future internet

Review

Dynamic Risk Assessment in Cybersecurity: A Systematic Literature Review

Pavlos Cheimonidis * and Konstantinos Rantos *

Department of Computer Science, International Hellenic University, 654 04 Kavala, Greece
* Correspondence: paxeimw@cs.ihu.gr (P.C.); krantos@cs.ihu.gr (K.R.)

Abstract: Traditional information security risk assessment (RA) methodologies and standards, adopted by information security management systems and frameworks as a foundation stone towards robust environments, face many difficulties in modern environments where the threat landscape changes rapidly and new vulnerabilities are being discovered. In order to overcome this problem, dynamic risk assessment (DRA) models have been proposed to continuously and dynamically assess risks to organisational operations in (near) real time. The aim of this work is to analyse the current state of DRA models that have been proposed for cybersecurity, through a systematic literature review. The screening process led us to study 50 DRA models, categorised based on the respective primary analysis methods they used. The study provides insights into the key characteristics of these models, including the maturity level of the examined models, the domain or application area in which these models flourish, and the information they utilise in order to produce results. The aim of this work is to answer critical research questions regarding the development of dynamic risk assessment methodologies and provide insights on the already developed methods as well as future research directions.

Keywords: cybersecurity; dynamic risk assessment; machine-learning; quantitative risk assessment

Citation: Cheimonidis, P.; Rantos, K. Dynamic Risk Assessment in Cybersecurity: A Systematic Literature Review. *Future Internet* **2023**, *15*, 324. https://doi.org/10.3390/fi15100324

Academic Editors: Thomas Loruenser and Stephan Krenn

Received: 24 August 2023
Revised: 20 September 2023
Accepted: 26 September 2023
Published: 28 September 2023

1. Introduction

According to NIST SP 800-160 Vol.1 [1] and ISO Guide 73:2009 [2], RA is the "overall process of risk identification, risk analysis, and risk evaluation". NIST SP 800-53 Rev. 4 [3] defines RA as "the process of identifying risks to organisational operations (including mission, function, image, reputation), organisational assets, individuals, other organisations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analysis, and considers mitigations provided by security controls planned or in place".

RA based on typical standardised risk management frameworks and methodologies, like ISO 31000:2018 [4] and the NIST 800-37 Risk Management Framework [5] cannot maintain the security posture of the organisation to the required levels, since they cannot adapt well to the modern and dynamic environment in which organisations operate [6]. Organisations cannot rely on rigid and static RA processes because they cannot adapt in the current rapidly changing environment and, in addition, they create a misconception about the threats and their potential impacts [7]. Companies face an increasing number of malicious actions from various sources, which necessitate the need for an effective dynamic real-time RA and management process [8].

As a result, the scientific community has turned its attention to the so-called "dynamic risk assessment". Although there are many definitions for RA, when it comes to the definition of DRA there is a lack in the literature. The definition that is considered to be the most appropriate for this study is the following: dynamic risk assessment is the continuous process of identifying and assessing risks to organisational operations, dynamically and in a (near) real-time manner. The idea behind DRA is to identify and assess the risk on the spot and to make quick decisions on how to best mitigate this risk. For the purpose of our research, we characterised as dynamic, any system, model, or framework that used as input any kind of real-time data coming from its environment and, based on them, calculated the risk.

DRA constitutes a very useful tool that could help to evaluate and counter cyber threats in current environments, which are complex and evolve rigorously, as well as to maintain the organisation's security posture or improve it to the most appropriate level. Thus, our motivation to write this article stemmed from the need to analyse the current status around the area of DRA in cybersecurity. Our work focused on the DRA models proposed in the literature in the area of cybersecurity, regardless of the domain in which these models have been applied or the analysis method they have used. We tried to examine this topic holistically, having no prior limitation.

The main contribution of this paper was an analysis of the existing literature regarding DRA schemes in the field of cybersecurity to identify methods and techniques that were being applied in the respective models. We further classified these schemes, based on the primary analysis method they utilised for the risk assessment process, and we identified the domain(s) that each of them was being applied. Moreover, we examined both the output (quantitative or qualitative risk analysis) that these models utilised, as well as the input data they used. Finally, we examined the proposed models with respect to their maturity status. To the best of the authors' knowledge, this is the first literature review focused on DRA in the field of cybersecurity, regardless of the proposed approach and the domain in which these models are being applied.

The rest of this paper is structured as follows: Section 2 presents related work and Section 3 presents the research methodology used for this work. Section 4 provides the detailed results of the DRA models found in the literature, categorised under the primary analysis method they apply. Meanwhile, Section 5 undertakes a thorough discourse on these results. Section 6 concludes the study.

2. Related Work

In the past few years, several surveys have focused on RA related topics in various domains. A review of RA methods for SCADA systems only was conducted by Cherdantseva et al. [9]. The authors studied 24 methods, and concluded that because of the nature of SCADA systems and the available data relating to cyber attacks, probabilistic RA methods tend to underestimate the probability of the occurrence of a cyber event. Accordingly, the calculated risk, which depends on the probability of the occurrence of an attack along with the estimated losses from the attack, tends to be lower than the actual one.

Eckhart et al. [10] focused on quantitative RA methods in industrial control systems (ICSs), to report the absence of DRA methods tailored to the complex needs of an ICS. Jiang et al. [11] concluded that DRA is a necessary tool for enhancing the safety of a network and they analysed the key technologies that are used in each RA method (qualitative, quantitative, comprehensive).

Lopez et al. [12] tried to give prominence to the need for DRA in the information systems domain. They asserted that despite the existence of numerous standards, they tend to view RA as a periodic process rather than a real-time one. In recent years, there has been a turning from classic RA to DRA, which adopts the use of information originating from databases, such as the National Vulnerability Database (NVD), as input, in order to keep the system up to date, and also the use of attack trees to define possible attack patterns against the information system.

The closest to our work is the research that was conducted by Erdogan et al. [13], in which the authors reported that the number of papers about artificial intelligence (AI)-supported security RA has been increasing since 2010, with a growth rate of 133% between 2010 and 2020. Their approach focused mostly on identifying and/or estimating security risks, and primarily made use of Bayesian networks and neural networks as supporting AI methods/techniques. Although the aforementioned literature review is close to ours, they focused only on the connection between AI and RA, leaving out other supported methods. In addition, our work provides useful information regarding the input data that these models used along with the produced results. We also examined the maturity level of each of the proposed models.

3. Research Methodology

According to NISTIR 8170 [14], cybersecurity is "The ability to protect or defend the use of cyberspace from cyber attacks". Hence, cybersecurity is the framework of securing anything that is vulnerable to hacks, attacks, or unauthorised access which mainly consists of computers, devices, networks, servers, and applications. It also refers to the protection of any kind of digital data.

Such a definition of cybersecurity is provided by NIST 800-53 Rev. 5 [3], according to which, cybersecurity is "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation". The same Special Publication defines information security as "The protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability".

Although there is some overlapping between these two terms, cybersecurity refers clearly to the protection of any kind of electronic information, while information security is referring to the protection of any kind of information both in electronic and physical form, such as the counter-measures that should be applied in order to protect information stored in paper forms.

Although in this respect, information security can be considered as a superset of cybersecurity and, therefore, papers about DRA in information security might also address cybersecurity-related aspects, in this review paper, we focused only on those with a clear orientation on cybersecurity.

Considering the above, the initial set of papers was provided by SCOPUS using as a search string the keywords "dynamic risk assessment" AND "cybersecurity" or "cybersecurity" or "cyber" and "security". More specifically, our search string was: (TITLE-ABS-KEY (dynamic AND risk AND assessment) AND (TITLE-ABS-KEY (cybersecurity) OR TITLE-ABS-KEY (cyber AND security))), and it was conducted on the 21 May 2023. Based on this query, SCOPUS returned 271 papers for the period 2001–2023. Having completed an initial check based on the papers' abstracts, we eliminated 204 as not relevant to our query. Subsequently, we conducted a more comprehensive scrutiny of the residual 67 papers. This evaluation resulted in the identification of 51 papers specifically addressing topics pertaining to DRA within the realm of cybersecurity. Within the definitive set of 51 papers, a comprehensive total of 50 papers were considered appropriate for inclusion in our review. The sole remaining paper was excluded due to its lack of suggestion for any dynamic methodologies. Instead the excluded paper proposed an extension of the incident object description exchange format (IODEF) to IODEF-DRA, with the intention of enabling utilisation by DRA tools [15]. Figure 1 presents the outline of our research methodology.

The following research questions (RQ) regarding the DRA models proposed in the literature were answered through our analysis.

RQ1: What primary analysis methods are being used by the proposed DRA models?
RQ2: What are the domains or application areas to which the proposed DRA models were applied?
RQ3: Are the proposed DRA models based on quantitative or qualitative methods?
RQ4: What are the main sources of data that the studied models use?
RQ5: What is the maturity level of the proposed models?

Each of the above research questions is succinctly summarised and juxtaposed with the findings obtained from other studies. This critical examination is expounded upon in

Section 5, with dedicated subsections that scrutinise and contextualise the outcomes in relation to the existing body of research.

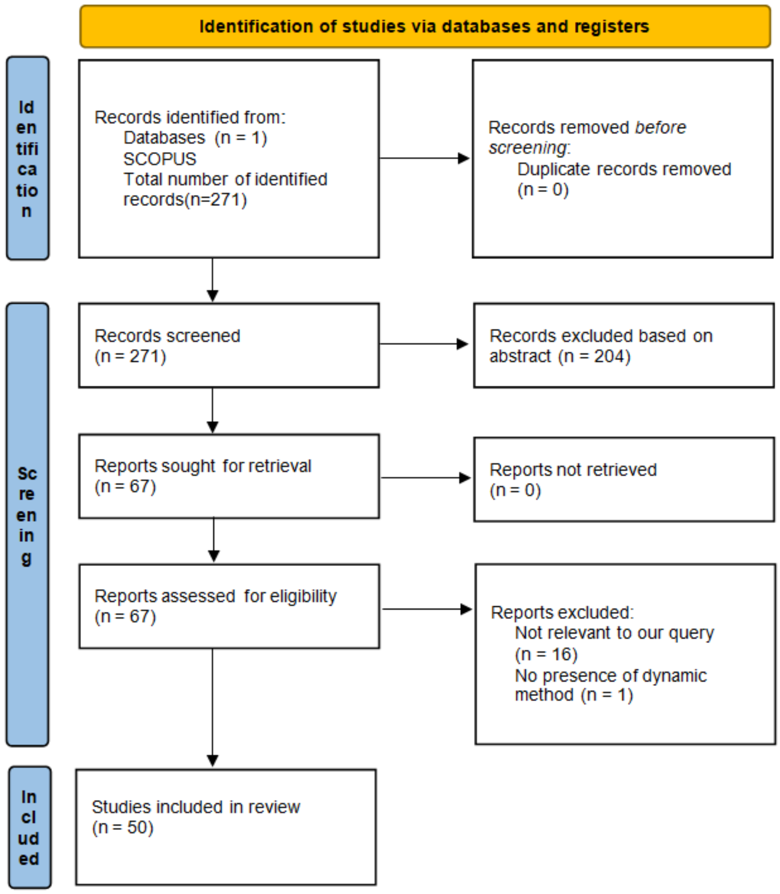
Identification of studies via databases and registers
Identification
Records identified from:
Databases (n = 1)
SCOPUS
Total number of identified records(n=271)
Records removed *before screening*:
Duplicate records removed (n = 0)
Screening
Records screened (n = 271)
Records excluded based on abstract (n = 204)
Reports sought for retrieval (n = 67)
Reports not retrieved (n = 0)
Reports assessed for eligibility (n = 67)
Reports excluded:
Not relevant to our query (n = 16)
No presence of dynamic method (n = 1)
Included
Studies included in review (n = 50)

Figure 1. Research methodology outline.

