited resources and capacity for cyber resilience, complex regulatory and compliance environment, as well as an evolving cybersecurity risk environment. In general, CSOs continue to experience marginalisation within the cybersecurity domain as far as threat intelligence reporting, direct technical support for incident handling, and capacity-building is concerned. As a result, most CSOs adopt ad-hoc and haphazard cybersecurity management practices, further perpetuating their precarity and vulnerability.

Further, this report details an investigation of the cyber resilience posture of civil society organisations in the local context of Macau SAR - China and finds that the organisations are similarly operating in the context of increased cybersecurity vulnerability and limited resources and capacity for cyber resilience, which has been exacerbated by the COVID-19 pandemic.

The report recommends that **civil society organisations**:

- undertake capacity-building for senior management,
- adopt appropriate cyber resilience management models,
- allocate and prioritise funding for cybersecurity,
- undertake targeted organisation-wide capacity-building,
- leverage external support and partnerships for cybersecurity.

As far as the **private sector** is concerned, the report recommends that they:

- define clear service level agreements for CSOs with specific cybersecurity commitments

- provide context-sensitive and informed solutions to CSOs.

Finally, the project recommends for the **governments** (especially in their role as funders) to:

- prioritise cybersecurity in CSOs' funding instruments,
- strengthen the local cybersecurity ecosystem to provide specific support for CSOs,
- provide capacity-building for CSOs,
- develop locally relevant cybersecurity resources for CSOs,
- strengthen cybersecurity threat intelligence research and communication.

Key messages:

- Digital technologies play a critical role in supporting the resilience of civil society organizations during stresses, shocks, and disasters – as has been evidenced during the ongoing pandemic.
- Notwithstanding the positive effects and benefits of digital technologies, they also expose civil society organizations to new and advanced forms of cyber risks.
- Many civil society organizations remain in a vulnerable and precarious position due to their limited resources, expertise, capability, and influence for cyber resilience. This has been exacerbated by the increasing reliance on digital technologies and by the increase in the frequency, sophistication, and severity of adverse cyber incidents.
- Enhancing societal cyber resilience in general and specifically civil society organizations' cyber resilience requires systemic and holistic interventions that actively engage the civil society sector in policy and strategy formulation, capacity-building, and incident handling.
- It is crucial to ensure that we leave no civil society organization behind in cybersecurity because societies remain as resilience as their weakest sectors.

Recommended Citation:

Un, C., Thinyane, M. and Christine, D. (2021) "**Civil Society Organizations' Cyber Resilience - leaving no civil society organization behind in cyber resilience**", United Nations University ISBN: 978-92-808-9131-7

Authors:

Christy Un is a visiting researcher with the Smart Citizen Cyber Resilience project at the United Nations University Institute in Macau. She holds a bachelor's degree in politics and international relations from the London School of Economics and Political Science.

Mamello Thinyane is a principal researcher at the United Nations University Institute in Macau, where he leads research on the Smart Citizen Cyber Resilience project. This project is undertaking research and developing tools to enhance the resilience of citizens and civil society stakeholders against adverse cyber incidents in smart digital futures.

Before joining UNU, Mamello was an Associate Professor in the Department of Computer Science at the University of Fort Hare in South Africa, as well as the Director for the Telkom Centre of Excellence

in ICT for Development at the same institute. He is a former Visiting Researcher at the Australian Centre of Cyber-Security at the University of New South Wales in Canberra.

Debora Christine is a researcher within the Data and Sustainable Development and Smart Citizens Cyber Resilience projects at the United Nations University Institute in Macau. Her primary interests are on the nexus of development, media, ICTs, inequality and social exclusion, and the construction of knowledge.

Debora received her MSc in media, communication and development from the London School of Economics and Political Science (LSE) and her BSocSc from Universitas Indonesia (University of Indonesia), specializing in media and communication studies.