Postprint of: Leszczyna R., Review of Cybersecurity Assessment Methods: Applicability Perspective, COMPUTERS & SECURITY (2021), DOI: 10.1016/j.cose.2021.102376

Review of Cybersecurity Assessment Methods: Applicability Perspective

Rafał Leszczyna*

Gdańsk University of Technology, Faculty of Management and Economics, Narutowicza 11/12, 80-952 Gdańsk, Poland
e-mail: rle@zie.pg.gda.pl

Abstract

Cybersecurity assessments are crucial in building the assurance that vital cyberassets are effectively protected from threats. Multiple assessment methods have been proposed during the decades of the cybersecurity field. However, a systematic literature search described in this paper reveals that their reviews are practically missing. Thus, the primary objective of this research was to fulfil this gap by comprehensively identifying and analysing cybersecurity assessment methods described in the scientific literature. A structured research method and transparent criteria were applied for this purpose. As a result, thirty-two methods are presented in this paper. Particular attention is paid to the question of the methods' applicability in realistic contexts and environments. In that regard, the challenges and limitations associated with the methods' application as well as potential approaches to addressing them have been indicated. Besides, the paper systematises the terminology and indicates complementary studies which can be helpful during assessments. Finally, the areas that leave space for improvement and directions for further research and development are indicated. The intention is to support researchers and practitioners in choosing the method to be applied in their assessments and to indicate the areas that can be further explored.

Keywords: cybersecurity, assessment, methods, applicability, usability, management, computer security, information security, risk assessment, organisational management, business management

1. Introduction

With growing cybersecurity challenges to organisations and individuals resulting, among the others, from the growing number and sophistication of threats [8, 110, 143, 34, 29, 57] including the advent of AI-based cyberthreats [63] or rapidly evolving malicious software [12], increases the importance of cybersecurity assessments. A security assessment is a process of determining the present cybersecurity posture of an information system [31, 107, 112] and evaluating the fulfilment of security objectives [116]. If performed methodologically, it assures that critical cyberassets are protected from threats [8, 63, 86] and that the underlying communication infrastructure will not induce failures or facilitate intrusions by malicious agents. It also supports developing the comprehension of the impact of cyberattacks [43]. Lack of cybersecurity evaluation prevents new technologies from being deployed into their target fields [40, 20]. Besides, regular performance of cybersecurity assessments is becoming increasingly required by governments and industry regulators, what in particular regards critical sectors [3, 2, 101, 100]. As a result, organisations seek effective and applicable cybersecurity assessment methods.

Throughout the years of the development of the cybersecurity domain multiple assessment techniques have been proposed. However, as this study reveals (see Section 3.5), their reviews are practically missing. During a thorough literature search process, only two systematic reviews dedicated to cybersecurity assessment methods have been identified. Yet they have a very specific scope (artificial intelligence approaches applied to vulnerability assessments and the standards for security assessments in the electricity sector) [65, 77] or the low level of descriptions' detail [118].

In consequence, practitioners or researchers willing to choose a security assessment method in a systematic manner, based on clear criteria would not find proper support in the literature. This formed an important gap that needed to be addressed. The main objective of the research described in this paper was to comprehensively identify cybersecurity assessment methods presented in the scientific literature, using a structured process and evident selection and evaluation criteria. Special attention was devoted to the aspect of applicability of the methods i.e. the quality of being applicable or fit to be applied [78]. Applicability is higher if a method is well-documented, accompanied by supporting tools, well-tested, easy-to-learn, and preferably has been already applied in other contexts [78]. Thus, the evaluation criteria utilised in the research reflect these properties and include, for instance, the documentation level of detail, required skills or supporting tools. The intention was to provide the readers with indications on the feasibility of a method's application and the associated effort. At the same time, the primary research questions posed for this study regarded the number of available security assessment methods, the fraction of methods that could be directly applied by the industry, methods' characteristics and limitations, challenges related to the application of the methods and potential ways of addressing them. The anal-

*Corresponding author

ysis of the methods based on the predefined evaluation criteria enabled responding to these questions.

The main contributions of the research are:

- 32 cybersecurity assessment methods were identified in a structured manner by applying the research method derived from the Webster and Watson's [135] as well as Kitchenham and Brereton's [69] approaches.
- The methods were analysed and compared based on transparent evaluation criteria and classified into five categories that reflect the most common types of cybersecurity assessment techniques.
- Complementary studies that can be useful during cybersecurity assessments that concern metrics, models, tools etc. were identified.
- Conceptual ambiguities that arose during the development of the cybersecurity domain were resolved by introducing a consistent conceptual framework.

The rest of the article is organised as follows. In the next section, the fundamental concepts associated with cybersecurity assessments are introduced and terminology ambiguities are resolved by introducing a coherent conceptual framework. In Section 3 related works i.e. the existing studies that aim at reviewing cybersecurity assessment methods are discussed. The research method applied in the study is explained in Section 4. Section 5 is devoted to the presentation of the core results of the study i.e. the 32 cybersecurity assessment methods documented in the scientific literature. Complementary proposals related to cybersecurity assessments that exhibit significant usefulness are indicated in Section 6. Finally, the main findings of the research are described in Section 7. Based on them, the improvement areas and potential further actions could be determined (see Section 8). The paper ends with concluding remarks.

2. Concepts, definitions

To provide a clear view of the notions related to cybersecurity assessments, a conceptual framework presented in Figure 1 has been introduced. This section explains the relevant concepts that are presented in the diagram, starting from the resolution of conceptual ambiguities that arose during the development of the cybersecurity domain.

2.1. Cybersecurity assessment and risk assessment

Cybersecurity assessment aims at determining the cybersecurity state of an assessed entity (*an assessment object*) [31, 107, 112]. It answers the question of how effectively the entity fulfils specific security objectives [116]. It is a cyclic process of confronting assets with their cybersecurity requirements, taking into account potential risks, threat consequences and related costs [58]. With protection measures established in the system, the cybersecurity assessment aims at evaluating correct implementation and operation of the controls as well as their adequateness and effectiveness in regard to satisfying security requirements for the system [96, 23, 121].

Risk assessment is the process devoted to the identification, analysis and evaluation of cybersecurity risks [62, 134, 99, 98]. *Risk* can be defined as a two-dimensional combination of events and consequences (of an activity) and associated uncertainties[1] [13]. Risk assessment results in the compilation of prioritised cybersecurity risks that may affect an organisation or its environment [99]. During *risk identification*, risks are being searched for, recognised and described, including the identification and description of risk events their sources and causes as well as potential consequences [60]. *Risk analysis* aims at developing an understanding of the nature of the risks and determining the risk level. During *risk evaluation*, the results of risk analysis are referred to risk criteria to determine which risks are acceptable of tolerable [60]. Risk assessment is an essential part of *risk management* – a compound activity that among the others incorporates also the treatment of the assessed risks [99].

It is evident that security assessment and risk assessment, while not completely disjoint, are two different tasks. Security assessment aims at recognising the level of protection of the system from threats, while risk assessment indicates what are the threats and the associated events, consequences, uncertainties and expectations [52]. While it is not their primary focus, cybersecurity assessments may help in identifying cybersecurity risks [31]. At the same time, risks identified and analysed during risk assessment often serve for planning security assessment activities [37].

2.2. Cybersecurity assessment method types

In general, cybersecurity assessment methods are based on testing, examination or interviewing [116, 23, 54]. *Testing* regards exercising an assessed system or a component in a defined environment. It can be passive or active [116]. *Passive cybersecurity testing* does not involve any direct interaction with the assessment object, while *active cybersecurity testing* enables the interactions to stimulate and evaluate system reactions [116]. *Examination* is related to analysing, observing, checking, inspecting, reviewing or checking the assessed object. *Interviewing* involves oral, questionnaire-driven or technologically aided discussions with individuals or groups of the characteristics of the assessed object [116]. The most common types of cybersecurity assessment include checklist-based evaluation, compliance checking, vulnerability identification and analysis, penetration testing, simulation or emulation-based testing, formal analysis and reviews.

2.2.1. Checklist-based evaluation, compliance checking

Checklist-based evaluation utilises a list of activities, functions or properties to structure the assessment process. The elements are subsequently taken from the list and the security state

[1] Multiple definitions of the *risk* concept exist in the literature, some of them based on probability, uncertainty or expected values, other centring around vulnerabilities or focused on impact [51, 13]. A comprehensive discussion of these concepts and the associated development processes is presented by Terje Aven [13].

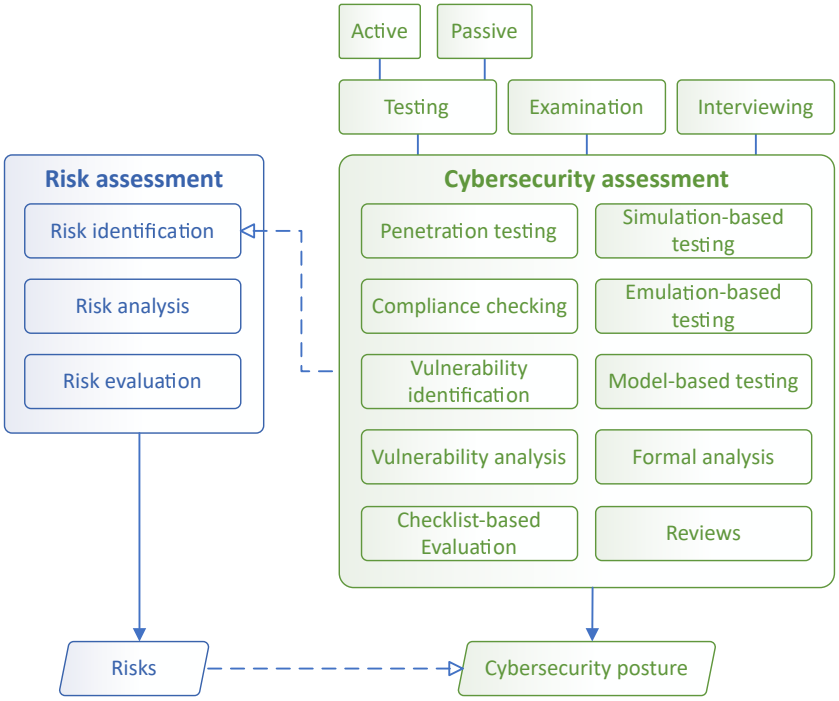

Figure 1: Cybersecurity assessment conceptual framework. The notion of cybersecurity assessment and risk assessment needs to be clearly distinguished. Solid line arrows depict cause-result relationship. Dashed arrows indicate that a source component may (optionally) provide an input to the destination one. Solid lines represent categorisations.

of the evaluated system is confronted with them [144]. *Compliance checking* can be perceived as a special case of checklist-based evaluation. It determines if assessment objects are in agreement with the defined cybersecurity objectives, requirements or assumptions. Usually, compliance checking is performed in reference to specifications defined in standards or regulations [23, 20, 131, 54, 61].

2.2.2. *Vulnerability identification and analysis*

Vulnerability identification aims at recognising flaws in the assessed entity that can result in a cyberincident. Vulnerability identification techniques include network discovery, port scanning, vulnerability scanning, wireless scanning, and application security examination. This task is usually strongly supported with automated tools which, for instance, can search a communication system for a list of predefined vulnerabilities [23, 28, 116]. *Vulnerability analysis* (*vulnerability validation* [116]) embraces manual or automated exploring of identified vulnerabilities to confirm their existence and to elaborate further on the consequences of their exploitation. Utilised techniques include password cracking, penetration testing, social engineering and application security testing [116].

2.2.3. *Penetration testing*

Penetration testing employs analogous techniques and approaches as malicious intruders do [31, 50, 103], but is performed with authorisation of the analysed organisation [103].

2.2.4. *Simulation or emulation-based testing*

Simulation or emulation-based testing utilises simulation and emulation techniques in support of the testing process. The techniques are usually used to model or replicate the context or the environment of the assessment object. However, they can also be used to replicate the assessment object itself e.g. when operating conditions prevent performing experiments on-site [53, 44].

2.2.5. *Model-based testing, formal analysis*

Model-based testing relies on the modelling of the assessed system or component, together with its relevant context [37]. *Formal analysis* additionally restricts this approach only to the models that are strictly mathematical or specified formally to enable manual or automated examinations that resemble proving of mathematical theorems and provide analogous strength of argument [33].

2.2.6. *Reviews*

Reviews involve passive, usually manual, examinations of documentation related to the assessed object. The documentation commonly reviewed during security assessments includes technical specifications, logs, rules and configuration files [116, 61].

3. Related work – the reviews' search

In this section the related work i.e. the existing studies that aim at reviewing cybersecurity assessment methods are presented. To identify the studies in a comprehensive way the

research method described in Section 4 was applied. A combination of keyphrases "security assessment", "review" and "survey" was applied to the search. When possible the results were refined to the computer science and related domains, or to research and review papers. The outcome of the process is summarised in Table 1. Two reviews related to different areas of cybersecurity assessment (methods, standards and tools) and two reviews that combine risk and security assessment methods, as well as 13 overviews that present mixed selections of cybersecurity assessment tools, techniques or approaches have been identified. In this section, these results are described. Also, five notable risk assessment techniques that provided important reference to this study, as far as the research method or criteria are concerned, are briefly presented.

3.1. Cybersecurity assessment methods reviews

Khan and Parkinson [65] review artificial intelligence approaches applied to vulnerability assessments. Solutions based on machine learning, automated planning and expert systems are described. The authors identify knowledge gaps and form recommendations for further research. Although the study focuses on artificial intelligence, a substantial part is devoted to manual, computer-aided and automated vulnerability assessment techniques. This includes the discussion of their drawbacks and associated challenges.

Leszczyna [77] surveyed standards that could be applied to cybersecurity assessments in the modern electricity sector. The study evidenced the lack of a dedicated, sector-specific standard that addresses this topic. At the same time, more than 30 standards related to the field were identified. Among them, seven general-applicability standards that provide comprehensive security assessment guidance (with NIST SP 800-115 standing out [116]). The study was based on a systematic research method and transparent standards' selection and evaluation criteria.