4. Results

Considering the primary analysis method that each of the 50 studied proposed models utilised, we categorised them in three distinct areas: "artificial intelligence–machine learning" (AI/ML), "mathematical-model-based", and "unclassified". Table 1 demonstrates that the majority of the studied models belonged to the AI/ML category. The models associated with each of the aforementioned categories were organised and presented in a chronologically exclusive order for each category.

Table 1. Number of papers per category.

Category	AI/ML	Mathematical Model Based	Unclassified
# of Papers	24	13	13
Percentage	48%	26%	26%

Figure 2 presents the basic categorisation of DRA models regarding the primary risk analysis method.

Our research also focused on the domain in which each DRA model was applied. As many of the examined models targeted the same domain but this domain was referred in a different way, we applied grouping in order to create the following categories for each domain:

1. Information and communications technology (ICT) domain, which includes information systems, networks, computing infrastructures, and every other computer

environment (such as small and medium-sized enterprises (SMEs), hospitals, fog, and high-performance computing).

2. Industrial control systems (ICSs) domain, which includes SCADA and industrial production systems (IPSs), electrical power and energy systems (EPESs), cyber-physical systems (CPSs), and critical infrastructures (CI).
3. Smart city (SC) domain, which contains large-scale, dynamic, and complex IoT networks.

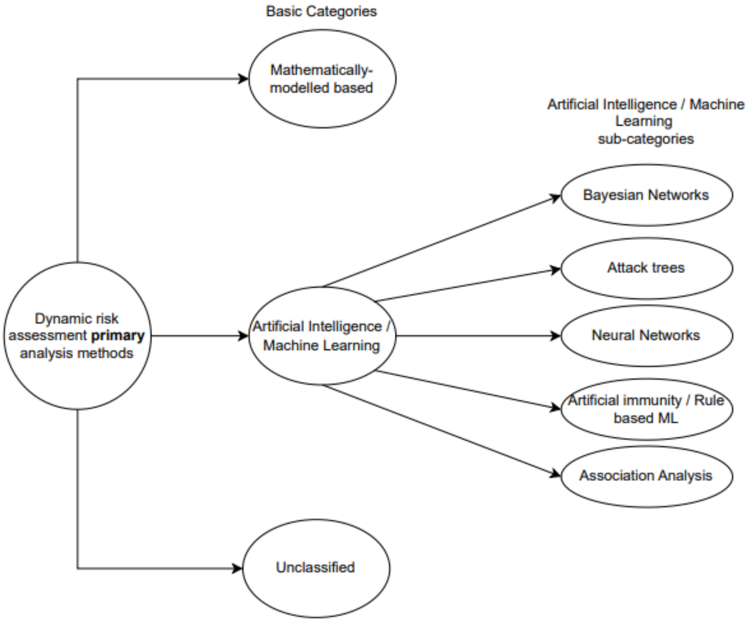
Basic Categories
Mathematically-modelled based
Artificial Intelligence / Machine Learning sub-categories
Bayesian Networks
Attack trees
Dynamic risk assessment **primary** analysis methods
Artificial Intelligence / Machine Learning
Neural Networks
Artificial immunity / Rule based ML
Association Analysis
Unclassified

Figure 2. Primary analysis methods.

Based on the aforementioned classification, Table 2 presents the number of models that were proposed for each domain.

Table 2. Number of applied models per domain.

Domain	ICT	ICS	SC
# of Models	21	26	3
Percentage	42%	52%	6%

4.1. *Artificial Intelligence/Machine Learning*

Models in this category utilise AI and ML techniques as their primary analysis method. The vast majority of the studies (47%) and their proposed models belong to the AI/ML category. Due to the number of papers and the variety of techniques applied to this category, we further classified them based on the specific AI or ML method they utilised. This resulted in the adoption of the following subcategories: Bayesian networks, attack trees, neural networks, artificial immunity, and association analysis. For those models that utilise multiple techniques, such as incremental learning algorithms in cases of incomplete or missing data, we classified them based on their primary analysis method. Table 3 presents the number of papers that belong to each subcategory and the respective percentage.

Table 3. AI/ML-based categories of DRA methods.

Sub-Category	Bayesian Networks	Attack Trees	Neural Networks	Artificial Immunity	Association Analysis
# of Models	11	7	3	2	1
Percentage	45.8%	29.2%	12.5%	8.3%	4.2%

4.1.1. Bayesian Networks

Cam et al. [16] proposed a mission assurance policy, that adapts to the dynamic security status of all assets using a Petri net model along with binary or multilevel logic decision, to determine the security status of cyber assets. The main goal of the proposed model was to determine if a mission could be completed. Mission assurance policy is the continuous assessment of cyber assets which are necessary for an organisation to fulfil specific tasks. Assets fulfil certain tasks, which accomplish specific missions accordingly. This quantitative model is based on a risk management policy which consists of five steps:

1. Assets' vulnerability assessment, based on a vulnerabilities database such as the NVD.
2. Identification of likelihood and threats, based on data from the intrusion detection system (IDS).
3. Determination of impact and counter-measures (cost-benefit analysis).
4. Quantitative risk assessment using Bayesian networks.
5. Risk assessment evaluation (risk mitigation options and prioritisation).

According to the authors, their proposed model can give a clearer picture to decision-makers about their system in real time. Its application was demonstrated through a simple example.

Another model was presented by Cam et al. [17] to dynamically and quantitatively assess risks on networks. This model requires the use of a vulnerability scanner in order to detect vulnerabilities of the examined system. A Bayesian network is then used to capture relationships between detected vulnerabilities. The authors then use the common vulnerability scoring system (CVSS) model and expand it by taking into consideration the criticality of an asset's mission, the current damage of an asset (the impact of an attack on a specific asset), and how this vulnerability is going to affect other assets' vulnerabilities. They also use a hidden Markov model (HMM) and Bayesian networks to dynamically model cyber operations, events, and observations (originating from IDS, firewall, etc.) in order to use them to assess dynamically the exploit likelihood in the network. Risk is estimated by pinpointing the most likely path of exploited vulnerabilities, their likelihood of exploitation, and their associated impacts. The authors perform a simulation utilising synthetic data to demonstrate that, given the vulnerabilities of a network, their model is able to quantify and assess risk.

Henshel et al. [18] introduced a dynamic quantitative RA approach which models both the system (software, hardware, network) and the human factor. The authors used Bayesian networks in order to analyse and assess the cyber risks (low–medium–high) along with direct acyclic graphs (DAGs) to represent the connections between nodes. This model, which is built using experts' opinions to define the risk variables of the system (in this case a structured query language (SQL) server), takes into consideration the dependencies between cyber assets and their interactions with the respective events in order to quantify assets' vulnerabilities, the impact of attacks, and the risks. The authors demonstrated its application in a scenario that included an SQL injection attack.

Zhang et al. [19] recommend a multilevel Bayesian network to describe the propagation of the risk caused by cyber attacks. It consists of an incident model, a function model, and an attack model. In addition, a novel multimodel-based approach to assess the cybersecurity risk for ICSs is developed. This approach can determine the current cybersecurity risk value by estimating probabilities and quantifying the consequences of numerous potentially hazardous scenarios arising from malicious attacks. The model uses both offline and online/real-time data. The offline data originate from vulnerability scanners, statistical analysis, experts' opinions, and they are used to determine the probabilities of an attack, the dependencies between functions, the relations between incidents, and the risk propagation. The online data, which comprise the input of the system, originate from attack evidence (IDS) and anomaly evidence (anomaly detection system—ADS). ADS data are compared with normal values to produce information related to the system's malfunction. All these data are processed using Bayesian networks. The authors performed a simulation on a chemical reactor control system to demonstrate that their approach was able to calculate the cybersecurity risk of an ICS in real time.

A dynamic, quantitative model based on Bayesian networks was presented by Huang et al. [20] in order to address cyber risk for SCADA environments. The model combines the posterior probability along with the value of an asset in the SCADA environment to calculate the risk. The first step is to differentiate the nodes into two categories: the vulnerability nodes (nodes that have vulnerabilities which can be discovered by a vulnerability scanner software or by querying the common vulnerabilities and exposures database—CVE) and the privilege escalation nodes (nodes that can be used to damage the system). Bayes' theorem is used to predict the posterior probability based on real-time data/evidence collected from the IDS. The authors used multiple techniques in order to make more accurate risk predictions, such as:

- A leaky noisy-OR gate to predict unknown attacks.
- Offline batching (although complete datasets existed offline, they utilised the expectation maximisation principle to fill the missing values because it is quite common for the attack sample to be incomplete for SCADA systems).
- Online incremental learning in order for the model to be able to update and adapt to real-time observations.

The model combines historical data and real-time observations, using machine learning techniques to make accurate predictions. A chemical process network was simulated by the authors to demonstrate that the proposed model is able to provide real-time risk calculations for known and unknown attacks.

Peng et al. [21] proposed a method to quantitatively calculate cyber risk in ICS environments. Real-time data (evidence from attack) are fed to the Bayesian network along with the ICS security knowledge, which contains information about vulnerabilities, functions, accidents, and assets. The output of the Bayesian network is the probability of occurrence of an event which is combined with the impact, to calculate the real-time risk. The value of the impact depends on the severity of the affected asset. An expectation maximisation algorithm is chosen in case the data are incomplete. The authors conducted a case study on a simulated chemical control process to show that their model can achieve a high level of risk accuracy in real time.

Zhu et al. [22] introduced a model to quantitatively assess the risk in IPSs by calculating the probabilities and consequences of an abnormal event (tampering with control strategies). The model consists of two parts, probability inference and loss calculation, which were combined to produce real-time risk. An extended multilevel flow model (EMFM) is used to describe the production process (structures and functions of the system) quantitatively, and based on this, the model is able to forecast the consequences of an abnormal event (loss calculation). Regarding the probability inference, a Bayesian network based on the EMFM is used to infer the probabilities of an abnormal event. The system uses as input established control strategies and attack evidence from the IDS. The authors carried out simulations on a chemical process system to present the ability of the proposed model to quantify the risk.

