International Journal of Information Security (2025) 24:18
https://doi.org/10.1007/s10207-024-00910-3

REGULAR CONTRIBUTION

PROGRESS: the sectoral approach to cyber resilience

Lior Tabansky[1] · **Eynan Lichterman**[2]

Accepted: 16 October 2024 / Published online: 7 November 2024

Abstract
Each critical infrastructure and vital service represents a unique instance of a complex socio-technical–economic system. Resilience in complex systems is an emergent behaviour that occurs from interactions between components and is not easily predictable from understanding each component in isolation. Yet, cybersecurity practice and maturity models still focus on the robustness of separate components: organizational units, firms, or IT applications. Such a fundamental mismatch between theory and tools is among the causes of pervasive cyber insecurity. We introduce the sectoral capability maturity model to enable a comprehensive improvement of systemic resilience. The promoting global cyber resilience for sectors cyber-capability maturity model incorporates the science of complex systems, cybersecurity frameworks, and two decades of CIP operations experience. The model was successfully applied in resilience assessment projects in a dozen countries. Real-life experience emphasizes the benefits of the sectoral approach to cyber resilience: creating feedback loops within the sector, integrating supply chain and third-party risks, facilitating information flows between stakeholders, enabling cooperation with and among ministries, departments and other authorities, weighting in the links and processes between actors in cybersecurity issues. The established value of the sectoral approach calls for applications that will improve the resilience of essential services while lowering sector-wide cybersecurity expenditures.

Keywords Critical infrastructure protection (CIP) · Cybersecurity · Cyber resilience · C2M2 · Socio-technical systems

1 Introduction: scaling up cyber resilience through a sectoral approach

Societies strive to improve cybersecurity, particularly within critical infrastructures. Capability maturity models (CMMs) have long been employed as essential tools for assessing and developing cybersecurity practices. Traditionally, these CMMs have focused on individual organizations or, less commonly, entire national economies. However, such approaches are of limited utility because they struggle to reflect the interdependencies of complex socio-technical–economic systems (STES).

This paper introduces a novel approach rooted in complex systems theory. Such an approach recognizes that the sector level is optimal for assessing and building the most fitting capabilities, offering a more detailed and holistic understanding of dynamic interaction between nodes and links within a given industry.

The theory of complex systems emphasizes that different parts of a system interact in non-linear ways, creating emergent behaviour, which is not predictable from understanding each component in isolation. Every sector or critical infrastructure is a private case of a complex system and functions as an intricate network of interdependent organizations, processes, and technologies, making them ideal candidates for applying complex systems theory.

Resilience in complex systems emerges from the interaction between components and constituents of the system and external inputs, including shocks. Increasing the robustness of each component, or *node*, does not linearly advance systemic resilience. Addressing the *links* rather than nodes can generate more significant and faster improvement in resilience in STES. Systemic resilience is a function of the depth, intensity, and agility of communication, connectivity, and cooperation between the nodes of an STES.

✉ Lior Tabansky
liort@tauex.tau.ac.il

[1] Blavatnik Interdisciplinary Cyber Research Center (ICRC), Tel Aviv University, Tel Aviv, Israel

[2] Liacom Systems Ltd, Holon, Israel

1.1 The lack of a sectoral approach

A 'referent object' to be secured against threats from cyberspace may be of varying scale. Four such categories of scale are evident: global, national, sectoral and firm. While global-level models hold rather a theoretical value, the national models, such as Oxford CMM[1] or CRI 2.0,[2] serve their purposes but are naturally too high-level for operational applications.

Previous initiatives have sought to implement a sector-focused approach to cybersecurity, with varying degrees of success. Here, we will list the most significant.

1. NIST Cybersecurity Framework (CSF).[3] While the National Institute of Standards and Technology (NIST) developed the CSF primarily for organizations, it offers implementation guides for sectors such as manufacturing and healthcare. However, it remains an enterprise-centric framework, rather than providing a comprehensive sector view.
2. The U.S. Department of Energy (DoE), together with the Department of Homeland Security (DHS), started developing the first version of Cybersecurity Capabilities Maturity Model (C2M2) for the electricity subsector in 2012. This approach was expanded to other (sub)sectors. In time, multiple industry-specific CCMMs were built, among them:
   a. Electricity subsector C2M2 (ES-C2M2),[4]
   b. Oil and Natural Gas Subsector C2M2 (ONG-C2M2)[5]
   c. Dams-C2M2[6]

Most of them, even when being called sectoral, maintain an enterprise-centric approach: to assess and increase the cyber capabilities of a single enterprise in a sector. The models' mission definitions corroborate this.

Examples: "*The ES-C2M2 is designed for use with a self-evaluation methodology and toolkit… for an organization to measure and improve its cybersecurity program*."[7]

"The ONG-C2M2 is designed for use with a self-evaluation methodology and toolkit… for an organization to measure and improve its cybersecurity program"[8]

Other derivatives of the original C2M2 also carry this designation. Therefore, we can confidently conclude that many so-called 'sectoral' models are actually enterprise-oriented models specifically fine-tuned for application in particular sectors.

Thus, a gap in knowledge is evident. The importance of scaling up cyber resilience through the sectoral approach has driven the development of the PROGRESS CCMM. Our approach fills the structural gap between the (few) national-level and numerous firm-level cybersecurity frameworks, instruments, and practices.

