YEARBOOK OF UNWE (2021), PUBLISHING HOUSE – UNWE
ISSN (print): 1312-5486; ISSN (online): 2534-8949; http://unwe-yearbook.org/en/
DOI: https://doi.org/10.37075/YB.2021.2.02

COMPARATIVE ANALYSIS OF THE CYBER SECURITY CAPABILITIES MATURITY MODELS

Venelin Georgiev[1]
e-mail: vgeorgiev@nbu.bg

Abstract

Everything that is being done in the field of cybersecurity, cyber resilience and the fight against cybercrime can be focused on one term and that is the term cybersecurity capabilities. Cybersecurity capabilities demonstrate the ability to implement policies, standards, guidelines, and operational procedures for the security of information systems, networks, applications, and information. In turn, cybersecurity capabilities are a dynamic object that is built, maintained, developed, modified and adapted to the changing security environment. The dynamics of security capabilities require measuring the degree of their maturity and comparing them with the target levels. The article makes a comparative analysis of existing models for assessing the maturity of cybersecurity capabilities, thus creating an opportunity for a reasoned choice of such a method for the needs of specific assessment.

Key words: capabilities, cybersecurity, cyber resilience, levels of maturity, cybersecurity areas, a model for measuring the maturity of cybersecurity capabilities

JEL: A10, F60

Introduction

If the focus of a study is on cybersecurity capabilities, it will not be difficult to find appropriate arguments to justify the relevance of this study. Examples of such arguments include:

- the continuous increase of the scope and scale of application of information technologies in the business, public administration and private life of the citizens;
- the emergence of new and modified threats to the security of information systems, networks, applications and information;
- the huge damage, financial and non-financial that consumers in the face of companies, government institutions and individual consumers suffer as a result of cyber attacks and cybercrime, etc.

Cybersecurity capabilities are a dynamic entity whose management requires the ability to measure their level of maturity and compare operational values with

[1] Prof., PhD, National and International Security Department, New Bulgarian University

predetermined target values (most often in national cybersecurity strategies). For the purposes of measuring the level of maturity of cybersecurity capabilities, a model is needed that is adequate to the object whose capabilities are being measured. In the general case, individual companies or countries as a whole can be defined as such sites.

Measuring the degree of maturity of cybersecurity capabilities can be done using an existing model or using a specially designed model. The comparative analysis of existing models for measuring the maturity of cybersecurity capabilities assists users in choosing the appropriate model or by identifying good practices in case a new model is developed.

The thesis of the study, the results of which are presented in the article, states that the measurement of the maturity of cybersecurity capabilities depends on the characteristics of the model used. The wrong choice of model would make the measurement unproductive and the measurement results themselves misleading. The aim of the research is to increase the level of awareness of cybersecurity specialists about the existing models for measuring the maturity of cybersecurity capabilities and the possibilities for their application in practice. To achieve this goal, the study solves tasks related to the review of scientific publications describing such models, performing a comparative analysis of selected examples of models for assessing the maturity of cybersecurity capabilities, formulating recommendations for the application of these models in practice. The study is limited to selected models for assessing the maturity of cybersecurity capabilities. In the course of the research the methods of document analysis, analysis and synthesis, comparative analysis were used. The study is addressed to cybersecurity professionals whose responsibilities include measuring and assessing the degree of maturity of cybersecurity capabilities.