Zhang et al. [23] presented a novel dynamic quantitative model to address the cybersecurity risk assessment in ICS. The model feeds a fuzzy probability Bayesian network with cyber attack knowledge, system function knowledge, hazardous incident knowledge, and the system's asset knowledge. The authors used fuzzy probability in order to replace the crisp probabilities required in Bayesian networks. In addition, the model receives as input anomaly evidence detected by anomaly detectors, as well as attack evidence detected by the IDS. Based on this information the fuzzy probability Bayesian network interference engine calculates the posterior probability. Finally, the risk is calculated based on the posterior probability and asset losses. Simulations on a simplified chemical reactor were conducted by the authors to present the ability of their model to evaluate risk in a timely manner.

A DRA approach that aims to reduce the cyber risk of CI was presented by Zhu et al. [24], taking into consideration the cyber-physical interaction. A typical CI consists of a several stations and a control centre. The model consists of two components: DRA and decision making. With respect to the DRA component, every station employs a Bayesian network that utilises real-time attack data from the IDS as input, and generates probabilities for station capacities as output. The station capacity is the capability of a station to work as planned. Then, the probabilities of all station capacities are obtained the same way. The final output of the risk assessment process is the real-time system risk caused by an attack strategy. The decision-making approach for cyber-risk reduction is based on the attack strategy detected by the IDS and the counter-measures that can be applied in order to reduce the risk. Finally, the net benefit of each counter-measure is calculated. A simulation was carried out on a simplified water supply system in order for the authors to prove that their model is able to evaluate cyber risk in real time and to provide the optimal decision-making approach.

Debneath et al. [25] recommended HPCvul, a novel approach for vulnerability and risk assessment in high-performance computing (HPC) networks utilising the NVD repository, CVSS scoring, and a network monitoring tool such as IDS. HPCvul agencies are deployed in HPC subnetworks to collect information such as hosts' configurations and services, deployed software, topology, etc. HPCvul uses a Bayesian attack graph to conduct real-time RA by examining vulnerabilities and their dependencies within the network. This allows the model to detect potential attack paths and evaluate the likelihood of an HPC target being compromised by an attacker. Furthermore, quantitative RA metrics are defined to aid in security decision making. Relative case studies were conducted to showcase that this approach is able to assess the probability of compromising a target in dynamic environments.

A dynamic model to quantitatively address cybersecurity risk in distributed CPSs was proposed by Zhou et al. [26]. Based on a distribution network topology and the CVSS scoring mechanism, a Bayesian network model is built. The attacker's selectivity in attacking targets during cyber attacks is taken into consideration using a combination of the fuzzy analytic hierarchy process (FAHP) and entropy weight method, incorporating both subjective expert opinions and objective indicators. In addition, the model considers the available defence resources. The authors used GeNle to create three different attack scenarios simulations in order to evaluate their model.

4.1.2. Attack Trees

Kotenko et al. [27] presented a security metrics model, which is used for the assessment of risk in distributed information systems. The model takes into consideration the topological dependencies, the severity of attack actions, the skills of adversaries, and the current security state of the system (events, security level, attack surface). The system is able to calculate both static and dynamic risk. The dynamic (performance-based) risk is based on real-time data. This technique uses an external vulnerability database along with the target environment's network topology to generate attack graphs, and combines the latter with information from the IDS in order to dynamically calculate the attacker's position and their possible network path.

A quantitative risk assessment methodology based on attack–defence trees (ADTs) was recommended by Ji et al. [28], taking into consideration both the attack cost and the defence cost. The overall idea is to build the ADT based on the description of the system's vulnerabilities. The model is capable of calculating many variables such as cost of attack/defence, probability of success, impact cost, revised attack cost, revised impact, etc. (revised means that counter-measures are applied). The authors implemented a case study for a SCADA system to demonstrate that the revised attack cost, i.e., what the attacker needs to spend, increases when the counter-measures are applied. Accordingly, the revised impact is reduced.

A model aiming to evaluate the current and the future security posture of an enterprise's computer network was introduced by Abraham et al. [29]. In order to forecast how the security posture of the network will vary over time, the authors construct an attack graph that captures the interdependencies of all vulnerabilities discovered in the enterprise software. The model determines the initial value of a vulnerability and how this value will develop over time by taking into account the characteristics of the CVSS metric framework. Incorporating the prior analysis (relationships between various network vulnerabilities), they use a Markov model to explain the attacks. The probability that the attacker would succeed in their objective is expressed using a probabilistic path. Although the proposed model is used as a predictive model, it can be used to assess the current risk of an enterprise in a quantitative manner. A case study showed that the proposed model was able to visualise and objectively evaluate network security.

Kanoun et al. [30] presented a model in order to bridge the gap between technical and organisational risk in ICT systems. In their work, they introduced two primary concepts: elementary risk (ER), which pertains to a single detrimental incident affecting a strategic asset, resulting from a possible technical attack scenario which involves a singular supporting asset, e.g., a server; and composite risk (CR), which aggregates the ER based on a specific criteria (technical or organisational, based on specific detrimental events). Their proposed model consists of:

1. An attack graph generator, which takes into consideration the system topology along with a vulnerability database, such as NVD.
2. "Elementary risk instantiation" (based on attack graphs and the organisation's database, which includes information about assets, supporting assets, detrimental events, and mapping between them).
3. ER calculation (likelihood, impact). Likelihood of occurrence depends on the attack scenario and the affected vulnerabilities and it is calculated with the use of Markov modelling. Impact depends on the consequences of the attack scenario.
4. CR calculation (aggregation of ERs).
5. Analysis of results.

By conducting a case study of a medium-sized ICT system, the authors were able to show how the proposed model can dynamically quantify an organisation's risk, and that the concept of ER and CR improves the organisation security posture.

Gonzalez et al. [31] proposed a dynamic risk management response system (DBRMS) which aims to quantify the risk of the monitored system and to produce response plans consecutively, in order to address cyber threats. The authors utilised an attack graph generator which uses as input information about connections among devices, a vulnerability inventory, and a business model of the organisation (e.g., crucial assets), and produces as output all possible attack scenarios. A Markov chain is used to determine the probability that an attack will succeed, based on the attack path, along with properties associated with the difficulty of exploiting a vulnerability. The impact is calculated based on the consequences of the exploited vulnerability that resides in the business device. The threat quantification module, through the use of elementary risk, calculates the risk value of an event based on the probability and the impact. Using data collected from scans in a SCADA system, the authors conducted experiments to demonstrate that the proposed model is dynamic, since it can adapt to different input data and produces suitable response plans in an automated way.

Wu et al. [32] recommended a security assessment approach based on an ontology and an attack graph for ICS. The system's assets, vulnerabilities, attacks, counter-measures, and relationships between them are represented by an ontology using OWL. The created security ontology represents attacks that pose a threat to assets (based on identified vulnerabilities) using SWRL rules. The attack graph is subsequently created through the utilisation of an efficient algorithm, harnessing the inference capabilities of the security ontology. The evaluation of the algorithm in different topologies and network sizes showed that the proposed approach is suitable for enterprise networks.

Ivanon et al. [33] presented a method to assess risk based on an attack graph and two security indicators for smart city infrastructures. The first indicator shows the importance (type of node, running services) of the node which is being attacked, and the second one (topological) presents the number of connected nodes that are going to be affected, also taking into consideration their importance. The attack graph can be constructed as an output of penetration testing. In the next step, the total value of the system at risk is calculated based on the aforementioned indicators. Afterwards, the protective measures are applied in order to eliminate the most critical vulnerabilities. Then, the total risk value of the system is recalculated (the value is reduced).

4.1.3. Neural Networks

Fu et al. [34] proposed a method for integrating quantitative and qualitative analyses to provide an information security risk assessment for CPS. They used a Petri net for the description of the system and its relationship with big data analysis (performed by experts) in order to provide the right indexes for the neural network, so that the latter could provide risk evaluation.

Ashiku et al. [35] presented a model according to which risk value in an organisation's network depends on the following variables: the quantity of workstations, typical user roles, super user roles (users with increased awareness), daily work hours, open ports, third-party users, data volume, and frequency of daily briefings to strengthen security. The model receives additional enhancement through the utilisation of a balanced dataset (network traffic) which is used as input for an external neural network. These are combined to calculate the risk value. In addition, the model takes into account the applied defence mechanism. Simulations showed that the risk value is linked to the annual incident cost and it depends on the aforementioned variables and the defence mechanism in place.

Krundyshev et al. [36] analysed all possible risk assessment methods and suggested that the most efficient methods to conduct risk assessments in smart city environments are those which are based on AI, such as ANN, because they can deal with big data, and they are quick and accurate. The authors used synthetic datasets and NS-3 to construct a potential dynamic network of a smart city. They specified five potential attack types (grey hole, black hole, DoS, DDoS, and wormhole) along with the probability of occurrence. In the next step, device types were identified, based on the supposition that they performed the same function in the system and interacted with the same number of devices of another type. Device types could be traffic lights, medical sensors, vehicles, etc. In addition, they took into consideration the interaction between devices. The authors established a threshold for unacceptable risk, guided by the principle that assets impacting people's lives and health should have the lowest acceptable failure probability. In their simulated environment, they created one training dataset and one test. Their neural network model was built with the help of CORAS and TensorFlow, and it included:

- a 38-neuron input layer;
- one covert layer containing 20 neurons;
- one output layer.

They achieved 97% maximum classification accuracy.

4.1.4. Artificial Immunity—Rule-Based Machine Learning

A quantitative, immune-based dynamic risk control model for network security, consisting of three different levels (user, processing, hardware), was introduced by Lin et al. [37]. The risk assessment module, the intrusion detection module, and the dynamic risk control module were located at the processing layer. The first module was responsible for estimating damage in a computer network or a system according to the threat level and the vulnerabilities of the system. It was based on artificial immune theory, according to which each attack category is simulated as an immune memory cell, and the antibody concentration value of the immune memory cells is calculated according to the intrusion detection results. The risk assessment relies on the antibody concentration of immunological memory cells, which, in turn, is influenced by detected data packages. When the system is under attack, the concentration value is increasing and when the detection results are normal, the concentration value is decreasing in real time. Experiments validated that the antibody concentration and risk values increased while the attack was continuing.

Another immune-based DRA method for digital virtual assets was proposed by He et al. [38]. It comprises four stages: data collection and pre-processing, immune detector training, antibody cell concentration, attack hazard value evaluation and threat risk assessment. Based on the hierarchical division negative selection algorithm (HD-NSA), the immune detector component identifies attacks or illegal behaviours on digital virtual assets. The detected attacks are then categorised according to the taxonomy of digital virtual asset attacks. By simulating the mechanism of antibody concentration alteration, the threat to digital virtual assets is assessed upon the discovery of an attack. Immune memory cell formation increases during active attacks and decreases as the attack intensity diminishes. The final risk value is determined based on both antibody cell concentration and the evaluation of the attack. The authors used data from a Bitcoin dusting attack in order to show that the proposed method had the capability to rapidly and precisely detect attacks, while concurrently evaluating the real-time risk of various users being attacked.