2 Complex systems: aiming for smart resilience

Complex networks are found in various domains such as ecosystems, social networks, and technological infrastructures. Resilience refers to a network's ability to withstand and recover from failures or attacks, ensuring continuous functionality and adapting to withstand similar failures in the future.

Robustness is defined as the capacity of the network to maintain its functions despite disruptions. In contrast, **Resilience** is the ability of the network to restore functions after a disruption and adapt for the future, 'bouncing forward'.[9]

These concepts are commonly visually presented at a Rieger's Disturbance and Impact Resilience Evaluation Curve (Fig. 1).[10]

Rieger's curve was introduced in 2014 and updated in 2017 with 'R'-phases of a disturbance event.

Since Rieger and co-authors focused on electricity grid applications, the timeline of X axis was supposed to be logarithmic, disturbance-failure event taking seconds, and recover-restore phases taking months.

For cybersecurity applications, we modify the last phase, which should be presented as: **Restore and Evolve**.

A common mistake is restoring the system to its prior level of optimal performance, that failed to prevent the incident. The incident may have exploited human, process or technical vulnerabilities. Smart resilience requires learning lessons and evolving. Restore and evolve means an altered optimal operational configuration that would be resilient to the

[1] Oxford Cybersecurity Capacity Maturity Model for Nations // https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

[2] Potomac Institute Cyber Readiness Index 2.0 // https://potomacinstitute.org/images/CRIndex2.0.pdf

[3] The NIST Cybersecurity Framework (CSF) 2.0 // https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[4] http://energy.gov/oe/downloads/electricity-subsector-cybersecurity-capability-maturity-model-may-2012

[5] https://www.energy.gov/sites/default/files/2014/03/f13/ONG-C2M2-v1-1_cor.pdf

[6] https://www.cisa.gov/resources-tools/resources/dams-sector-cybersecurity-capability-maturity-model-c2m2-2022

[7] http://energy.gov/oe/downloads/electricity-subsector-cybersecurity-capability-maturity-model-may-2012

[8] https://www.energy.gov/sites/default/files/2014/03/f13/ONG-C2M2-v1-1_cor.pdf

[9] [Cornish [6]].

[10] [Rieger 23; Mcjunkin and Rieger [16]].

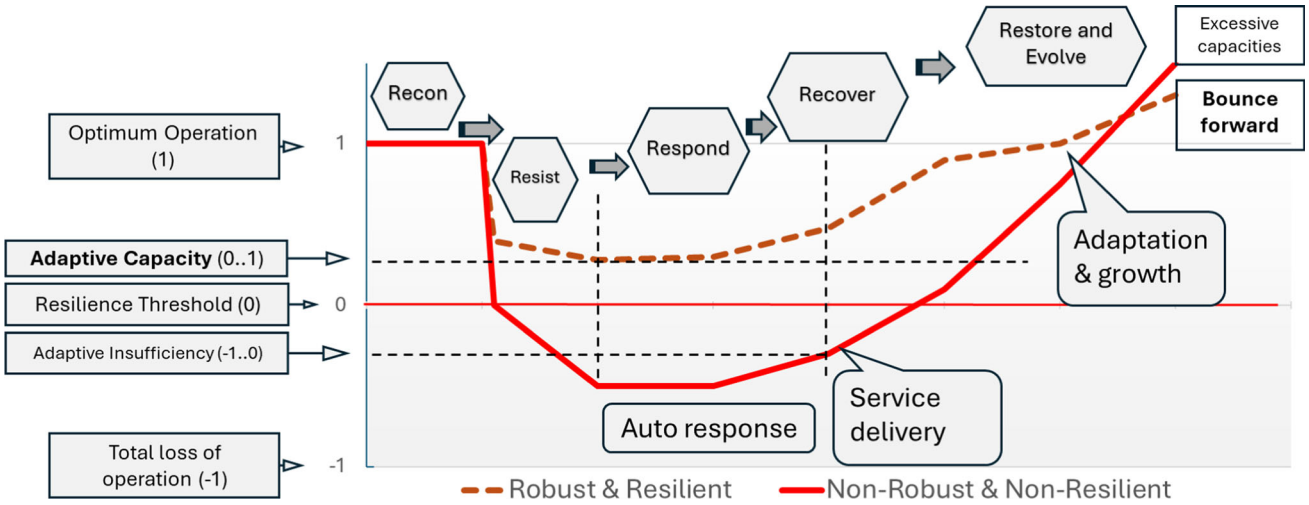

Fig. 1 Disturbance and impact resilience evolution curve. original idea: [Rieger, 2014]

exploited vulnerabilities, cascading effect or attack pattern. It may include changes in operational procedures, developing and deploying new equipment, altering security protocols, adding slack reserve capacities.[11]

A similar mistake is to over-invest in compensating controls: adding too much slack, buying the latest and most expensive cybersecurity solution, reengineering major components of the integrated system.

The optimal trajectory of a truly resilient system is adapting and "bouncing forward", finding a new optimal operation level.

Figure 1 presents two complex systems, which have experienced a failure or an incident, as two lines.

The dotted line system is *robust* and *resilient*—it withstood the incident, used up its adaptive capacity, but continued operation and recovered. Having been restored, it integrated the knowledge from the incident as new capabilities and widened its adaptive capacity.

