The Cyber Resilience Lab
Tel Aviv University

ADVANCING CYBER RESILIENCE FOR SUSTAINABLE DIGITAL TRANSFORMATION

WHO WE ARE

The Cyber Resilience Lab at the internationally renowned Tel Aviv University is a leading global provider of comprehensive cyber resilience and digital transformation research and advisory services.

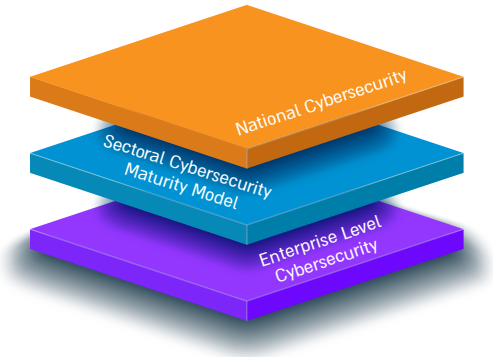
THE CHALLENGE

As developing countries increasingly operate modern cyber-physical systems and digital infrastructure, the need for digital resilience becomes acute.

INTEGRATING CYBER CAPACITY BUILDING IN SUSTAINABLE DEVELOPMENT

Digital transformation offers substantial dividends for sustainable development. Each Sustainable Development Goal (SDG) includes a digital component, with some SDGs more digitally-oriented than others.

The international development community needs better tools for integrating cyber capacity building into every project.

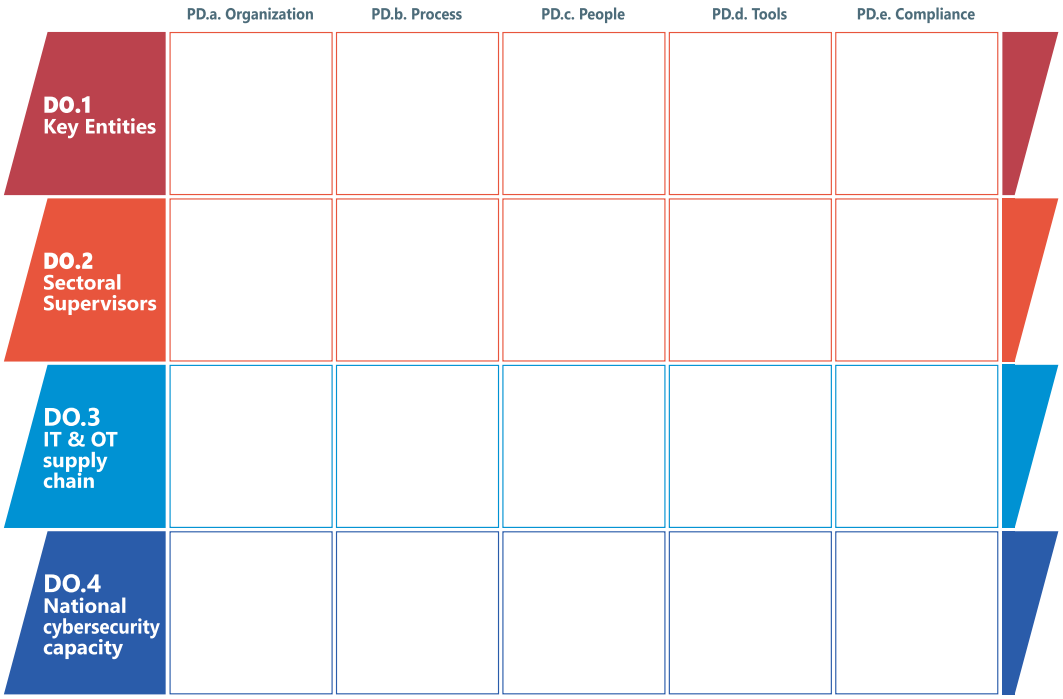


A single organization is the unit of analysis of most cybersecurity frameworks. On the opposite end are national-level cybersecurity and capacity-building instruments. Neither suffices for developing actionable and holistic roadmaps to maximize the benefits of digital transformation while enhancing cyber resilience. Comprehensive and sustainable digital resilience requires bridging this gap between the national and organizational levels.

THE SECTORAL APPROACH TO CYBER RESILIENCE AND CRITICAL INFRASTRUCTURE PROTECTION

We developed a Sectoral Cyber Capability Maturity Model, "PROGRESS - Promoting Global Cyber Resilience for Sectors and Society," to advance cyber resilience. This sectoral approach complements national and organizational practices.

PROGRESS analyses a sector of the economy as a socio-technical-economic system (STES). The science of complex systems established that resilience is an emergent property: a function of the interaction of different system parts. In other words, increasing the robustness of individual components of any system does not linearly improve the system's resilience. Therefore, the four dimensions of operation of PROGRESS CCMM incorporate key sector entities, national cyber capacity, supply chain, and sectoral regulatory authorities in a unified, comprehensive architecture.



Using PROGRESS CCMM brings the different stakeholders to the table and generates impactful, cooperative, and actionable progression paths.

Recommendations span people, processes, and technology across the four dimensions of operation. PROGRESS incorporates industry best practices and methodologies, especially regarding operational technology (OT) and industrial control systems (ICS). Most of the topics and indicators in PROGRESS are well-aligned with NIST CSF: the leading authoritative cybersecurity framework.

WHY US?

Building upon the diverse pool of interdisciplinary researchers at Tel Aviv University and Israel's tech industry experts, the Cyber Resilience Lab delivers applied solutions for sectoral Critical Infrastructure Protection (CIP) in support of sustainable development and capacity building.
Governments and global development institutions seeking to raise cybersecurity capability and achieve sustainable progress in large-scale socio-economic development benefit from our bespoke service.

The World Bank chose us as an exclusive knowledge partner to develop a new sectoral cyber capacity-building methodology.

We successfully applied PROGRESS CCMM in twelve developed and developing countries in Europe, Central Asia, and West Africa in collaboration with governments and Multilateral Development Banks (MDB).

We develop a bespoke system-wide roadmap for resilient digital transformation and cybersecurity capability-building for our customers.

We bring together leading practitioners and researchers through a public-private partnership to help our customers manage risks and optimize investments.

GET IN TOUCH TO LEARN MORE ABOUT HOW WE CAN HELP YOU.

Dr. Lior Tabansky, Head of the Cyber Resilience Lab at Tel Aviv University.

liort@tauex.tau.ac.il

The Cyber Resilience Lab
Tel Aviv University

https://rcrl.tau.ac.il/