3.2. Reviews and overviews that combine risk and security assessment methods

In the review paper of Quassim et al. [107] both, cybersecurity and risk assessment methods for industrial control systems, are studied. The authors elicit 11 standards and guidelines based on clear selection criteria. Each of the documents is briefly described and evaluated based on the criteria that concern the coverage of cybersecurity management processes (including those unrelated to cybersecurity assessments). Also, Cherdantseva et al. [26] studied both cybersecurity and risk assessment techniques for industrial control systems. The research was based on a systematic approach that employed predefined selection and evaluation criteria and embraced 24 methods. Fabisiak et al. [35] shortly described and compared 8 methods that are more or less-tightly related to cybersecurity management (including risk and security assessments). Although the methods' elicitation procedure has not been described, neither selection criteria, the set of introduced comparison criteria is notable and can be used as a reference. It consists of as much as 35 elements.

3.3. Overviews of cybersecurity assessment tools, techniques and approaches

Overviews are studies that do not aim to be comprehensive. They briefly present certain selections of cybersecurity assessment tools, techniques or general approaches, usually without a justification of the particular choice of solutions. Also, they do not describe a research method for the identification and analysis of the solutions, nor indicate whether such a method was applied.

A comparative study of 20 cybersecurity testing methods based on seven analysis criteria was performed by Shahriar and Zulkernine [118]. The criteria include vulnerability coverage, source of test cases, test generation method or granularity of test cases. Besides, the automation aspect of the methods is investigated. This interesting study locates itself between an overview and a systematic review. It presents a large number of techniques, but a structured method of their identification is not described. The paper would certainly benefit from being updated and presented in a full-length article as the six-pages format of a conference paper allowed solely for demonstration of the criteria and a brief comparative discussion of methods without descriptions of individual assessment methods and their detailed analyses.

Shah and Mehtre [117] provide an overview of vulnerability assessment and penetration testing techniques. After a detailed introduction to the subject area, the authors indicate four frameworks that are commonly adopted worldwide as far as cybersecurity assessments are concerned: Open Source Security Testing Methodology Manual (OSSTMM), Payment Card Industry Data Security Standards (PCI-DSS), Open Web Application Security Project (OWASP) and ISO/IEC 27001. Besides, compilations of several freely available tools for automated static analysis and penetration testing, including RATS, Flawfinder, Metasploit or Nessus are introduced. Also, Coffey et al. [27] present an overview of a selection of vulnerability identification tools for SCADA systems. The tools include Nmap, Zmap, Nessus, Shodan and Passive Vulnerability Scanner (PVS).

Alternatively, a more structured approach is applied by Li et al. [84] who evaluated five open-source vulnerability identification tools, namely ASIDE, ESVD, LAPSE+, SpotBugs and Find Security Bugs (FindSecBugs). This useful study focuses on analysing the effectiveness (the number of detected vulnerabilities, recall, precision, and discrimination rates) and the usability of the applications based on clearly defined metrics and research questions. Analogous research was conducted by Holm at al. [55]. Using a well-specified set of properties and a comparison framework, seven network scanners i.e. AVDS, Patchlink scan, Nessus, NeXpose, QualysGuard, SAINT and McAfee VM were analysed. Also, Lykou et al. [88] analyse cybersecurity assessment tools in a more systematic manner. The tools comprise the Control System Cyber Security Self-Assessment Tool (CS^2SAT), Cyber Security Evaluation Tool (CSET), SCADA Security Assessment Tool (SSAT) and Cyber Resilience Review Self-Assessment Package (CRR). They contain features that make them particularly suitable to the evaluations of industrial control systems and critical infrastructures.

Table 1: Reviews' search summary. Abbreviations: RA – risk assessment, SA – security assessment.

Source	All meta-data	Title	Abstract	Keywords	Manual search	Relevant	RA-related	SA-related	SA-related surveys
ACM DL	120	3	64	1	n.a.	3	2	1	0
Elsevier SD	n.a.	1	32		n.a.	8	3	5	2
Emerald	136	1	50	n.a.	n.a.	2	0	2	1
IEEE Xplore	384	7	143	3	n.a.	4	0	4	1
Springer	2853*	121	n.a.	n.a.	200	3	4	4	1
Wiley	n.a.	0	n.a.	0	n.a.	8	3	8	0
EBSCOhost†	n.a.	6	41	0	n.a.	2	1	1	0
Scopus†	6242	10	92	22	92	4	1	2	0
WoS†	120	7	n.a.	89	n.a.	0	0	0	0
Total	9855	156	422	115	292	34	14	27	5‡

* The search embraced entire document contents but was restricted to computer science domain.
† Search results partially repeated findings from searches in other databases.
‡ Search results included three surveys focused on cybersecurity assessments and two reviews that combined security assessment with risk assessment methods.

In another study dedicated to industrial control systems [54], the authors evaluated tools that support cybersecurity assessments in respect to their compliance to the NERC's cybersecurity requirements that are obligatory for critical infrastructures in the U.S. [97].

The Bertoglio and Zorzo's [31] overview focused on penetration testing, points out the OSSTMM, Information Systems Security Assessment Framework (ISSAF), Penetration Testing Execution Standard (PTES), NIST SP 800-115 guidelines and OWASP. The authors identified 72 tools that support penetration testing. Among them, Acunetix, WebInspect, AppScan, Metasploit, Nessus, NeXpose, Nikto, Nmap, Paros, QualysGuard, WebScarab and Wireshark are indicated as the most common. An overview dedicated to vulnerability assessments in autonomic systems is presented by Barrère et al [16]. A substantial part of the article is devoted to vulnerability description languages such as Common Vulnerabilities and Exposures (CVE), the Intrusion Detection Message Exchange Format (IDMEF) or Open Vulnerability and Assessment Language (OVAL). This is followed by the presentation of several tools for vulnerability identification, modelling and assessment, including Nessus, OpenVAS or SAINT, but also MulVAL, DOVAL and ACML. The paper concludes by demarcating the directions of future research in the field. The overview of Li et al. [85] is focused on model-based security assessments. Several techniques that employ tree structures, graphs and Petri Nets are briefly described.

An overview that concentrates on approach types rather than individual techniques of security assessment is given in [136]. Also, Nath [94] focuses on approaches rather than individual techniques, however, the study is concentrated on vulnerability assessments. The approaches include model-based vulnerability analysis, vulnerability assessments using honeynets or combined black-box and white-box testing.

3.4. Notable reviews of risk assessment techniques

During the search for reviews of cybersecurity assessment methods several studies concentrated exclusively on risk assessment [51, 134, 93, 59, 48] were identified. Although they do not provide information on cybersecurity assessment methods, it is important to note them as they apply systematic research approaches that are worth analysing and following. For instance, Gritzalis et al. [51] applied a structured research method with predefined selection and evaluation criteria to comprehensively evaluate 10 risk assessment methods commonly applied by the industry. Wangen et al. [134] systematically developed a framework for evaluating the completeness of risk assessment methods and applied it to evaluate 11 popular approaches chosen based on transparent selection criteria. An alternative structured study of risk assessment techniques was conducted by Ionita and Hartel [59], who analysed 14 methods, based on transparent inclusion and analysis criteria.

3.5. Reviews' search summary

As has been described earlier in this section, only two systematic reviews dedicated to cybersecurity assessment methods have been identified. These studies aim at the comprehensiveness of results by applying a transparent (described in the paper) research method. However, the scope of the papers was narrowed to artificial intelligence approaches applied to vulnerability assessments [65] or the standards for security assessments in the electricity sector [77].

Overviews, on the other hand, only briefly present mostly small selections of solutions without describing the method of their identification, nor justifying the choice of the particular set of the solutions. Thus, the completeness or comprehensiveness of the studies can not be evaluated. As a result, they do not provide confidence that any important contributions have not been omitted. Besides, a substantial part of the results was related to

tools or risk assessments. The latter, although connected to security assessment should be properly distinguished from it (see Section 2).

It has become evident, that despite the importance of the subject, the studies that would systematically identify, compile and evaluate cybersecurity assessment methods are missing. This finding created the main incentive for performing an extensive and systematic literature analysis that is presented in the reminder of this paper.

4. Research method

This study adopts the guidelines of Webster and Watson's [135] as well as Kitchenham and Brereton [69] on performing systematic literature reviews. The literature was sought primarily in journals and books, in the databases of established publishers that address the topics of information security, communication systems, computer science and similar, namely the ACM Digital Library, Elsevier, Emerald, IEEE Xplore, Springer and Wiley. Then, it was followed by the search in aggregative databases that store records of various publishers – EBSCOhost, Scopus and Web of Science. Additionally, the search was complemented with a short search of conference proceedings and the Internet. When identified papers referred to other relevant papers, also the papers were introduced to the analysis (*backward analysis* [135]).

The key stages of the literature review together with utilised main data sources are presented in Figure 2. In the first stage potential alternative reviews were searched to avoid any duplication of work. The results of the process are described in Section 3. Originally, the study was intended to conclude at that stage, as a substantial amount of results (review studies) that would indicate a potentially complete set of cybersecurity assessment methods was expected. However, the shortage of available reviews and their limitations led to the extension of the study into the autonomous research of cybersecurity assessment domain with respect to method proposals (the methods search). For the research, the results of the reviews' analysis provided a reference for deriving methods' selection and evaluation criteria, building the conceptual framework as well as designing the structure of the study. The particular criteria used in the study are presented further in this section (Subsections 4.1 and 4.2).

Both, the *reviews search* as well as the *methods search* stage comprised three principal components, i.e. the literature search, data analysis and selection data extraction. As far as keywords utilised during the two stages are concerned:

- In the *reviews search* stage, phrases containing the keywords "security assessment", "review" and "survey" were applied.
- During the *literature search*, combinations of the keywords "security", "assessment", "method" and "approach" were utilised.

Several iterations were performed to narrow down the number of results. Depending on the capabilities of the search engines, the initial iterations focused on titles, abstracts, keywords or other metadata. Then, the descriptions of the publications were read (*manual search*), to finally browse the contents of the documents in the concluding iteration (*in-depth analysis*). When possible, the search was restricted to computer science or a cognate domain. In the *literature analysis* stage, the documents were read partially or entirely to identify knowledge about cybersecurity assessment methods and the related concepts.

In the *literature search* stage, selection criteria were applied to excluded irrelevant publications. The most remarkable contents were highlighted and copied to a separate summary document (*data extraction*). The data were grouped according to the *evaluation criteria* and analysed. The criteria are described in the following sections.

4.1. Selection criteria

Selection criteria are used to decide whether a method should be included in the analysis. Based on the criteria utilised in the reviews, overviews and guidelines related to security and risk assessments [107, 26, 69, 54, 118, 51, 134, 59, 37, 36, 48, 93, 35, 117, 16, 136, 84, 55, 88], the following selection criteria were derived:

- English documentation [107],
- the coverage of security assessment processes [26],
- a cybersecurity-related origin [26],
- presence of a security assessment method description [51].

Preferably, the publications should present the following properties:

- detailed descriptions [107],
- the number of citations larger than 5 for publications older than 10 years [134],
- timeliness (of citations) [134] (last 10 years),
- application to an existing system or a system design.

It needs to be emphasised that all cybersecurity risk assessment approaches were excluded.

4.2. Evaluation criteria

Evaluation criteria enable structured analyses of the methods' characteristics and facilitate comparisons. For this research, the criteria that repeated among the analysed studies [107, 26, 69, 54, 118, 51, 134, 59, 37, 36, 48, 93, 35, 117, 16, 136, 84, 55, 88] were adopted in the first place. They regard:

- the aim, purpose or objectives of a method [26, 59, 48, 93],
- the method's focus or scope [59, 48],
- the method's application domain [26, 93, 118],
- the method's coverage of the assessment tasks [59, 26, 107],

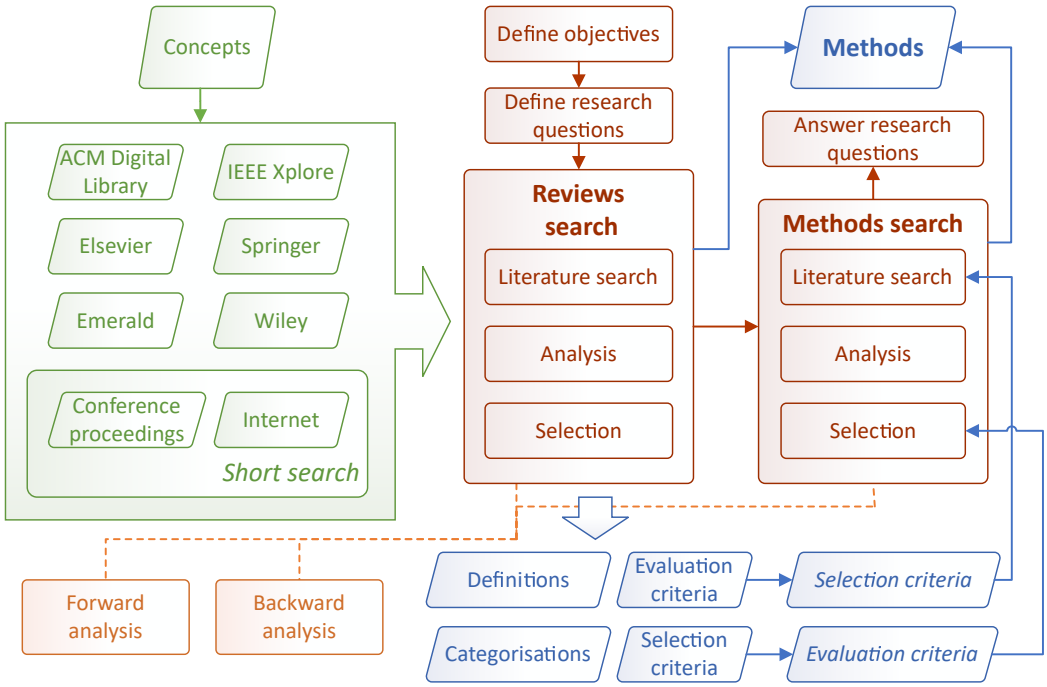

Figure 2: The key tasks and data sources employed during the review process.

- the target users of the method [59, 48],
- and the availability of supporting tools [93, 26, 59].