Information about the compared objects based on the selected criteria

Based on the above arguments, a comparative analysis of models for measuring the maturity of cybersecurity capabilities was performed. The study compared the following models:

- Cybersecurity Capabilities Maturity Model (C2M2) – M1 (Georgiev, 2021; ENISA (n.d.), CSIRT Maturity – Self-assessment Tool);
- National Capabilities Assessment Framework (NCAF) – M2 (ENISA, 2012; Georgiev, 2021; ENISA 2020);
- Cybersecurity Capacity Maturity Model for Nations (CCMM) – M3 (Sharkov, 2020);
- Framework for Improving Critical Infrastructure Cyber Security (FICICS) – M4 (NIST, 2018);

- Qatar Cybersecurity Capability Maturity Model (Q-C2M2) – M5 (Georgiev, 2021);
- Cybersecurity Maturity Model Certification (CMMC) – M6 (NIST, 2018);
- The Community Cyber Security Maturity Model (CCSMM) – M7 (White, 2007);
- Information Security Maturity Model for NIST Cyber Security Framework (ISMM) – M8 (NIST, 2018; Institute of Internal Auditors, 2009);
- The Global Cybersecurity Index (GCI) – M9 (ITU, 2018);
- The Cyber Power Index (CPI) – M10 (Georgiev, 2021).

In order to simplify the use of the individual models in the course of the comparison, they are assigned the corresponding codes, consisting of the letter M and the corresponding numerical index (the codes are listed above, when listing the models themselves).

The criteria on the basis of which the comparison was made are the following:

- organization that developed the model;
- the level of cybersecurity capabilities to which the model relates;
- goals and purpose of the model;
- structuring the areas in the field of cybersecurity;
- maturity levels used.

Assumptions made before the comparison:

- the different models are based on different levels of scientific validity and assurance;
- the degree of connectivity and mutual influence between the separate components of the models is different;
- information with different levels of detail can be found for different models;
- the choice of models included in the comparative analysis is made on the basis of artistic abstraction.

1. Organization that developed the model

M1 – The model was developed by the U.S. Department of Energy (DOE).

M2 – The model was developed by the European Union Agency for Cybersecurity (ENISA) in 2012.

M3 – The model was developed by the Global Cyber Security Capacity Center, which is part of Oxford University. The model was originally developed in 2014, and in 2016 it was updated based on the recommendations of eleven countries that have implemented it.

M4 – The framework was developed by NIST and is designed to guide cybersecurity and risk management activities in organizations.

M5 – The model was developed by Qatar University's College of Law in 2018. It is based on various existing models for assessing and enhancing cybersecurity capabilities.

M6 – The model was developed by the US Department of Defense in collaboration with Carnegie Mellon University Johns Hopkins University Applied Physics Laboratory.

M7 – The model was developed by the Center for Infrastructure Assurance and Security in collaboration with The University of Texas in 2007.

M8 – The model was developed at a university in Saudi Arabia in 2017.

M9 – The initiative to develop the index is of the International Telecommunication Union.

M10 – The index was developed under the program of the Economist Intelligence Unit in 2011.

2. The level of cybersecurity capabilities to which the model relates

M1 – The model is addressed to assess the maturity of cybersecurity capabilities of organizations of all types, sectors and scales.

M2 – The model is designed to create opportunities to measure the maturity of cybersecurity capabilities at the country level.

M3 – The model is addressed to measure the maturity of cybersecurity capabilities at the country level.

M4 – The model can be applied to assess the maturity of cybersecurity capabilities for organizations of any type, regardless of the scale of their business, the type of risks and the specifics of the cyber environment and cybersecurity.

M5 – The model is addressed to measure the maturity of cybersecurity capabilities at the country level.

M6 – The model is addressed to measure the maturity of cybersecurity capabilities of the defense industrial base.

M7 – The model is addressed to measure the maturity of the cybersecurity capabilities of individual countries.

M8 – The model is applicable in measuring the maturity of cybersecurity capabilities at the organizational level.

M9 – The model is applicable when measuring cybersecurity capabilities at the country level.

M10 – The model is applicable to determine the level of cybersecurity capabilities of an individual country.

3. Aims and purpose of the model

M1 – The purpose of the model is to assist organizations in evaluating and developing their cybersecurity programs and increasing their operational resilience.