The continuous line system is *neither robust*, *nor resilient*—due to the incident it lost capacities down to the level of *adaptive inefficiency*. Auto response measures did not recover it to *resilience threshold*, so a manual recovery and restoration were necessary. After the event, the fear of another incident on the same level caused the system owners to over-invest into the reserve capacities, decreasing the cost-efficiency of the whole system.

2.1 Systems theory as the foundation of the sectoral approach

As a fundamental review of the systems theory holds, "a network is a collection of units (nodes) non-trivially connected with each other by means of edges or links. Understanding how the structure and function of a network is affected by the failure of individual elements (nodes and/or edges) is a challenging task. Microscopic failures do not sum linearly and, although most failures may not heavily affect the functionality of the underlying system, the removal of specific elements may cause its collapse. The more abrupt the transition to a dysfunctional state, the more challenging it is to capture early-warning signals to prevent it or to devise effective responses to mitigate it".[12]

A common approach to testing a network for robustness and resilience is to use percolation theory, modelling the removal of nodes or links and observing the network's structural response. The final goal is to dismantle the network and record all important parameters along the way.

Optimal percolation strategies and network dismantling techniques are targeted at identifying the minimal set of nodes or links whose removal would disrupt the network at the largest scale. Simple strategies focus on attacking nodes in the order of their centrality score, while more complex strategies adjust quickly during the dismantling process. Also, crucial nodes may not always be the most connected ones: sometimes, nodes with few connections but strategic locations within the network are more significant.

Network failures not only happen in the cases of deliberate attacks. A failure of a systemically important node or a link can lead to the collapse of the network through cascading failures.

[11] These phases can also be linked to the NIST CSF 2.0 framework, although CSF functions are not as sequential on the timeline. "Recon" relates to Identify (ID) and Detect (DE), "Resist" – to Protect (PR). "Respond", "Recover" and "Restore" phases correlate with Respond (RS) and Recover (RC) functions. "Evolve" phase corresponds with the CSF 2.0 major change from CSF 1.1 version with the introduction of Govern (GV) function.

[12] [Artime, O., Grassia, M., De Domenico, M. et al. [3]].

Cascading failures occur when localized failures propagate through the network, spreading the collapse and rapidly diminishing the 'giant component'. This phenomenon is observed in power grids,[13] financial systems (bank runs) and social networks (viral fakes or security leaks). Load redistribution mechanisms play a significant role in cascading failures, where the failure of one component can overload others, causing a chain reaction (e.g. bank run).

Failures spread through interdependencies, a central concept in systems theory. Interdependent parts of a network need each other to sustain the functionality of the network. Mapping and measuring interdependencies between different parts of the network with appropriate models allows us to predict and to mitigate the spread of failures.

The primary focus of sectoral security thus is ensuring that the entire sector remains functional, rather than just individual organizations. A sector must be both robust and resilient, able to withstand disruptions and recover swiftly to maintain overall functionality and adapt to new challenges.

When components of a system report on themselves, it mirrors the concept of **feedback loops** in systems theory. Feedback loops allow the system to self-regulate and adapt by providing information that components use to adjust their behaviours and interactions.

Intensified exchange of information within a system leads to increased connectivity and resilience, as follows from Complex Adaptive Systems (CAS) theory. The latter provides a framework for understanding how systems evolve, adapt, and become more robust and resilient.

Complex adaptive systems are composed of interacting agents that follow the predefined rules, adapting to changes in their environment. This adaptation leads to self-organization, when the system dynamically evolves and becomes more efficient even without the central control.[14] The rules of interaction remain, but new complex interactions, which are not covered by the predefined set of rules, may emerge.

Systems with multiple components often exhibit large-scale emergent behaviours that cannot be directly inferred from the behaviours of their components.[15] As components of the system interact and learn about each other, emergent behaviours may occur that were not explicitly programmed or designed.[16] These behaviours can lead to new patterns of connectivity and robustness.

Networks become more resilient through the development of redundant pathways and robust connections. When components of a system report to each other and adapt, they create multiple pathways for information flow, enhancing the system's ability to withstand failures.[17]

Organizations within a sector should collaborate on defence strategies, sharing threat intelligence and best practices to achieve overall resilience. Collaborative efforts can help identify and address vulnerabilities more effectively than isolated actions. While this conclusion might look obvious, field applications of the PROGRESS CCMM have shown that this very component provides significant resilience boosts when implemented properly. In other words, being too obvious, it is too often left unattended.

The PROGRESS CCMM implementation follows these very ideas, galvanizing information exchange between beneficiaries, who might appear as sector regulator(s), cybersecurity providers, third-party providers, national-level cybersecurity agency, CERT(s) and cybersecurity departments of the sector′s largest players. It was more than once that the beneficiaries discovered new ways of interacting or integrating existing sectoral assets through this exchange, fuelled by PROGRESS CCMM execution. In this way, the authors were able to observe in person the effects of self-organizing adaptive systems.

A few of the information exchanges dynamics during the PROGRESS implementation followed the well-known Barabási-Albert model,[18] tending to group around the more knowledgeable and powerful participants. To keep the sector resilient, the model output recommendations were designed to maintain the rich and redundant signal pathways.

Incorporating the science of complex systems, the study of cybersecurity frameworks, and over two decades of CIP operations, the PROGRESS CCMM provides for improvements in scale, speed and quality of cyber resilience.