Additionally, the following criteria were employed in the study:

- release date [59] – the date when the latest version of the method was published or documented,
- real-world application [59] – this attribute indicates whether the method has been practically applied to an existing system or a system design,
- number of citations [134] – the number of references to the method in the scientific literature, preferably in peer-reviewed journals,
- documentation level of detail [107] – depicts completeness of the method's documentation especially in regard to its application. A *high* level of documentation's detail indicates that the method is described comprehensively with details sufficient to enable its application, while *low* level of detail describes overview-type documentation, where descriptions are general. *Moderate* is an intermediate level which denotes, for instance, that the documentation is detailed overall, but certain specifications necessary for the application of the method are missing,
- required skills [59] – proficiency necessary to implementation and usage of the method,
- evaluation procedure [26] – the procedure applied to evaluate the assessment method. Venable et al. [126] distinguish four main types of evaluation that span in two dimensions. As far as the evaluation environment is concerned, *naturalistic* evaluations are performed in real conditions while *artificial* ones are conducted based on a theoretical model. The second dimension concerns the time when the evaluation is performed. *Ex-ante* assessment is performed before instantiation (implementing and using) the analysed method. *Ex-post* evaluation is executed after the instantiation [126, 26].
- form (see Section 2): checklist-based evaluation, compliance checking, vulnerability identification, vulnerability analysis, penetration testing, simulation or emulation-based, testing, model-based testing, formal analysis and a review,
- testing mode [118] – the way in which the testing is conducted: white-box (unit or integration), black-box or hybrid testing.

The criteria can be divided into methods' *purpose*, *applicability* [78] and *structure* indicators. All the criteria are summarised in Table 2.

5. Results of the analysis: security assessment methods

As already mentioned in Section 4, identifying the lack of systematic reviews of cybersecurity assessment methods became the incentive for performing a dedicated literature analysis of individual cybersecurity assessment methods. To achieve the comprehensiveness and transparency of the study, the research method explained in Section 4 was applied. Combinations of the keyphrases "security", "assessment", "method" and "approach" were applied.

Table 2: Method evaluation criteria.

Purpose	Applicability	Structure
Aim	Release date	Form
Scope	Number of citations	Testing mode
Application domain	Documentation level of detail	Coverage of the assessment tasks
Target users	Required skills	
	Real-world application	
	Method's evaluation procedure	
	Supporting tools	

A quantitative summary of the research is demonstrated in Table 3. After the in-depth analysis of 139 publications, more than 40 documents that describe cybersecurity methods (depicted as *relevant* in the table) and over 50 that present complementary proposals such as models or metrics (in the table labelled as *low-relevant*) were identified[2]. 32 cybersecurity assessment methods described in the scientific literature were identified.

In this section, the methods are described and characterised in regard to the evaluation criteria. They are grouped into the key categories described in Section 2. It does not mean, however, that the methods unequivocally fall into each category. As the majority of the tools take advantage of several concepts and approaches, the leading, primary concept or approach component served as a reference for categorisation. Within each category, more generic methods are presented in the first order, followed by other techniques that pertain to specific fields.

During the literature analysis, a considerable set of supplementary proposals that can prove useful during assessments were identified. These solutions address specific aspects of the evaluations rather than defining a compound analysis methodology, including models, metrics or training. The studies are characterised in Section 6.

5.1. Checklist-based evaluation, compliance checking

You et al. [144] proposed a checklist-based evaluation procedure that emphasises cybersecurity controls' elicitation phase to obtain the set of checklist items that are best tailored to the application field and the organisations' business context. There, reference controls mostly adapted from cybersecurity standards and guidelines such as ISO/IEC 27001 or NIST SP 800-53 are refined to reflect the destination environment and classified into mandatory, significant or recommended. The classification is based on the existing legislation and the calculation of correlation coefficients for each control. An experimental study of the method was performed in the context of 15 thermal power plants in South Korea.

Qiangmin et al. [108] support checklist-based assessments where the checklist is formed from an information system security tree model that contains various attributes related to cybersecurity such as access control policy, user registration or user password management. The authors proposed a method to reduce the number of attributes in the model.

The method of Vogel and Broer [131] encompasses the real-time component which results from the identification of gaps in business-applied security monitoring practices based on the survey of several organisations' management representatives. According to the analysis, implemented procedures lack (near) real-time discovery of non-compliance, continuous compliance monitoring or accurate status information. These findings were transformed into requirements for the developed method. In effect, the Security Compliance Monitoring (SCM) approach focuses on timely correlation and analysis of security data provided by various sources, enhancing it with business context information and reporting which enables efficient decision-making. A case study related to the telecommunication industry is briefly introduced.

Buccafurri et al. [20] propose a method that structures the process of compliance assessment dividing it between support and core activities. The supportive actions are related to the identification of cybersecurity concerns and preparation and maintenance of the list of standards. The core actions regard a detailed analysis of the assessment object, selection of relevant security concerns, standards and protective measures and the evaluation of the obtained compliance level. The organised approach supported with the utilisation of predefined templates aims at facilitating analyses of complex systems. As an illustration, an application of the method to the assessment of an Italian postal service provider is described.

Williams [138] adapted Capability Maturity Model [104, 15] to evaluations of cybersecurity capacities in medical environments. In comparison to the original CMM, which adheres to a long-term perspective of capabilities' maturing processes [138], the adapted version is more operational-timespan oriented. Cybersecurity areas specified in the ISO/IEC 27001 predecessor i.e. ISO/IEC 17799 were applied to measure maturity levels. In the presented example of applying the method to the evaluation of a backup-service, in-depth interviews were utilised as a source of evidence.

Khattak et al. [66] developed a security assessment framework for Internet banking services based on a proposed taxonomy of 93 domain-specific security requirements classified into nine categories. The taxonomy was derived from the existing Pakistani security regulations and worldwide good practices. The framework was applied to analyse the cybersecurity of 21 banks that provide Internet banking services in Pakistan.

[2] It must be noted that the search results in the EBSCOhost, Scopus and Web of Science databases mostly pointed to the same documents as the searches the individual publishers' databases.

Table 3: The summary of the search for the literature on cybersecurity assessment methods.

Source	All metadata	Title	Abstract	Keywords	Manual search	In-depth analysis	Relevant	Low-relevant
ACM DL	1780	181	975	101	181	40	12	14
Elsevier SD	n.a.	49	1867		49	4	0	3
Emerald	32000	2	215	n.a.	215	5	1	0
IEEE Xplore	4554	178	2255	47	178	21	4	8
Springer	599560*	0	n.a.	n.a.	500	41	13	14
Wiley	n.a.	17	n.a.	24	41	1	0	0
EBSCOhost†	n.a.	152	4820	139	291	6	1	3
Scopus†	275860	490	10371	3267	490	16	8	8
WoS†	11875	311	n.a.	9090	311	5	3	2
Total	925629	1380	20503	12668	2256	139	42	52

* The search embraced entire document contents but was restricted to computer science domain.
† Search results partially repeated findings from searches in other databases.

Internet resources served as a main indicated input for the evaluation. As far as the applicability of the proposal is concerned, the framework was applied by its authors to obtain the security picture of the analysed banks and to derive recommendations for banks, customers and the State Bank of Pakistan. No indications have been provided regarding other potential users of the framework. Also, although multiple descriptions of questions pertaining to the evaluation checklist are provided, the lack of complete documentation of the list prevents its direct application by other stakeholders.

The two latter studies [138, 66] drive into the direction of sectoral security assessments, where multiple organisations pertaining to a specific sector are evaluated and benchmarked. Such analysis can be conducted on various levels of detail, but due to practical considerations, usually more general exercises are performed. On a high level, the sectoral assessment may take the form of a survey conducted in reference to a specifically designed compliance checklist or a list of requirements. In that regard, Szczepaniuk et al. [122] assessed the security of 50 public administration agencies. The implementation-level of information security management systems and compliance with regulations in force and the ISO 27001 standard were evaluated. Based on the assessment, recommendations for increasing the level of information security in the public administration were derived. For a broader application of the assessment approach, providing the questionnaire used in the research and describing it in more detail is indispensable.

Cayetano et al. [22] focus on the important subject of cybersecurity in the supply chain that requires special attention nowadays [89]. The authors propose the development of specialised checklists which comprise sector-specific cybersecurity characteristics obtained through surveys and interviews with field experts as well as sectoral standards and guidelines. While positive responses to the checklist questions confirm cybersecurity compliance, lack of addressing a particular item indicates a vulnerability. Rule-based creation of cybersecurity action plans to mitigate the vulnerabilities is introduced. Also, the authors promote the development of sectoral repositories of common vulnerabilities based on the assessments of multiple representatives. The approach was applied to the assessments of four semiconductor manufacturers in China and Korea.

A comparison of the methods in reference to the evaluation criteria is presented in Table 4.

5.2. Vulnerability identification and analysis

Großmann and Seehusen [52] describe a methodology that consolidates security assessments with risk assessments based on ISO 31000 and ISO/IEC/IEEE 29119 standards. In the risk-based security testing, security evaluation experiments are selected, performed and analysed on the outcome of risk assessments, while in test-based risk assessments, the testing enables identification of threats and vulnerabilities, including the associated risk likelihoods. Evaluation of the method by case studies of banking, e-Health and software development scenarios performed during the RASEN European project is mentioned.

The framework of Großmann and Seehusen [52] was followed up by Viehmann and Werner [128]. To facilitate application of the integrated risk-security assessment method, a software platform called RACOMAT was developed. The toolkit enables semi-automated evaluations that comprise graph-based system analysis and modelling, tests' preparation and execution as well as results' analysis and processing. Additionally, the approach emphasises the creation of generalised, high-level views on the cybersecurity situation in an organisation to support their comprehension and decision-making. The method is described in the context of a case study based on a remote ICT infrastructure administration system.

Chen et al. [24] proposed an analytical framework that integrates modelling of security objectives, entity and attack graphs into a Goal, System and Attacker graph (GSA-graph). Workflows are employed to derive structures that represent transposition of security objectives onto enterprise processes. Based on the resulting GSA-graph a quantitative argumentation that regards the security state of the system can be delivered, assuming that (mostly statistical) evidence is delivered to the graph nodes. Such evidence includes, for instance, statistical data about the availability of specific components or probabilities of different attack scenarios.

An automated framework was proposed by Wang et al. [133]. The system takes advantage of the National Vulnerability Database

Table 4: Checklist-based evaluation or compliance checking methods. Supporting tools – not indicated, testing mode – not applicable. Abbreviations: Cit. – number of citations (Scopus), Det. – documentation level of detail: L – low, M – moderate, H – high, Application - real-world application, Evaluation – methods' evaluation procedure, Coverage – coverage of assessment tasks.

	Method	Purpose			Applicability						Structure
		Aim, scope	App. domain	Target users	Rel. date	Cit.	Det.	Required skills	Application	Evaluation	Coverage
1.	Advanced security measurement tailored to the organisation's business profile [144]	Checklist-based accurate measurement of security	General	Cybersecurity officers	2016	4	L	Mathematical familiarity	N. a.	Simulation	System security level evaluation
2.	Rough set-based security assessment method [108]	A minimal set of attributes in the security assessment reference model	General	N. a.	2007	2	M	Mathematical	21 universities	Case study	System security level evaluation
3.	Security compliance monitoring [131]	Tool-based correlation and analysis of security information from various sources, enriching results with business context information, visual support for decision-making	Business	Decisive personnel	2013	N. a.	L	Basic cybersecurity knowledge in the business domain	N. a.	Case study	System security level evaluation, non-compliance discovery
4.	Analytical processing approach to supporting cybersecurity compliance assessment [20]	Design-stage and operational compliance assessment of complex services supported by (semi-)automated tools	Services	Compliance analysts	2015	3	M	Cybersecurity knowledge	N. a.	Case study	System analysis, tests preparation, vulnerability identification and analysis
5.	Operational framework for security capability assessment [138]	Operational security capability assessment based on CMM	Healthcare	N. a.	2008	24	M	Cybersecurity knowledge	N. a.	Case study	System security level evaluation
6.	Security assessment approach for Internet banking services [66]	Computationally secure and intelligent framework for security assessment of Internet banking services	Banking	Not specified	2020	1	M	Cybersecurity knowledge	21 Pakistani banks	Case study	System security level evaluation
7.	Information security assessment in public administration [122]	Assessing information security management in public administration agencies	Public administration	Not specified	2020	5	L	Basic cybersecurity knowledge	50 public administration agencies	Case study	System security level evaluation
8.	Cyber-physical IT vulnerability assessment for semiconductor companies [22]	Vulnerability analysis of policy, procedures and controls of semiconductor companies in the manufacturer's supply chain	Semiconductor companies	IT security, audit and data centre teams	2018	0	M	Cybersecurity knowledge	4 manufacturers in China and Korea	Case studies	Vulnerability identification

(NVD) and a proprietary, OVAL-based vulnerability scanner to produce an attack graph. The graph is then extended into a Bayesian Attack Graph using probability values derived from CVSS scores. Three metrics adapted from Fault Tree Analysis (FTA), namely the Unreliability of the Top Event, Criticality of Bottom Events and The Most Critical System Component are utilised to analyse the tree and obtain the final assessment figures. The complexity of the method is polynomial at the attack graph generation stage, but the graph analyses and calculation of the metrics demonstrate exponential dependencies. The authors mention a practical application of the framework to a 15-hosts laboratory setting but the description lacks details.

The proposal of Kotenko et al. [71] lies on the border between security assessments and situational awareness. The techniques utilised in the approach, based on attack graphs, cybersecurity metrics and ontologies are commonly used in cybersecurity assessments. However, they were adapted to enable real-time calculations and integrated with typical operational components i.e. Security Information and Event Management (SIEM) systems, intrusion detection systems or anti-malware suites. Moreover, the assessment results are intended to support the fast selection of reactive attack countermeasures. Although the authors mention experimental evaluation of the framework, the description would benefit from additional details, regarding, for instance, the technical implementation of the prototype and the model.

