Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

George Sharkov, *Connections QJ* 19, no. 4 (2020): 5-24
https://doi.org/10.11610/Connections.19.4.01

Research Article

Assessing the Maturity of National Cybersecurity and Resilience

George Sharkov

Ministry of Defense, Republic of Bulgaria, https://mod.bg/

European Software Institute – Center Eastern Europe, Sofia, Bulgaria, https://esicenter.bg/

Abstract: This article provides an overview of maturity levels and assessment methodologies for the evaluation of cybersecurity and resilience in relation to their applicability and usefulness at sectoral and national levels. Reference maturity models and assessment frameworks, such as CERT Resilience Management Model, Cybersecurity Capacity Maturity Model for Nations, C2M2 (Cybersecurity Capability Maturity Model), are compared and analyzed for their applicability in designing and implementing national cybersecurity strategies and programs to achieve cyber resilience. Cyber readiness indexes are also outlined in view of their use to indicate possible improvements. The author explores the development of national cybersecurity strategies with a focus on cyber maturity and provides examples. A maturity-based approach for the Bulgarian cyber resilience roadmap is also described within the context of the evolving cyber-empowered hybrid threats and the need for an institutionalized collaborative public-private resilience.

Keywords: cyber resilience, capability maturity models, cybersecurity maturity assessment, maturity indicators, hybrid resilience

Introduction

Modern digitized societies and economies are globally interconnected and increasingly interdependent as a result of global digital connectivity and dependency on digital infrastructure, communications, and systems. The analysis of these interdependencies and emerging complex vulnerabilities and threats re-

quires a holistic approach, which goes well beyond the personal, the enterprise, or the sectoral cybersecurity measures. The enhancement of cybersecurity and the protection of critical infrastructures require coordinated efforts at national, regional, and international levels. In addition, due to the multi-layered "cyber terrain" (a term introduced by the US Department of Defense, DoD, and further detailed by Shawn Riley[1]) and complex systems interdependencies, the new risks and threats become "unknown unknowns" and require upgrading of the established since centuries resilience principles of the society to the entirely new maturity level of "cyber resilience."

Achieving cybersecurity and resilience at the national level is a shared responsibility of all stakeholders – government, private sector, and civil society. Coordinated actions and a multi-stakeholder approach are required to develop and execute national cybersecurity strategies and plans. Various methodologies, guidelines, and templates for defining well-structured and comprehensive national or sectoral cybersecurity strategies are provided by world organizations like ITU, OECD, EU's ENISA, OSCE, standardization bodies, and academic research. Most of them have already postulated "cyber resiliency" as a new main goal to upgrade 'cybersecurity.' Strategies are also reflected in roadmaps outlining the steps and goals to achieve at different phases of the improvement plans. The challenge is how to evaluate the level of achievements, the efficiency, and effectiveness of the measures, and more generally, how to assess the overall level of readiness, capacity and objectively evaluate security and resilience capabilities at the sectoral and national level. There is also a need for a unified methodology to monitor the progress and to compare the achieved status among organizations, sectors, countries, and societies.

For decades, the approach based on maturity models has been widely used in IT companies and technology sectors, as well as by public procurement, starting with defense, to assess the organizations' readiness and capability to deliver high-quality products and services within the required scope, time and budget. On the other hand, organizations, communities, and nations must live and comply with a constantly increasing number of regulations, standards, and requirements, such as the NIST Cybersecurity Framework[2] and related NIST standards and EU Regulations, e.g., the "Cybersecurity Act"[3] with the expected Cybersecurity Certification Scheme, the "NIS Directive,"[4] and others. To cope with all that

---

1 Shawn Riley, "Cyber Terrain: A Model for Increased Understanding of Cyber Activity," 2014, accessed September 15, 2020, https://www.linkedin.com/pulse/20141007190806-36149934--cyber-terrain-a-model-for-increased-understanding-of-cyber-activity/.

2 "Cybersecurity Framework," ver. 1.1., 2018, NIST, USA, accessed October 10, 2020, https://www.nist.gov/cyberframework.

3 "EU Cybersecurity Act," Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019, https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act.

4 "The Directive on Security of Network and Information Systems (NIS Directive)," Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016,

and yet meet the organization's specific business goals, the maturity models and assessment methods turned out to be the most efficient and effective way for larger and smaller organizations.[5]

In this survey, we cover several most popular representatives of the huge diversity of cybersecurity maturity models and give a brief analysis of their suitability for application at a higher level for the purposes of community, sectoral or national cybersecurity maturity evaluation, and furnish national cybersecurity strategies with well-structured improvement programs, like "roadmap to maturity."

Maturity Models and Digital Society

The Origin and Types of Maturity Models

The concept of maturity models for software/ICT industry was initially sponsored by the US military who wanted to develop a method to objectively evaluate software/ICT subcontractors' process capability and maturity.[6] Due to various emerging technologies, standards, different sizes and capacities of the suppliers, there was a need to objectively assess in a unified manner the level of reliability, trust, and associated risks of software/ICT service quality. Maturity models provide a measurable transition as well between different levels (or steps, stages). They allow to compare organizations by their "maturity levels" and provide a structured and prioritized approach for improvement plans.

The maturity models can be grouped into three types:

- *Progression Maturity Models*, frequently illustrated by a 'journey,' represents a simple progression or scaling of an attribute, characteristic, indicator, a pattern where the movement up the maturity levels indicates the progression of attribute's maturity. Levels describe the next "higher states" of achievement, advancement, or 'steps' in the evolution and provide a clear transformative roadmap. In practice, however, they measure neither process maturity nor capabilities;
- *Capability Maturity Models (CMMs)*: the dimensions that are evaluated represent organizational capabilities around a set of characteristics, indicators, or patterns, often expressed as 'practices.' They are usually refer-

ongoing consultations for update in 2021, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

5 Doug Hudson, Jason Macallister, and Mandy Pote, "A Guide to Assessing Security Maturity," White paper, Carbon Black, 2019, accessed September 15, 2020, https://www.carbonblack.com/resources/a-guide-to-assessing-security-maturity/.