M2 – The purpose of the model development is to provide a tool for self-assessment of the level of maturity of cybersecurity capabilities of the EU member states on the basis of their national cybersecurity strategies. The idea is thus to increase the effectiveness of efforts to create and develop cybersecurity capabilities at both the strategic and operational levels.

M3 – The aim of the model is to increase the efficiency of the process for building cyber security capabilities of the country.

M4 – The purpose of the model is to assist organizations in managing activities in the field of cybersecurity and risk management.

M5 – The purpose of the model is to provide an applicable tool that can use the benchmark concept in measuring and developing Qatar's cybersecurity.

M6 – The main purpose of the model is to assess the degree of protection for the information of the defense industrial base.

M7 – The aim of creating the model is to improve the opportunities for assessing and developing cybersecurity capabilities by creating a roadmap for efforts in this area.

M8 – The purpose of developing the model is to create an opportunity to assess the cybersecurity capabilities of the organization.

M9 – The aim of the model is to create opportunities to review and evaluate cybersecurity commitments in Africa, the Americas, the Arab countries, the Asia-Pacific region and Europe.

M10 – The model is designed to perform a dynamic quantitative and qualitative assessment of specific characteristics of the cyber environment and cyber capabilities.

4. Structuring the areas in the field of cybersecurity in which the maturity of cybersecurity capabilities is assessed

M1 – The cybersecurity capabilities being assessed are structured in ten areas. Each area has unique goals at the strategic and operational level. The ten areas include: risk management; asset, change and configuration management; identity and access management; threat and vulnerability management; situational readiness; responding to cybersecurity incidents and events; management of supply chains and external dependence; personnel management; cybersecurity architecture; cybersecurity program management.

M2 – The model assesses the maturity of cybersecurity capabilities in four areas: leadership and cybersecurity standards (measures a country's ability to build adequate leadership, standards and good practices in cybersecurity; various aspects of cybersecurity and cyber defense are taken into account); capacity to build cybersecurity capabilities and consumer awareness (the country's ability to raise consumer awareness of cybersecurity threats and risks, as well as how to counter them, is assessed; the country's capacity-building capabilities are also assessed for cybersecurity and for conducting research in the field); laws and regulations (measuring the ability of countries to enforce laws and regulations in response to growing cybercrime and the growing number of cyber incidents, as well as to protect critical infrastructure); cooperation (assessing the degree of cooperation and exchange of information between the parties and stakeholders;

forms of cooperation are seen as tools to improve disruption and respond to changes in threats coming from the environment). Within the four areas listed above, the model also defines the respective objectives (17 in total).

M3 – Five areas in the field of cybersecurity are included and reported in the model. In each area, there are factors that describe the details of building cybersecurity capabilities. For each factor, aspects are defined that specify the scope of the factor. Aspects help to formulate sub-areas with a smaller scope. Each aspect is assessed using metrics/indicators describing the steps, actions and conditions that are included in the respective level of maturity. The five areas in the field of cybersecurity that are considered in the model are: creation of a cybersecurity policy and strategy which contains six factors; raising the organizational culture of cybersecurity in a society that contains five factors; expanding the body of knowledge in the field of cybersecurity which includes three factors; creating a sufficiently effective legal and regulatory framework in the field of cybersecurity which contains three factors; risk management for cybersecurity which contains seven factors.

M4 – The model uses five areas (functions), which considered together provide a strategic perspective on the life cycle for cybersecurity risk management in the organization. Next, there are categories and subcategories for each of the areas, seeking compliance with standards, guidelines and good practices. The five areas of the model are: cybersecurity risk identification; asset protection; detection of cybersecurity incidents; response to a cybersecurity incident; recovery after a cybersecurity incident.

M5 – The model adapts the NIST model to use five key functions as key areas in the field of cybersecurity. Each of the five areas includes sub-areas that exhaust the range of cybersecurity capabilities whose maturity is measured. The five areas and the sub-areas included in them are: “Understanding”; “Security”; “Risk exposure”; “Answer”; “Sustainability”.