Also the study of Yang et al. [142] aims at integrating situation awareness with security assessment which itself is a very interesting idea that should be more broadly explored. In the approach, deep learning is applied to assess the security situation in terms of attack probabilities and impacts based on collected traffic information. As far as the implementation side is concerned, the paper focuses on the attack detection part of the architecture. The proposal's evaluation centres around compar-

ing its classification capabilities with four deep learning-based intrusion detection systems. The NSL-KDD dataset is used for that purpose. The description of the assessment part of the architecture is mostly theoretical.

Kupsch et al. [73] proposed a security assessment approach for clouds and grid computing systems. The First Principles Vulnerabilities Assessment (FPVA) starts with the identification and analysis of the most critical system components and the interactions between them. The steps result in a set of diagrams that represent the analysed system. Subsequently, the code of the most critical assets is analysed manually. The approach was applied to 7 grid computing systems including Condor workload management system, Storage Resource Broker or MyProxy and compared to two commercial automated code analysis tools. According to the authors, their proposal proves higher effectiveness, especially concerning the number of detected vulnerabilities as well as reported false positives.

Barrère et al. [17] developed Ovaldroid – an automated framework for periodic cybersecurity assessments in mobile environments. To adjust the computations to the limited resources of mobile devices, the authors proposed a probabilistic approach in which instead of executing the entire batch of tests in each tests' cycle, a selection of tests is performed, based on calculated test utilities and a specified threshold. Experiments conducted with a prototype toolkit proved the feasibility of the approach and its resource-saving capabilities. The system was developed using Java, MySQL and OVAL.

Another automated framework, dedicated to cyber-physical systems, was proposed by Potteiger et al. [106]. Ruckus comprises three key modules: firmware discovery, vulnerability discovery and correlation that are interconnected by a common database storage interface. Firmware discovery integrates manual activities based on reverse engineering with automated searching of Internet sources. Proposed vulnerability discovery process consists of binary analysis, symbolic execution and fuzzing. An implementation of the architecture that to a large extent takes advantage of open source software is described. Also, a case study of analysing automotive firmware with Ruckus is presented.

A comparison of the methods in reference to the evaluation criteria is presented in Table 5.

5.3. Penetration testing

Rennoch et al. [111] present results from the European project – DIAMONDS. A risk-based testing approach is proposed where test preparation stages, namely the tests' planning and selection, are driven by the results of independent risk evaluations. In this way, the testing is focused on the most critical system components and threats, with well-adjusted testing scenarios and techniques. The described approach heavily depends on the tools developed during the project. 12 mostly proprietary, internal applications for test modelling, generation, execution, analysis and monitoring, such as CORAS, FUZZINO or KameleonFuzz are indicated. Among them, CORAS is publicly available on an open-source sharing platform. A case study of assessing the security of a banknote processing system is presented. Also, standardisation efforts associated with contributing to the European Telecommunication Standardization Institute (ETSI) activities are described.

While the study of Ghosh et al. [46] centres around a toolkit called NetSecuritas, the introduced method is built upon the framework that embraces fundamental cybersecurity assessment stages, namely the system analysis, threat identification, vulnerability identification and analysis as well as attack graph generation. Based on automated penetration testing and vulnerability analysis a system model is created. This model is confronted with a database of threats to obtain the overall cybersecurity picture visualised in the form of an exploit dependency graph.

Caselli and Kargl [21] promote a standardised method for cybersecurity assessments of critical infrastructures. Their proposal derives from earlier achievements in the domain and prescribes a new structure of the component tasks rather than a completely new evaluation process. To develop the method, four common, practically applied techniques, namely OSSTMM, NIST SP 800-115, ISSAF and NESCOR were analysed. Also, the authors surveyed industry representatives and academic experts to obtain their views on cybersecurity assessments, including challenges, expectations and employed practices. As a result, penetration testing-based evaluations composed of general and practical analyses as well as pre-assessment and post-assessment phases was proposed. In the paper, solely an overview of the approach is presented, with a reference to the deliverables of the European research project CRISALIS for further details. However, currently, the referenced resources are unavailable.

Although the method of Brandstetter et al. [19] might indicate a component-orientation, the components are understood more broadly here and include compound systems such as control centres for energy production or delivery. The approach, originated in the industry (Siemens) emphasises practical applicability (pragmatism), cost-efficiency and connection to industry standards. It consists of three interdependent stages, namely the risk assessment, theoretical assessment and practical assessment, supported with pre- and post- assessment activities. Risk assessments take advantage of collective expert knowledge from various domains related to system manufacturing including product development, system testing, maintenance, sales and marketing and product management obtained during interviews and workshops. During theoretical assessments, compliance checklists are derived from relevant standards and subject to experts' assessment. Practical criteria were introduced to evaluate the standards. They regard the authorship (industry bodies, customers or operators, regulatory bodies, international standardisation bodies), type of publication (technical or management), focus (industry-specific or general IT security) and life cycle stage (development or operation). Assessments utilise penetration and other tests to further explore critical areas identified during the complementary stages. The approach follows the security by design philosophy i.e. the assessments are mostly conducted in the system design and development phases.

Permann and Rohde [105] describe a practical approach to assessing cybersecurity of SCADA systems derived from experiences with testing vendor systems. The method comprises standard elements, namely the tests' planning, preparation of

Table 5: Vulnerability identification and analysis methods. Target users – not indicated. Abbreviations: App. domain – application domain, Rel. date – Release date, Cit. – number of citations (Scopus), Det. – documentation level of detail: L – low, M – moderate, H – high, App. – real-world application, Eval. – methods' evaluation procedure, Mode – testing mode, Coverage – coverage of assessment tasks.

	Method	Purpose		Applicability							Structure	
		Aim, scope	App. domain	Rel. date	Cit.	Det.	Required skills	App.	Eval.	Supporting tools	Mode	Coverage
1.	Integration of cybersecurity assessments with risk assessments [52]	Standards-based integration of cybersecurity assessments with risk assessments	General	2015	3	M	Penetration testing and technical	N. a.	Case studies	N. a.	N. a.	System modelling and analysis, tests preparation, vulnerability identification and analysis
2.	Risk Assessment COMbined with Automated Testing (RACOMAT) [128]	A tool-supported, semi-automated consolidated security and risk assessments	General	2015	1	M	Intermediate technical	N. a.	Case study	ARIS, RACOMAT	N. a.	System modelling and analysis, tests preparation, vulnerability identification and analysis
3.	Work flow-oriented security assessment [24]	Automated quantitative assessment based on information in various formats	General	2013	11	M	Technical, mathematical	N. a.	Case study	Protype developed in Python	N. a.	Modelling of security objectives, system and attacker
4.	Bayesian attack graph-based quantitative assessment [133]	Automated assessment with quantitative metrics	General	2011	7	M	Intermediate technical	N. a.	Experiments with prototype, theoretical	Mentioned, but no details	Black-box	System analysis, vulnerability identification and analysis
5.	AI and Metrics-Based Vulnerability-Centric Cyber Security Assessment [71]	Automated, real-time cybersecurity assessments that enable reactive selection of attack countermeasures	General	2018	N. a.	L	Intermediate technical	N. a.	Prototype-based lab experiments	N. a.	N. a.	System analysis, vulnerability identification and analysis
6.	Network security situation assessment method based on deep learning [142]	Automated, real-time attack detection and security situation assessment	General	2021	0	L	Technical, mathematical	N. a.	Comparison to 4 attack detection methods	N. a.	N. a.	Vulnerability identification and analysis
7.	First principles vulnerabilities assessment [73]	Vulnerability analysis of critical system components	Cloud and grid computing	2010	11	L	Technical	7 grid systems	Comparative	N. a.	White-box	System analysis, vulnerability identification and analysis
8.	Ovaldroid [17]	Non-invasive, lightweight and effective security solutions able to efficiently increase vulnerability detection capabilities in mobile environments	Mobile environments	2013	3	H	Intermediate technical	N. a.	Experiments with prototype	A prototype	White-box	System analysis, vulnerability identification and analysis
9.	Ruckus [106]	Autonomous identification and analysis of firmware and vulnerabilities	Cyber-physical systems	2020	0	M	Intermediate technical	N. a.	Case study	Open-source software and proprietary solutions	White box, black box	Vulnerability identification and analysis

the testing environment, tests' execution as well as results' analysis and reporting. As far as the form of assessments is concerned, the authors opt for penetration testing. It should be performed in a safe environment detached from the evaluated one, but reconstructing it accurately. Original hardware and software components can be applied for this purpose, but also simulation or emulation. Several tools that support the assessments of SCADA systems i.e. Nmap, Nessus, STAT Scanner, Ethereal, Ettercap and Metasploit, but also debuggers, fuzzers, disassemblers or code analysers are indicated. Besides, practi-

cal recommendations regarding the performance of the assessments are presented.

A comparison of the methods in reference to the evaluation criteria is presented in Table 6.

5.4. Simulation or emulation-based testing

Leszczyna et al. [81, 90, 80] introduced a cybersecurity assessment method for critical infrastructures that is particularly suitable to the facilities that rely on continuous operation of the underlying information infrastructure (e.g. process control systems in nuclear power plants). To prevent from undesired consequences of interactions with the evaluated system, testing is performed off-site in a specifically prepared laboratory equipped with hardware devices and software necessary to reproduce the system, as well as auxiliary components that support the performance of experiments. To achieve high accuracy of the system reproduction, an emulation-based technique with simulations are combined. A mobile agents-based tool for simulation of malware called MAlSim [82, 79] was developed to support the assessments, while visual representations of analysed elements and automatic explorations of generated graphs are enabled by a proprietary toolkit called InSAW (Industrial Security Assessment Workbench) [38, 92, 39]. The method was applied to cybersecurity evaluations of several electric power facilities [81, 90].

An alternative technique dedicated to critical infrastructures is described by Genge et al. [45]. The Assessment/analysis platform for Multiple Interdependent Critical Infrastructures (AMICI) aims at enabling attack experiments and evaluation of the associated consequences in complex, interconnected critical systems and facilities. To achieve that, emulation of ICT infrastructures using the Emulab platform is combined with Simulink-based simulation of cyber-physical systems. This approach facilitates the integration of multiple physical process models, allows for experiments with real software and attacks and supports automated execution of tests. A case study regarding the assessment of attack disturbances' proliferation among three interconnected infrastructures, namely a power grid, a railway system and the underlying ICT infrastructure is described.

Saxena et al. [115] describe another proposal (see the work of Kotenko et al. [71] introduced in the preceding subsection) that positions itself on the boundary between cybersecurity assessment and situational awareness. The concept of simulations performed in (near) real-time to obtain state estimations of system-level communications, impact assessments of cyber-attacks and cybersecurity assessments based on simulations of the entire infrastructure dedicated to smart grids is presented. Although the authors indicate several frameworks to facilitate implementation, deployment details are missing to assess the applicability of the solution. Also, the research would benefit from a thorough, multifaceted evaluation of the proposal that regards its efficiency and effectiveness.

Tundis et al. [123] present a security assessment approach dedicated to smart grids which takes advantage of simulations performed in a modelled environment. The distinguishing feature of the method is that it is intended to be applied during the design phase of a smart grid infrastructure, yet before its deployment. As a result, any disruptive events related to the tests' execution are avoided. As a case study, primary analyses with a model of a basic smart grid configuration are presented.

A comparison of the methods in reference to the evaluation criteria is presented in Table 7.

5.5. Model-based testing, formal analysis

Valenza et al. [124] present a concept of a method that aims at evaluation of the correctness of network configuration policies based on their formalised specification and automated generation of network flows. The proposal would benefit from being further elaborated as currently solely a brief overview is provided.

Olivero et al. [102] describe preliminary results of the study on a cybersecurity assessment method for systems of systems. The authors introduce a rather standard approach that encompasses system modelling and vulnerability identification and analysis. Although the authors advise using the mKAOS notation for modelling of systems of systems and borrow several concepts from agile development, at the current stage of the research it is not explained how the compound picture of the cybersecurity of a system of systems can be derived from the assessment results of its components.

Lange et al. [74, 75] developed a vulnerability analysis-oriented approach focused on the identification of threat consequences (by means of affected network services) in interdependent large area network infrastructures that interconnect multiple network services and devices. Vulnerability and network model expressed in the mathematical notation with vulnerability metrics derived from the Common Vulnerability Scoring System (CVSS) was proposed. Provided a set of valid vulnerabilities and network traffic data, the approach enables automated reasoning on the consequences of a potential attack. The framework was evaluated experimentally based on real as well as probabilistically generated data. A tool called Mission Oriented Network Analysis (MONA) is mentioned in this context.

Krautsevich et al. [72] presented initial developments of a method for assessing cybersecurity of compound business processes that integrate several services. For each service an independent Service Level Agreement (SLA) that includes security metrics can be specified. A business process is modelled with a design graph derived from a Business Process Modelling Notation (BPMN) representation. Semirings are used to express security metrics in the model. With such a representation of a security problem, graph analysis methods can be applied to obtain security status indicators. Analysis of several business process alternatives enables selecting the most protected one.

Masera and Fovino [91] studied cybersecurity assessments of critical infrastructures. They introduced a service-oriented approach that centres around the system-of-systems concept. It enables analyses of attack propagation and diffusion of attack consequences between interconnected infrastructure components. Experimental evaluation using a proprietary software InSAW applied to several real-world-originated scenarios is mentioned.

Table 6: Penetration testing methods. Abbreviations: App. domain – application domain, Rel. date – Release date, Cit. – number of citations (Scopus), Det. – documentation level of detail: L – low, M – moderate, H – high, App. – real-world application, Evaluation – methods' evaluation procedure, Coverage – coverage of assessment tasks.