3 The new Promoting Global Resilience for Sectors Cyber-Capability Maturity Model

This section proposes an sectoral approach to cyber resilience: Promoting Global Resilience for Sectors—a Cyber-Capability Maturity Model (PROGRESS CCMM). It is a **hybrid** capability maturity model, offering diagnostics as well as guiding improvements. A capability maturity model focuses on a capability identified against a context of characteristics, indicators, attributes, or patterns (often expressed as "processes"). Repeatable processes reflect maturity, whereby capabilities become institutionalized in the culture of the organization or the community. Using a maturity model as the

[13] [Buldyrev et al., [5]].

[14] [Holland, [13]].

[15] [Siegenfeld, Bar-Yam [25]].

[16] [Miller, Page, [17]].

[17] [Newman [18]].

[18] [Barabási, Albert [4]].

foundation for improving practices, processes, and performance provides organizations, industries, and communities of practice with several lasting benefits.[19]

PROGRESS CCMM is built upon following propositions:

1.Capability-building is the preferred route to sectoral cybersecurity. **Capacity** refers to the potential to achieve an ideal state. Being applied, this becomes too broad a target. **Capability** is derived from the performance requirements of the particular service levels the given sector must deliver, as well as the specific conditions in that sector. The goals must be specific and measurable: to transmit and distribute 5 GWh of electricity in the region, with 99% reliability; to enroll 90% of the province's population and 99% of primary and secondary medical care providers in the Electronic Medical Records system by Q3 2025, etc. To simplify, the goal is to develop just enough cybersecurity capabilities to support the business goal.

2.Resilience rather than security is the aim. Resilience includes the capability to resist an attack or a failure, recover its function, and 'bounce forward'to a more advantageous position. Security mostly focuses on preventing an attack or a failure.

3.1 Aim and scope

The PROGRESS CCMM is designed to support digital resilience in a particular sector by gradually maturing specific system-level cybersecurity capabilities. A common saying "cybersecurity is a shared responsibility" reflects the intuitive understanding that current approaches are incomplete. Modern complexity science demonstrates that components alone cannot generate resilience for STES. A more inclusive and broader scope is required to bridge the gap between the complex STES and firm-level practice.[20] PROGRESS develops the sector concept as the unit of analysis. A sector is a coordinated group of organizations providing a particular service in a defined region.[21] The definition of a sector encompasses the following three characteristics:

1. Functional cooperation between several organizations – constituents, stakeholders, and community members – each involved to some extent in producing and delivering a service inherent to the sector.
2. Coordination and oversight. One or more ministries, departments or agencies (MDAs) set performance targets, coordinate, oversee, and regulate activity, and often administer relevant resource allocation in this sector.
3. A shared role, mission, and service level within a defined geography. It can be subnational (e.g., a district, city, or province), national (e.g., fully coterminous with sovereign borders), or supranational (e.g., the EU or the West African Monetary and Economic Union (WAEMU)).

Certain sectors, infrastructures and essential services are considered critical infrastructure (CI)[22] with a growing number of countries officially defining them as such to better manage the risks. The PROGRESS methodology can address any sector or sub-sector, whether it is defined officially as a sector, within the CI, or otherwise. Sectoral resilience is the overriding objective rather than the individual goals of the various constituents.

4 The model architecture

4.1 Structure: dimensions of operation of a sector

To operate in an integrated, cross-system way, the model introduces and examines four Dimensions of Operations (DO) common to any sector of an advanced economy:

1. Key Entities (DO.1)
2. **Sector supervision** (DO.2)
3. **IT & operational technology** (OT) **supply chain** (DO.3)
4. **State-grade/national cybersecurity** (DO.4).

The First Dimension of Operation is a typical, individual firm-based analysis of large organizations and their capabilities.

The Second Dimension of Operation includes the regulatory agencies and their multi-directional interactions with key entities and others. These first two dimensions are explored within the sector.

The Third Dimension of Operation captures the roles of specialist service providers directly impacting cybersecurity capabilities available to the sector. These typically reside outside of the sector. Investigation of the third dimension (DO.3) allows to identify specific supply chain issues even in cases when other dimensions′ capability maturity appears advanced.

[19] [Allen and Mehravari [1]].

[20] The science of complex systems and socio-technical systems (STS) demonstrates that resilience of critical infrastructure is an emergent behaviour. While this topic exceeds the scope of the paper, see:

[Gao, Barzel, and Barabási [9]; Argollo de Menezes and Barabási [2]].

[Thurner, Klimek, and Hanel [31]; Pagani and Aiello [21]; Buldyrev et al. [5]].

[21] [Shaked, Tabansky, and Reich [24]].

[22] [OECD [19]; Katina and Keating [14]; Curt and Tacnet [7]] [Tabansky [30]; Tabansky [28]].

The Fourth Dimension of Operation examines the roles of national-level organizations that reside outside the sector. These include the competent national cybersecurity agency, the critical infrastructure protection (CIP) agency, and technical communities such as computer security and incident response/emergency teams (CSIRTs & CERTs). Where absent, law enforcement and intelligence agencies typically hold similar roles and responsibilities.

As indicated, DO.1 and DO.2 typically represent the core of the sector in question, while DO.3 and DO.4 represent the sources of cybersecurity capability outside the sector. In all cases, PROGRESS explicitly focuses on multi-directional interactions within and between the Dimensions of Operation. Together, these four Dimensions of Operation enable a profoundly networked analysis of a sector as a complete system, rather than focusing unevenly and arbitrarily on the behaviour and robustness of discrete activities and organizations.