M6 – The model takes into account seventeen areas representing clusters in cybersecurity processes and capabilities. Each of the areas includes processes and capabilities assessed within five levels of maturity. Cybersecurity capabilities are detailed in practices that also correspond to maturity levels. The areas themselves can be described as follows: access control; asset management; accountability and auditing; consumer awareness and training; configuration management; identification and authentication; response to cybersecurity incidents; maintaining a safe environment; media protection; personal security; physical security; recovery after a cybersecurity incident; cybersecurity risk management; data security assessment; situational readiness; protection of systems and communications; integrity of systems and information.

M7 – The model uses six areas that provide different aspects of cybersecurity. The areas are: cybersecurity threats; cybersecurity metrics; information sharing; technologies; consumer education; cybersecurity testing.

M8 – The model uses the areas of cybersecurity identified in the NIST model, complementing these areas with a new one – conformity assessment.

M9 – The model "steps" on the five columns (areas) of the Global Cybersecurity Agenda. These columns form five sub-indices, each of which includes specific indicators related to cybersecurity and cybercrime. The areas can be described as follows: "Regulatory", "Technical", "Organizational", "Capacity Building", "Cooperation in the field of cybersecurity".

M10 – The index uses four drivers (areas) for cybersecurity and cyberpower, each of which is measured using indicators. The areas are: "Legal and regulatory framework"; "Economic and social context"; "Technological infrastructure"; "Application in industry".

5. Maturity levels used in the model to assess cybersecurity capabilities

M1 – The model uses four levels of maturity of cybersecurity capabilities. Level 0: No cybersecurity procedures apply. Level 1: Initial cybersecurity procedures apply, but this becomes ad-hoc. Level 3: The applied cybersecurity practices are documented and provided with resources; the staff performing the procedures is trained and has the necessary skills; the roles and responsibilities for the implementation of the procedures are distributed. Level 4: Practices are defined on the basis of cybersecurity policies and standards, and are regularly reviewed and updated.

M2 – The model uses five levels of maturity which follow the process of building and developing cybersecurity capabilities, i.e. they represent increasing levels of maturity. The levels build on the level 1 cybersecurity capacity maturity assessments: the country does not have a clear approach to building and assessing cybersecurity capabilities. There may be some goals that are described too broadly. It is also possible to conduct occasional surveys in the field of cybersecurity capabilities, up to level 5: the national strategy for building cybersecurity capabilities is dynamic and adaptable to changes in the environment (threats, new technologies, large-scale cyber conflicts, etc.). The information obtained is used in decision-making to develop cybersecurity capabilities. There are opportunities to quickly improve the current level of cybersecurity capabilities.

M3 – The model uses five levels of maturity: initial or entry level (at this level there are no cybersecurity capabilities or there are some, but their level of maturity is extremely low); formative (in some areas abilities appear, but they are created ad-hoc, disorganized and vaguely defined); constructive (individual components of cybersecurity capabilities are available and implemented. There is not enough rationality in the allocation of resources); strategic (prioritize areas in the field of cybersecurity, as well as aspects considered in the model); dynamic (there are mechanisms for reviewing the areas and aspects reported in the model in relation to changes in the environment. There is a sufficiently fast process for decision-making and allocation of resources for the needs of cybersecurity capabilities).