	Method	Purpose			Applicability							Structure	
		Aim, scope	App. domain	Target users	Rel. date	Cit.	Det.	Required skills	App.	Evaluation	Supporting tools	Testing mode	Coverage
1.	Risk-based testing [111]	Cybersecurity testing driven by the results of risk assessments	General	N. a.	2014	1	L	Penetration testing	N. a.	Case studies	12 tools indicated	Hybrid	System analysis, tests preparation, vulnerability identification and analysis
2.	NetSecuritas [46]	A tool-supported security assessment methodology for critical infrastructures	General	N. a.	2015	8	M	Penetration testing	N. a.	Theoretical, simulations	NetSecuritas	Black-box	System analysis, threat identification, vulnerability identification and analysis, attack graph generation
3.	Standardised method to cybersecurity assessments of critical infrastructures [21]	Structured method to ensure good coverage and valid, reproducible and well-documented results	Critical infrastructures	Cybersecurity officers, pentesters, ICS operators	2016	0	L	Penetration testing	N. a.	N. a.	N. a.	Black-box	System analysis, tests preparation, vulnerability identification and analysis
4.	Structured security assessment methodology for manufacturers of critical infrastructure components [19]	Practically applicable, cost-efficient and industry standards-based security assessment method applied uduring development of critical infrastructure systems	Critical infrastructures	Cybersecurity assessors, product developers, system testes, maintenance, sales and marketing, product management	2009	1	M	Cybersecurity knowledge, technical	Siemens systems	Practical application	Various pentesting tools such as nmap, nessus, wireshark, bastille, john the ripper	Hybrid	Tests preparation, compliance checking, vulnerability identification and analysis
5.	Cyber-assessment method for SCADA security [105]	Practical method for assessing SCADA systems built upon experiences from testing real products	SCADA systems	N. a.	2006	1	M	Cybersecurity knowledge, technical	Vendor systems	N. a.	Nmap, Nessus, STAT Scanner, Ethereal, Ettercap and Metasploit	Hybrid	System analysis, experiments preparation, vulnerability identification and analysis

Zalewski et al. [145] approach cybersecurity assessments of cyber-physical systems using Discrete-Time Markov Chain models. The models require the assignment of probability values to state transitions. Two techniques for obtaining these values that originate in threat modelling are briefly discussed namely the DREAD and CVSS scoring systems. Also, a generic model of a cyber-physical system is introduced and a case study of CAN network outlined.

A comparison of the methods in reference to the evaluation criteria is presented in Table 8.

6. Results of the analysis: other related proposals

A considerable set of complementary proposals related to cybersecurity assessments has been identified during the study. They address specific aspects of the assessments rather than defining a methodology for the evaluation of the entire information system that consists of multiple heterogeneous elements. This section is devoted to the presentation of the complementary proposals.

6.1. Component-focused cybersecurity assessment techniques

Component-focused developments describe assessment techniques focused on individual elements of the technical infrastructure, such as singular devices and applications. They in-

Table 7: Simulation or emulation-based testing methods. Target users – not indicated. Abbreviations: App. domain – application domain, Rel. date – Release date, Cit. – number of citations (Scopus), Det. – documentation level of detail: L – low, M – moderate, H – high, App. – real-world application, Eval. – methods' evaluation procedure, Mode – testing mode, Coverage – coverage of assessment tasks.

	Method	Purpose		Applicability							Structure	
		Aim, scope	App. domain	Rel. date	Cit.	Det.	Required skills	App.	Eval.	Supp. tools	Mode	Coverage
1.	Approach to security assessment of critical infrastructures [81]	Non-disruptive assessment of infrastructures that require continuous operation	Critical infrastructures	2011	15	M	Intermediate technical	Power plants, industrial control systems	Case studies	MAlSim, InSAW	Black-box	System analysis, experiments preparation, vulnerability identification and analysis
2.	Assessment/ analysis platform for Multiple Interdependent Critical Infrastructures (AMICI) [45]	Analysis of complex interdependencies between multiple critical infrastructures, flexible integration of multiple physical process models, experiments with real software and threats, automated experiment management capabilities	Critical infrastructures	2013	17	L	Penetration testing and technical	N. a.	Case study	N. a.	Black-box	Vulnerability analysis
3.	Cyber-physical security assessment [115]	Real-time simulator of cyber-physical parts of smart grids, state estimations of system-level communications, security assessments of steady-state cyberattack impact, simulation of the entire smart grid for cybersecurity assessment	Smart grids	2017	5	L	Cybersecurity knowledge, intermediate technical	N. a.	Case study	CPSA Simulator, PowerWorld	N. a.	Vulnerability identification
4.	Smart grids assessment through simulation [123]	Simulation-based assessments performed during the design phase, thus non-intrusive to the evaluated system	Smart grids	2017	0	L	Cybersecurity knowledge	N. a.	Case study	Smart Grid Simulator (SGS)	N. a.	System modelling and analysis, tests preparation, vulnerability identification and analysis

clude the framework for privacy-preserving data search systems that fosters repeatability and reusability of evaluations [125], an aggregated set of common flows for testing of software developed in the NIST Software Assurance Reference Dataset Project [56], a framework for quantitative evaluation of commercial-off-the-shelf software components [25] or a method of verifying satisfaction of security requirements by software applications based on developing an argument tree [68]. Wu et al. [140, 141] proposed a five-stages, model-based approach for assessing network security that takes advantage of a security ontology and automated generation of attack graphs. Kang and Lee [64] explore fault data injection techniques for testing application network services. Bahtiyar et al. [14] introduced a technique that enables continuous monitoring of conformance to the PCI-DSS standard in dynamically changing infrastructures. Similarly, continuous monitoring of cloud applications to detect configuration changes and trigger automated vulnerability identification was proclaimed by Vijayakumar and Arun [130]. The important feature of *usable* security is assessed in the approach of Al-Zahrani [6]. There, the analytic network method, fuzzy sets and the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) are employed collaboratively to evaluate security and usability of healthcare software. A concept of an approach where directed graphs are utilised to represent software applications and search algorithms are applied for analyses was introduced by Lunkeit [87]. Rahman et al. [109] along with the proposal of a new protection architecture for integrated circuits described an approach of assessing the security of the hardware components that is based on formal analysis and component modelling.

6.2. Metrics

Metrics support objective, reproducible and quantifiable measurements and ratings or enable calculation of aggregate system properties. In this context, Nath et al. [95] developed metrics for deriving aggregate values from results reported by multiple vulnerability scanners. Ghosh and Ghosh [47] proposed a probabilistic security metric and an attack resistance metric to assess relative security levels of different network configurations. Arabsorkhi and Ghaffari [11] discuss the literature on metrics that can be used during cybersecurity assessments. Additionally, they present a useful selection of (mostly quantitative) metrics and a metric taxonomy. Cybersecurity indicators for cyber-physical systems are described by Zegzhda et al. [146]. An assignment of weights to security property values communication networks for integrated substation automation systems was proposed by Gao and Dai [42]. Venkataramanan et al. [127]

Table 8: Model-based testing methods. Real-world application – not indicated, testing mode – not applicable. Abbreviations: App. domain – application domain, Cit. – number of citations (Scopus), Det. – documentation level of detail: L – low, M – moderate, H – high, Sup. tools – supporting tools, Evaluation – methods' evaluation procedure, Coverage – coverage of assessment tasks.

	Method	Purpose			Applicability						Structure
		Aim, scope	App. domain	Target users	Rel. date	Cit.	Det.	Required skills	Evaluation	Sup. tools	Coverage
1.	Online and offline security policy assessment [124]	Automated evaluation of the correctness of network configuration policies	General	N.a.	2016	1	L	Proficient cybersecurity and technical	N.a.	KVM, Libvirt, Scapy, Drools, MOEA	System modelling, tests preparation, vulnerability identification
2.	Testing Security for Systems of Systems (TeSSoS) [102]	Security assessment of systems of systems, design of security requirements models for SoS and producing test cases to evaluate SoS	General	System analysts, security experts	2019	N. a.	L	Technical, penetration testing	N.a.	N.a.	System modelling and analysis, tests preparation, vulnerability identification and analysis
3.	Mission Oriented Network Analysis (MONA) [74]	Identification of network activities affected by a cyberattack in large area networks that interconnect multiple devices and services	Communication networks	N.a.	2016	1	L	Mathematical	Case studies (realistic and artificial)	MONA	System modelling, model-based testing
4.	General method for assessment of security in complex services [72]	Assessment of cybersecurity of compound, multi-service business processes	Business processes	N.a.	2011	6	M	Mathematical	N.a.	N.a.	System modelling, model-based testing
5.	Service-oriented approach for assessing critical infrastructure security [91]	Service-oriented vulnerability and threat assessments that grasp multifold interdependencies between system components	Critical infrastructures	N.a.	2008	5	L	Cybersecurity knowledge, intermediate technical	Experiments based on real-world scenarios	InSAW	System modelling, vulnerability analysis
6.	Cybersecurity assessment of cyber-physical systems using Discrete Time Markov Chain model-based simulations [145]	Cybersecurity assessment of cyber-physical systems during operation	Cyber-physical systems	N.a.	2013	6	L	Cybersecurity knowledge, mathematical	Case study	Microsoft SDL Threat Modeling Tool	System modelling, model-based testing

proposed a cyber-physical security assessment metric which integrates quantitative factors that affect resilience and embraces concepts from graph-theoretic analysis, the probabilistic model of availability, attack graph metrics, and vulnerabilities across different layers of the microgrid system. The metric is primarily oriented towards situational awareness. However, it may be also considered during periodic cybersecurity assessments.

6.3. Models

Models represent various elements of the entire evaluation context, the analysed information infrastructure and the involved actors. They can be combined during an assessment of a complete system. Proposals in this area regard communications networks [132, 114, 140, 141] and attackers [114]. They enable simulations [132], theoretical analyses or provide other supportive functions. As far as the latter is concerned, the model of Salfer and Eckert [114] supports evaluations by automatically generating attack graphs, while Solic et al. developed an ontology-based reference model for identifying critical components of the evaluated system and determining its overall security grade [120].

6.4. Tools

The studies related to the tools that support cybersecurity assessments include an automated tool for categorisation and summarising of daily posted vulnerability CVE descriptions [113], a tool for assessments of VoIP networks based on scenarios defined in XML [5] or a solution for reducing the complexity of attack graphs based on removing redundancies from network models [147]. Developments of a tool for automated determination of CVSS scores are described by Zou et al. [148]. Rosa et al. [32], based on a study of relevant literature and the analysis of 19 ontologies, created an ontology that aims at the systematisation of security assessment terminology and removing ambiguities. A freely available visual tool for the design and analysis of attack trees is described by Gadyatskaya et al. [41]. Another tool that enables attack tree analyses and its extension with attacker profiling was introduced by Lenin et al. [76]. Khoury

et al. present the results of testing web vulnerability scanners in a dedicated testbed [67]. The Automated Validation of Internet Security Protocols and Applications (AVISPA) framework [129] was applied by Gomaa et al. [49] to analyse the security of virtual identity mechanisms for cloud computing. The framework employs formal methods. It was developed during a project run over a decade ago [1], but the literature shows that it has been utilised to evaluate the security of several solutions till today [49, 10, 9, 119].

6.5. Other aspects of cybersecurity assessments

The studies that regard cybersecurity assessments' *teaching* comprise the descriptions of academic courses where students evaluate open-source software [30] or large enterprise networks [139]. As far as the *human component* is concerned, Widdowson and Goodliff [137] identified 57 human-related root causes of cybersecurity incidents by applying the human factors approach. These indicators can be utilised during checklist-based evaluations or incorporated into reference models. Additionally, further complementary aspects of cybersecurity assessments were addressed. For instance, Oakley [101] directs attention to the importance of an assessment's initial perspective i.e. the location where a security assessment is commenced. Four main perspectives are distinguished i.e. external, DMZ, internal and critical. Depending on the choice of the perspective, threats of different likelihoods and impacts will be evaluated and attack surfaces covered. Also, based on the selected perspective, performing an analysis introduces particular risks, requires different collaboration efforts and focuses on various attack types. Kong at al. [70] proposed the application of rough set theory to eliminate the subjectiveness of the assessments that require values' assignments to evaluation metrics. where need to be assigned. Allodi et al. [7] analysed data types determined during CVSS-based vulnerability assessments in respect to their impact on the accuracy of the evaluations. The results show that enhanced information on assets, attacks and vulnerabilities increases the precision while the knowledge about common threats may lead to the distortion of the assessment outcome.

7. Findings

This section denotes the main observations from the analysis of the identified methods. The findings refer to the evaluation criteria specified in Section 4.2. As the study emphasised the applicability aspect of the proposals, a substantial number of criteria that regard it was taken into account.

7.1. Methods' primary objectives

The scientific proposals aim at improving cybersecurity assessments by increasing their accuracy [144], efficiency [17] and completeness [19], introducing structure [19] and methodicalness as well as enabling quantitativeness [24, 133] and reproducibility [19]. They target facilitating evaluations of complex systems [115, 74, 72] and grasping interdependencies between systems and components [91, 45]. They pursue automated or semi-automated performance [24, 128, 133, 71, 45] and enhance tool-support [46, 128]. Also, non-invasiveness [17, 81, 123] and real-time operation [71, 115, 145] is fostered. Some approaches emphasise practicability and cost-efficiency [19, 105].

7.2. Scope

As far as the scope of the methods is concerned, besides the primary topic of cybersecurity assessment, the methods focus on enhancing the integration of diverse sources of security information [131, 24, 74, 45], risk-driven testing or consolidation of risk and security assessment [111, 52, 128] as well as linkage to standards [19, 52]. Also, the design and development stages of the system life cycle [20, 19] and evaluation of policies and procedures [22, 124] attracted particular attention. Besides that, the approaches explore various aspects of compliance [20], capability or maturity [138], vulnerability detection and analysis [17, 22, 73, 91], decision making support [131] and reference model optimisation [108].

7.3. Application domain

The proposals address diverse domains, including healthcare, business, semiconductor companies, critical infrastructures, industrial control systems, clouds and grid computing, mobile environments or smart grids. 11 methods aim at general applicability in various types of environments.

7.4. Target users

Among all the 32 methods, only seven depict target users i.e. the personnel participating in or responsible for performing security assessments. This information is not provided for any vulnerability identification and analysis method, neither for simulation or emulation-based testing techniques. For the remaining seven methods, cybersecurity roles such as cybersecurity officers, cybersecurity assessors, compliance analysts, pentesters, system analysts and testers, security experts or dedicated IT security, audit and data centre teams are indicated. Additionally, the involvement of decisive personnel, product developers, system operators, maintenance, sales and marketing and product management is recommended.