The resilience of a sector is a function of the depth, intensity, durability and effectiveness of cooperation between all four Dimensions of Operations. Taken together, the **interactions of multiple organizational entities and their respective cybersecurity capabilities generate sectoral capability maturity and resilience**. These interactions are less tangible, but they contribute to cybersecurity capabilities and resilience.

PROGRESS gleans insights and information about the cybersecurity practices of a key entity via interaction with both the assessed entity and also with others, such as with the sector regulator or system integrators who work in the sector. Thus, the PROGRESS methodology makes it possible to uncover interactions between constituents and stakeholders systematically and to subject these interactions to analysis.

While enterprise-level CCMM's are focused on the first Dimension of Operations, and national level CCMM's are considering mainly DO.2 and DO.4, it is the sectoral approach that integrates all Dimensions and emphasizes links and information flows across them.

The next step in applying the PROGRESS CCMM is to combine the four Dimensions of Operation (DO 1–4) with five Practice Domains (PD a–e: Organization, Process, People, Tools, and Compliance) in a single, coherent architecture.

To explain the full potential of the CCMM approach and to show which of its practice areas might be most impactful and informative, the PROGRESS methodology draws upon a first-of-its-kind analysis of two decades of Critical Infrastructure Protection (CIP) operations and desk research.[23] With this broad analytical and operational background, cybersecurity and CIP experts were able to refine the most important and consequential set of topics.[24] The topics were then grouped into the five Practice Domains—Organization, Process, People, Tools, and Compliance. The empty template (Fig. 2) and artificial sample results (Fig. 3) of this PROGRESS CCMM test assessment are presented below:

Fig. 2 Dimensions of operation and practice domains

Fig. 3 A fictional result of the PROGRESS CCMM assessment

To identify specific, actionable recommendations for improvements to be made in a sector as a whole, the PROGRESS CCMM does not seek a single grade or ranking. Instead, the overall assessment results in 20 maturity level (ML) scores (Fig. 3), enhancing the analysis resolution and substantiating recommendations.[25]

Footnote 25 continued

[23] See for example [Hathaway and Spidalieri [11].

[24] The base version of PROGRESS has less than 50 topics to assess. The low count reduces assessment fatigue, increases agility and flexibility. The number of indicators and topics to assess in each of the PDs can be easily extended to better fit the use case. The topics are cross-mapped to the most widely used framework and vocabulary: the US National Institute of Science and Technology Cybersecurity Framework (NIST CSF v1.1).

[25] PROGRESS adopts the five maturity levels (ML1-ML5) used by the Oxford Cybersecurity Capacity Maturity Model for Nations (CMM)

4.2 What information to collect, from whom and how?

Let's consider a fictional financial services sector example. Banking and mobile money corporations are the key entities (DO.1) of the financial services sector, with Central Banks, Treasury, and other agencies performing oversight and regulatory roles (DO.2).

PROGRESS CCMM delves into various underlying and fundamental issues that should properly inform a capabilities gap analysis:

1. Typically, any sector has several key entities (DO.1). Most likely, their cyber resilience capabilities vary: in this example, a newly established mobile money operator exhibits mature network security, while several traditional banks that operate vastly larger balance sheets have obsolete network switches or firewalls. What are the reasons for this variance? Are there structural issues that inhibit or support maturity? Self-assessment or limiting the scope to the large bank itself cannot suffice to understand why exactly a bank does not operate a modern network security (or is not allowed to). It would then be impossible to know how the bank could improve its capabilities. Such insights emerge from the assessment of DO.2, DO.3, and DO.4, in parallel with—and separate from—the evaluation of DO.1. Capability-building depends on crystallizing the specific findings and insights—derived from each DO—and developing an actionable roadmap to address these. The value of expanding the scope to include all dimensions of government agencies (DO.4.), sector regulators (DO.2), IT/OT service providers (DO.3), or own employees (DO.1) will become clear for producing findings and actionable recommendations.
2. What informs the organization's cyber risk posture, IT security controls, management's security awareness, etc.? Naturally, regulation and oversight play a vital role in driving roles and responsibilities, information sharing, legal environment, cyber situational awareness. Stricter risk management regulation is typically reserved for Systemically Important Financial Institutions (SIFIs). PROGRESS delves into DO.2 and DO.4 organizations' capabilities and their interactions with DO.1 and among themselves.
3. Assuming that a sector player is eager to spend on cybersecurity, where could a DO.1 organization source cybersecurity products and services from? The underlying explanations might include human resources training and education, labour market, domestic and cross-border business supply chains (DO.3) and the capabilities of competent agencies (DO.4.)