6 Richard Caralli, Mark Knight, and Austin Montgomery, "Maturity Models 101: A Primer for Applying Maturity Models to Smart Grid Security, Resilience, and Interoperability," White paper (Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2012), https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=58916.

red to as "process models." The typical levels of CMM models are named around the *maturity of the processes*, for example:

ad-hoc → managed → defined → quantitatively managed → optimized

- *Hybrid Maturity Models* combine characteristics of progressive models with capability attributes from capability maturity models and reflect transitions between levels related to capabilities' maturity while architecturally using the attributes, indicators, and patterns of a progression model. They are relatively easy to use and understand, especially in specific subject matter domains.

Maturity models, regardless of their type, have a similar structure that ensures a harmonized linkage between objectives, best practices, and assessments, and also facilitates the definition of improvement roadmaps between current capabilities and target ones within the context of business goals, standards, and domain-specific characteristics. A typical structure includes:

- *Maturity levels*: represent transitional states (also steps); in a hybrid approach they could be also mapped to "capability levels";
- *Model domains:* groups of attributes and activities into areas, usually referred to as "process areas";
- *Attributes:* the core content of the model, grouped by domain and level, based on practices, prescriptions, knowledge, standards;
- *Appraisal methods:* assessments in a unified manner that produce comparable and meaningful scoring (more than just checkboxes). The main use is to objectively evaluate adherence to the model, provide measurable indicators for achievements and progress, rather than comparing organizations. Appraisals could be formal (expert-led) and informal (including self-assessment);
- *Improvement plans (roadmaps):* appraisal methods provide an evaluation of the current state, gap analysis towards target level, identification of improvement scope and priorities, improvement planning, and verifying the results (achieving next or maintaining the current level).

Maturity Models for the Digital Society and Economy

The introduction and the early use of maturity models were in software/IT industry. After the first use of a staged maturity model by Richard L. Nolan in 1973, and the following work of Watts Humphrey, initially at IBM and after 1986 at the Software Engineering Institute (SEI), Carnegie Mellon University (CMU), the US Department of Defense requested a formalized process maturity framework from SEI by to be able to evaluate software contractors. In the early 1990s, SEI introduced the formal Capability Maturity Model (CMM) with five maturity levels. Subsequently, in 2002, a much more comprehensive and integrated model, Capability Maturity Models Integration (CMMI) was published, with the most popular version 1.3 of 2010. It applies to software engineering, systems engi-

neering, software and systems acquisition, and service delivery as different constellations with a common core. The CMMI was further administered by the CMMI Institute (a spin-off of CMU), which was acquired in 2016 by ISACA. A new version 2.0 was released in 2018. The five maturity levels defined by CMMI to reflect the maturity of the established and institutionalized processes are:

Initial -> Managed -> Defined -> Quantitatively managed -> Optimizing

Since then, capability maturity models have been introduced widely in domains such as ICT infrastructure, all kinds of software engineering, service management, business process management, manufacturing, civil engineering, and cybersecurity. The CMMI Institute published in 2018 the "CMMI Cyber maturity Platform" to address the cyber resilience assessments.

Capability Maturity Models for Cybersecurity and Cyber Resilience

During the past decade, multiple cybersecurity and resilience frameworks have been proposed. A recent study [7] identified more than 25 research activities in 36 different industries attempting to achieve increased clarity about the scope, characteristics, synergies, and gaps that would facilitate scientific research advancement in this area. A 2017 technical mapping comparing maturity models used in various sectors, including education and awareness, provided another source for our survey.[8] The study classifies frameworks as either strategic or operational, by the hierarchy of their decision influence, by the attacks addressed, through the methods used and implementation area. As an exercise to determine the popularity of the terms, we conducted a simple search in Google Scholar, which brought more than 10,000 results for "cybersecurity maturity model," and around 12,000 hits for "cyber resilience maturity assessment." For our survey, we selected a few of the frameworks identified in previous research and added more recent work, as we aim at identifying the applicability at higher than organizational level (like sectors, community, nations), the similarity of assessment results, and possibilities for interdisciplinary, cross-sectoral and cross-border application. In the sub-sections below, we comment on some popular cybersecurity indexes.

CERT Resilience Management Model (CERT-RMM)

CERT-RMM became the reference model for cyber resilience developed by the CERT Division of SEI, Carnegie Mellon University. It had a strong influence on

---

[7] Daniel A. Sepúlveda Estay, Rishikesh Sahay, Michael B. Barfod, and Christian D. Jensen, "A Systematic Review of Cyber-resilience Assessment Frameworks," *Computers & Security* 97 (2020), 101996, https://doi.org/10.1016/j.cose.2020.101996.