4.1.5. Association Analysis

A model to address cyber risk in a dynamic way for ICSs, based on association analysis, was recommended by Qin et al. [39]. The model consists of two main components: probability inference and risk quantification. In the first part, system knowledge (description of the system) along with historical security data are used to construct an association network, which is the first input to probability inference component. In the second part, state variables (crucial assets of the ICT system) are mined together to create the association matrix. The aforementioned process is described as the offline stage. In the online stage, real-time data from the IDS are fed to the probability inference (second input) in order to predict the probabilities of the system being attacked. The output of the probability inference is fed to the risk quantification matrix and combined with the association matrix in order to produce the final output (system's risk). An association network is used to describe the association matrix, which consists of three different layers of nodes (vulnerability layer, host layer, state variable layer). A maximum likelihood estimation is used to create conditional probabilities inside each layer. A case study was carried out by the authors on a coupling tanks control system which showed that the model is able to adjust the system's risk in real time when the attack evidence from the IDS is increased.

4.2. Mathematical Model Methods

Models in this category utilise mathematical equations as their primary analysis method.

An automated risk quantification approach for computing infrastructures was suggested by Awan et al. [40]. The risk score is defined as a product of:

- conditional probability of threat, which is calculated based on real-time traffic logs extracted from the IDS over a specific time period;
- evaluation of the severity of each threat from the administrator;
- a constant weighting factor which ensures that threats with higher severity would always have higher impacts (compared with threats with lower severity).

The authors tested their model using the seven most frequently occurring threats, which were found in the collected log sample, to show that values of the specific threats in the proposed model were different compared to values in other approaches, such as snapshots, which only represented the value of the threat at a specific time slot. Their model also provided a clear picture about pre- and post-variation trends in threats. They concluded that their model can help a network administrator to evaluate potential threats effectively.

A similar framework was introduced by Awan et al. [41] to calculate the risk score of a specific host on the network based on the software running on it. This framework uses a formula which takes into consideration the conditional probability of a threat, which is calculated from real-time data extracted from the IDS, the severity of the specific threat, and a weighting factor (from the administrators' evaluation), in order to calculate the risk score quantitatively for a specific time period. By using real-time logs, the authors proved that the risk associated with different software applications fluctuated over time.

A model to quantify the risk of network's vulnerabilities was proposed by Shu-Lee et al. [42]. The model considers how a node is exposed to an untrusted network (danger zone), the applied security mechanisms, and the CVSS values of all vulnerabilities at a specific host, in order to calculate the adjusted vulnerability score for this host. The final risk of a host is the combination of the adjusted vulnerability of this host and the adjusted vulnerabilities values of its neighbours. The total risk of the network is calculated by aggregating the risk of each host. The authors used a network simulation to prove that the total risk of the network was reduced much more by eliminating the top vulnerabilities ranked by their model compared to the elimination of the top vulnerabilities ranked by the CVSS.

Two almost similar models were presented by Hong et al. [43] and by Qiao et al. [44] for risk calculation. The first model applies on "energy internet infrastructure" and the second on a computer network. Both of them depend on:

- Asset identification, which is based on experts' opinions.
- Estimation of the dynamic threat, which is based on the rolling mechanism algorithm, according to which a dynamic threat value is calculated based on historic past events, similar to conditional probability.
- Vulnerability identification and scoring, for example, based on CVSS.
- Security relations between assets, which depend on the dependency structure matrix (DMS) technique. According to DSM theory, there are three types of dependency relationships:
    1. Parallel relationship: the functions of asset A do not affect asset B.
    2. Sequential relationship: the functions of asset A affect asset B, but the functions of asset B do not affect the function of asset A.
    3. Coupled relationship: the functions of asset A and asset B depend on each other.
- Overall risk estimation, which is based on the propagation or conduct effect.

Both models illustrated their proposed approach with an example.

Tweneboah-Koduah et al. [45] proposed a model to address risk dynamically in CI environments (such as the energy sector and its supporting technologies), based on causal-loop diagrams, which are used to describe interdependencies between systems' key variables. Their model is based on eight vectors:

1. System characterisation—environment to be assessed.
2. Asset identification—critical assets to be protected, their value, container, and custodian.
3. Threat analysis based on the system's surroundings.
4. Vulnerability analysis—the system's overall vulnerability and critical components which are vulnerable.
5. Threat–vulnerability pair (TVP)—matching a threat to a vulnerability.
6. Control analysis—effectiveness of current counter-measures.
7. Likelihood, defined as the probability of a threat to exploit a vulnerability of an asset, also taking into account the available counter-measures, which are graded based on their effectiveness.
8. Impact analysis, which is proportional to the value of an asset.

Simulation results showed that a system's security risk exposure depends on the complexities of infrastructure interdependencies and the applied counter-measures.

A model which is based on an ontology was presented by Vega-Barbas et al. [46]. The model collects information about assets and threat events for a specific administrative domain in order to evaluate them and present them by utilising an ontology language (OWL). In addition, the model uses a semantic reasoner (SWRL) in order to create security-related rules and to calculate the risk of a specific device or an operating system for a specific asset. The model uses simple equations to calculate the total risk of the respective administrative domain. The authors conducted a case study to show that their model is able to calculate the total risk in real time and that this risk depends on the number of threats.

Wang et al. [47] developed a fuzzy fractional differential equation-based method for dynamic real-time network security risk detection. Accordingly, a quantitative network risk model based on antibody concentration is applied in order to assess the risk. A tolerance method is used in order for the system's false positive rate to be reduced. The authors carried out an experiment in a network security attack and defence laboratory, using 40 computers and simulating 20 kinds of attack, to prove that their proposed model can quantitatively analyse the network's current security state in real time.

Xiong et al. [48] introduced a model based on a dynamic offensive/defensive game in order to evaluate quantitatively systems' risk at CPSs. The authors used equations to describe both the attacker's and defender's actions. The model considers constraints on both sides, such as the quantity of resources available, their distribution, cost effectiveness, and the number of attacked nodes. The model is built based on the logic that both the attacker and the defender try to maximise their benefits by adjusting their resource allocation. Simulations showed that their success depends on their resource allocation strategy.

A different approach for DRA calculation in fog computing was presented by Feng et al. [49]. More specifically, the authors proposed a model composed of three entities: a fog computing provider, an attacker, who belongs to an APT (advanced persistent threat) group, and a cyber insurer. The model shows that in order for the fog provider to prevent potential losses due to successful cyber attacks, a dynamic subscription to the cyber insurer for each fog node is necessary. The model uses mathematical formulas to calculate the probability of a successful APT attack/defence and the expected payoffs accordingly.

A model addressing cybersecurity-related risks in nuclear power plants was recommended by Vaddi et al. [50]. The model employs mathematical formulas and equations to calculate the system's state at any given time, along with computing the expected rewards for game theory-based cyber attack modelling, providing a quantitative approach to risk assessment.

Liu et al. [51] suggested a quantitative and DRA framework aimed at analysing threats and vulnerabilities in AC/DC hybrid transmission systems under coordinated physical-cyber attacks with the use of CVSS scoring. In the proposed framework, the actions of the defender and the attacker are mathematically formulated to determine their optimal strategies. The dynamic game theory is employed to show the interactions between the two aforementioned parties, where the attacker's goal is to maximise their impact on the system, and the defender tries to minimise the potential damage caused by attacks. The authors conducted case studies using a modified IEEE 14-node AC/DC hybrid test system, demonstrating how defence and attack strategies affect the system's functionality under coordinated attacks. In addition their findings revealed that false data injection (FDI) attacks pose a great threat to AC/DC hybrid systems.

Yan et al. [52] proposed a DRA model for CPSs. The model assesses the physical consequences that can be caused in a SCADA system by cyber attacks quantitatively. The CVSS scoring is used to estimate the severity and exploiting probability of software vulnerabilities (SVs). The model takes into account various attributes such as time, the attacker's characteristics, network security defence mechanisms, and propagation, utilising mathematical formulas in order to assess the probability of exploiting different possible attack paths. The effectiveness of the model was validated through simulations on modified IEEE 14-bus and 118-bus systems. Additionally, the model identifies high-risk substations within the CPS network.

4.3. Unclassified

This category includes models that do not fit into any of the aforementioned categories.

Naumov et al. [7] proposed a DRA framework (in an initial version) using system dynamics to understand how the vectors of risk and the exposure of organisations to these risks changes over time, based on casual-loop diagrams (CLDs).

Rao et al. [53] utilised cumulative distribution functions (CDFs) in order to model the normal behaviour of a medical device which is used to quantify the probability of a security threat in real time. In this way, the model detects deviations from normal executions and they estimate the presence of a threat which affects each operation. Each component is assigned an initial risk value based on its criticality. When a threat is detected and the risk value exceeds the threshold, the mitigation measures are applied. Medical devices of this kind are considered complex CPS. A smart-connected pacemaker case study illustrated the effectiveness of the proposed approach.

A dynamic impact assessment approach for ICS was presented by Li et al. [54]. The system abstracts an asset alongside with its properties, and then it uses function and performance properties to categorise assets into five categories (based on the functionality of an asset inside the system), and then the component-level asset model is formed. A system-level asset model is formed based on the interactive relationships amongst assets. In addition, the system uses as input information originating from the IDS, which is injected into the asset model (component and system) in order to form impact propagation analysis. A combination of the knowledge from the asset, attack, and hazardous incident domains is analysed in order to form the quantification of impact. The latter is combined with the output of the impact propagation analysis to produce the total impact. Simulations on a simplified chemical process control system showed the ability of the proposed approach to predict dynamically and in a timely fashion the impact of a cyber attack.

A qualitative risk assessment method which could be used by all stakeholders was introduced by Erdogan et al. [55]. The method is composed of three steps:

1. Creation of a security risk model with the use of CORAS, which contains indicators about a system's vulnerabilities, suspicious events, and potential consequences on business processes. CORAS is a method which can be used for risk analysis.
2. Development of the security risk assessment algorithm with the use of CORAS and DEXi to create the attributes and relationships of the system and to calculate the risk based on them. DEXi is a programme that is used for multi-attribute decision making. The specific algorithm facilitates the continuous risk assessment process.
3. Validation of the results.

The authors applied the proposed method to develop CORAS models and corresponding DEXi models for 10 common cyber attacks and concluded that their method is easy to use and it can be easily adopted by security and risk practitioners.

