Information & Security

Published since 1998

T. Tagarev, M. Pappalardo & N. Stoianov
vol. 47, no. 1 (2020): 13-26
https://doi.org/10.11610/isij.4701

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

A Logical Model for Multi-Sector Cyber Risk Management

Todor Tagarev [a] (✉), ***Salvatore Marco Pappalardo*** [b,c], ***Nikolai Stoianov*** [d]

[a] *Institute of Information and Communication Technologies, Bulgarian Academy of Sciences, Sofia, Bulgaria, http://www.iict.bas.bg/EN*

[b] *Software Engineering Italia S.r.l., Via Santa Sofia 64, Catania, Italy http://www.swing-it.net/*

[c] *Italian Consortium of Medical Research (CIRM), Viale Zara 81, Milan, Italy*

[d] *Bulgarian Defence Institute, Sofia, https://www.di.mod.bg/*

ABSTRACT:

The increasing reliance on digital infrastructures makes whole sectors of the economy and public services vulnerable to attacks through cyberspace. Some progress has been made in understanding vulnerabilities and ways of reducing cyber risk at the sub-sectoral level. While the sectoral level remains a significant challenge, this study goes beyond, also addressing cyber risk resulting from the cross- and multi-sectoral interdependencies in a consistent logical model. The paper presents the scope of this logical model, outlines the problem of risk assessment, structured around the triplet “Threats – Vulnerabilities – Impact,” and the structuring of risk mitigation around types of risk reduction measures, the objective of decision-making on risk treatment, and the modalities of application. We provide examples of the implementation of the logical model, underlying the ECHO Multi-sector Assessment Framework, and conclude by emphasising the advantages the logical model and the framework provide.

ARTICLE INFO:

RECEIVED: 28 APR 2020
REVISED: 16 MAY 2020
ONLINE: 18 MAY 2020

KEYWORDS:

cybersecurity, critical infrastructure, essential services, interdependencies, cyber risk assessment, E-MAF, ECHO project

✉ E-mail: tagarev@gmail.com

Introduction

The incorporation of emerging information technologies and evolving infrastructures allow businesses to be more efficient and effective in meeting customers' needs and expectations. The increasing reliance on digital infrastructures, however, makes whole sectors vulnerable to attacks through cyberspace. Some of these vulnerabilities have already been exploited, thus triggering massive research on the problem and its potential solutions. As a result, we already have a much better understanding of the cyber threats to industrial control systems [1] and opportunities to protect better electrical energy grids [2] or ships,[3] to take just a few examples.

There are also relevant developments attempting to address comprehensively cybersecurity concerns at the sectoral level, e.g. the HITRUST common security frameworks for the healthcare sector, but progress so far has been limited. The challenge becomes even more significant in attempting to take cross-sectoral interdependencies into account and the possible cascading effects of a cyberattack across sectors.

With the study presented here, we are embarking on this challenge by creating a multi-sectoral cyber risk assessment framework. This study is part of the research programme of the Horizon 2020 ECHO project (European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations, 2019-2023) and supports the development of the ECHO Multi-sector Assessment Framework (E-MAF).

Towards that purpose, the design of the logical model presented here pursues two main goals:

1. To present the key factors and considerations in multi-sectoral cyber risk assessment in their relationship; and
2. To make explicit the scope of E-MAF and the topics to be covered in the lifetime of the ECHO project.

The next section provides the rationale for defining the scope of the logical model and, thus, of E-MAF. It is followed by elaboration on risk assessment, structured around the triplet "Threats – Vulnerabilities – Impact" and the methods used for risk estimation, and then by presenting the structuring of "risk mitigation" around the types of risk reduction measures, scope and objectives of decision-making on risk treatment, and the approach to the application of the risk management cycle. The final section concludes with a view on the forthcoming implementation of this logical model and E-MAF and emphasises the advantages of our approach.

Scope of the E-MAF Logical Model

E-MAF, like most of the existing frameworks [4] and standards,[5, 6, 7] goes beyond risk assessment *per se*, and supports *risk management* decision-making, i.e. it provides a framework for understanding cyber risks and, on that basis, supports decisions on where to invest human, technological and financial resources to reduce those risks to an acceptable degree.

Resource allocation decisions are most often taken at the organisational level. However, E-MAF goes beyond the level of an individual organisation and will support risk management at the sectoral level, cross- and multi-sectoral level, national and pan-European levels.