[8] Angel Marcelo Rea-Guaman, Tomás San Feliu, Jose A. Calvo-Manzano, and Isaac Daniel Sanchez-Garcia, "Comparative Study of Cybersecurity Capability Maturity Models," in *Software Process Improvement and Capability Determination,* ed. Antonia Mas, Antoni Mesquida, Rory V. O'Connor, Terry Rout, and Alec Dorling (Cham, Switzerland: Springer, 2017), 100-113, https://doi.org/10.1007/978-3-319-67383-7_8.

most of the contemporary cybersecurity maturity assessment methods and frameworks. Although not explicitly stated in the title, the model is dedicated to achieving an operational resilience of organizations in a digitized society and economy, i.e., what we currently mean by *cyber resilience*. A stable version 1.1 of the model was published in 2011,[9] with an update to the last published version 1.2 in 2016.[10] The model is based on the "Operationally Critical Threat, Asset, and Vulnerability Evaluation" (OCTAVE) method for information security risk management and the experience of application in the financial and other sectors. The cyber risk management aspects have been combined with the process-oriented approach and common CMMI-related taxonomy, with terms like "process areas" and generic goals and practices, introduced along with mapping to the engineering and service delivery and continuity process areas from CMMI for services and development.

The model defines the following 26 process areas grouped in 4 categories:

- *Category "Enterprise Management"*: Communications; Compliance; Enterprise focus; Financial Resource Management; Human Resource Management; Organizational Training & Awareness; Risk Management;
- *Category "Operations Management"*: Access Management; Environmental Control; External Dependencies Management; Identity Management; Incident Management & Control; Knowledge & Information Management; People Management; Technology Management; Vulnerability Analysis & Resolution;
- *Category "Engineering"*: Asset Definition and Management; Controls Management; Resilience Requirements Development; Resilience Requirements Management; Resilience Technical Solutions Engineering; Service Continuity;
- *Category "Process Management"*: Measurement and Analysis; Monitoring; Organizational Process Development; Organizational Process Focus.

The "resilience strategy" is based on achieving resilience of the four basic assets: *people*, *information*, *technology*, and *facilities*. Thus, 'resilience' is 'translated' to *protect* and *sustain* measures for the assets. The structure of the model follows the classical CMMI architecture. For each of the 26 process areas, a set of specific goals (total of 94) are defined and must be fulfilled by implementing specific practices (251, typically with several sub-practices). The model prescribes the use of three generic goals and 13 generic practices to measure the level of maturity. To facilitate assessments, some more granulated Maturity In-

[9] Richard A. Caralli, Julia H. Allen, and David W. White, *CERT Resilience Management Model: A Maturity Model for Managing Operational Resilience*, CERT-RMM Version 1.1 (Boston, MA: Addison-Wesley, 2011).

[10] Richard A. Caralli, Julia H. Allen, David W. White, Lisa R. Young, Nader Mehravari, and Pamela D. Curtis, "CERT Resilience Management Model. Version 1.2," Technical Report, Carnegie Mellon University, 2016, https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=514489.

dicator Levels (MIL) were subsequently introduced. The mapping of capabilities levels to maturity indicator levels is shown below:

- *Capability Level 0*: *Incomplete* – MIL0: Incomplete;
- *Capability Level 1*: *Performed* – MIL1: Performed;
- *Capability Level 2*: *Managed* – with MIL2: Planned; MIL3: Managed; MIL4: Measured;
- *Capability Level 3*: *Defined* – MIL5: Defined and new MIL6: Shared (addressing the maturity for overall improvements of the community).

Cybersecurity Capability Maturity Model (C2M2) for Critical Infrastructures

The Cybersecurity Capability Maturity Model (C2M2) [11] was introduced in 2014 by the Department of Energy (US DOE) as an upgrade of an earlier version of C2M2 for the Electricity Subsector (ES-C2M2) by removing sector-specific references and making it applicable more widely to Critical Infrastructures. It was supported by the White House initiative led by the DOE, the Department of Homeland Security (DHS), and SEI, CMU. C2M2 is structured in 10 domains (listed in Table 1) and a set of practices per domain, which represent the capability in the domain. The practices are grouped by objectives and ordered by four maturity indicator levels (MIL0 to MIL3).

The 'objectives' are of two types – *approach objectives (one or more per domain, unique for domains)*, supported by a progression of specific practices, and *management objectives (one per domain),* supported by a progression of 'generic' practices that describe institutionalized activities. The progression is measured by a set of practices characterizing *maturity indicators levels*, applied to approach progression and institutionalization progression. Like in CMMI and CERT-RMM models, the MILs are 'cumulative.' The model is mapped to most of the known models and frameworks in information security and cybersecurity, like ISO/IEC 27001/2, NIST frameworks on cybersecurity, critical infrastructures, supply chains. Remarkably, all 10 domains with objectives and practices meet a subset of the CERT-RMM.[12] A new version 2.0 is currently under consultation.[13]

3-D Community Cybersecurity Maturity Model (CCSMM)

To face the problem that most government agencies, industry partners, critical infrastructure operators, school systems, nonprofit and other organizations exist and operate at the local level and are not equally prepared to defend against cyber threats that could affect the entire community, the Center

[11] Cybersecurity Capability Maturity Model (C2M2) Program, US Department of Energy, accessed September 30, 2020, www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0.

[12] Cybersecurity Capability Maturity Model (C2M2), Version 1.1, February 2014, https://www.energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

[13] Cybersecurity Capability Maturity Model (C2M2), Version 2.0, June 2019, https://apps.dtic.mil/sti/pdfs/AD1078768.pdf.

Table 1. The Domains in C2M2, New Version 2.0 (under Consultation).