Armenia et al. [56] recommended a new dynamic model in order to assess the cybersecurity risk in SMEs, which is named SMECRA (SME cyber risk assessment), and it is mostly based on the Italian cybersecurity framework for cybersecurity and data protection [57]. The model considers various interdependent aspects addressed by NIST and their relationship over time in order to create stocks and flows to describe the as-if (current) situation of the system. Stocks and flows are interconnected and a change to one of them may lead to a bigger or smaller change to another (stock or flow). The CLD approach is used to map relationships between elements. Then, the model utilises a snapshot survey (the paper contains 15 essential controls for SMEs) with the combination of a weighting system to model the relative importance of its question with respect to the category it belongs. More than 50 equations are used to describe relationships between variables in the system and to produce the respective results (e.g., expected damage loss from a successful attack). The authors used two real companies as references, one with a low cybersecurity posture and one with high. Simulation results showed that even when the second company operated in a high-threat environment and the first in a low, the second company was much more resistant to cyber attacks, and hence expected damage loss from a cyber attack was lower.

Gonzales-Granadillo et al. [58] proposed AMBIENT, a model which is capable of handling both cyber and privacy risks within the same toolkit. The part that handles the cyber risk is the cyber risk assessment component, which gathers large volumes of cybersecurity-related data in real time and correlates them in order to assess the risk. The CORAS tool is used for graphical risk analysis, DEXi and fuzzy logic are used to produce qualitative results in terms of risk (likelihood, impact), while the R programming language is used to produce quantitative reports in monetary terms. Afterwards, the appropriate counter-measures are proposed in order to reduce the risk. The model was tested using a real test-bed scenario considering the working environment of a hospital from the ICT perspective. The results of the test showed that the model was able to quantify risk in monetary terms, and also to provide effective mitigation measures. The efficacy of the proposed measures was validated by experts.

Liatifis et al. [59] presented a framework which enhances the cybersecurity of EPES infrastructure. The framework relies on a security information and event management system (SIEM) that detects and correlates diverse security events, utilising comprehensive input data from various sources such as IDSs and firewalls. Each security event is assigned a risk value derived from a predefined quantitative formula involving asset value, event priority, and event reliability. The RA module examines new energy-related cyber threats and vulnerabilities from various public repositories, such as CTI sharing modules and CVSS scores to compute risk values.

Rao et al. [60] recommended a risk evaluation methodology for life-critical embedded devices, including medical devices, named FIRE, which integrates both static and dynamic RA in order to produce quantitative results. This methodology also relies on CDFs which are used to define the static risk thresholds. The dynamic risk is based on the run-time risk determined by comparing the actual risk in each mode to the static risk thresholds. FIRE's effectiveness was demonstrated through a case study, demonstrating successful threat mitigation and achieving a 0% false-positive rate.

Semertzis et al. [61] proposed a quantitative DRA model for cyber attacks on CPSs, with a specific focus on power systems. The authors use probability distribution along with CDFs to model the skills of attackers, employ NVD data to identify vulnerabilities, and examine potential attack paths using attack graphs. The simulations showed that certain cyber attacks could cause serious impact on power systems, such as cascading failures and blackouts.

Hu et al. [62] introduced a dynamic risk propagation and evaluation approach, which predicts attacks and quantitatively analyses system's risk. This approach utilises a "partitioned cellular automata" model to handle variations amongst different parts of the CPSs. In addition, it takes as input information originating from an IDS. It comprises two modules: the offline, which is used for creating risk analysis models considering the impact of attacks; and the online, for the prediction of risk propagation and quantification of the risk. The effectiveness of the proposed approach was validated through a case study utilising a co-simulation platform that included communication control and electrical power networks.

A tool named CyberSAGE was presented by Temple1 et al. [63]. It consists of three main inputs:

1. The system architecture, which is represented as a graph of interconnected components along with device specifications and mitigation properties.
2. The malactivity scenario, which describes the attacker's steps to compromise the system.
3. The adversary profile, which provides details regarding the attacker's skills, resources, access, and intentions.

The rule engine then combines the aforementioned inputs to generate a security graph which demonstrates how the attack steps in the malactivity scenarios can be applied to the system architecture in order for the attackers to achieve their goal. An evaluation of the tool was conducted on communication systems on two railway lines to illustrate the tool's application and validity.

Riesco et al. [64] proposed a model that connects two different domains, the cyber threat intelligence (CTI) domain, which acts in real time, and the RA domain, which acts periodically based on collected data. This model proposes the use of web ontology language (OWL) to capture real-time CTI information in OWL format and feeds them into the DRA ontology. Then, a semantic web rule language (SWRL) is used to create rules based on business logic. Finally, the Pellet incremental reasoner is applied in order to automate the risk discovery process based on the collected CTI data and the SWRL rules. The model was tested simulating a real-world watering-hole attack in a cybersecurity organisation and managed to update risk values based on collected information.

Collen et al. [65] suggested a DRA framework (DRAF) for IoT-enabled environments, focusing on the smart home domain. This model utilises an ontology-based approach to model risk assessment in order to provide a risk scoring model. The DRAF incorporates data from multiple sources along with reports from various strategies, adapting risk scores using expert weight values and feedback from end-users to produce quantitative results. The framework was validated through real-life trials, demonstrating its ability to detect risks and provide mitigation advisories in a timely manner.

5. Discussion

In this paper, we analysed 50 DRA models, and we classified them into three distinct categories based on the underlying technique or primary analysis method they utilised. The vast majority (24/50) of the examined models employ AI/ML techniques as their primary analysis method. This finding agrees with Erdogan et al. [13], who pointed out that RA processes should adopt AI techniques in order to be able to identify and estimate cyber risk in high-threat environments. Another noteworthy finding is the presence of three models categorised as "unclassified", that employ CDFs in conjunction with other techniques to construct their DRA models.

5.1. Primary Analysis Method

Regarding the specific AI/ML primary analysis method, it is clear from our research that the majority (11/24) of the examined models adopt Bayesian networks. The second most used method of this category is attack-trees. This finding partially agrees with the results from Erdogan et al. [13] who found out that Bayesian networks along with neural networks were the two most used methods. Tables 4 and 5 present the aforementioned findings, also providing the answer to RQ1. In further detail, Table 4 illustrates the distribution of models across each domain (vertical axis) in relation to the primary methods employed by those models (horizontal axis). Similarly, Table 5 presents the results focusing on the specific analysis methods from the AI/ML category and their corresponding domains.

Table 4. Primary analysis method applied to each domain.

Domains	AI/ML	Mathematical	Unclassified
ICT	9	6	6
ICS	13	7	6
SC	2		1

Table 5. AI/ML primary analysis methods applied to each domain.

Domains	Bayesian Networks	Attack Trees	Neural Networks	Artificial Immunity	Association Analysis
ICT	4	3		2	
ICS	7	3	2		1
SC		1	1		

5.2. Domains and Application Areas

Another significant outcome of our analysis pertained to the domains where the proposed DRA models were applied (RQ2). Utilising a grouping technique, we sought to investigate three distinct domains. These were the SC domain, the ICT domain, and the ICS domain. More specifically, 3 DRA models (6%) were applied in the SC domain, 21 DRA models (42%) were applied in the ICT domain, and 26 DRA models (52%) were applied in the ICS domain. The obtained result was anticipated, given the inherent significance of the ICS domain in the context of cybersecurity. Moreover, the crucial functions performed by ICS and the potential severe consequences of cyber attacks, which could even result in fatalities, naturally drive significant attention towards bolstering cybersecurity measures for ICS systems. The successful execution of a cyber attack on an ICS infrastructure could indeed lead to catastrophic outcomes. Hence, there exists a compelling rationale for intensifying efforts in detecting and mitigating cyber threats specifically targeting the ICS domain.

5.3. Quantitative or Qualitative Methods

Regarding our third research question (RQ3), 42 out of the 50 models seem to apply quantitative risk analysis. Four of the examined models can be characterised as hybrid since they use both quantitative and qualitative risk analysis. All models currently employed within the ICS domain utilise quantitative risk analysis, with the exception of one. This result agrees with Qin et al. [39], who claimed that quantitative risk analysis methods are gaining the majority of attention in the ICS domain. Additionally, the vast majority of the examined models applied in the ICT domain currently utilise a quantitative risk analysis method, which is the preferred RA method in IT security management [66]. Four models cannot be classified in terms of the quantitative or qualitative risk analysis method. The results are summarised in Table 6.

Table 6. Quantitative vs. qualitative methods.

Methods	**Quantitative**	**Hybrid**	**Qualitative**	**Cannot Be Classified**
# DRA models	42	4	1	3

Models that utilise quantitative risk analysis collect data from their environment and analyse them using a predefined method [39]. Quantitative methods provide a more accurate reflection of the system status than qualitative [67]. Qualitative RA methods provide subjective results and lack precision [68]. In addition, the output of quantitative risk analysis is measurable and more accurate compared to qualitative [39]. Therefore, DRA, apart from the dynamic response to emerging threats, can also contribute to the use of more objective and measurable outputs in risk assessment.

5.4. Input Data

Regarding the input that the proposed models use (RQ4), many of them collect and use the system's information (system's knowledge) originating from the environment in which they operate, such as network topology, assets, dependencies, and relationships between nodes, the system's functions, and services. The component that is used the most (16/50) is the IDS, which provides the DRA models with real-time data. In addition, 22 of the examined models use some kind of vulnerability-related data as input. These data originate from local vulnerability databases or inventories, or from open sources (NVD, CVSS) used for evaluating and scoring known vulnerabilities, or are the output of a vulnerability scanner.

Another noteworthy remark regarding the input data utilised by the examined models is that 13 of them incorporate experts opinions and estimations from system administrators. Before being fed into the model, this type of data are integrated with information sourced from objective outlets like IDS, historical data, or system knowledge. Most of the examined DRA models use a combination of input data, for example, system knowledge and data from an IDS. This finding aligns with the assertions of Berestov et al. [69], who emphasised the importance of a system's capacity to collect and correlate diverse data types to facilitate process automation. This is particularly relevant to DRA models, as they can effectively incorporate and utilise such processes. Additionally, it is in line with the perspectives put forth by Ralston et al. [70], who highlighted the necessity of synthetic data (multiple sources) for the analysis of cybersecurity risk through most quantitative methods. Furthermore, the result is consistent with the observations made by Larriva et al. [71], who emphasised the potential benefits of utilising the substantial volume of data generated by organisations and companies to discover emerging threats in RA methodologies.

5.5. Maturity Level

Regarding our study's last research question, about the maturity level of the proposed methods (RQ5), we applied grouping once again and adopted three different levels of maturity. Level 3 maturity applies to those models that present relative simulations, case studies, and experiments. Models classified under this category showed the highest maturity level since they were proven to be efficient and ready to be applied. Level 2 maturity applies to models which presented examples and proof of concepts to demonstrate their functionality. Level 1 maturity models were those which did not provide any of the above. Table 7 presents the number of models that belong to each of the aforementioned categories. In total, 46 models validated their proposed approach, although there is a difference between level 3 and level 2 with respect to maturity, since models categorised in level 2 present the effectiveness of the proposed model with a more simple and less complex example compared to models that were categorised under level 3.