'Sectoral' here may mean both a 'sector', for example, the 'Energy' sector defined in Directive 2008/114/EC,[8] or a 'sub-sector,' e.g. 'Electricity' (including "infrastructures and facilities for generation and transmission of electricity in respect of supply electricity" [9]) or the 'Rail transport' sub-sector of the 'Transport' sector.

'Cross-sectoral' are resource allocation decisions taking into account cross-sector effects resulting from interdependencies between interconnected systems and infrastructures.[10] Among the examples here are the interdependencies between telecommunications and electricity distribution or the dependence of banking and financial services on the digital infrastructure.

'Multi-sectoral' are, on the one hand, the cases accounting for interdependencies among three or more sectors and potential cascading effects of a cyberattack. On the other, multiple sectors can benefit from the application of a specific measure to reduce cyber risks. An example would be the institutionalisation of an accredited training program providing cybersecurity competencies needed in several sectors. Such cases are designated below as 'transversal.'

Finally, E-MAF may be used at national and European Union levels in the elaboration of policies and measures aiming to reduce the cyber risks in the design and operation of critical infrastructures and the provision of essential services.

This scope of E-MAF is presented in the first row of Figure 1, followed by two groups of 'risk assessment' and 'risk mitigation,' examined in the following subchapters. Issues listed in the cells with the dark-grey background are considered in the first version of E-MAF; those in cells with light-blue background – in the second version of the framework. Due to resource and time limitations, the issues in white cells will not be treated in detail during the lifetime of the ECHO project.

Risk assessment

In the traditional understanding, reflected, for example, in ISO 27005, the risk is defined by the likelihood of the occurrence of an unwanted event and the consequences that would follow from that event. This understanding is directly incorporated for dealing with risk in some security fields, for example, in capabilities-based planning methodologies and guidelines used in defence,[11] homeland security,[12, 13] and the broader security sector.[14] Determination of the risk in all these examples is based on a set of plausible, and agreed, scenarios, describing one or a series of interrelated events in their context. TOGAF also incorporates capability-based planning and the use of business scenarios to discover and refine capability requirements.[15]

Coverage	Organisational	Sectoral	Cross-sectoral	Transversal	EU/national
Risk assessment					
Threats	Cyber threats	Cyber-Physical interdependencies	Natural hazards, industrial accidents, terrorist attacks		
Vulnerabilities	Hardware	Software	Networking	Organisation	
Impact	Negative consequences	Opportunities/ benefits of risk mitigation measures			
Negative consequences	*Direct (physical, loss of information, financial)*	*Injuries, death, health & safety*	*Reputational*	*Lost opportunities*	*Social impact*
Risk estimation	Qualitative	Quantitative	Combination of Qualitative & Quantitative		
Risk mitigation					
Measures to enhance:	Awareness	Protection	Response and recovery	Resilience and adaptiveness	Prevention
Decisions on measures	Selective	Prioritisation	Optimisation		
Application	Ad-hoc	Recurring	Proactive (based on predictive analytics)		

Figure 1: The Logical Model of the ECHO Multi-sector Assessment Framework.

The number of scenarios used in a planning cycle can range from 15 in the case of the U.S. Department of Homeland Security [16] to several dozens. The use of scenarios is beneficial in representing uncertainty, providing transparency, and involving senior decision-makers. However, by itself, the process of elaborating and selecting a set of scenarios cannot guarantee the *comprehensive* treatment of all risks, especially in a diverse, ill-defined and evolving field such as cybersecurity.[17]

In a similarly diverse and evolving [18] field of disaster risk management, the assessment of risk covers natural and human-induced *hazards*, *exposure* of humans, infrastructure and ecosystems, systems' *vulnerability*, and the impact of a disaster.[19]

"Hazard – exposure – vulnerability" is not the only structuring suitable for comprehensive treatment of risks. The risk assessment and treatment process in ISO 27001 is based on "asset – threat – vulnerability" analysis.[20] ISO 27005 further specifies that:

- the examination of an asset involves its valuation,
- the impact of an information security incident is estimated with an account of direct and indirect, operational and future business effects from a full or partial loss of an asset, and

- in the first assessment (when no new security measures are considered), the estimate of an impact is very close to the value of the concerned asset.

This relation between a broadly defined asset value and the estimated impact, or consequence, of an incident allows to assess cybersecurity risk using the 'triplet' of "threat – vulnerability – consequence."[21] The same simple framework is used in related security fields, for example, in the risk analysis conducted by the U.S. Department of Homeland Security.[22] For these reasons, this is the structuring adopted in the E-MAF logical model.