7.5. Release date

Practically all the methods have been released during the last decade. The study of Williams [138] is the most cited in the scientific literature (28 citations). Also, the publications of Genge et al. [45], Leszczyna et al. [81], Chen et al. [24] and Kupsch et al. [73] stand out in this respect with more than ten citations (17, 15, 11 and 11 respectively). Recent publications have low citation grades for obvious reasons.

7.6. Documentation detail

Half of the documents are overview-type with a low level of documentation detail. The same number of publications provide more extensive descriptions, however, without the details sufficient for the implementation and application of the methods. Certainly, publishers' paper volume restrictions play a role in this context. However, supplementary documentation could be also provided in the form of technical reports.

7.7. Required skills

Six methods that mostly belong to the vulnerability identification and analysis group require technical skills that are available to regular network administrators. For around ten methods cybersecurity knowledge is essential. At the same time, the implementation or application of the remaining half of proposals may pose a challenge as it requires specialised mathematical or penetration testing capabilities.

7.8. Real-world application

Real-world application of the proposals is occasional. It is not described for any of model-based testing techniques, while other types of methods have singular representatives where a proposal was utilised in a real-world scenario. However, even for them, the application is at most mentioned, without substantial details. The areas of these applications comprise universities [108], grid computing systems [73], industrial control systems [19, 81], control system vendors' infrastructures [105], semiconductor manufacturers [22] and power plants [81].

7.9. Evaluation procedure

A case study is the most popular procedure for evaluating the methods by their authors. It was employed for more than half of the proposals (16). All simulation or emulation-based testing methods were assessed in this way. Usually, the case studies concern applying a method to cybersecurity assessment of a specific setting. This can evidence the feasibility of the method's usage in the given settlement and provides a context for some practical explanations. More methodological approaches applied to evaluate the proposals included simulation [144, 46], theoretical analyses [46, 133], prototype-based experiments [17, 133, 71, 91] and a comparative study in reference to other proposals [73]. For five methods there is no evaluation method indicated. Three of them belong to the model-based testing group.

7.10. Supporting tools

None of the seven checklist-based evaluation or compliance checking methods indicates tools for supporting the evaluations. Penetration testing methods point out the applications that are commonly used in this area such as nmap, nessus, wireshark or metasploit. Besides that, Ghosh et al. [46] developed a framework for supporting security assessment at all stages, called NetSecuritas, while the study of Rennoch et al. [111] references 12 tools for test modelling, generation, execution, analysis and monitoring that are mostly proprietary with the exception of CORAS which is freely available. Two prototypes, a tool in development (RACOMAT) and a proprietary application (ARIS) are depicted in the vulnerability identification and analysis methods' group. There, three methods do not describe any tool support, while one only mentions it. A similar situation concerns the remaining two groups of assessment methods, where the tools, if indicated, are mostly internal, at the development stage or described without details. Valenza et al. [124] indicate openly available applications that may support cybersecurity evaluations i.e. the Kernel-based Virtual Machine (KVM) and Libvirt for the creation and management of virtual environments, Scapy for the generation of network packets, and Drools and MOEA for the development of verification models. Zalewski et al. [145] take advantage of the freely available Microsoft Threat Modeling Tool[3], while Saxena et al. [115] utilise PowerWorld to simulate power systems.

7.11. Testing mode

The testing mode attribute concerns only selected groups of security assessment methods, namely the penetration testing methods, vulnerability identification and analysis methods as well as simulation or emulation-based testing methods. All three types of approaches are covered. Two methods apply white-box testing, five – black-box testing and three – hybrid testing. For six methods (out of 16), the mode is not indicated.

7.12. Coverage of the assessment tasks

As far as the coverage of the assessment tasks is concerned, practically all methods encompass the initial stage of analysing or modelling the evaluated system. The majority of methods (20) comprise vulnerability identification and/or analysis tasks, among them three focus solely on these activities. Also, tests preparation is well covered by the methods (9). Relatively less attention is given to threat identification [46, 52] and analysis [74, 75, 145, 140, 24, 133, 71, 91], including the generation of attack graphs and modelling of the attacker. Singular methods support these activities. Activities of four methods, all in the checklist-based evaluation and compliance checking category progress towards obtaining the cumulative value of the security level of the entire system.

8. Gaps, future research directions

It becomes evident that the real-world applications of the methods are extremely scarce. Even if the utilisation of a method in a practical scenario is mentioned, the description exhibits noticeable shortcomings. Most of the implementations regard preliminary configurations, pilot or demonstration sites and hypothetical scenarios that in the best case refer to the real world. At the same time, the methods' documentation does not provide details sufficient for the implementation and application of the methods. None of the descriptions contains information regarding the time and effort necessary to employ a method (see the NESCOR [4] as a good example). Supporting tools, if indicated, are mostly internal, at the development stage or described without details. Target users are practically not designated. The evaluation of the solutions requires further research. Some methods are not evaluated at all, some only based on a case study, an unrealistic scenario or a model. Minor attention is given to threat identification and analysis. Singular methods support these activities. Practically none of the methods indicate means to achieve completeness of the assessment and the criteria for its determination. The areas for improvement are presented in Table 9.

[3] According to the information on the Microsoft website, the application's life cycle ended in October 2019.

Table 9: Methods' areas for improvement according to the evaluation criteria.

Area	Gap
Real-world applications	Scarce
Methods' evaluation	Limited, mostly case studies
Supporting tools	Scarce, mostly internal, at the development stage or described without details
Documentation	Insufficient to implement the methods
Target users	Practically not indicated
Coverage of the assessment tasks	Less attention given to threat identification and analysis
Assessment completeness	No techniques to achieve and no indicators defined

Several directions for prospective research and development activities can be taken to address these challenges. They are presented further in this Section and summarised in Table 10.

8.1. Evidence of the method's application

First of all, better evidence of the application of proposed methodologies is demanded. The funding of research projects should require operational implementations and verify the fulfilment of this requirement at the end of the projects. The projects should be conducted in collaboration with industry and real customers. The transfer of technology needs to be supported with adequate training. Moreover, research projects with a longer timespan that enables the implementation of the proposal, but also its deployment and popularisation (promotion, training, awareness raising) should be envisaged. Alternatively, the projects that follow up previous undertakings, but focus on the implementation and absorption by the market need to be promoted. These solutions seem to be recognised by several funding bodies, but the effectiveness of their enforcement needs furtherance.

8.2. Methods' documentation

Additional effort should be undertaken to enhance the documentation of the methods so the level of details would enable their unproblematic deployment and exploitation. Companion to papers or book chapters extensive reports need to be published that are publicly and continuously available. Ideally, they should explain the relevant concepts, components and tasks based on illustrative examples. For each activity, an estimation of the effort, time and complexity should be provided.

8.3. Supporting tools

Tools enable reducing the complexity and the cost of a solution without decreasing its quality and scope [128]. Reliable, easy-in-use and economic tools are highly demanded [41]. Practice shows that this is especially important at the initial stages when an organisation commences its first security assessments. To overcome the entry barriers of no-knowledge and experience, straightforward solutions are sought rather than elaborated ones. Similarly, facilitated, more self-explaining methods that enable application by regular IT personnel are in demand. Also, an important factor is the availability of the tools which together with detailed documentation should be published in easily accessible locations, possibly on open platforms on the Internet. The tools should be continuously maintained which is reflected in the associated activities. It is not encouraging if the latest activity related to a tool was recorded a decade or a half ago.

8.4. Methods' evaluation

A great extent of work needs to be carried out in the area of the evaluation of the proposals. With a case study, that is currently the most common procedure of claiming methods' quality attributes, the overall excellence of the methods, including their effectiveness and efficiency, remains declarative. Case studies can evidence only a limited set of variables related to the utilisation of a method, usually associated with a particular setting and circumstances. To provide a convincing argument that a method satisfies the requirements for correctly assessing cybersecurity of critical systems, structured methodologies of evaluation that employ criteria, metrics and repeatable procedures need to be followed.

8.5. Other research directions

Despite the large number of existing proposals, new, alternative ones are still being introduced. They often repeat the earlier approaches, unaware of their existence. The path that builds upon existing methodologies, enforces their strengths and eliminates weaknesses should be taken instead. For that, comprehensive studies of related work conducted by the research teams and periodically repeated literature surveys are necessary. It is also very important to disambiguate the concepts of risk assessment and security assessment in the studies to avoid confusion of potential recipients of a solution. Another interesting area that requires further research is the integration of security assessment with situational awareness and threat intelligence [83]. In the concept, system information gathered in real-time from multiple sensors deployed in various locations is automatically processed and analysed to provide indications on the current security level of the system. The research challenges associated with the domain primarily concern the efficiency and scalability of solutions as well as their attack detection and classification capabilities. Also, there is space for scientific exploration in decision-support methods and tools for security assessments and assessment-based decisions on the architecture of security management systems [18].

9. Conclusion

The paper presented the results of a systematic study that aimed at the identification and analysis of cybersecurity assess-

Table 10: Activities to improve cybersecurity assessment areas.

Area	Action
Evidence of the method's application	Fostering long term projects that encompass method's implementation, deployment and popularisation
	Promoting follow-up projects focused on implementation and market-delivery
	Enforcing operational implementations by funding bodies
	Conducting research projects in collaboration with industry and customers
	Delivering training and courses to support the transfer of technology
Methods' documentation	Enhancing the level of details to enable methods' deployment and utilisation
	Publishing detailed reports with illustrative examples
	Including estimations of the effort, time and complexity of assessment activities
Supporting tools	Developing reliable, easy-in-use and economic tools
	Sharing in easily accessible locations, possibly on open platforms in the Internet
	Continuously maintaining
Methods' evaluation	Developing structured evaluation methodologies
	Introducing criteria, metrics and repeatable procedures
Other	Building upon existing methodologies
	Conducting comprehensive studies of related work, periodic literature surveys
	Disambiguating the concepts of risk assessment and security assessment
	Integration of security assessment with situational awareness
	Decision-support methods and tools for security assessments and assessment-based decisions

ment methods. The research followed the Webster and Watson's as well as Kitchenham and Brereton approach and comprised a two-stages search process in the established scientific databases. The first stage focused on existing literature reviews, the second stage concerned individual methods. The reviews' search evidenced a practical lack of existing reviews. Only two proper reviews were identified, yet their scope was limited to particular application domains. This motivated performing the second stage of the research. Based on evident selection and evaluation criteria, 32 cybersecurity assessment methods were identified and analysed. The main observations from the research are described in the previous two sections. Findings (Section 7) are grouped into categories related to the evaluation criteria, which in turn reflect the methods' purpose, structure and applicability characteristics. Important gaps that primarily concern the application of the methods have been identified (Section 8). Namely, the methods' practical use in operational contexts is extremely scarce and the proposals are limited to pilot or demonstration sites, hypothetical scenarios or some preliminary configurations. This can be visibly connected to the methods' applicability properties that have been revealed during the analysis. For instance, the methods' documentation may not be sufficiently detailed to facilitate the method's deployment and practical use, no information on the time and effort necessary to employ a method is provided or there is a lack of supporting tools. These observations give a clear indication of the areas of improvement and research directions that are described in more detail in Section 8. Primarily, a great extent of work needs to be performed in the area methods' evaluation. This involves following structured methodologies of evaluation that employ criteria, metrics and repeatable procedures when assessing the methods. Also, better evidence of methods' application needs to be provided, efficient supporting tools designed and implemented, and methods' documentation significantly improved.

References

[1] (2006). The AVISPA Project. `http://www.avispa-project.org/`

[2] (2014). S.2521 - Federal Information Security Modernization Act of 2014.

[3] (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[4] (2019). EPRI — SmartGrid Resource Center - NESCOR.

[5] Abdelnur, H., Cridlig, V., State, R., and Festor, O. (2006). VoIP security assessment: methods and tools. In *1st IEEE Workshop on VoIP Management and Security, 2006.*, pages 29–34.

[6] Al-Zahrani, F. A. (2020). Evaluating the Usable-Security of Healthcare Software through Unified Technique of Fuzzy Logic, ANP and TOPSIS. *IEEE Access*, 8.

[7] Allodi, L., Banescu, S., Femmer, H., and Beckers, K. (2018). Identifying Relevant Information Cues for Vulnerability Assessment Using CVSS. In *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*, CODASPY '18, pages 119–126, New York, NY, USA. ACM.

[8] Alshamrani, A., Myneni, S., Chowdhary, A., and Huang, D. (2019). A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. *IEEE Communications Surveys Tutorials*, 21(2):1851–1877.

[9] Amin, R., Islam, S. K., Kumar, N., and Choo, K. K. R. (2018a). An untraceable and anonymous password authentication protocol for heterogeneous wireless sensor networks. *Journal of Network and Computer Applications*.

[10] Amin, R., Kumar, N., Biswas, G. P., Iqbal, R., and Chang, V. (2018b). A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment. *Future Generation Computer Systems*.

[11] Arabsorkhi, A. and Ghaffari, F. (2018). Security Metrics: Principles and Security Assessment Methods. In *2018 9th International Symposium on Telecommunications (IST)*, pages 305–310.

[12] Aslan, Ö. A. and Samet, R. (2020). A Comprehensive Review on Malware Detection Approaches. *IEEE Access*, 8:6249–6271.

[13] Aven, T. (2012). The risk concept-historical and recent development trends. *Reliability Engineering and System Safety*, 99(0951):33–44.

[14] Bahtiyar, b., Gür, G., and Altay, L. (2014). Security Assessment of Payment Systems under PCI DSS Incompatibilities. In Cuppens-Boulahia, N.,

Cuppens, F., Jajodia, S., Abou El Kalam, A., and Sans, T., editors, *ICT Systems Security and Privacy Protection*, pages 395–402, Berlin, Heidelberg. Springer Berlin Heidelberg.

[15] Bamberger, J. (1997). Essence of the capability maturity model. *Computer*, 30(6):112–114.

[16] Barrere, M., Badonnel, R., and Festor, O. (2014). Vulnerability assessment in autonomic networks and services: A survey. *IEEE Communications Surveys and Tutorials*, 16(2):988–1004.

[17] Barrère, M., Hurel, G., Badonnel, R., and Festor, O. (2013). A probabilistic cost-efficient approach for mobile security assessment. In *2013 9th International Conference on Network and Service Management, CNSM 2013 and its three collocated Workshops - ICQT 2013, SVM 2013 and SETM 2013*, pages 235–242. IEEE Computer Society.