Domains	Purpose statement
Risk Management	Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, and mitigate cybersecurity risk
Asset, Change, and Configuration Management	Manage the organization's IT and OT assets, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives
Identity and Access Management	Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets
Threat and Vulnerability Management	Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities
Situational Awareness	Establish and maintain activities and technologies to collect, analyze, alarm, present, and use operational and cybersecurity information, status and summary information from other domains, to establish situational awareness for operational state and cybersecurity state
Event and Incident Response	Establish and maintain plans, procedures, and technologies to detect, analyze, mitigate, respond to, and recover from cybersecurity events and incidents
Supply Chain and External Dependencies Management	Establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities, commensurate with the risk to critical infrastructure and organizational objectives
Workforce Management	Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel
Cybersecurity Architecture	Establish and maintain the structure and behavior of the organization's cybersecurity controls, processes, and other elements
Cybersecurity Program Management	Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with the organization's strategic objectives and the risk to critical infrastructure

for Infrastructure Assurance and Security (CIAS) at The University of Texas at San Antonio (UTSA) created the Community Cyber Security Maturity Model (CCSMM).[14] A program was developed to help communities (and states) im-

[14] "Community Cyber Security Maturity Model (CCSMM)," Center for Infrastructure Assurance and Security (CIAS) at The University of Texas at San Antonio (UTSA), accessed September 15, 2020, https://cias.utsa.edu/the-ccsmm.html.

plement the model and piloted in seven states helping them begin the development of their own programs,[15] as the community cybersecurity is arguably the weak link in the nation's cybersecurity chain. The 'levels' in CCSMM are less formal and defined as 'levels of improvement':

- *Level 1 – Initial*: some processes or programs may be in place, but a community does not have all the program elements for a basic program;
- *Level 2 – Established*: a basic program has been established with elements and processes in place for all four dimensions;
- *Level 3 – Self-Assessed*: a minimal viable and sustainable program has been implemented;
- *Level 4 – Integrated*: cybersecurity is integrated across the community, includes all citizens and organizations, the community is working with the state and other communities within the state;
- *Level 5 – Vanguard*: the community is maintaining a fully-vigilant cybersecurity posture.

These levels of improvement are focused on four areas called dimensions, shown in Table 2.

Table 2. Dimensions in the Community Cybersecurity Maturity Model (CCSMM).

Dimensions	Description
Awareness	Most people understand that cyber threats exist. However, not as many understand the extent of the threat, the current attack trends, how a cyber incident can impact a community, which vulnerabilities should be addressed, what the cascading effects may be if a community was under a cyberattack
Information Sharing	Addresses what to do with information on a cyber incident and where the information should be reported. In addition, how one sector can share information with another, allowing the second sector to potentially prevent the incident from occurring
Policy	Addresses the need to integrate cyber elements into the policies or guiding principles and includes all guiding regulations, laws, rules, and documents that govern the community's daily operation. Policies should be evaluated to ensure cybersecurity principles are reflected in everything we do and will establish expectations and limitations
Plans	Communities have established plans to address many different hazards and this dimension ensures cybersecurity elements are included in those plans enabling the community to address cyber incidents that could impact the operations of the community

[15] Natalie Sjelin and Gregory White, "The Community Cyber Security Maturity Model," in Cyber-Physical Security. Protecting Critical Infrastructure, ed. Robert M. Clark and Simon Hakim (Cham, Switzerland: Springer, 2017), 161-183, https://doi.org/10.1007/978-3-319-32824-9_8.

This model's distinguishing point is that it is 3-dimensional, with 'geography' added as a third coordinate, with three values: organization, community, and state. This 3-D Community Cybersecurity Model can serve to define a roadmap for individuals, organizations, communities, states, and the nation, and as:

- a '*yardstick*' to measure the present status of a community's cybersecurity program and attitudes;
- a *roadmap* to help a community understand the steps needed to improve its security posture;
- a *common point of reference* allowing individuals from different states and communities to compare and relate to individual programs.

It is declared to be compliant with other known frameworks, like the NIST Cyber Security Framework, the DoD's CMMC, and to support the Cybersecurity Workforce Framework from the National Initiative for Cybersecurity Education (NICE).

Cybersecurity Capacity Maturity Model for Nations (CMM-GCSCC[16])

CMM-GCSCC[17] is a methodical framework designed to review the maturity of a country's cybersecurity capacity. It was developed by the Global Cyber Security Capacity Centre (GCSCC) through a global collaborative exercise launched in 2014. For each of its five dimensions (shown in Table 3), the model provides factors (24 in total for this version), which define criteria to demonstrate the respective cybersecurity capacity. Most factors are examined from several viewpoints, and composed of a series of indicators within the five stages of maturity for each dimension, named as follows: *start-up; formative; established; strategic; dynamic.*

CMM-GCSCC is among the most popular assessment tools applicable to countries and regions, used by international organizations like ITU, Organization of American States (OAS), the World Bank, Oceania Cyber Security Centre, Cybersecurity Capacity Centre for Southern Africa, RAND Corporation, etc. It has been deployed to over 80 nations with more than 110 assessments and two regional studies by OAS. Many country profiles are publicly available and levels achieved could be reviewed, along with recommended improvements.[18] A new version is planned for publication in the second half of 2020. It should be noted that 'capacity' is not equivalent to 'capability,' and the model is less formal than maturity assessments, although dimensions and factors may match.

---

[16] Indicated here as "CMM-GCSCC" (vis-à-vis the original use "CMM"), to distinguish from the classical "Capability Maturity Model" by SEI, CMU.

[17] "Cybersecurity Capacity Maturity Model for Nations (CMM)," Revised Edition, accessed October 18, 2020, https://gcscc.ox.ac.uk/the-cmm.

[18] "GCSCC: CMM Reviews Around the World," Global Cyber Security Capacity Centre, accessed October 10, 2020, https://gcscc.ox.ac.uk/cmm-reviews.

Table 3. Cybersecurity Capacity Maturity Model for Nations (CMM of GCSCC).