Threats

Threats can be classified in a number of ways, e.g. depending on the intent of the attacker (a group of attackers), his or her knowledge and skills, selected targets, attack vectors, tactics, techniques and procedures, etc.[23]

At the highest level, E-MAF distinguishes between three groups of threats:

1. Cyber threats *per se*, e.g., threats of DDoS attacks, malware, social engineering, etc.
2. Threats as results of cyber-physical interdependencies, e.g., power outage, disruption of communications (due for example to an electromagnetic storm), etc.
3. Threats of physical destruction or disruption as results of either deliberate actions (e.g. terrorism, warfighting, sabotage, vandalism, theft, traffic accidents) or unintentional (natural disasters, industrial accidents).

For more detailed classification of threats, E-MAF builds on ENISA's Threat Taxonomy.[24]

Vulnerabilities

Cyber vulnerabilities can also be classified in several ways. For example, ENISA, reflecting on the 1998 report by John Howard and Thomas Longstaff of Sandia National Laboratories, considers *design*, *implementation*, and *configuration* vulnerabilities.[25]

More focused studies, e.g. on cybersecurity of in the context of Industry 4.0,[26] distinguish vulnerabilities related to:

- Operating systems or firmware;
- Application software;
- Industrial communication protocols; and
- Smart devices (embedded sensors and actuators).

In the ECHO project, to provide for compatibility with other activities, e.g. the development of the skills framework, E-MAF implements a vulnerability taxonomy including four main groups:

1. Hardware-related vulnerabilities, e.g. use of unencrypted personal devices;

2. Software-related vulnerabilities, e.g. use of unpatched operations systems and applications;
3. Networking vulnerabilities, e.g. related to the use of Wi-Fi, VPNs, and remote access;
4. Organisation-related vulnerabilities, e.g. related to skills and awareness of personnel, business processes, etc.

Consequences

In the traditional understanding, the risk is equated to the "chance or probability of loss." This focus on 'loss' is reflected, for example, in ISO/IEC 27005:2008, which examines the negative impact of an information security incident. Since its 2009 version, ISO 31000 defines risk as "effect of uncertainty on objectives," allowing thus to consider negative as well as positive consequences of uncertainty.

Respectively, the E-MAF logical model examines two main groups of consequences:

1. Negative consequences;
2. Positive consequences in terms of opportunities and benefits of risk mitigation measures, e.g. higher general competences of personnel that has undergone cybersecurity training or new business opportunities resulting from investments in the development and/or implementation of particular cybersecurity technology.

A negative consequence may result from a damaged or fully destroyed device, loss of data or communications and lead to reduced effectiveness, adverse operating conditions, loss of business, reputation, etc.[27] Without making a claim for comprehensiveness, ISO 27005 recommends considering operational consequences of incident scenarios in terms of:

- Investigation and repair time;
- (Work)time lost;
- Opportunity lost;
- Health and Safety;
- The financial cost of specific skills to repair the damage;
- Image reputation and goodwill.

The E-MAF logical model implements the following high-level classification of negative consequences:

- Direct consequences, including physical damage, loss of data and information, disrupted business process, and short-term financial losses;
- Injuries, death, health and safety;
- Reputational damage;
- Lost business opportunities;

- Social impact, e.g. disruption to people's daily lives, widespread anxiety or loss of confidence in online services or technology more generally.[28]

Risk estimation

Depending on the available information and capacity, the estimation of both the likelihood of a cybersecurity incident and its consequences may be qualitative, quantitative, or through a combination of the two.[29] This is also the classification of approaches and methods to risk estimation adopted in the E-MAF logical model.

In qualitative terms, the consequences of an incident are estimated using a scale of qualitative attributes. In its simplest form, the scale includes 'Low,' 'Medium,' and 'High.' The same scale may be used to assess the likelihood of occurrence of those consequences. ISO/IEC 27005 provides an example (p. 50) of the use of five-degree scales and how qualitative estimates can be transformed into numbers.

Related security fields (e.g. in the development of the national security strategy of The Netherlands [30]) provide relevant examples of the use of other scales of qualitative indicators:

- 'very rare,' 'rare,' 'unlikely,' 'possible,' 'probable' in estimating likelihood; and
- 'insignificant,' 'minor,' 'moderate,' 'significant,' 'catastrophic' in estimating impact.