An in-depth analysis should uncover some of the higher-order reasons, including the following:

4. National cybersecurity strategy, policy, and organization (DO.4.). Top-level maturity at the national level permeates the economy, increasing overall resilience. The lack of a strategy or a designated organization may render the function even of top-notch private cybersecurity solutions futile.
5. Regulatory arbitrage (DO.2, DO.4). In regulated industries, firms may get away with inferior cyber capabilities under inconsistent or outdated regulations. For example, mobile money service providers often enjoy operating under looser regulation and supervision than banks in the financial services sector.[26]
6. Regulatory (in)effectiveness. Organizations may gage that the relevant regulators lack the will or capabilities to audit compliance and enforce the regulated standards. Such a belief will move these organizations to opt for neglecting efforts to comply with existing IT-security directives.
7. Spill-over of foreign capability. Organizations with superior cyber capabilities (DO.1) may have foreign corporate parents in more cyber-mature jurisdictions, and corporate cybersecurity spills over (DO.3) to increase the capabilities of domestic divisions.
8. Inelastic labour supply leads to zero-sum competition for talent. Organizations with inferior cyber capabilities may lose competition to those who have hired the few knowledgeable people. To optimize the use of scarce human resources, promoting managed service providers model (DO.3) instead of in-house hiring may increase the overall resilience.
9. Management awareness is another criterion to consider. Individual preferences matter in hierarchical structures. A cyber-aware CEO or owner can realign incentives and resources, first and foremost shaping the corporate culture.

Footnote 25 continued
for consistency with familiar and respected terminology and scale. ["Oxford Cybersecurity Capacity Maturity Model for Nations (CMM)" [20]].

[26] [Suárez [27]; Lashitew, van Tulder, and Liasse [15]; Pelletier, Khavul, and Estrin [22]].

4.2.1 From whom is the information collected

For all Dimensions of Operation, PROGRESS systematically compares findings sourced from key entities, sectoral regulators, IT/OT service providers, and government agencies (DO.4.) to assess maturity. This mixed approach, combining direct and indirect methods, exposes multifaceted issues that a direct "yes/no/partial" assessment cannot reveal.

Practice Domain topics are replicated in each Dimension of Operation for which they are relevant.[27] This is because the firm's capability, operation, and performance must be assessed in the sectoral context.

Having discussed *what* data and information PROGRESS collects, and from *whom*, we now move on to *how*.

4.2.2 How to collect information from stakeholders

A characteristic finding in cybersecurity assessments would be that organizations *employ an outdated network security solution, that no longer suffices to detect and prevent new threats.* The relevant indicators of existing methods thus would be *no or partial capability maturity*.[28]

Traditional organization-based cybersecurity practices deliver a point-in-time assessment against a benchmark or standard, followed by a gap analysis. Organization-centric cybersecurity assessments use the *"yes/no/partial"* structure and self-assessment questionnaires. For example, an assessment of a bank's capability maturity or compliance typically relies on humans working with a spreadsheet questionnaire.

Organization-centric cybersecurity methods rarely produce deep insights, thus PROGRESS employs neither the *"yes/no/partial"* format nor self-assessment questionnaires.[29]

Instead, PROGRESS employs a **semi-structured focus group** method for an interactive assessment. In-person focus groups are instrumental in uncovering insights through less formal communications and dynamics between stakeholders and peers. The aim is to create discussions during which information flows freely. By design, the information gathered is refined, enriched, and even refuted by exploring the same topic via additional focus groups from other sectoral perspectives.

For example, information about a key entity's cybersecurity practice can be gleaned from a focus group within that key entity. Engaging with a sample of key entities (DO.1) using the focus group method uncovers whether some peer competitors exhibit higher cyber capabilities in some PDs.

To generate objective metrics PROGRESS also may leverage machine-based technical scans (applying solutions in Attack Surface Management and Breach and Attack Simulation categories) alongside the insights gathered in semi-structured focus groups. While recent technological advances enable affordable and cheap machine-based assessments, organizations often resist such scans. PROGRESS CCMM is designed to be able to achieve the goals by using interactive human assessment only, and we have indeed demonstrated this in the fieldwork.

4.3 Outputs: generating actionable recommendations for sectoral resilience

CCMM frameworks that analyse a single organization do not generally consider the reasons *why* an organization employs an outdated network security solution. Continuing the example, the finding that the bank *"employed an outdated network security solution, that no longer suffices to detect newer classes of threats"* will lead to nothing more than the recommendation to *"Within a year, procure and deploy an up-to-date network security solution."* While such a recommendation may appear reasonable, clear, and actionable, it is also superficial and of little lasting value. There are always reasons why a better network security solution was *not* employed. Only a multifaceted analysis of the specific context can reveal the root causes for the gaps. Training the staff with the current security solution and establishing links with national CERTs or with the national cybersecurity supervisor might have a better effect on resilience involving far lower costs.

5 Discussion on the approach benefits

Our sector-wide systemic approach is designed to expand the breadth and depth of assessment and analysis to generate actionable, specific, and impactful recommendations. PROGRESS is designed to tackle the underlying reasons for the inadequate practices. The root causes stem from the context and how various sector stakeholders and constituents operate within the sector and with external sources of cybersecurity capabilities.

PROGRESS CCMM is designed to obtain specific findings from a broader context, enabling the formulation of tailored, actionable and more impactful recommendations. Such actionable recommendations are informed by and address the specific roles and responsibilities of suppliers, regulators, foreign organizational units, and so on. While the need to deploy modern network security solutions in key entities is clear, the PROGRESS recommendations go beyond

[27] Thus, as most of the 46 distinct topics can be assessed using insights from more than one Dimension of Operation, the assessment covers 121 individual areas.

[28] For example, NIST CSF PR.AC-5: Network integrity is protected; PR.DS-2: Data-in-transit is protected; PR.PT-4: Communications and control networks are protected.