Dimensions	Factors
Cybersecurity Policy and Strategy	National Cybersecurity Strategy; Incident Response; Critical Infrastructure (CI) Protection; Crisis Management; Cyber Defense; Communications Redundancy
Cyber Culture and Society	Cybersecurity Mindset; Trust and Confidence on the Internet; User Understanding of Personal Information Protection Online; Reporting Mechanisms; Media and Social Media
Cybersecurity Education, Training and Skills	Awareness Raising; Framework for Education; Framework for Professional Training
Legal and Regulatory Frameworks	Legal Frameworks; Criminal Justice System; Formal and Informal Cooperation Frameworks to Combat Cybercrime
Standards, Organizations, and Technologies	Adherence to Standards; Internet Infrastructure Resilience; Software Quality; Technical Security Controls; Cryptographic Controls; Cybersecurity Marketplace; Responsible Disclosure

Cybersecurity Assessment for Financial Institutions – CAT FFIEC Tool

In 2015, the US Federal Financial Institutions Examination Council (FFIEC) introduced the maturity-model-based Cybersecurity Assessment Tool (CAT)[19] for banking institutions to evaluate bank's risks and cybersecurity readiness by measuring levels of risk and corresponding controls. Five maturity levels are used: *Baseline, Evolving, Intermediate, Advanced, and Innovative*, based on five domains characterizing the institution's behaviors, practices, and processes that support cybersecurity preparedness. The five domains consist of a total of 15 "assessment factors" with 497 "declarative statements" used to assess the maturity level achieved per domain. The five domains are:

- Cyber Risk Management and Oversight
- Threat Intelligence and Collaboration
- Cybersecurity Controls
- External Dependency Management
- Cyber Incident Management and Resilience.

For each domain, the assessment determines a maturity level on the following scale:

- *Baseline*: The management reviews and evaluates guidelines;

[19] "Cybersecurity Assessment Tool," Federal Financial Institutions Examination Council (FFIEC), accessed September 30, 2020, https://www.ffiec.gov/cyberassessmenttool.htm.

- *Evolving*: Additional procedures and policies are set. Cybersecurity is increased to include information assets and systems;
- *Intermediate*: Detailed processes occur, controls remain consistent, risk-management is integrated into business strategies;
- *Advanced*: Cybersecurity practices and analytics are included in all businesses; continuous improvement in risk management processes;
- *Innovative*: There is driving innovation in the people, processes, and technology (new tools, new controls, new information-sharing groups).

CAT FFIEC is meant to be completed periodically, but also after significant technological or operational changes. It is a self-assessment, which could be validated by an auditor. After disputes on the "voluntary assessment," the tool has evolved to map better to the NIST Cybersecurity Framework (revision in progress since 2019). Auditors also increasingly require that companies complete an assessment to demonstrate CAT FFIEC compliance.

Cyber Resilience Review (CRR) by DHS

The self-assessment package was designed by the Department of Homeland Security (DHS) in partnership with the CERT Division of SEI, Carnegie Mellon University, as a derivative of the CERT-RMM tailored to the needs of critical infrastructure owners and operators.[20]

As in CERT-RMM, CRR considers that an organization deploys its assets (people, information, technology, facilities) to support specific operational missions or critical services. Then the assessment of capabilities in performing, planning, managing, measuring, and defining operational resilience practices and behaviors is performed in the following ten domains: Asset Management; Controls Management; Configuration and Change Management; Vulnerability Management; Incident Management; Service Continuity Management; Risk Management; External Dependency Management; Training and Awareness; Situational Awareness. The domains are derived from CERT-RMM and are similar to the ten domains of C2M2. The assessment is based on the CERT-RMM method and could be performed in two ways: self-assessment or in a facilitated session.

Cybersecurity Maturity Model Assessment (CMMC) by US DoD

CMMC is the new Cybersecurity Maturity Model Assessment requirement for all Defense Industrial Base (DIB) members that are suppliers to the DoD. All DIB companies will be required to get third-party certification to meet one of five maturity levels required to submit proposals on government contracts.[21] We include this model in the review as it contains the most detailed up-to-date requirements and assessment criteria not only for the organization's resilience but

[20] "Cyber Resilience Review (CRR)," Cybersecurity & Infrastructure Security Agency, accessed October 10, 2020, https://us-cert.cisa.gov/resources/assessments.

[21] Cybersecurity Maturity Model Certification (CMMC), www.acq.osd.mil/cmmc/.

for the entire ecosystem (such as national security and defense). The model specifies 17 capability domains with 43 capabilities and 171 practices across five maturity levels to measure technical capabilities: *Performed*, *Documented*, *Managed*, *Reviewed*, *Optimizing* (somewhat different from the levels in CMMI and CERT-RMM). The logic of the CMMC levels is different, as it provides a means of improving the alignment of maturity processes and cybersecurity practices with the sensitivity of the information to be protected and the range of threats. Accordingly, the levels are defined as:

Level 1: Safeguard Federal Contract Information (FCI)

Level 2: Serve as a transition step in the progression to protect CUI

Level 3: Protect Controlled Unclassified Information (CUI)

Levels 4-5: Protect CUI and reduce the risk of Advanced Persistent Threats.

The domains correspond to the security-related areas in Federal Information Processing Standards (FIPS) and the related security requirements from NIST frameworks. The 17 domains are: Access Control; Asset Management; Audit and Accountability; Awareness and Training; Configuration Management; Identification and Authentication; Incident Response; Maintenance; Media Protection; Personnel Security; Physical Protection; Recovery; Risk Management; Security Assessment; Situational Awareness; System and Communications Protection; System and Information Integrity.