Often, qualitative estimation is used first to identify major risks and obtain a general indication of the level of risk.[31] The reliance on qualitative estimates is unavoidable if historical data or data from rigorous modelling of events and their impact is lacking.

Quantitative estimation may include estimates of the probability or a frequency of cybersecurity incidents over a given period and assessments of the actual impact of such incidents, preferably based on verified historical records. Other sources of information that can be used for quantitative estimates are the cybersecurity exercises and the results of rigorous modelling. In some cases, one can use statistical approaches and methods, e.g. the Delphi method, to process expert opinions and derive quantitative data.

While adding rigour and transparency to risk management, the accuracy of quantitative estimates depends on the completeness and reliability of historical data and models. When models are not validated, or historical incident data in incomplete or unreliable, the quantitative approach may create an illusion of worth and accuracy of the risk assessment.[32]

E-MAF provides for estimates through a combination of qualitative and quantitative methods. With the accumulation of experience and data, these opportunities will grow, allowing, for example, a combination of qualitative scorecard assessment to determine the level of cyber risk exposure and a Bayesian network to model the financial loss of cyber incidents.[33]

E-MAF examines relevant aspects of the "risk evaluation" activity, described as part of "risk assessment" in ISO 31000 and ISO 27005, in the following subsection.

Risk Mitigation

"Risk mitigation" is one of the synonyms of the "Risk treatment" activity – a term used in ISO 31000 and ISO 27005. "Risk mitigation" was preferred as it already denotes a wide variety of strategies and measures that can be used to reduce cyber risks. Just as "risk treatment," this term allows to consider the recommendations in ISO 31000 by:

- avoiding the risk by discontinuing or not starting the risk generating activity;
- taking or increasing risk in order to pursue an opportunity;
- removing the source of risk;
- changing the likelihood of occurrence;
- taking measures to reduce the consequences;
- sharing the risk with another party or parties (including contracts and risk financing);[34]
- taking an informed decision to retain the risk,

as well as longer-term measures such as developing training programmes or new risk mitigation technologies and solutions.

Measures

The above list may be used as a starting point to design a taxonomy for cyber risk reduction measures.

E-MAF, however, adopts a structure of existing and potential risk reduction measures with five main groups of measures aiming respectively to:

- increase *awareness* of policy-makers, staff or wider society on cyber risks;
- enhancing the *protection* of assets and systems, including by remedying identified vulnerabilities and reducing exposure to cyberattacks;
- strengthening the capacity for *response and recovery*, e.g. by increasing the use of predictive analytics to enhance agility in responding to incidents;[35]
- enhancing *resilience and adaptiveness*, e.g. through collaboration,[36] design measures such as compartmentalisation of information systems and networks, redundancy and diversification,[37] organisational agility allowing to adapt quickly to changing circumstances;[38]
- *preventing* the realisation of cyber threats by deterrence,[39] performing active defensive functions in cyberspace,[40, 41] or other measures.

Decisions on measures to be implemented

Decisions on what strategies and measures to apply to reduce cyber risk can be taken by:

1. Focusing *selectively* on one or a small number of issues, usually related to high-visibility cases on the attention of decision-makers, for example, a recent, high-impact attack in the same industry sector;[42]
2. Prioritisation among competing demands, e.g. based on prioritised gap analysis;[43]
3. Optimisation.

Applicable ISO standards recommend at least prioritisation of risks and measures (controls); yet, option 1 may be the only available option for the elaboration of policies common for a given sector or several interdependent sectors.

Any of these options requires an understanding of the costs and benefits of the application of risk reduction measures. Decisions in options 2 and 3 are set in a resource constraint framework and require the use of an agreed number of risk evaluation criteria, against which to compare potential risk mitigation measures.

Application

ISO 27005 recommends to conduct a risk assessment and take respective risk mitigation decisions in two or more iterations: first, to carry out a high-level assessment to identify potentially high risks that justify further assessment; and then to conduct in-depth analysis, possibly using a different method.

The cycle may include monitoring the implementation of risk mitigation measures and incorporation of lessons learned on the results and performance of measures implemented in previous cycles.[44]

This whole iterative cycle may be applied *ad-hoc*, on a *recurring* basis, or *proactively* to meet foreseen risks. These are the three respective fields in the E-MAF logical model.