Table 7. Number of models to each maturity Level.

Maturity Level	**3**	**2**	**1**
# DRA models	38	8	4

5.6. Limitations of DRA Models and Challenges

Our research revealed a noteworthy limitation among the majority of proposed models, i.e., their deficiency in proactive capabilities due to the limited integration of CTI-related information. DRA models primarily focus on real-time data concerning ongoing activities within an organisation's environment, typically sourced from systems like an IDS. Embedding proactive functionality within these DRA frameworks holds substantial potential for enhancing organisations' security postures by enabling proactive threat preparedness. The significance of CTI knowledge has been underscored as a pivotal instrument for proactive cyber risk mitigation [72]. By integrating relevant CTI data, such as information on recently discovered vulnerabilities and emerging threats, DRA models are capable of proactively reassessing the existing risk level.

A similar limitation illuminated by our research reveals that a significant majority of DRA models do not harness historical data or incorporate past events into their analyses; instead, they predominantly concentrate on monitoring ongoing activities. This dearth of historical context within DRA modelling can hinder their ability to derive valuable insights from past incidents, potentially leading to a less comprehensive understanding of threat dynamics.

Our research substantiates that DRA models rely on a wide range of data sources for input. Distributed data fusion, a process involving the integration and analysis of information from diverse data sources, emerges as a pivotal method for achieving a comprehensive and precise understanding of a given environment or system. Within the domain of DRA models, the attainment of real-time and precise results assumes paramount significance. The utilisation of data fusion techniques has demonstrated effectiveness in various applications. The LLPTE scheme [73] can improve DRA models to amalgamate disparate, inconsistent, uncertain, or even redundant data. Additionally, this framework for threat intelligence extraction and fusion [74] can provide DRA models assistance in correlating and unifying data. By employing these techniques, DRA models can enhance the quality of input data assimilated, leading to more consistent and accurate outcomes.

In addition to data fusion, the incorporation of trust evaluation techniques can further enhance the accuracy and precision of fused results [73]. Trust evaluation techniques assume an even more critical role when contemplating the deployment of DRA models within a zero trust environment (ZTA). In such a context, DRA models are tasked with processing substantial volumes of data, serving as input for real-time risk-based decision making. Given the diverse array of data sources, including untrusted and even potentially malicious ones, the utilisation of trust evaluation techniques by DRA models can enhance their trustworthiness. Trust evaluation methods, such as TFL-DT [75], have demonstrated their efficacy in identifying malicious users and should be adopted by DRA models. In addition, trust evaluation models can also be used not only to identify malicious users (data sources) but also to quantitatively evaluate the source of information [76] in order to increase even further the accuracy and preciseness of the data used as input by DRA models.

Future DRA models should prioritise the development of effective operations within a ZTA environment, giving due consideration to both data fusion and trust evaluation schemes. These techniques will enhance the quality of input data, a significance that becomes even more pronounced in a ZTA environment, enabling DRA models to produce accurate and precise results while upholding the imperative of delivering real-time outcomes.

5.7. Study's Limitations

Not all models provided relative information about the necessary resources in order to operate efficiently and, hence, we were not able to provide an analysis on this subject. In addition, few of the proposed approaches proved their effectiveness by providing relative evaluations without utilising any of the categories we used in the maturity levels classification, and we had to match their respective evaluation to the most suitable one of our categories. Finally, no adequate information was provided by all methods with regards to the actual risk assessment parameters they contribute to, i.e., asset impact, threat likelihood, vulnerability criticality, risk calculation and, therefore, we could not clarify them under this categorisation.

6. Conclusions and Future Work

From our study it was clear that most of the proposed DRA models in the area of cybersecurity adopted AI and ML techniques as their primary analysis method. Among all of the techniques in this category, Bayesian networks were the most used. Furthermore, predicated upon our analysis, it becomes evident that the domain of ICS garners the majority of attention concerning DRA models within the realm of cybersecurity. The vast majority of the examined models seemed to have adopted quantitative risk analysis. DRA models utilise objective data sources derived from their respective environments, with the most frequently used component being the IDS. Furthermore, a notable proportion of these models integrate various types of vulnerability-related data as part of their input. Most of the examined models validated their approach providing a relative case study or simulation example, thereby demonstrating a commendable level of maturity in their approach.

Our future work will focus on the development of a DRA model that harnesses information originating from its environment, akin to the aforementioned models. This approach will be augmented by the assimilation of insights from CTI, thereby endowing our model with the capability to exhibit not only reactive but also proactive behaviour. We hold a firm conviction that the integration of CTI into DRA models will significantly enhance their overall effectiveness, empowering them with the capability to proactively respond to emerging threats.

Prospective research endeavours can employ this literature review as an inaugural cornerstone, facilitating the attainment of a robust comprehension concerning DRA models within the domain of cybersecurity. We earnestly advocate for forthcoming studies to make reference to Table A1. This tabular representation encapsulates all the aforementioned findings in a systematic and analytical manner, offering conclusive insights into the five research inquiries delineated in this manuscript.

Author Contributions: Conceptualisation, K.R.; methodology, K.R.; investigation, P.C.; formal analysis, P.C.; writing—original draft preparation, P.C.; writing—review and editing, K.R.; visualisation, P.C.; project administration, K.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

ADS	Anomaly detection system
ADTs	Attack–defence trees
AI	Artificial intelligence
ANNs	Artificial neural networks
APT	Advanced persistent threat
CDFs	Cumulative distribution functions
CI	Critical infrastructures
CLDs	Casual-loop diagrams
CPSs	Cyber-physical systems
CR	Composite risk
CTI	Cyber threat intelligence
CVE	Common vulnerabilities and exposures database
CVSS	Common vulnerability scoring system
DAG	Direct acyclic graph
DBRMS	Dynamic risk management response system
DRA	Dynamic risk assessment
DRAF	Dynamic risk assessment framework
DSM	Dependency structure matrix
EMFM	Extended multilevel flow model
EPESs	Electrical power and energy systems
ER	Elementary risk
FAHP	Fuzzy analytic hierarchy process
HD-NSA	Hierarchical division negative selection algorithm
HMM	Hidden Markov model
HPC	High-performance computing
ICSs	Industrial control systems
ICT	Information and communications technology
IDS	Intrusion detection system
IODEF	Incident object description exchange format
IPSs	Industrial productions systems
LPPTE	Lightweight privacy-preserving trust evaluation
ML	Machine learning
NVD	National vulnerability database
OWL	Web ontology language
RA	Risk assessment
RQ	Research question
SC	Smart city
SIEM	Security information and event management
SMECRA	SME cyber risk assessment
SMEs	Small and medium-sized enterprises
SQL	Structured query language
SV	Software vulnerabilities
SWRL	Semantic web rule language
TVP	Threat vulnerability pair
ZTA	Zero trust architecture

Appendix A

Table A1. Research papers included in the review and their characteristics.

Author	Year	Domain	Risk Analysis	Input	Maturity
Bayesian Networks (Section 4.1.1):					
Cam et al. [16]	2013	ICT	Quantitative	IDS + NVD + network of cyber assets	example
Cam et al. [17]	2015	ICT	Quantitative	IDS + vulnerability scanner + CVSS	simulation
Henshel et al. [18]	2016	ICT	Quantitative	experts' opinion	example
Zhang et al. [19]	2016	ICS	Quantitative	attack evidence (IDS) + anomaly evidence + system's knowledge (vulnerabilities related data included)	simulation
Huang et al. [20]	2017	ICS	Quantitative	IDS + vulnerability scanner/CVE + historical data/experts' opinion	simulation
Peng et al. [21]	2018	ICS	Quantitative	security Knowledge DB (vulnerabilities related data included) + real-time attack evidence	simulation
Zhu et al. [22]	2018	ICS	Quantitative	attack evidence (IDS) + system's knowledge + control strategies	simulation
Zhang et al. [23]	2018	ICS	Quantitative	attack evidence (IDS) + anomaly evidence + system's Knowledge	simulation
Zhu et al. [24]	2019	ICS	Quantitative	IDS	simulation
Debneath et al. [25]	2022	ICT	Quantitative	system's knowledge + CVSS + IDS	experiment
Zhou et al. [26]	2022	ICS	Quantitative	network topology + CVSS	simulation
Attack Trees (Section 4.1.2):					
Kotenko et al. [27]	2013	ICT	Hybrid	IDS + CVSS + network topology data	
Ji et al. [28]	2013	ICS	Quantitative	system's vulnerabilities	case study
Abraham et al. [29]	2015	ICT	Quantitative	CVSS + network model + services on each host	case study
Kanoun et al. [30]	2016	ICT	Quantitative	vulnerability DB + system topology + detrimental events	case study
Gonzalez et al. [31]	2018	ICS	Quantitative	system's knowledge + vulnerability inventory	case study
Wu et al. [32]	2018	ICS	Quantitative	security knowledge of the system (vulnerabilities related data included)	simulation
Ivanov et al. [33]	2020	SC	Quantitative	penetration test/security scanner output	example
Neural Networks (Section 4.1.3):					
Fu et al. [34]	2017	ICS	Hybrid	big data analysis by experts	
Ashiku et al. [35]	2020	ICS	Quantitative	system's knowledge + network traffic dataset	simulation
Krundyshev et al. [36]	2020	SC	Quantitative	synthetic data	simulation
Artificial Immunity (Section 4.1.4):					
Li et al. [37]	2018	ICT	Quantitative	IDS	experiment
He et al. [38]	2021	ICT	Quantitative	asset-related data of cyber attacks	experiment
Association Analysis (Section 4.1.5):					
Qin et al. [39]	2021	ICS	Quantitative	IDS + historical data + system's knowledge	case study
Mathematical model methods (Section 4.2):					
Awan et al. [40]	2015	ICT	Quantitative	IDS + administrators' estimations	experiment
Awan et al. [41]	2015	ICT	Quantitative	IDS + administrators' estimations	experiment
Shu-Lee et al. [42]	2015	ICT	Quantitative	topological data + applied security mechanism + CVSS	simulation
Hong et al. [43]	2017	ICS	Quantitative	CVSS + experts' opinion + historical data	example
Qiao et al. [44]	2018	ICT	Quantitative	experts' opinion + historical data	example
Tweneboah-Koduah et al. [45]	2018	ICS	Quantitative	experts' evaluation	simulation
Vega-Barbas et al. [46]	2019	ICS	Quantitative	assets + threats events	case study
Wang et al. [47]	2020	ICT	Quantitative	current and historical network security data	simulation
Xiang et al. [48]	2020	ICS	Quantitative	constrain conditions on both sides	simulation
Feng et al. [49]	2021	ICT	Quantitative	resources of attacker and fog computer provider	example
Vaddi et al. [50]	2022	ICS	Quantitative	system's knowledge + abnormal events	proof of concept