Cyber Resilience Metrics of MITRE

We briefly cover one more systematic and architectural view of the MITRE methodology for assessing cyber resiliency which is based on the Systems-of-Systems (SOS) [22] approach and allows to define and assess the cyber resilience metrics at different levels and scope, going up to national and transnational enterprises:

- At the systems level, including directed systems-of-systems (SoS);
- Missions, including acknowledged SoS within an organization;
- Organizations where the CERT-RMM or the DHS CRR could be applied;
- Sectors (e.g., critical infrastructure sectors or sub-sectors), regions, and missions supported by multiple organizations, via collaborative SoS;
- Nations and transnational enterprises supported by virtual SoS.

The proposed metrics can facilitate the development of technical indicators to assess the risks and dependability (thus the possible cascading effects, escalating impact) of systems and then prioritize improvement programs.

[22] Deborah Bodeau, John Brtis, Richard Graubart, and Jonathan Salwen, "Resiliency Techniques for System of Systems: Extending and Applying the Cyber Resiliency Engineering Framework to the Space Domain," MTR 130515 (Bedford, MA: MITRE, September 2013), www.mitre.org/sites/default/files/publications/13-3513-Resiliency Techniques_0.pdf.

Cybersecurity Indexes and Maturity

With the increasing interest and ambition of nations to accelerate improvement programs and promote their achievements internationally, another instrument of evaluation and ranking countries' status is the international/global indexes. There are many indexes established already for decades in areas like information society development, digital readiness, internet connectivity, computer literacy, etc. ITU published in 2017 an "Index of cybersecurity indices" [23] with the most popular international cybersecurity indexes. We will comment on three of them with a focus on assessing countries.

Global Cybersecurity Index (GCI), ITU [24]: An assessment framework based on the Global Cybersecurity Agenda (GCA) of ITU. The GCI measures the commitment of countries to cybersecurity at a global level. The assessment measures a country's level of development or engagement through a question-based online survey structured along five pillars—Legal Measures, Technical Measures, Organizational Measures, Capacity Building, and Cooperation—using 25 indicators and additional sub-indicators, and then calculating an overall score. Since the first survey in 2013, GCI promotes cybersecurity initiatives through comparison. The third issue of GCI (in 2018), covering more than 193 countries and producing three regional reports, shows considerable improvements in cybersecurity worldwide, as more countries have cybersecurity strategies, national plans, response teams, and specific legislation. However, a significant gap between regions is still observed.

National Cybersecurity Index (NCSI) [25]: Global index, measuring the preparedness of countries to prevent cyber threats and manage cyber incidents, crime, and crises on a large scale. The Estonian e-Governance Academy develops it in cooperation with the Estonian Foreign Ministry. The index emphasizes the public aspects of national cybersecurity implemented by the central government. The index has 12 main indicators with sub-indicators, divided into three groups: General Cyber Security, Baseline Cyber Security, Incident and Crisis Management. The indicators have been tied to information society and cybersecurity issues such as e-identity, digital signature, and the existence of a secure environment for e-services. NCSI provides publicly available evidence materials and a tool for national cybersecurity capacity building. The country ranking is compared to GCI (ITU), the ICT Development Index, and the Networked Readiness Index.

[23] "Index of Indices," International Telecommunication Union, 2017, accessed October 18, 2020, https://www.itu.int/en/itu-d/cybersecurity/documents/2017_Index_of_Indices.pdf.

[24] "Global Cybersecurity Index," International Telecommunication Union, www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

[25] National Cybersecurity Index, Estonia, https://ncsi.ega.ee/.

Cyber Readiness Index 2.0 (CRI 2.0)[26]: Evaluates a nation state's cyber maturity as well as its overall commitment to cyber issues, defines the meaning of being "cyber ready" while proposing actionable blueprints to follow. The index uses a set of seven indicators: national strategy, incident response, e-crime and law enforcement, information sharing, investment in R&D, diplomacy and trade, defense, and crisis response. One hundred twenty-five countries were studied, and the methodology is based on similar pillars as those of the ITU's Global Cybersecurity Agenda. Each country is assigned a score, while the addition of military capabilities goes beyond that covered by the ITU GCI. However, CRI 2.0 does not offer any ranking despite its scoring mechanism.

Although these and other known indexes (Kaspersky Cybersecurity Index, Cyber Maturity in the Asia-Pacific Region, etc.) are quite popular and easy to promote countries, their use as cyber maturity assessment indicators is doubtful. The areas and indicators look similar to those of the maturity models, but they lack the rigor and granularity of the maturity levels and the assessments. There are no levels, and improvement plans could not be prioritized and structured with clear stages and targets. A higher rank in the index could be a success indicator, but it is unlikely to be set as a target. The question-based scores depend largely on the engagement and motivation of local bodies to provide evidence.

Focus on Maturity in National Cybersecurity Strategies

The focus on cybersecurity maturity is already incorporated, and maturity assessments are recommended in most of the updated manuals and guidelines for the development of national cybersecurity strategies. In ENISA's National Cyber Security Strategy (NCSS) Good Practice Guide (updated in 2016)[27], there are two references to maturity and assessments during the lifecycle of strategy development and implementation. To establish baseline security measures, several complex aspects should be considered: different levels of maturity among the stakeholders, differences in terms of the operational capacity of each organization, and the different standards existing in each critical sector. Among the actions recommended is to "Create *maturity self-assessment tools* and encourage the stakeholder to use them." According to Recommendation 9: "*Enhance capabilities of the public and private sector*," after baseline requirements have been defined, existing capabilities need to be evaluated to identify gaps and deviations. To develop improvement plans and assess results, governments are advised to "actively support capacity building by publishing national standards, *designing cyber security capability maturity models*, promote and encourage the exchange of knowledge….."