M4 – The model uses four levels of maturity (executive chains), each of which is determined using three components: a risk management process; integrated risk management program; external participation. The description of these chains can be made as follows: first level "Partial" (the organization does not have formalized procedures and practices for risk management for cybersecurity; the risk is managed ad-hoc and often a reactive approach is applied; the organization has limited awareness of cybersecurity risks, risk management is not a regular activity, but is carried out only when a specific case arises as risk management information is not shared in the organization, the organization does not understand its role in a wider ecosystem as a dependent party and as an influencing party, the organization is often not prepared for the cyber risks coming from the products for the delivery of products and services that it supplies and receives); second level "Informed risk" (the risk management procedures in the organization are approved by the strategic management, but are not integrated into organizational policy; the organization is aware of the risks of cybersecurity, but there is no sufficiently comprehensive approach to managing these risks; the organization's cybersecurity risk is not addressed regularly, the organization understands its role in the wider ecosystem in terms of its dependence, as well as in terms of the impact it has, the organization pays attention to the cyber risk associated with supply chains , but does not formally address these risks); Level 3 "Repeatable" (the organization's cybersecurity risk management practices are integrated into an appropriate policy; these practices are regularly reviewed and updated based on ongoing changes in business, technology and the external environment; the organization applies a comprehensive risk management approach to cybersecurity; policies, processes and procedures for managing cybersecurity risk are defined, implemented and improved; the organization understands its role as part of a wider ecosystem and contributes to the overall understanding of cybersecurity risks); fourth level "Adaptive" (the organization adapts its practices in the field of cybersecurity based on the results of past and current activities, lessons learned, use of metrics and indicators; the organization applies a comprehensive approach to managing cybersecurity risk using policies, processes and risk-informed procedures to respond to potential cybersecurity events; the organization understands its place and role in a wider ecosystem and contributes to a broader understanding of cybersecurity risk).

M5 – The model uses five levels of maturity, which are used to measure the level of maturity of cybersecurity capabilities of public and private organizations at the function level. The description of the levels of maturity can be made as follows: first level "Initiation" (within this level ad-hoc procedures and practices for cybersecurity in the respective field are applied); second level "Implementation" (adapted policies are implemented to implement cybersecurity activities in each of the areas, seeking complementarity with new activities); third level "Development" (policies are imple-

mented to improve and develop activities in the field of cybersecurity in each of the areas); Fourth level "Adaptation" (review of activities in the field of cybersecurity and approval of new practices based on predictive indicators from previous research and training); Fifth level "Flexibility" (ensuring the dynamism of activities in the field of cybersecurity in their implementation in different areas).

M6 – The model uses five levels of maturity, determined on the basis of processes and practices in the field of cybersecurity. Recognition of each of the levels of maturity requires the implementation of relevant processes and practices, as well as the processes and practices of previous levels. The description of maturity levels can be done as follows: first level "Implementation" (the organization implements cybersecurity practices ad-hoc without documenting them; the practices are focused on information security and meet basic security requirements); second level "Documentation" (there are documented policies and practices in the organization that guide cybersecurity efforts; documenting practices helps them to be implemented in the same way by different people; documenting practices is seen as part of the building process cybersecurity capabilities, the applied practices in the field of cybersecurity meet the requirements of NIST SP800-171, as well as the requirements of other standards); third level "Management" (the organization develops, implements and provides resources for a plan to build cybersecurity capabilities; practices focus on information security and include the requirements of NIST SP 800-171, as well as other standards); Fourth level "Control" (the organization reviews and measures the effectiveness of practices and on this basis corrective decisions are made; practices focus on information protection and include a set of security requirements; they are aimed at creating cybersecurity capabilities that are adequate to threats from the environment); fifth level "Optimization" (the organization standardizes and optimizes the processes of building cybersecurity capabilities; practices are focused on information security; with the help of additional practices increases the depth and complexity of cybersecurity capabilities).

M7 – The model uses five levels of maturity, determined on the basis of the type of threats and relevant activities. A description of maturity levels can be made as follows: first level "Awareness" (organizations and consumers are informed about threats, problems and solutions related to cybersecurity); second level "Development of a process" (creation and continuous improvement of a process that meets the problems of cybersecurity); third level "Information Sharing" (the organization pays special attention to improving the ability to share information in a secure way), fourth level "Tactical Development" (the organization develops proactive methods (including preventive methods) to detect and respond to cyberattacks); fifth level "Complete set of operational capabilities for cybersecurity" (the organization has full operational readiness to respond to cybersecurity threats).