[18] Bettaieb, S., Shin, S. Y., Sabetzadeh, M., Briand, L. C., Garceau, M., and Meyers, A. (2020). Using machine learning to assist with the selection of security controls during security assessment. *Empirical Software Engineering*, 25(4):2550–2582.

[19] Brandstetter, T., Knorr, K., and Rosenbaum, U. (2009). A Structured Security Assessment Methodology for Manufacturers of Critical Infrastructure Components. pages 248–258. Springer, Berlin, Heidelberg.

[20] Buccafurri, F., Fotia, L., Furfaro, A., Garro, A., Giacalone, M., and Tundis, A. (2015). An Analytical Processing Approach to Supporting Cyber Security Compliance Assessment. In *Proceedings of the 8th International Conference on Security of Information and Networks*, SIN '15, pages 46–53, New York, NY, USA. ACM.

[21] Caselli, M. and Kargl, F. (2016). A security assessment methodology for critical infrastructures. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 8985, pages 332–343. Springer Verlag.

[22] Cayetano, T. A., Dogao, A., Guipoc, C., and Palaoag, T. (2018). Cyber-Physical IT Assessment Tool and Vulnerability Assessment for Semiconductor Companies. In *Proceedings of the 2Nd International Conference on Cryptography, Security and Privacy*, ICCSP 2018, pages 67–71, New York, NY, USA. ACM.

[23] Chapple, M., Stewart, J. M., and Gibson, D. (2018). *(ISC) CISSP Certified Information Systems Security Professional Official Study Guide*.

[24] Chen, B., Kalbarczyk, Z., Nicol, D. M., Sanders, W. H., Tan, R., Temple, W. G., Tippenhauer, N. O., Vu, A. H., and Yau, D. K. (2013a). Go with the flow: Toward workflow-oriented security assessment. In *ACM International Conference Proceeding Series*, pages 65–76.

[25] Chen, J., Lu, Y., Wang, H., and Mao, C. (2013b). A quantitative assessment approach to COTS component security. *Mathematical Problems in Engineering*, 2013.

[26] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., and Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, 56:1–27.

[27] Coffey, K., Maglaras, L. A., Smith, R., Janicke, H., Ferrag, M. A., Derhab, A., Mukherjee, M., Rallis, S., and Yousaf, A. (2018). Vulnerability Assessment of Cyber Security for SCADA Systems. pages 59–80.

[28] Conrad, E., Misenar, S., and Feldman, J. (2017). *Eleventh Hour CISSP®*. Elsevier.

[29] Corallo, A., Lazoi, M., and Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Computers in Industry*, 114:103165.

[30] Crain, S. P. (2017). Open Source Security Assessment As a Class Project. *J. Comput. Sci. Coll.*, 32(6):41–53.

[31] Dalalana Bertoglio, D. and Zorzo, A. F. (2017). Overview and open issues on penetration test. *Journal of the Brazilian Computer Society*, 23(1):1–16.

[32] de Franco Rosa, F., Jino, M., and Bonacin, R. (2018). Towards an Ontology of Security Assessment: A Core Model Proposal. In Latifi, S., editor, *Information Technology - New Generations*, pages 75–80, Cham. Springer International Publishing.

[33] Dondossola, G. (1999). Formal Methods for the engineering and certification of safety-critical Knowledge Based Systems. In Vermesan, A. and Coenen, F., editors, *Validation and Verification of Knowledge Based Systems: Theory, Tools and Practice*, pages 113–130. Springer US, Boston, MA.

[34] El-Rewini, Z., Sadatsharan, K., Selvaraj, D. F., Plathottam, S. J., and Ranganathan, P. (2020). Cybersecurity challenges in vehicular communications. *Vehicular Communications*, 23:100214.

[35] Fabisiak, L., Hyla, T., and Klasa, T. (2012). Comparative Analysis of Information Security Assessment and Management Methods. *Studia i Materialy Polskiego Stowarzyszenia Zarzadzania Wiedza / Studies & Proceedings Polish Association for Knowledge Management*, (60):55–70.

[36] Felderer, M. and Schieferdecker, I. (2014). A taxonomy of risk-based testing. *International Journal on Software Tools for Technology Transfer*, 16(5):559–568.

[37] Felderer, M., Zech, P., Breu, R., Büchler, M., and Pretschner, A. (2016). Model-based security testing: A taxonomy and systematic classification. *Software Testing Verification and Reliability*, 26(2):119–148.

[38] Fovino, I. N. and Masera, M. (2008). InSAW-Industrial Security Assessment Workbench. In *2008 First International Conference on Infrastructure Systems and Services: Building Networks for a Brighter Future (INFRA)*, pages 1–5. IEEE.

[39] Fovino, I. N., Masera, M., and Decian, A. (2007). Integration of Cyber-Attack within Fault Trees. In *17th European Safety and Reliability Conference (ESREL)*, volume 3, pages 2571–2578.

[40] Furfaro, A., Garro, A., and Tundis, A. (2014). Towards Security as a Service (SecaaS): On the modeling of Security Services for Cloud Computing. In *Proceedings - International Carnahan Conference on Security Technology*, volume 2014-Octob. Institute of Electrical and Electronics Engineers Inc.

[41] Gadyatskaya, O., Jhawar, R., Kordy, P., Lounis, K., Mauw, S., and Trujillo-Rasua, R. (2016). Attack trees for practical security assessment: Ranking of attack scenarios with ADTool 2.0. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 9826 LNCS, pages 159–162. Springer Verlag.

[42] Gao, H. and Dai, X. (2011). Security Assessment of Communication Networks for Integrated Substation Automation Systems. In Liu, C., Chang, J., and Yang, A., editors, *Information Computing and Applications*, pages 448–455, Berlin, Heidelberg. Springer Berlin Heidelberg.

[43] Genge, B., Kiss, I., and Haller, P. (2015). A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. *International Journal of Critical Infrastructure Protection*, 10:3–17.

[44] Genge, B. and Siaterlis, C. (2013). Analysis of the effects of distributed denial-of-service attacks on MPLS networks. *International Journal of Critical Infrastructure Protection*, 6(2):87–95.

[45] Genge, B., Siaterlis, C., and Hohenadel, M. (2013). AMICI: An assessment platform for multi-domain security experimentation on critical infrastructures. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 7722 LNCS, pages 228–239.

[46] Ghosh, N., Chokshi, I., Sarkar, M., Ghosh, S. K., Kaushik, A. K., and Das, S. K. (2015). NetSecuritas: An integrated attack graph-based security assessment tool for enterprise networks. In *ACM International Conference Proceeding Series*, volume 04-07-Janu. Association for Computing Machinery.

[47] Ghosh, N. and Ghosh, S. K. (2009). An Approach for Security Assessment of Network Configurations Using Attack Graph. In *2009 First International Conference on Networks Communications*, pages 283–288.

[48] Giannopoulos, G., Filippini, R., and Schimmer, M. (2012). *Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art.*

[49] Gomaa, I., Abd-Elrahman, E., Hamdy, A., and Saad, E. M. (2021). Automated Security Assessment for IDaaS Framework. *Wireless Personal Communications*, 116(4):3465–3490.

[50] Gordon, A. (2016). *The Official (ISC) 2® Guide to the CCSP SM CBK ®*. John Wiley & Sons, Inc.

[51] Gritzalis, D., Iseppi, G., Mylonas, A., and Stavrou, V. (2018). Exiting the risk assessment maze: A meta-survey. *ACM Computing Surveys*, 51(1):1–30.

[52] Großmann, J. and Seehusen, F. (2015). Combining security risk assessment and security testing based on standards. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 9488, pages 18–33. Springer Verlag.

[53] Gupta, B. B. and Akhtar, T. (2017). A survey on smart power grid: frameworks, tools, security issues, and solutions. *Annals of Telecommunications*, 72(9-10):517–549.

[54] Hahn, A. and Govindarasu, M. (2011). An evaluation of cybersecurity assessment tools on a SCADA environment. In *IEEE Power and Energy*

Society General Meeting.

[55] Holm, H., Sommestad, T., Almroth, J., and Persson, M. (2011). A quantitative evaluation of vulnerability scanning. *Information Management and Computer Security*, 19(4):231–247.

[56] Hoole, A. M., Traore, I., Delaitre, A., and de Oliveira, C. (2016). Improving Vulnerability Detection Measurement: [Test Suites and Software Security Assurance]. In *Proceedings of the 20th International Conference on Evaluation and Assessment in Software Engineering*, EASE '16, pages 27:1—-27:10, New York, NY, USA. ACM.

[57] Huang, K., Siegel, M., and Madnick, S. (2018). Systematically Understanding the Cyber Attack Business: A Survey. *ACM Comput. Surv.*, 51(4):70:1—-70:36.

[58] IEC (2007). IEC/TS 62351-1: Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues.

[59] Ionita, D. and Hartel, P. (2013). *Current Established Risk Assessment Methodologies and Tools*. PhD thesis.

[60] ISO/IEC (2011). ISO/IEC 27005:2011: Information technology – Security techniques – Information security risk management. Technical report, ISO/IEC.

[61] ISO/IEC (2013). ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems – Requirements.

[62] ISO/IEC (2018). ISO/IEC:2018 Information technology Security techniques Information security management systems Overview and.

[63] Kaloudi, N. and Li, J. (2020). The AI-Based Cyber Threat Landscape: A Survey. *ACM Comput. Surv.*, 53(1).

[64] Kang, H. and Lee, D. H. (2007). Security Assessment for Application Network Services Using Fault Injection. In Yang, C. C., Zeng, D., Chau, M., Chang, K., Yang, Q., Cheng, X., Wang, J., Wang, F.-Y., and Chen, H., editors, *Intelligence and Security Informatics*, pages 172–183, Berlin, Heidelberg. Springer Berlin Heidelberg.

[65] Khan, S. and Parkinson, S. (2018). Review into State of the Art of Vulnerability Assessment using Artificial Intelligence. pages 3–32.

[66] Khattak, S., Jan, S., Ahmad, I., Wadud, Z., and Khan, F. Q. (2020). An effective security assessment approach for Internet banking services via deep analysis of multimedia data. *Multimedia Systems*.

[67] Khoury, N., Zavarsky, P., Lindskog, D., and Ruhl, R. (2011). Testing and Assessing Web Vulnerability Scanners for Persistent SQL Injection Attacks. In *Proceedings of the First International Workshop on Security and Privacy Preserving in e-Societies*, SeceS '11, pages 12–18, New York, NY, USA. ACM.

[68] Kienzle, D. M. and Wulf, W. A. (1997). A Practical Approach to Security Assessment. In *Proceedings of the 1997 Workshop on New Security Paradigms*, NSPW '97, pages 5–16, New York, NY, USA. ACM.

[69] Kitchenham, B. and Brereton, P. (2013). A systematic review of systematic review process research in software engineering. *Information and Software Technology*, 55(12):2049–2075.

[70] Kong, L., Ren, X., and Fan, Y. (2009). Study on assessment method for computer network security based on rough set. In *Proceedings - 2009 IEEE International Conference on Intelligent Computing and Intelligent Systems, ICIS 2009*, volume 3, pages 617–621.

[71] Kotenko, I., Doynikova, E., Chechulin, A., and Fedorchenko, A. (2018). AI- and Metrics-Based Vulnerability-Centric Cyber Security Assessment and Countermeasure Selection. In *Guide to Vulnerability Analysis for Computer Networks and Systems*, pages 101–130.

[72] Krautsevich, L., Martinelli, F., and Yautsiukhin, A. (2011). A general method for assessment of security in complex services. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 6994 LNCS, pages 153–164.

[73] Kupsch, J. A., Miller, B. P., Heymann, E., and César, E. (2010). First principles vulnerability assessment. In *Proceedings of the ACM Conference on Computer and Communications Security*, pages 87–92.

[74] Lange, M., Kuhr, F., and Möller, R. (2016). Using a Deep Understanding of Network Activities for Network Vulnerability Assessment. In *Proceedings of the 1st International Workshop on AI for Privacy and Security*, PrAISe '16, pages 6:1—-6:8, New York, NY, USA. ACM.

[75] Lange, M. and Möller, R. (2017). Time series data mining for network service dependency analysis. In *Advances in Intelligent Systems and Computing*, volume 527, pages 584–594. Springer Verlag.

[76] Lenin, A., Willemson, J., and Sari, D. P. (2014). Attacker Profiling in Quantitative Security Assessment Based on Attack Trees. In Bernsmed, K. and Fischer-Hübner, S., editors, *Secure IT Systems*, pages 199–212, Cham. Springer International Publishing.

[77] Leszczyna, R. (2018). Standards on Cyber Security Assessment of Smart Grid. *International Journal of Critical Infrastructure Protection*, 22:70–89.

[78] Leszczyna, R. (2021). Aiming at methods' wider adoption: Applicability determinants and metrics. *Computer Science Review*, 40:100387.

[79] Leszczyna, R., Fovino, I., and Masera, M. (2008a). MAlSim - Mobile Agent Malware Simulator. In *SIMUTools 2008 - 1st International ICST Conference on Simulation Tools and Techniques for Communications, Networks and Systems*.

[80] Leszczyna, R., Fovino, I. N., and Masera, M. (2008b). Simulating Malware with MAlSim. In Filiol, E. and Broucek, V., editors, *Proceedings of 17th EICAR Annual Conference 2008*, pages 243–261, Laval, France. EICAR.

[81] Leszczyna, R., Fovino, I. N., and Masera, M. (2011). Approach to security assessment of critical infrastructures' information systems. *IET Information Security*, 5(3):135.

[82] Leszczyna, R., Nai Fovino, I., and Masera, M. (2010). Simulating malware with MAlSim. *Journal in Computer Virology*, 6(1):65–75.

[83] Leszczyna, R. and Wróbel, M. R. (2019). Threat intelligence platform for the energy sector. *Software: Practice & Experience*.

[84] Li, J., Beba, S., and Karlsen, M. M. (2019). Evaluation of open-source IDE plugins for detecting security vulnerabilities. In *ACM International Conference Proceeding Series*, pages 200–209. Association for Computing Machinery.