[26] Cyber Readiness Index (CRI), Potomac Institute for Policy Studies, https://potomacinstitute.org/academic-centers/cyber-readiness-index.

[27] "NCSS Good Practice Guide," ENISA, https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

Nevertheless, a quick review of the national cybersecurity strategies (listed on ENISA's website) shows that the word "maturity" is barely mentioned, and "maturity levels" or models are not referred to. This observation might be incomplete, as the issue might be addressed in plans and roadmaps. Some of the mentions of cyber maturity and maturity models are:

- The UK strategy adopted in 2016 states that the UK Government's level of support for each sector is defined "taking into account its cyber maturity." A Cyber Assessment Framework (CAF) by NCSC is introduced to guide organizations from vitally important services;[28]
- in the third Cybersecurity Strategy of Estonia (2019) a "tested level of maturity" is considered among the main strengths of Estonia. Various areas of capabilities and maturity type of indicators are defined, with a detailed description of 'start' and 'target' levels, clear objectives and activity areas (which indeed makes it a good example of an actionable strategy), but no further elaboration on the eventual introduction of "cyber maturity models" or assessments are covered;
- the Cybersecurity Strategy of Lithuania (2018) specifies as its first target *"to strengthen cybersecurity in the country and to develop cyber defense capabilities"*;
- the strategy of Finland (updated in 2019) recommends that "each administrative branch make its risk assessment and maturity analysis...," which is further developed in the Implementation Program, where the Secretariat of the Security Committee will "*carry out a research project to create an updated maturity model and instrumentation for the purpose of monitoring the status of Finland's cyber security and the achievement of the goals … The maturity model and the instruments will be used to provide regular reports on the status …*"

Case Study: Resilience and Maturity in Bulgarian National Cybersecurity Strategy

A maturity-based approach, encouraged mainly by the experience in implementing the CERT-RMM, was selected in the development of the National Cybersecurity Strategy in Bulgaria, targeting "Cyber Resilient Bulgaria in 2020."[29] Cyber resilience was defined as a target state upon implementing the strategy. According to the strategy, "the achievement of cyber resilience at national level necessitates coordinated activities regarding the security and reliability of all cyberspace components and assets: information, technology, people and facilities, of the

[28] UK NCSC Cyber Assessment Framework (CAF), www.ncsc.gov.uk/collection/caf/cyber-assessment-framework.

[29] "Cyber Resilient Bulgaria 2020," National Cybersecurity Strategy (in Bulgarian), 2016, http://www.cyberbg.eu.

design and deployment of communication channels and services, their interdependency and interoperability."

The strategy has an "actionable architecture" and defines nine domains (areas) with several goals per domain and sets of measures (practices) with capabilities' indicators. For the description of 'maturity,' a three-layered definition of security in cyberspace is used, based on two well-established aspects[30]:

- the implementation of the fundamental 'triad' from information security of Confidentiality, Integrity, and Availability (CIA);
- the extent of our knowledge on risks and threats – adapting the *"known unknowns"* classification, coming from the finances and structured in Nassim Taleb's "Black Swan" theory, but also used in other fields, including for national security and cyberspace.

These two aspects helped to structure goals and measures at three levels and introduce them as a generalized 'label' to express the kind of maturity levels not only of the organizations, but also of the *state, ecosystems, community and nation.* These 'nested' levels are briefly outlined as follows:

- *Level 1 – Information/IT Security ("known knowns")*: protect and defend information assets and infrastructure against known "CIA threats";
- *Level 2 – Cybersecurity ("known unknowns")*: dealing with combined threats, various advanced persistent threats (APTs), attacks against the reputation of people and organizations, disinformation campaigns, and other unpredictable consequences of the mass migration of activities to cyberspace, large-scale information breaches (on a national, regional, and global scale) requiring enhanced and systematic application of the CIA concept to all assets of the digital ecosystem – people, facilities, technologies, and information (informal description of the cyber security);
- *Level 3 – Cyber Resilience ("unknown unknowns"):* preparing for the unknown: unexpected, unforeseeable threats in cyberspace, dynamically changing risks and complex impacts with unpredictable implications necessitating flexibility and resilience of systems, processes, and organizations, as well as introducing appropriate requirements when developing and deploying systems and processes – the essential characteristics of the status of cyber resilience.

Furthermore, the strategy implementation phases are defined as achieving the "maturity levels" and a *transition from cybersecurity to cyber resilience* for the entire country, namely:

[30] George Sharkov, "From Cybersecurity to Collaborative Resiliency," in *Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense (SafeConfig '16)*, 2016, ACM, New York, USA, 3–9, https://doi.org/10.1145/2994475.2994484.

Phase 1 – Initiation ("Cyber secure institutions"): Common agreement on the priorities of the National Cybersecurity Strategy and the Roadmap. Adopt a coordinated approach and establish a common national cybersecurity system framework. Define the main structures and core capacity, development processes, and principles in coordination with key stakeholders. Catch up with NATO and the EU and ensure baseline cybersecurity. Focus on the required basic level of *information security* and build upon it to achieve cybersecurity at the level of the individual organizations. Define "cyber crisis" in the National Cybersecurity Coordination Network. Conduct sector-specific and cross-sector exercises involving entities such as state bodies, businesses, and academia.

Phase 2 – Development ("From capacity to capabilities"): Focus on cyber-resilient organizations and cyber-secure society, develop a coordinated response to cyber crises at the national level. Continue the prevention activities, institutionalize a robust mechanism of interaction and collaboration in case of incidents and crises. Monitor the overall "cyber picture" (situational awareness). Build basic capabilities for operational and strategic analysis and assessment, operational and technical collaboration with NATO, EU, and other international networks.