M8 – The model uses five levels to assess the maturity of cybersecurity capabilities, which are not detailed. The levels can be defined as: running

process; managed process; built process; predictable process; optimized process for building cybersecurity capabilities.

M9 – The index is not a model for assessing the level of maturity of cybersecurity capabilities and therefore it does not use maturity levels. The index is used to compare the levels of cybersecurity capabilities for individual countries and regions.

M10 – The index does not use levels to assess the maturity of cybersecurity capabilities.

The summarized results of the comparative analysis of the models included in the study for measuring the maturity of cybersecurity capabilities, using the defined criteria, are presented in Table 1.

Table 1: Summary results of the study

Criteria **Models**	**Organization that developed the model**	**The level of cybersecurity capabilities to which the model relates**	**Goals and purpose of the model**	**Structuring the areas in the field of cybersecurity**	**Maturity levels used**
C2M2	US - DOE	organization	assisstance	ten areas	four levels
NCAF	ENISA	country	tool for self-assessment	four areas	five levels
CCMM	GCSCC	country	increase the effectiveness	five areas	five levels
FICICS	NIST	organization	assisstance	five areas	four levels
Q-C2M2	QUCL	country	provide an applicable tool	five areas	five levels
CMMC	US - DoD	organization	assisstance	seventeen areas	five levels
CCSMM	CIAS - UT	country	improve the opportunity	six areas	five levels
ISMM	SAU	organization	create an opportunity	six areas	five levels
GCI	ITU	country	ireate an opportunity	five areas	n.a.
CPI	EIU	country	assisstance	four areas	n.a.

Source: Summary of the comparative analysis made above

Conclusion

Based on the results of the comparative analysis, the following conclusions can be formulated:

- The studied models are developed by scientific organizations in close cooperation and with the help of academic organizations, government agencies and private business companies. This proves both the importance of the issue of building adequate cybersecurity capabilities and the comprehensive nature of this issue;
- some of the analyzed models are addressed to measuring cybersecurity capabilities at the company level, while other models allow measuring the maturity of cybersecurity capabilities at the state level;
- as a general goal for all models is set the support of users in the process of building and maintaining cybersecurity capabilities, prioritizing future efforts and projects in the field of cybersecurity, eliminating existing weaknesses and gaps;
- the analyzed models include in their structure a different number of areas, with the help of which the whole field of cybersecurity is covered. The structuring of these areas follows a different logic, which supports the application of each model in a specific environment;
- The models included in the study use maturity levels that take into account the possibilities for performing various activities in the field of cybersecurity.

The comparative analysis of models for measuring the maturity of cybersecurity capabilities is useful on the one hand for the specific information about the nature and features of individual models, and on the other hand for indicating the urgency of measuring the cybersecurity capabilities of government agencies and private sector companies in Bulgaria, as well as in the country as a whole.

References

European Network and Information Security Agency (ENISA). (2012). NCSS: Practical Guide on Development and Execution, available at: https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide

European Union Agency for Cybersecurity (ENISA). (2020). National Capabilities Assessment Framework.

ENISA. (n.d.). CSIRT Maturity – Self-assessment Tool, available at: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

Georgiev, V. (2021). Scenario planning for cybersecurity capabilities, Avangard, Sofia.

Institute of Internal Auditors (ed.). (2009). Internal audit capability model (IA-CM) for the public sector: overview and application guide, Altamonte Springs, Fla: Institute of Internal Auditors, Research Foundation.

International Telecommunication Union (ITU). (2018). The Global Cybersecurity Index, available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, MD: National Institute of Standards and Technology, available at: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Sharkov, G. (2020). Assessing the Maturity of National Cybersecurity and Resilience, Connections: The Quarterly Journal 19, no. 4, pp. 5-24.

White, G. (2007). The Community Cyber Security Maturity Model, in 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07).