Table A1. *Cont.*

Author	Year	Domain	Risk Analysis	Input	Maturity
Liu et al. [51]	2023	ICS	Quantitative	attackers'/defenders' strategies + CVSS	case study
Yan et al. [52]	2023	ICS	Quantitative	system's knowledge + CVSS	simulation
Unclassified (Section 4.3):					
Naumov et al. [7]	2016	ICT			
Rao et al. [53]	2017	ICS	Quantitative	run-time metrics	case study
Li et al. [54]	2018	ICS	Quantitative	IDS + Knowledge from related domains	simulation
Erdogan et al. [55]	2018	ICT	Qualitative	system's vulnerabilities + suspicious events + potential consequences on business process	example
Armenia et al. [56]	2021	ICT	Hybrid	snapshot survey	case study
Gonzales-Granadillo et al. [58]	2021	ICT	Hybrid	vulnerabilities + business Indicators + system's data	case study
Liatifis et al. [59]	2022	ICS		SIEM security logs	
Rao et al. [60]	2022	ICS	Quantitative	run-time metrics	case study
Semertzis et al. [61]	2022	ICS	Quantitative	known vulnerabilities + skills of attacker	simulation
Hu et al. [62]	2023	ICS	Quantitative	IDS	case study
Temple et al. [63]	2023	ICT	Quantitative	system's architecture + mal-activity scenario + adversary profile	case study
Riesko et al. [64]	2019	ICT		system's knowledge	simulation
Collen et al. [65]	2022	SC	Quantitative	system's knowledge + strategies + experts' opinion	case study

References

1. Ross, R.; McEvilley, M.; Oren, J.C. *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*; Technical Report NIST SP 800-160v1; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018; Volume 1. [CrossRef]
2. *ISO Guide 73:2009*; Risk Management—Vocabulary. ISO: Geneva, Switzerland, 2009.
3. Joint Task Force Interagency Working Group. *Security and Privacy Controls for Information Systems and Organizations*, 5th ed.; Technical report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020. [CrossRef]
4. *ISO 31000:2018*; Risk Management—Guidelines. ISO: Geneva, Switzerland, 2018.
5. Joint Task Force Transformation Initiative. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*; Technical Report NIST SP 800-37r2; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018. [CrossRef]
6. Linkov, I.; Anklam, E.; Collier, Z.; DiMase, D.; Renn, O. Risk-based standards: Integrating top-down and bottom-up approaches. *Environ. Syst. Decis.* **2014**, *34*, 134–137. [CrossRef]
7. Naumov, S.; Kabanov, I. Dynamic framework for assessing cyber security risks in a changing environment. In Proceedings of the 2016 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 2–4 November 2016; pp. 1–4.
8. Sánchez-Zas, C.; Villagrá, V.A.; Vega-Barbas, M.; Larriva-Novo, X.; Moreno, J.I.; Berrocal, J. Ontology-based approach to real-time risk management and cyber-situational awareness. *Future Gener. Comput. Syst.* **2023**, *141*, 462–472. [CrossRef]
9. Cherdantseva, Y.; Burnap, P.; Blyth, A.; Eden, P.; Jones, K.; Soulsby, H.; Stoddart, K. A review of cyber security risk assessment methods for SCADA systems. *Comput. Secur.* **2016**, *56*, 1–27. [CrossRef]
10. Eckhart, M.; Brenner, B.; Ekelhart, A.; Weippl, E. Quantitative security risk assessment for industrial control systems: Research opportunities and challenges. *J. Internet Serv. Inf. Secur.* **2019**, *9*, 52–73. [CrossRef]
11. Jiang, M.; Li, M.; Cai, M.; Fang, Y. Research on Key Technologies of Network Security Multidimensional Dynamic Risk Assessment. *J. Phys. Conf. Ser.* **2021**, *1744*, 032189. [CrossRef]
12. Lopez, D.; Pastor, O.; Garcia Villalba, L. Dynamic Risk Assessment in Information Systems: State-of-the-Art. In Proceedings of the 6th International Conference on Information Technology, Jordan, Aman, 8–10 May 2013; pp. 8–10.
13. Erdogan, G.; Garcia-Ceja, E.; Hugo, A.; Nguyen, P.H.; Sen, S. A Systematic Mapping Study on Approaches for AI-Supported Security Risk Assessment. In Proceedings of the 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 12–16 July 2021; pp. 755–760. [CrossRef]
14. Barrett, M.; Marron, J.; Pillitteri, V.Y.; Boyens, J.; Quinn, S.; Witte, G.; Feldman, L. *Approaches for Federal Agencies to Use the Cybersecurity Framework*; Technical report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2021. [CrossRef]
15. Lopez, D.; Pastor, O.; Garcia Villalba, L. Data model extension for security event notification with dynamic risk assessment purpose. *Sci. China Inf. Sci.* **2013**, *56*, 1–9. [CrossRef]

16. Cam, H.; Mouallem, P. Mission assurance policy and risk management in cybersecurity. *Environ. Syst. Decis.* **2013**, *33*, 500–507. cited By 3. [CrossRef]
17. Cam, H. Risk assessment by dynamic representation of vulnerability, exploitation, and impact. In *Proceedings of the Cyber Sensing 2015*; Ternovskiy, I.V., Chin, P., Eds.; International Society for Optics and Photonics, SPIE: Bellingham, WA, USA, 2015; Volume 9458, p. 945809. [CrossRef]
18. Henshel, D.; Alexeev, A.; Cains, M.; Rowe, J.; Cam, H.; Hoffman, B.; Neamtiu, I. Modeling cybersecurity risks: Proof of concept of a holistic approach for integrated risk quantification. In Proceedings of the 2016 IEEE Symposium on Technologies for Homeland Security (HST), Waltham, MA, USA, 10–11 May 2016; pp. 1–5. [CrossRef]
19. Zhang, Q.; Zhou, C.; Xiong, N.; Qin, Y.; Li, X.; Huang, S. Multimodel-Based Incident Prediction and Risk Assessment in Dynamic Cybersecurity Protection for Industrial Control Systems. *IEEE Trans. Syst. Man Cybern. Syst.* **2016**, *46*, 1429–1444. [CrossRef]
20. Huang, K.; Zhou, C.; Tian, Y.C.; Tu, W.; Peng, Y. Application of Bayesian network to data-driven cyber-security risk assessment in SCADA networks. In Proceedings of the 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, VIC, Australia, 22–24 November 2017; pp. 1–6. [CrossRef]
21. Peng, Y.; Huang, K.; Tu, W.; Zhou, C. A Model-Data Integrated Cyber Security Risk Assessment Method for Industrial Control Systems. In Proceedings of the 2018 IEEE 7th Data Driven Control and Learning Systems Conference (DDCLS), Enshi, China, 25–27 May 2018; pp. 344–349. [CrossRef]
22. Zhu, Q.; Qin, Y.; Zhou, C.; Gao, W. Extended multilevel flow model-based dynamic risk assessment for cybersecurity protection in industrial production systems. *Int. J. Distrib. Sens. Netw.* **2018**, *14*. [CrossRef]
23. Zhang, Q.; Zhou, C.; Tian, Y.C.; Xiong, N.; Qin, Y.; Hu, B. A Fuzzy Probability Bayesian Network Approach for Dynamic Cybersecurity Risk Assessment in Industrial Control Systems. *IEEE Trans. Ind. Inform.* **2018**, *14*, 2497–2506. [CrossRef]
24. Zhu, Q.; Zhao, Y.; Fei, L.; Zhou, C. A Dynamic Decision-Making Approach for Cyber-Risk Reduction in Critical Infrastructure. In Proceedings of the 2018 IEEE 8th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), Tianjin, China, 19–23 July 2018; pp. 595–600. [CrossRef]
25. Debnath, J.K.; Xie, D. CVSS-based Vulnerability and Risk Assessment for High Performance Computing Networks. In Proceedings of the 2022 IEEE International Systems Conference (SysCon), Montreal, QC, Canada, 25–28 April 2022; pp. 1–8. [CrossRef]
26. Zhou, B.; Sun, B.; Zang, T.; Cai, Y.; Wu, J.; Luo, H. Security Risk Assessment Approach for Distribution Network Cyber Physical Systems Considering Cyber Attack Vulnerabilities. *Entropy* **2022**, *25*, 47. [CrossRef]
27. Kotenko, I.; Doynikova, E. Security metrics for risk assessment of distributed information systems. In Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), Berlin, Germany, 12–14 September 2013; Volume 2, pp. 646–650.
28. Ji, X.; Yu, H.; Fan, G.; Fu, W. Attack-defense trees based cyber security analysis for CPSs. In Proceedings of the 2016 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), Shanghai, China, 30 May–1 June 2016; pp. 693–698.
29. Abraham, S.; Nair, S. A novel architecture for predictive cybersecurity using non-homogenous markov models. In Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland, 20–22 August 2015; Volume 1, pp. 774–781.
30. Kanoun, W.; Papillon, S.; Dubus, S. Elementary risks: Bridging operational and strategic security realms. In Proceedings of the 2015 11th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), Bangkok, Thailand, 23–27 November 2015; pp. 278–286.
31. Gonzalez-Granadillo, G.; Dubus, S.; Motzek, A.; Garcia-Alfaro, J.; Alvarez, E.; Merialdo, M.; Papillon, S.; Debar, H. Dynamic risk management response system to handle cyber threats. *Future Gener. Comput. Syst.* **2018**, *83*, 535–552. [CrossRef]
32. Wu, S.; Zhang, Y.; Chen, X. Security assessment of dynamic networks with an approach of integrating semantic reasoning and attack graphs. In Proceedings of the 2018 IEEE 4th International Conference on Computer and Communications (ICCC), Chengdu, China, 7–10 December 2018; pp. 1166–1174.
33. Ivanov, D.; Kalinin, M.; Krundyshev, V.; Orel, E. Automatic security management of smart infrastructures using attack graph and risk analysis. In Proceedings of the 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, 27–28 July 2020; pp. 295–300.
34. Fu, Y.; Zhu, J.; Gao, S. CPS information security risk evaluation system based on Petri net. In Proceedings of the 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC), Shenzhen, China, 26–29 June 2017; pp. 541–548.
35. Ashiku, L.; Dagli, C. Agent based cybersecurity model for business entity risk assessment. In Proceedings of the 2020 IEEE International Symposium on Systems Engineering (ISSE), Vienna, Austria, 12 October–12 November 2020; pp. 1–6.
36. Krundyshev, V. Neural network approach to assessing cybersecurity risks in large-scale dynamic networks. In Proceedings of the 13th International Conference on Security of Information and Networks, Merkez, Turkey, 4–7 November 2020; pp. 1–8. [CrossRef]
37. Lin, P.; Yang, J.; Li, T.; Ai, L. An immune based dynamic risk control system. In Proceedings of the 2018 IEEE Symposium Series on Computational Intelligence (SSCI), Bangalore, India, 18–21 November 2018; pp. 1130–1137. [CrossRef]
38. He, J.; Li, T.; Li, B.; Lan, X.; Li, Z.; Wang, Y. An immune-based risk assessment method for digital virtual assets. *Comput. Secur.* **2021**, *102*, 102134. [CrossRef]
39. Qin, Y.; Peng, Y.; Huang, K.; Zhou, C.; Tian, Y.C. Association Analysis-Based Cybersecurity Risk Assessment for Industrial Control Systems. *IEEE Syst. J.* **2021**, *15*, 1423–1432. [CrossRef]