[29] [Shaked, Tabansky, and Reich [24]].

the trivial, articulating structural and durable solutions. The PROGRESS CCMM guidance uncovers the root causes to develop detailed recommendations across the four DOs. The model implementation makes it possible to detail and substantiate improvement roadmaps, such as where to place the capability, how to source it, how to assess its performance and value, and which roles and responsibilities to reassign. Improving capability maturity of a key entity can be achieved by leveraging capacities of others in the sector: another key entity, a different DO, or by enhancing the connection and collaboration between them. The sectoral approach is best suited to advance such systemic capability maturity. Instead of a "one-size-fits-all", actionable recommendations will be specifically tailored for each of the above examples. In summary, the PROGRESS CCMM model offers 6 major benefits:

1. Reduced implementation deficit by offering actionable recommendations that identify and prioritize the most impactful, feasible and cost-effective actions to build sectoral resilience.
2. Comprehensive understanding of a unique unit of analysis, an entire sector that can even transcend regional and national borders.
3. Rapid, light-touch and cost-effective cyber capability assessment of an entire sector across people, process and technology.
4. Bridging the gaps between organizational/corporate and governmental stakeholders.
5. Natural integration of supply chain and third-party risks.
6. Feedback loops and adaptation. The model implementation creates loops of feedback information, allowing all stakeholders to establish or improve communications and better integrate the sector capacities.

Organisational level C2M2's would indicate sectoral level threats, but getting the relevant authorities to address them would require sectoral level involvement. A holistic approach that evaluates not only sector components, but also the links between them, brings stronger overall maturity growth.

The resilience of a sector is a function of the depth, intensity, durability and effectiveness of cooperation across all four Dimensions of Operations.

6 Conclusion and further research

The information revolution is far from being in a state of happy equilibrium, whereby the benefits of participation at least match, and ideally outweigh the costs. In both the developed and developing world, digital trust, security, reliability, robustness, and resilience are all qualities in short supply. This mainly stems from the fact that cybersecurity practice and maturity models focus on the robustness of separate components.

PROGRESS CCMM incorporated the science of complex systems with cybersecurity capabilities maturity assessment frameworks and CIP operations to enable a comprehensive and systematic improvement of capabilities through a sector-wide vision. The sector, as established in the paper, is the optimal unit of analysis and resilience management.

The value of the sectoral approach was proven through real-life mode implementation in four critical sectors—health, financial services, electricity, and digital infrastructure. The implementation projects have resulted in actionable recommendations outlining ways to mature specific cyber capabilities, increasing the overall maturity of the sector. Implementation experience emphasizes the benefits of the sectoral approach to cyber resilience development guidance: creating feedback loops within the sector, integrating supply chain and third-party risks, weighting in the links and processes between authority levels in cybersecurity issues.

The implementation experience also raised the need for further basic and applied research. A clear demand emerged for sector-specific instruments, each building upon the sectoral approach with necessary additions. A research stream to develop a PROGRESS CCMM for Operational Technology-intensive sectors (energy, manufacturing) has commenced.[30] With additional efforts, PROGRESS will mature into a reliable tool with which policymakers can manage long-term risks as well as the longitudinal measurement of success from which to derive consistent and curable key performance indicators. Applications will improve the resilience and critical infrastructure protection of essential services while lowering sector-wide cybersecurity expenditure.

Acknowledgements The authors gratefully acknowledge support from a research grant from the Blavatnik Interdisciplinary Cyber Research Center, Tel Aviv University, and the valuable input of Dr. A. Moiseev, researcher at the Tel Aviv University.

Author contribution L.T. wrote the manuscript and provided the figures. E.L. developed the initial concept. Both authors participated in the implementation of the model and subsequent improvements. Both authors reviewed the manuscript.

Funding Open access funding provided by Tel Aviv University.

Data availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare no competing interests.

Ethical approval The authors declare full compliance with ethical standards promoted by the journal.

[30] See the Tel Aviv University Cyber Resilience Lab for updates on the PROGRESS CCMM and its applications https://rcrl.tau.ac.il/.