[85] Li, X., Han, X., and Zheng, Q. (2011). Study on model-based security assessment of information systems. In *Communications in Computer and Information Science*, volume 233 CCIS, pages 401–406.

[86] Liu, Q., Li, P., Zhao, W., Cai, W., Yu, S., and Leung, V. C. M. (2018). A Survey on Security Threats and Defensive Techniques of Machine Learning: A Data Driven View. *IEEE Access*, 6:12103–12117.

[87] Lunkeit, A. (2014). A Graph-Based Approach for Analysis of Software Security. In Bauer, T., Großmann, J., Seehusen, F., Stølen, K., and Wendland, M.-F., editors, *Risk Assessment and Risk-Driven Testing*, pages 68–79, Cham. Springer International Publishing.

[88] Lykou, G., Anagnostopoulou, A., Stergiopoulos, G., and Gritzalis, D. (2019). Cybersecurity self-assessment tools: Evaluating the importance for securing industrial control systems in critical infrastructures. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 11260 LNCS, pages 129–142. Springer Verlag.

[89] Malatras, A., Skouloudi, C., and Koukounas, A. (2019). Industry 4.0 Cybersecurity: Challenges & Recommendations. Technical report, European Union Agency for Network and Information Security (ENISA).

[90] Masera, M., Fovino, I. I. N., and Leszczyna, R. (2008). Security Assessment Of A Turbo-Gas Power Plant. In *IFIP International Federation for Information Processing*, volume 290, pages 31–40. Springer, Boston, MA.

[91] Masera, M. and Fovino, I. N. (2008a). A Service-Oriented Approach for Assessing Infrastructure Security. In Goetz, E. and Shenoi, S., editors, *Critical Infrastructure Protection*, pages 367–379, Boston, MA. Springer US.

[92] Masera, M. and Fovino, I. N. (2008b). A Service Oriented Approach to the Assessment of Infrastructure Security. In *First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection*, volume 253 of {*IFIP*} *International Federation for Information Processing*, pages 367–380. Springer, eric goetz edition.

[93] Meriah, I. and Rabai, L. B. A. (2018). A survey of quantitative security risk analysis models for computer systems. In *Proceedings of the 2nd International Conference on Advances in Artificial Intelligence (ICAAI 2018)*, pages 36–40. Association for Computing Machinery.

[94] Nath, H. V. (2011). Vulnerability assessment methods - A review. In *Communications in Computer and Information Science*, volume 196 CCIS, pages 1–10.

[95] Nath, H. V., Gangadharan, K., and Sethumadhavan, M. (2012). Reconciliation Engine and Metric for Network Vulnerability Assessment. In *Proceedings of the First International Conference on Security of Internet of Things*, SecurIT '12, pages 9–21, New York, NY, USA. ACM.

[96] National Institute of Standards and Technology (NIST) (2013). *NIST SP*

800-53 Rev. 4 Recommended Security Controls for Federal Information Systems and Organizations. U.S. Government Printing Office.

[97] NERC (2017). CIP Standards.

[98] Nespoli, P., Papamartzivanos, D., Gómez Mármol, F., and Kambourakis, G. (2018). Optimal Countermeasures Selection Against Cyber Attacks: A Comprehensive Survey on Reaction Frameworks. *IEEE Communications Surveys Tutorials*, 20(2):1361–1396.

[99] NIST (2011). NIST SP 800-39 Managing Information Security Risk Organization, Mission, and Information System View. Technical Report March.

[100] NRC (2010). NRC RG 5.71 Cyber Security Programs for Nuclear Facilities. Technical report.

[101] Oakley, J. (2018). Improving Offensive Cyber Security Assessments Using Varied and Novel Initialization Perspectives. In *Proceedings of the ACMSE 2018 Conference*, ACMSE '18, pages 3:1—-3:9, New York, NY, USA. ACM.

[102] Olivero, M. A., Bertolino, A., Dominguez-Mayo, F. J., Escalona, M. J., and Matteucci, I. (2019). Security Assessment of Systems of Systems. In *Proceedings of the 7th International Workshop on Software Engineering for Systems-of-Systems and 13th Workshop on Distributed Software Development, Software Ecosystems and Systems-of-Systems*, SESoS-WDES '19, pages 62–65, Piscataway, NJ, USA. IEEE Press.

[103] Oriyano, S.-P. (2017). *Penetration Testing Essentials*. John Wiley & Sons, Inc.

[104] Paulk, M., Curtis, B., Chrissis, M., and Weber, C. (1993). Capability maturity model, version 1.1. *IEEE Software*, 10(4):18–27.

[105] Permann, M. and Rohde, K. (2006). Cyber assessment methods for control system security. In *16th Annual Joint ISA POWID/EPRI Controls and Instrumentation Conference and 49th Annual ISA Power Industry Division, POWID Symposium 2006*, volume 1, pages 212–223.

[106] Potteiger, B., Mills, J., Cohen, D., and Velez, P. (2020). RUCKUS: A Cybersecurity Engine for Performing Autonomous Cyber-Physical System Vulnerability Discovery at Scale. In *Proceedings of the 7th Symposium on Hot Topics in the Science of Security*, HotSoS '20, New York, NY, USA. Association for Computing Machinery.

[107] Qassim, Q. S., Jamil, N., Daud, M., Patel, A., and Ja'affar, N. (2019). A review of security assessment methodologies in industrial control systems. *Information and Computer Security*, 27(1):47–61.

[108] Qiangmin, W., Mengquan, L., and Jianhua, L. (2007). Method on network information system security assessment based on rough set. In *Proceedings - International Conference on Signal Image Technologies and Internet Based Systems, SITIS 2007*, pages 1041–1046.

[109] Rahman, M. S., Nahiyan, A., Rahman, F., Fazzari, S., Plaks, K., Farahmandi, F., Forte, D., and Tehranipoor, M. (2021). Security Assessment of Dynamically Obfuscated Scan Chain Against Oracle-Guided Attacks. *ACM Trans. Des. Autom. Electron. Syst.*, 26(4).

[110] Razaque, A., Amsaad, F., Jaro Khan, M., Hariri, S., Chen, S., Siting, C., and Ji, X. (2019). Survey: Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical Domain. *IEEE Access*, 7:168774–168797.

[111] Rennoch, A., Schieferdecker, I., and Großmann, J. (2014). Security Testing Approaches - For Research, Industry and Standardization. In *Communications in Computer and Information Science*, volume 426 CCIS, pages 397–406. Springer Verlag.

[112] Rogers, R. and Syngress Media, I. (2004). *Security assessment: case studies for implementing the NSA IAM*. Syngress.

[113] Russo, E. R., Sorbo, A. D., Visaggio, C. A., and Canfora, G. (2019). Summarizing vulnerabilities' descriptions to support experts during vulnerability assessment activities. *Journal of Systems and Software*, 156:84–99.

[114] Salfer, M. and Eckert, C. (2018). Attack Graph-Based Assessment of Exploitability Risks in Automotive On-Board Networks. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, ARES 2018, pages 21:1—-21:10, New York, NY, USA. ACM.

[115] Saxena, N., Chukwuka, V., Xiong, L., and Grijalva, S. (2017). CPSA: A Cyber-Physical Security Assessment Tool for Situational Awareness in Smart Grid. In *Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy*, CPS '17, pages 69–79, New York, NY, USA. ACM.

[116] Scarfone, K., Souppaya, M., Cody, A., and Orebaugh, A. (2008). NIST SP 800-115 Technical Guide to Information Security Testing and Assessment.

[117] Shah, S. and Mehtre, B. M. (2015). An overview of vulnerability assessment and penetration testing techniques. *Journal of Computer Virology and Hacking Techniques*, 11(1):27–49.

[118] Shahriar, H. and Zulkernine, M. (2009). Automatic testing of program security vulnerabilities. In *Proceedings - International Computer Software and Applications Conference*, volume 2, pages 550–555.

[119] Sharma, G. and Kalra, S. (2018). A lightweight multi-factor secure smart card based remote user authentication scheme for cloud-IoT applications. *Journal of Information Security and Applications*.

[120] Solic, K., Ocevcic, H., and Golub, M. (2015). The information systems' security level assessment model based on an ontology and evidential reasoning approach. *Computers and Security*, 55:100–112.

[121] Stewart, James M.; Chapple, Mike; Gibson, D. (2015). *CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide, 7th Edition*.

[122] Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., and Klepacki, B. (2020). Information security assessment in public administration. *Computers and Security*, 90.

[123] Tundis, A., Egert, R., and Mühlhäuser, M. (2017). Attack Scenario Modeling for Smart Grids Assessment Through Simulation. In *Proceedings of the 12th International Conference on Availability, Reliability and Security*, ARES '17, pages 13:1—-13:10, New York, NY, USA. ACM.

[124] Valenza, F., Vallini, M., and Lioy, A. (2016). Online and Offline Security Policy Assessment. In *Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats*, MIST '16, pages 101–104, New York, NY, USA. ACM.

[125] Varia, M., Price, B., Hwang, N., Hamlin, A., Herzog, J., Poland, J., Reschly, M., Yakoubov, S., and Cunningham, R. K. (2015). Automated Assessment of Secure Search Systems. *SIGOPS Oper. Syst. Rev.*, 49(1):22–30.

[126] Venable, J., Pries-Heje, J., and Baskerville, R. (2012). A comprehensive framework for evaluation in design science research. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 7286 LNCS, pages 423–438.

[127] Venkataramanan, V., Hahn, A., and Srivastava, A. (2020). CP-SAM: Cyber-Physical Security Assessment Metric for Monitoring Microgrid Resiliency. *IEEE Transactions on Smart Grid*, 11(2):1055–1065.

[128] Viehmann, J. and Werner, F. (2015). Risk assessment and security testing of large scale networked systems with RACOMAT. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 9488, pages 3–17. Springer Verlag.

[129] Viganò, L. (2006). Automated Security Protocol Analysis With the AVISPA Tool. *Electronic Notes in Theoretical Computer Science*.

[130] Vijayakumar, K. and Arun, C. (2019). Continuous security assessment of cloud based applications using distributed hashing algorithm in SDLC. *Cluster Computing*, 22(5):10789–10800.

[131] Vogel, M. and Broer, V. (2013). Security Compliance Monitoring The next Evolution of Information Security Management?! In *ISSE 2013 Securing Electronic Business Processes*, pages 183–194. Springer Fachmedien Wiesbaden.

[132] Wagner, N., Lippmann, R., Winterrose, M., Riordan, J., Yu, T., and Streilein, W. W. (2015). Agent-based Simulation for Assessing Network Security Risk Due to Unauthorized Hardware. In *Proceedings of the Symposium on Agent-Directed Simulation*, ADS '15, pages 18–26, San Diego, CA, USA. Society for Computer Simulation International.

[133] Wang, C., Wang, Y., Dong, Y., and Zhang, T. (2011). A novel comprehensive network security assessment approach. In *IEEE International Conference on Communications*.

[134] Wangen, G., Hallstensen, C., and Snekkenes, E. (2018). A framework for estimating information security risk assessment method completeness: Core Unified Risk Framework, CURF. *International Journal of Information Security*, 17(6):681–699.

[135] Webster, J. and Watson, R. T. (2002). Analyzing the past to prepare for the future: writing a literature review. *MIS Quarterly*, 26(2):xiii–xxiii.

[136] Weiss, S. (2008). Industrial approaches and standards for security assessment. In Eusgeld, I., Freiling, F., and Reussner, R., editors, *Dependability Metrics*, volume 4909 LNCS, pages 166–175.

[137] Widdowson, A. J. and Goodliff, P. B. (2015). CHEAT, an approach to incorporating human factors in cyber security assessments. In *10th IET System Safety and Cyber-Security Conference 2015*, pages 1–5.

[138] Williams, P. (2008). A practical application of CMM to medical security capability. *Information Management and Computer Security*, 16(1):58–73.

[139] Wooley, G. L. (2003). Results of Classroom Enterprise Security Assessment of Five Large Enterprise Networks. *J. Comput. Sci. Coll.*, 18(3):185–195.

[140] Wu, S., Zhang, Y., and Cao, W. (2017). Network security assessment using a semantic reasoning and graph based approach. *Computers and Electrical Engineering*, 64:96–109.

[141] Wu, S., Zhang, Y., and Chen, X. (2018). Security Assessment of Dynamic Networks with an Approach of Integrating Semantic Reasoning and Attack Graphs. In *2018 IEEE 4th International Conference on Computer and Communications (ICCC)*, pages 1166–1174.

[142] Yang, H., Zeng, R., Xu, G., and Zhang, L. (2021). A network security situation assessment method based on adversarial deep learning. *Applied Soft Computing*, 102:107096.

[143] Yener, B. and Gal, T. (2019). Cybersecurity in the Era of Data Science: Examining New Adversarial Models. *IEEE Security Privacy*, 17(6):46–53.

[144] You, Y., Cho, I., and Lee, K. (2016). An advanced approach to security measurement system. *Journal of Supercomputing*, 72(9):3443–3454.

[145] Zalewski, J., Drager, S., McKeever, W., and Kornecki, A. J. (2013). Threat Modeling for Security Assessment in Cyberphysical Systems. In *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, CSIIRW '13, pages 10:1—-10:4, New York, NY, USA. ACM.

[146] Zegzhda, D. P., Poltavtseva, M. A., and Lavrova, D. S. (2017). Systematization and security assessment of cyber-physical systems. *Automatic Control and Computer Sciences*, 51(8):835–843.

[147] Zhang, S., Ou, X., and Homer, J. (2011). Effective Network Vulnerability Assessment through Model Abstraction. In Holz, T. and Bos, H., editors, *Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 17–34, Berlin, Heidelberg. Springer Berlin Heidelberg.

[148] Zou, D., Yang, J., Li, Z., Jin, H., and Ma, X. (2019). AutoCVSS: An Approach for Automatic Assessment of Vulnerability Severity Based on Attack Process. In Miani, R., Camargos, L., Zarpelão, B., Rosas, E., and Pasquini, R., editors, *Green, Pervasive, and Cloud Computing*, pages 238–253, Cham. Springer International Publishing.