Ad-hoc is the application in the first time an organisation decides to become certified in accordance with one or more relevant standards. This decision may be based on organisational strategy, newly introduced legislative requirements, or may be triggered by a high-impact cyber incident involving the organisation itself or other organisations in the same sector or using similar technologies. At least initially, ad-hoc would be the application on the sectoral or multi-sectoral level.

Recurring is the application when a company, a sectoral or cross-sectoral network of organisations has procedures in place to conduct risk assessment regularly or upon considerable changes in the risk management environment, e.g. in the wake of an attack with sizeable consequences, a new significant threat or the discovery of a crucial vulnerability.

Proactive is the application when the organisation has a system in predictive analytics in place. Predictions may be based on time series analysis,[45] dynamic real-time probabilistic risk data and cyber risk analysis,[46] and other methods, applying, as a rule, some form of machine learning and artificial intelligence.

Implementation of the E-MAF Logical Model

Unlike most of the existing frameworks and standards, E-MAF covers not only the needs of a single organisation, but also of parties that are interested in sectoral, multi-sectoral, national, and even multinational, e.g. European Union level treatment of cyber risk. That may be sectoral or cross-sectoral associations, national governments or EU agencies concerned with the provision of cybersecurity.

The logical model of the framework is sufficiently broad to account for known historical events, treats and vulnerabilities, but also for future threats and vulnerabilities, e.g. new attack surfaces as a result of the proliferation of IoT devices [47] or potential emergent behaviour in meshed 'systems-of-systems.'[48]

The comprehensiveness of the framework provides flexibility to select threats, assets, and interdependencies to be accounted for in a risk management cycle, while the use of scenarios remains the state-of-the-art approach in risk assessment and planning aiming to optimise risk.[49] That includes the design of scenarios and use cases in the ECHO research, and adding new scenarios throughout the life of the project.

Acknowledgement

This work was supported by the ECHO project, which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no. 830943.

References

[1] Muhammad Rizwan Asghar, Qinwen Hu, and Sherali Zeadally, "Cybersecurity in Industrial Control Systems: Issues, Technologies, and Challenges," *Computer Networks* 165 (2019), 106946, https://doi.org/10.1016/j.comnet.2019.106946.

[2] Liang Che, Xuan Liu, and Zuyi Li, "Fast Screening of High-Risk Lines under False Data Injection Attacks," *IEEE Transactions on Smart Grid* 10, no. 4 (2019), 4003-4014, https://doi.org/10.1109/TSG.2018.2848256.

[3] Boris Svilicic, Junzo Kamahara, Jasmin Celic, and Johan Bolmsten, "Assessing Ship Cyber Risks: A Framework and Case Study of ECDIS Security," *WMU Journal of Maritime Affairs* 18, no. 3 (2019): 509-520, https://doi.org/10.1007/s13437-019-00183-x.

[4] *MAGERIT version 3: Methodology of Analysis and Risk Management Information Systems*, NIPO 630-12-171-8 (Madrid: Ministry of Finance and Public Administration, October 2012).

[5] ISO, “Risk management – Principles and Guidelines,” ISO 31000. The concrete references in the text below are to the ISO 31000:2009 version of the standard.

[6] ISO, “Information technology – Security techniques – Information Security Risk Management,” ISO 27005. The concrete references in the text below are to the BS ISO/IEC 27005:2008 version.

[7] NIST, “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,” NIST Special Publication 800-37 Rev. 2 (Gaithersburg, MD: National Institute of Standards and Technology, December 2018), https://doi.org/10.6028/NIST.SP.800-37r2.

[8] Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection, *Official Journal* L 345, 23 December 2008, pp. 75–82, http://data.europa.eu/eli/dir/2008/114/oj.

[9] Council Directive 2008/114/EC.

[10] Council Directive 2008/114/EC.

[11] Joint Systems and Analysis Group, “Guide to Capability-Based Planning,” The Technical Cooperation Program, 2004, https://www.hsdl.org/?view&did=461818.

[12] “Universal Task List,” version 2.1. Washington, D.C.: U.S. Department of Homeland Security, 2005.

[13] Sharon L. Caudle, “Homeland Security Capabilities-Based Planning: Lessons from the Defense Community,” *Homeland Security Affairs* 1, no. 2 (2005), www.hsaj.org/articles/178.

[14] Todor Tagarev, “Capabilities-based Planning for Security Sector Transformation,” *Information & Security: An International Journal* 24 (2009): 27-35, https://doi.org/10.11610/isij.2404.