References

1. Allen, J., Mehravari, N.: How to be a better consumer of security maturity models. In: Carnegie Mellon University, Software Engineering Institute (SEI). (2014) https://apps.dtic.mil/sti/tr/pdf/ADA614299.pdf
2. Argollo de Menezes, M., Barabási, A.L.: Separating internal and external dynamics of complex systems. Phys. Rev. Lett. **93**(6), 068701 (2004). https://doi.org/10.1103/PhysRevLett.93.068701
3. Artime, O., Grassia, M., De Domenico, M., Gleeson, J.P., Makse, H.A., Mangioni, G., Perc, M., Radicchi, F.: Robustness and resilience of complex networks. Nat. Rev. Phys. **6**(2), 114–131 (2024). https://doi.org/10.1038/s42254-023-00676-y
4. Barabási, A.-L., Albert, R.: Emergence of scaling in random networks. Science **286**(5439), 509–512 (1999). https://doi.org/10.1126/science.286.5439.509
5. Buldyrev, S.V., Parshani, R., Gerald Paul, H., Stanley, E., Havlin, S.: Catastrophic cascade of failures in interdependent networks. Nature **464**(7291), 1025–1028 (2010). https://doi.org/10.1038/nature08932
6. Cornish, P.: The deterrence and prevention of cyber conflict. In: Cornish, P. (ed.) The Oxford Handbook of Cyber Security, pp. 273–294. Oxford University Press (2021). https://doi.org/10.1093/oxfordhb/9780198800682.013.16
7. Curt, C., Tacnet, J.-M.: Resilience of critical infrastructures: review and analysis of current approaches. Risk Anal. **38**(11), 2441–2458 (2018). https://doi.org/10.1111/risa.13166
8. Fell, J., de Vette, N., Gardó, S., Klaus, B., Wendelborn, J.: Towards a Framework for Assessing Systemic Cyber Risk. November. (2022) https://www.ecb.europa.eu/press/financial-stability-publications/fsr/special/html/ecb.fsrart202211_03~9a8452e67a.en.html
9. Gao, J., Barzel, B., Barabási, A.-L.: Universal resilience patterns in complex networks. Nature **530**(7590), 307–312 (2016). https://doi.org/10.1038/nature16948
10. Hathaway, M., Demchak, C., McArdle, J., Spidalieri, F.: Cyber Readiness Index (CRI) 2.0. In: Great Falls, VA: Potomac Institute for Policy Studies. (2015)
11. Hathaway, M E., Spidalieri, F.: Global overview of existing cyber capacity assessment tools (GOAT). In: Global Forum on Cyber Expertise (GFCE). (2021)
12. Hathaway, M E., Spidalieri, F.: Integrating cyber capacity into the digital development agenda. In: Global Forum on Cyber Expertise (GFCE). (2021)
13. Holland, J.H.: Studying complex adaptive systems. J. Syst. Sci. Complex. **19**(1), 1–8 (2006). https://doi.org/10.1007/s11424-006-0001-z
14. Katina, P.F., Keating, C.B.: Critical infrastructures: a perspective from systems of systems. Int. J. Crit. Infrastruct. **11**(4), 316–344 (2015). https://doi.org/10.1504/IJCIS.2015.07384
15. Lashitew, A.A., van Tulder, R., Liasse, Y.: Mobile phones for financial inclusion: What explains the diffusion of mobile money innovations? Res. Policy **48**(5), 1201–1215 (2019). https://doi.org/10.1016/j.respol.2018.12.010
16. Mcjunkin, T., Rieger, C G.:Electricity distribution system resilient control system metrics. In: Conference: 2017 Resilience Week (RWS). (2017) https://doi.org/10.1109/RWEEK.2017.8088656
17. Miller, J H., Page. S E.: Complex adaptive systems: an introduction to computational models of social Life. In: STU-Student edition. Princeton University Press. (2007) https://www.jstor.org/stable/j.ctt7s3kx
18. Newman, M.: Networks. Oxford University Press, Oxford (2018). https://doi.org/10.1093/oso/9780198805090.001.0001
19. OECD: Digital Security and Resilience in Critical Infrastructure and Essential Services. (2019) https://doi.org/10.1787/a7097901-en.
20. Oxford Cybersecurity Capacity Maturity Model for Nations (CMM). In. 2021. University of Oxford, Global Cyber Security Capacity Centre. (2021)
21. Pagani, G.A., Aiello, M.: The power grid as a complex network: a survey. Physica A **392**(11), 2688–2700 (2013). https://doi.org/10.1016/j.physa.2013.01.023
22. Pelletier, A., Khavul, S., Estrin, S.: Innovations in emerging markets: the case of mobile money. Ind. Corp. Chang. **29**(2), 395–421 (2019). https://doi.org/10.1093/icc/dtz049
23. Rieger, C G.: Resilient control systems: practical metrics basis for defining mission impact. In: Conference: 7th International Symposium on Resilient Control Systems. (2014). https://doi.org/10.1109/ISRCS.2014.6900108
24. Shaked, A., Tabansky, L., Reich, Y.: Incorporating systems thinking into a cyber resilience maturity model. IEEE Eng. Manage. Rev. **49**(2), 110–115 (2021). https://doi.org/10.1109/EMR.2020.3046533
25. Siegenfeld, A.F., Bar-Yam, Y.: An introduction to complex systems science and its applications. Complexity **2020**, e6105872 (2020). https://doi.org/10.1155/2020/6105872
26. Smolyak, A., Levy, O., Vodenska, I., Buldyrev, S., Havlin, S.: Mitigation of cascading failures in complex networks. Sci. Rep. **10**(1), 16124 (2020). https://doi.org/10.1038/s41598-020-72771-4
27. Suárez, S.L.: Poor people's money: the politics of mobile money in Mexico and Kenya. Telecommun. Policy **40**(10), 945–955 (2016). https://doi.org/10.1016/j.telpol.2016.03.001
28. Tabansky, L.: Critical infrastructure protection from cyber threats. Milit. Strateg. Affairs **3**(2), 61–78 (2011)
29. Clark, R.M., Hakim, S. (eds.): Cyber-physical Security: Protecting Critical Infrastructure at the State and Local Level, vol. 3. Springer, Berlin (2016)
30. Tabansky, L., Israel, I.B.: The Israeli national cybersecurity policy focuses on critical infrastructure protection (CIP). In: Tabansky, L., Israel, I.B. (eds.) Cybersecurity in Israel, pp. 35–41. Springer International Publishing, Cham (2015). https://doi.org/10.1007/978-3-319-18986-4_5
31. Thurner, S., Klimek, P., Hanel, R.: Introduction to the Theory of Complex Systems. Oxford University Press, Oxford (2018). https://doi.org/10.1093/oso/9780198821939.001.0001