Phase 3 – Maturity ("Cyber resilient society"): Effectively collaborate at the operational and strategic levels on a national and international scale. Based on the engagement and commitment of all stakeholders, develop advanced joint capabilities in public, private, and research sectors. Identify niches, and work for leading positions and specialization in the region, EU, and NATO.

Subsequently, the national Cybersecurity Act (2018) utilized the "capability levels" approach to define requirements for essential services and critical infrastructures. Target capability levels are defined as follows: 'Baseline' (corresponding to cyber hygiene from the NIS Directive), 'Cybersecure' (or 'performed,' as defined by the State Agency for National Security), and 'resilient' (defined by the Ministry Defense in accordance to civil resilience plans and engagements to NATO and EU collective defense).

As seen, hybrid threats (like disinformation) have been addressed already in *"Level 2 – Cybersecurity,"* but a more systematic coverage of the "hybrid influence," especially in the context of increased specific interest in Eastern Europe, is ongoing for the current update of the National Resilience Strategy and a Roadmap, incorporating the new cyber/hybrid influence (also known as '*cybrid*') to both areas – peoples' minds and critical infrastructures.[31]

[31] Todor Tagarev, "Understanding Hybrid Influence: Emerging Analysis Frameworks," in *Digital Transformation, Cyber Security and Resilience of Modern Societies*, ed. Todor Tagarev, Krassimir Atanassov, Vyacheslav Kharchenko, and Janusz Kasprzyk (Cham, Switzerland: Springer, 2021).

Cyber Maturity and EU, NATO Strategies

The maturity levels approach was recommended for the incorporation of cybersecurity in the "EU Common Security and Defence Policy" (CSDP). In a study performed by ENISA and the Science and Technology Options Assessment Panel of the European Parliament, three aspects of a safer cyber domain in the context of CSDP are considered.[32] In the area of Capacity Building, it is stated that to facilitate capacity building, one has to be able to measure it. The study recommends using cybersecurity capacity models that allow the development and monitoring of cyber capacities and their maturity. The Cybersecurity Capability Maturity Model (CMM of GCSCC) is mentioned.

Another study on EU Financial services discusses the "…degree of digital operational resilience and cybersecurity maturity" that needs to be considered.[33]

A novel maturity assessment framework, Cybersecurity Maturity Assessment Framework (CMAF), was recently proposed and implemented as a pilot in Greece, dedicated to assessing the compliance with the requirements of the NIS Directive. Two main applications of CMAF are foreseen: for self-assessment from operators of essential services and digital service providers (identified according to the NIS Directive as adopted by the Member States) or as an auditing tool from the competent national authorities for cybersecurity.

ENISA also provided a CSIRT Maturity Self-assessment Tool [34] to assist the capacity and capabilities development of national and sectoral CERTs.

In addition to the highly demanding maturity models introduced for defense acquisitions and military supply chain (like the US DoD CMMC, presented above), NATO uses the maturity levels approach to plan and assess the nations' cyber defense capabilities development according to the ongoing Cyber Defense Pledge.[35]

---

[32] EU Parliament, "Cybersecurity in the EU Common Security and Defence Policy (CSDP): Challenges and Risks for the EU," 2017, accessed September 15, 2020, https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2017)603175.

[33] European Commission, "Digital Operational Resilience Framework for Financial Services: Making the EU Financial Sector More Secure," Consultation Document, 2019, accessed September 15, 2020, https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-financial-services-digital-resilience-consultation-document_en.pdf.

[34] ENISA, "CSIRT Maturity – Self-assessment Tool, accessed September 15, 2020, https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey.

[35] Jamie Shea, "Cyberspace as a Domain of Operations," *MCU Journal* 9, no. 2 (Fall 2018): 133-150, https://doi.org/10.21140/mcuj.2018090208.

Conclusion

To assess the cybersecurity and cyber resilience of a sector, community, country, or region, a unified approach to define goals and measurement indicators is needed. Capability maturity models provide such a mechanism since they implement a similar architecture and regardless of possible differences in scope and definitions of domains, they produce comparable scoring of achievements and facilitate the aggregation of target states. As shown, most of the popular models could naturally map, which allows organizations to choose the most suitable for their profile and business goals. At the national level, assessments and plans could still be effectively developed, as maturity and capability levels have identical meaning. However, this challenges the 'maturity' of the maturity models. Since 'cybersecurity' covers mainly the 'protection' side, resilience must be introduced to complete the protect-sustain cycle. Besides, new areas like cyber-empowered hybrid threats (named 'cybrid') should be introduced, as none of the models studied cover yet these aspects, and "*people's minds are not a sector that we know how to protect*." Same for new disrupting technologies like AI, Quantum, 5G – the 'innovation' capability at higher maturity levels is not sufficient, and new domains and indicators will certainly be needed. Maturity models are helpful to align ambition and programs at a higher level (like EU Member States, US States, or regions). They are also recommended to attract and involve the SMEs in the "roadmap to maturity."

Disclaimer

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

Acknowledgment

Connections: The Quarterly Journal, Vol. 19, 2020 is supported by the United States government.

About the Author

George Sharkov is an Adviser to the Minister of Defense and served as a National Cybersecurity Coordinator in the period 2014-2017. He led the development of the National Cybersecurity Strategy of Bulgaria, adopted in 2016. He holds a PhD in Artificial Intelligence and specialization in applied informatics, thermography, genetics, intelligent financial and security systems. Since 2003, he is the CEO of the European Software Institute – Center Eastern Europe, Head of the Cyber Resilience Lab (CyResLab), and since 2014 leads the Cybersecurity Lab at Sofia Tech Park. E-mail: gesha@esicenter.bg