40. Awan, M.S.K.; Burnap, P.; Rana, O.; Javed, A. Continuous monitoring and assessment of cybersecurity risks in large computing infrastructures. In Proceedings of the 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems, New York, NY, USA, 24–26 August 2015; pp. 1442–1447.
41. Awan, M.S.K.; Burnap, P.; Rana, O. An empirical risk management framework for monitoring network security. In Proceedings of the 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, Liverpool, UK, 26–28 October 2015; pp. 1764–1771.
42. Suh-Lee, C.; Jo, J. Quantifying security risk by measuring network risk conditions. In Proceedings of the 2015 IEEE/ACIS 14th International Conference on Computer and Information Science (ICIS), Las Vegas, NV, USA, 28 June–1 July 2015; pp. 9–14.
43. Hong, Q.; Jianwei, T.; Zheng, T.; Wenhui, Q.; Chun, L.; Xi, L.; Hongyu, Z. An information security risk assessment algorithm based on risk propagation in energy internet. In Proceedings of the 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, China, 26–28 November 2017; pp. 1–6. [CrossRef]
44. Hong, Q.; Jianwei, T.; Zheng, T.; Wenhui, Q.; Xi, L.; Hongyu, Z.; Shengsheng, C. An information security risk assessment method based on conduct effect and dynamic threat. In Proceedings of the 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 24–26 November 2017; pp. 782–786. [CrossRef]
45. Tweneboah-Koduah, S.; Buchanan, W. Security risk assessment of critical infrastructure systems: A comparative study. *Comput. J.* **2018**, *61*, 1389–1406. [CrossRef]
46. Vega-Barbas, M.; Villagrá, V.; Monje, F.; Riesco, R.; Larriva-Novo, X.; Berrocal, J. Ontology-based system for dynamic risk management in administrative domains. *Appl. Sci.* **2019**, *9*, 4547. [CrossRef]
47. Wang, Z.; Chen, L.; Song, S.; Cong, P.; Ruan, Q. Automatic cyber security risk assessment based on fuzzy fractional ordinary differential equations. *Alex. Eng. J.* **2020**, *59*, 2725–2731. [CrossRef]
48. Xiong, J.; Wu, J. Construction of information network vulnerability threat assessment model for CPS risk assessment. *Comput. Commun.* **2020**, *155*, 197–204. [CrossRef]
49. Feng, S.; Xiong, Z.; Niyato, D.; Wang, P. Dynamic Resource Management to Defend against Advanced Persistent Threats in Fog Computing: A Game Theoretic Approach. *IEEE Trans. Cloud Comput.* **2021**, *9*, 995–1007. [CrossRef]
50. Vaddi, P.K.; Zhao, Y.; Smidts, C. Dynamic Probabilistic Risk Assessment for Cyber Security Risk Analysis in Nuclear Reactors. In Proceedings of the Probabilistic Safety Assessment & Management Conference—PSAM 16, Honolulu, HI, USA, 26 June–1 July 2022.
51. Liu, X.; Shi, L. A dynamic game model for assessing risk of coordinated physical-cyber attacks in an AC/DC hybrid transmission system. *Front. Energy Res.* **2023**, *10*, 1082442. [CrossRef]
52. Yan, K.; Liu, X.; Lu, Y.; Qin, F. A Cyber-Physical Power System Risk Assessment Model Against Cyberattacks. *IEEE Syst. J.* **2023**, *17*, 2018–2028. [CrossRef]
53. Rao, A.; Carreon, N.; Lysecky, R.; Rozenblit, J. Probabilistic Threat Detection for Risk Management in Cyber-physical Medical Systems. *IEEE Softw.* **2017**, *35*, 38–43. [CrossRef]
54. Li, X.; Zhou, C.; Tian, Y.C.; Xiong, N.; Qin, Y. Asset-based dynamic impact assessment of cyberattacks for risk analysis in industrial control systems. *IEEE Trans. Ind. Inform.* **2018**, *14*, 608–618. [CrossRef]
55. Erdogan, G.; Refsdal, A. A method for developing qualitative security risk assessment algorithms. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Cham, Switzerland, 2018; Volume 10694, pp. 244–259. [CrossRef]
56. Armenia, S.; Angelini, M.; Nonino, F.; Palombi, G.; Schlitzer, M. A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decis. Support Syst.* **2021**, *147*, 113580. [CrossRef]
57. Angelini, M.; Ciccotelli, C.; Franchina, L.; Marchetti-Spaccamela, A.; Querzoni, L. Italian National Framework for Cybersecurity and Data Protection. In *Privacy Technologies and Policy*; Antunes, L., Naldi, M., Italiano, G.F., Rannenberg, K., Drogkaris, P., Eds.; Springer: Cham, Switzerland, 2020; pp. 127–142.
58. Gonzalez-Granadillo, G.; Menesidou, S.; Papamartzivanos, D.; Romeu, R.; Navarro-Llobet, D.; Okoh, C.; Nifakos, S.; Xenakis, C.; Panaousis, E. Automated cyber and privacy risk management toolkit. *Sensors* **2021**, *21*, 5493. [CrossRef]
59. Liatifis, A.; Alcazar, P.R.; Grammatikis, P.R.; Papamartzivanos, D.; Menesidou, S.; Krousarlis, T.; Alberto, M.M.; Angulo, I.; Sarigiannidis, A.; Lagkas, T.; et al. Dynamic Risk Assessment and Certification in the Power Grid: A Collaborative Approach. In Proceedings of the 2022 IEEE 8th International Conference on Network Softwarization (NetSoft), Milan, Italy, 27 June–1 July 2022; pp. 462–467. [CrossRef]
60. Rao, A.; Carreón, N.A.; Lysecky, R.; Rozenblit, J. FIRE: A Finely Integrated Risk Evaluation Methodology for Life-Critical Embedded Systems. *Information* **2022**, *13*, 487. [CrossRef]
61. Semertzis, I.; Rajkumar, V.S.; Stefanov, A.; Fransen, F.; Palensky, P. Quantitative Risk Assessment of Cyber Attacks on Cyber-Physical Systems using Attack Graphs. In Proceedings of the 2022 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES), Milan, Italy, 3 May 2022; pp. 1–6. [CrossRef]
62. Hu, B.; Zhou, C.; Tian, Y.C.; Du, X.; Hu, X. Attack Intention Oriented Dynamic Risk Propagation of Cyberattacks on Cyber-Physical Power Systems. *IEEE Trans. Ind. Inform.* **2023**, *19*, 2453–2462. [CrossRef]

63. Temple, W.G.; Wu, Y.; Cheh, C.; Li, Y.; Chen, B.; Kalbarczyk, Z.T.; Sanders, W.H.; Nicol, D. CyberSAGE: The cyber security argument graph evaluation tool. *Empir. Softw. Eng.* **2023**, *28*, 18. [CrossRef]
64. Riesco, R.; Villagrá, V. Leveraging cyber threat intelligence for a dynamic risk framework: Automation by using a semantic reasoner and a new combination of standards (STIX™, SWRL and OWL). *Int. J. Inf. Secur.* **2019**, *18*, 715–739. [CrossRef]
65. Collen, A.; Nijdam, N.A. Can I Sleep Safely in My Smarthome? A Novel Framework on Automating Dynamic Risk Assessment in IoT Environments. *Electronics* **2022**, *11*, 1123. [CrossRef]
66. Geiger, G. ICT Security Risk Management: Economic Perspectives. In Proceedings of the Federated Conference on Computer Science and Information Systems, Warsaw, Poland, 7–10 September 2014; pp. 119–122. [CrossRef]
67. Teixeira, A.; Sou, K.C.; Sandberg, H.; Johansson, K.H. Secure Control Systems: A Quantitative Risk Management Approach. *IEEE Control. Syst. Mag.* **2015**, *35*, 24–45. [CrossRef]
68. Henley, E.J.; Hiromitsu, K. *Probablistic Risk Assessment and Management for Engineers and Scientists*, 2nd ed.; Wiley—IEEE Press: Hoboken, NJ, USA, 2000.
69. Berestov, D.; Kurchenko, O.; Shcheblanin, Y.; Korshun, N.; Opryshko, T. Analysis of features and prospects of application of dynamic iterative assessment of information security risks. *CEUR Workshop Proc.* **2021**, *2923*, 329–335.
70. Ralston, P.; Graham, J.; Hieb, J. Cyber security risk assessment for SCADA and DCS networks. *ISA Trans.* **2007**, *46*, 583–594. [CrossRef] [PubMed]
71. Larriva-Novo, X.; Vega-Barbas, M.; Villagrá, V.A.; Rivera, D.; Sanz, M.; Álvarez Campana, M. Dynamic Risk Management Architecture Based on Heterogeneous Data Sources for Enhancing the Cyber Situational Awareness in Organizations. In Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES '20), New York, NY, USA, 25–28 August 2020. [CrossRef]
72. Wagner, T.D.; Mahbub, K.; Palomar, E.; Abdallah, A.E. Cyber threat intelligence sharing: Survey and research directions. *Comput. Secur.* **2019**, *87*, 101589. [CrossRef]
73. Liu, Z.; Ma, J.; Weng, J.; Huang, F.; Wu, Y.; Wei, L.; Li, Y. LPPTE: A lightweight privacy-preserving trust evaluation scheme for facilitating distributed data fusion in cooperative vehicular safety applications. *Inf. Fusion* **2021**, *73*, 144–156. [CrossRef]
74. Guo, Y.; Liu, Z.; Huang, C.; Wang, N.; Min, H.; Guo, W.; Liu, J. A framework for threat intelligence extraction and fusion. *Comput. Secur.* **2023**, *132*, 103371. [CrossRef]
75. Guo, J.; Liu, Z.; Tian, S.; Huang, F.; Li, J.; Li, X.; Igorevich, K.K.; Ma, J. TFL-DT: A Trust Evaluation Scheme for Federated Learning in Digital Twin for Mobile Networks. *IEEE J. Sel. Areas Commun.* **2023**, *early access*. [CrossRef]
76. Schaberreiter, T.; Kupfersberger, V.; Rantos, K.; Spyros, A.; Papanikolaou, A.; Ilioudis, C.; Quirchmayr, G. A Quantitative Evaluation of Trust in the Quality of Cyber Threat Intelligence Sources. In Proceedings of the 14th International Conference on Availability, Reliability and Security, Canterbury, UK, 26–29 August 2019; pp. 1–10. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.