[15] “Capability-Based Planning,” in *The TOGAF® Standard*, Version 9.2, Chapter 28, https://pubs.opengroup.org/architecture/togaf9-doc/m/chap28.html.

[16] Caudle, “Homeland Security Capabilities-Based Planning.”

[17] Dan Shoemaker, Anne Kohnke, and Ken Sigler, *A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce 2.0* (Boca Raton, FL: CRC Press, 2016).

[18] To reflect, among others, climate change and recent sources of disasters such as terrorist acts.

[19] “Integrating the Disaster Risk Management Cycle,” in *Science for DRM 2020: Acting Today, Protecting Tomorrow* (Ispra, Italy: Disaster Risk Management Knowledge Centre, 2020), in press.

[20] ISO/IEC, “Information technology – Security techniques – Information security management systems – Requirements,” ISO/IEC 27001:2013.

[21] Alexander A. Ganin, Phuoc Quach, Mahesh Panwar, Zachary A. Collier, Jeffrey M. Keisler, Dayton Marchese, and Igor Linkov, “Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management,” *Risk Analysis* 40, no. 1 (2020): 183-199.

[22] National Research Council, *Review of the Department of Homeland Security's Approach to Risk Analysis* (Washington, DC: The National Academies Press, 2010), Chapter 5, https://doi.org/10.17226/12972.

[23] For additional considerations, see Chris Simmons, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, Qishi Wu, "AVOIDIT: A Cyber Attack Taxonomy," Technical Report CS-09-003, University of Memphis, August 2009.

[24] *ENISA's Threat Taxonomy*, updated in September 2016, www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view.

[25] See "Common Language Security Incident Taxonomy," www.enisa.europa.eu/topics/csirt-cert-services/community-projects/figure11.png/view (accessed 28 April 2020).

[26] Angelo Corallo, Mariangela Lazoi, and Marianna Lezzi, "Cybersecurity in the Context of Industry 4.0: A Structured Classification of Critical Assets and Business Impacts," *Computers in Industry* 114 (2020): 103165, https://doi.org/10.1016/j.compind.2019.103165.

[27] ISO/IEC 27005:2008.

[28] Maria Bada and Jason R. C. Nurse, "The Social and Psychological Impact of Cyber-Attacks," in *Emerging Cyber Threats and Cognitive Vulnerabilities*, ed. Vladlena Benson and John McAlaney (London: Academic Press, 2020), 73-92.

[29] ISO 31000:2009.

[30] Michel Rademaker, "National Security Strategy of the Netherlands: An Innovative Approach," *Information & Security: An International Journal* 23, no. 1 (2009): 51-61, https://doi.org/10.11610/isij.2305.

[31] ISO/IEC 27005:2008.

[32] ISO/IEC 27005:2008.

[33] Zeinab Amin, "A Practical Road Map for Assessing Cyber Risk," *Journal of Risk Research* 22, no. 1 (2019): 32-43, https://doi.org/10.1080/13669877.2017.1351467.

[34] ISO 27005 emphasises "risk transfer" to another party, e.g. by insurance.

[35] Humza Naseer, *A Framework of Dynamic Cybersecurity Incident Response to Improve Incident Response Agility*, PhD Dissertation (Melbourne: School of Computing and Information System, The University of Melbourne, October 2018).

[36] George Sharkov, "From Cybersecurity to Collaborative Resiliency," 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense (SafeConfig'16), 2016, pp. 3-9, https://doi.org/10.1145/2994475.2994484.

[37] Benjamin Gittins and Ronald Kelson, "Input to the Commission on Enhancing National Cybersecurity," September 16, 2016, https://www.nist.gov/system/files/documents/2016/09/16/synaptic_rfi_advances-idmckm.pdf.

[38] Sessika Siregar and Kuo-Chung Chang, "Cybersecurity Agility: Antecedents and Effects on Security Incident Management Effectiveness," *23rd Pacific Asia Conference on Information Systems (PACIS 2019)*, China, July 8-12, 2019, www.pacis2019.org/wd/Submissions/PACIS2019_paper_307.pdf.

[39] Phil Lester and Sean Moore, "Responding to the Cyber Threat: A UK Military Perspective," *Connections: The Quarterly Journal* 19, no. 1 (Winter 2020): 39-44, https://doi.org/10.11610/Connections.19.1.04.

[40] Lester and Moore, "Responding to the Cyber Threat."

[41] Ludwig Leinhos, "Cyber Defence in Germany: Challenges and the Way Forward for the Bundeswehr," *Connections: The Quarterly Journal* 19, no. 1 (Winter 2020): 9-19, https://doi.org/10.11610/Connections.19.1.02.

[42] Ryan Black, "WannaCry, NotPetya, and Cyberwarfare's Threat to Healthcare," *Incide Digital Health*, June 11, 2018, https://www.idigitalhealth.com/news/wannacry-notpetya-and-cyberwarfares-threat-to-healthcare.

[43] Sri Nikhil Gupta Gourisetti, Michael Mylrea, and Hirak Patangia, "Cybersecurity Vulnerability Mitigation Framework through Empirical Paradigm: Enhanced Prioritized Gap Analysis," *Future Generation Computer Systems* 105 (2020): 410-431, https://doi.org/10.1016/j.future.2019.12.018.

[44] "Integrating the Disaster Risk Management Cycle," in *Science for DRM 2020*.

[45] MingJian Tang, Mamoun Alazab, Yuxiu Luo, and Matthew Donlon, "Disclosure of Cyber Security Vulnerabilities: Time Series Modelling," *International Journal of Electronic Security and Digital Forensics* 10, no. 3 (2018): 255-275, https://doi.org/10.1504/IJESDF.2018.093018.

[46] Petar Radanliev, David De Roure, Max van Kleek, and Stacy Cannady, "Artificial Intelligence and Cyber Risk Super-forecasting," pre-print, https://doi.org/10.13140/RG.2.2.34704.56322.

[47] Miao Yu, Jianwei Zhuge, Ming Cao, Zhiwei Shi, and Lin Jiang, "A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices," *Future Internet* 12, no. 2 (2020), article 27, https://doi.org/10.3390/fi12020027.

[48] Andrea Ceccarelli, Tommaso Zoppi, Alexandr Vasenev, Marco Mori, Dan Ionita, Lorena Montoya, and Andrea Bondavalli, "Threat Analysis in Systems-of-Systems: An Emergence-Oriented Approach," *ACM Transactions on Cyber-Physical Systems* 3, no. 2 (2018), article 18, https://doi.org/10.1145/3234513.

[49] Charia Griffy-Brown, Howard Miller, Vincent Zhao, Demetrios Lazarikos, and Mark Chun, "Making Better Risk Decisions in a New Technological Environment," *IEEE Engineering Management Review* 48, no. 1 (2020): 77-84, http://doi.org/10.1109/EMR.2020.2969121.

About the Authors

Todor **Tagarev** is a professor in the Institute of Information and Communication Technologies of the Bulgarian Academy of Sciences and Head of its Centre for Security and Defence Management. An engineer by education, Prof. Tagarev combines governmental experience with sound theoretical knowledge and background in cybernetics, complexity, and security studies – a capacity effectively implemented in numerous national and international multidisciplinary studies. https://orcid.org/0000-0003-4424-0201

Salvatore Marco **Pappalardo** graduated in Computer Engineering from the University of Catania in 2001. He has worked on INFN, INGV, and other companies and, from 2008, at Telespazio S.p.A., contributing to several EU projects in the field of secure IT and software for space programmes and dual-use earth observation (e.g. SICRAL 2G, COSMO-Skymed 2G, OPTSAT3000). He is an expert in distributed and parallel computing, cybersecurity, cross-reality and related applications (mainly in e-Health). Marco is member of the Italian Consortium of Medical Research (CIRM) and currently pursues a PhD degree in cognitive sciences at the University of Messina. Author of more than 20 scientific papers and co-author of the book "Grid Technology for Maximizing Collaborative Decision Management and Support: Advancing Effective Virtual Organisations." He coordinates the VESPA 2.0 project on 5D VR-based cognitive rehabilitation and leads Task 2.2 in the ECHO project developing its Multi-sector Assessment Framework. https://orcid.org/0000-0001-9950-7685.

Nikolai **Stoianov** is Colonel in the Bulgarian Armed Forces, associate professor and deputy director of the Bulgarian Defence Institute. He is also a principal member of the NATO Science and Technology Board and its "Information Systems Technologies" panel. Dr. Stoianov is Scientific and Technical Management Coordinator of the ECHO project and leads its largest work package on "Multi-sector needs analysis." https://orcid.org/0000-0002-4953-4172.