Computer and Information Security, 1(1), 11663.
https://doi.org/10.24294/cis11663

Review

Cases of dynamic risk management in cybersecurity: From traditional models to GenAI

Ilias Georgousis[1,*], Ioannis Stoitsis[2]

[1] Bellerophon Research & Development, 41259 Gothenburg, Sweden
[2] Department of Informatics, University of Western Macedonia, Kastoria 52100, Greece
*** Corresponding author:** Ilias Georgousis, ig@bellerophon.gr

CITATION

Georgousis I, Stoitsis I. Cases of dynamic risk management in cybersecurity: From traditional models to GenAI. Computer and Information Security. 2025; 1(1): 11663.
https://doi.org/10.24294/cis11663

ARTICLE INFO

Received: 7 April 2025
Accepted: 12 June 2025
Available online: 16 June 2025

Abstract: Dynamic risk assessment and management strategies are becoming more and more necessary in the cybersecurity field of companies to control the complexity and ongoing change of cyberthreats. Dynamic risk assessment and management solutions help companies to develop preventative cybersecurity plans, so addressing risks and so reducing expenses. Generative Artificial Intelligence (GenAI) has recently transformed these systems, by increasing capacity in real-time data analysis, allowing predictive threat modeling, and promoting initiative-taking defense mechanisms. By including cutting-edge AI models, including neural networks and LLMs, which enable anomaly detection, dynamic event prediction, and automatic compliance reporting, GenAI enhances conventional frameworks, including NIST and ISO standards. After reviewing the integration of GenAI with conventional cybersecurity models, this work emphasizes its dual influence as a tool for both defense and possible exploitation. By means of a comparative study, we investigate how these dynamic systems, enhanced with GenAI, optimize the security posture and support changing cybersecurity policies.

Keywords: dynamic cyber security; risk assessment; risk management; security posture; Generative AI; Large Language Models (LLMs); real-time threat mitigation

1. Introduction

The objective of this research is to compile methods and best practices that have been proposed for a cybersecurity professional, team, or department to be able to calculate and assess the risks and levels of security posture within an organization by considering the probable cyber threats and the internal and external environmental factors of the organization itself in a dynamic manner. Meaning to deploy any advanced statistical and machine learning models, AI, and visualization techniques that would permit a near real-time division of a proactive strategy. The research starts from traditional Artificial Intelligence like machine learning and deep learning models and algorithms and concludes with the latest developments in Generative AI.

The Cybersecurity and Infrastructure Security Agency (CISA) defines cybersecurity as the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

From traditional cybersecurity standards [1] to GenAI disruption that has brought Artificial Intelligence closer to end users and malicious users [2] and the need for new standards development. GenAI plays both a defensive and offensive role in cybersecurity, presenting new challenges for risk models [3]. While at the same time contributing to cybersecurity resilience in dynamic threat environments [4]. The need

for dynamic risk assessment and management is more crucial than ever to help us continue operating in a safe environment and implement guardrails, whether it comes to our work or personal lives [5]. Situational awareness is defined by NIST as "Within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future." [6].

Dynamic risk management is an optimized subset of all measures taken to assess and manage risks under the umbrella of situational awareness for various purposes ranging from the protection of critical infrastructure to smart cities and industrial control systems. In contrast to static risk assessment, as most of the traditional frameworks adhere to, dynamic risk assessment and dynamic cybersecurity posture involve all levels, tools, mechanisms, software, countermeasures, techniques, and analysis methods to achieve real-time information and evolving risk-based decisions for vulnerability and threat management to mitigate risks and damage control in both financial and human life protection terms.

While prior studies have explored the integration of AI into various domains, there remains a notable gap in systematically aligning AI-driven cybersecurity models with established frameworks like NIST and ISO. This review addresses this void by providing a structured taxonomy that bridges AI methodologies with traditional cybersecurity standards, offering a comprehensive perspective not previously consolidated in the literature. The present work is organized in the following way: The introduction presents the core meanings of cybersecurity posture and situational awareness; the second section presents related work on dynamic risk assessment and management when it comes to cybersecurity, more specifically, the related work and existing systems. The third section describes the research methods used to produce this review and the way this review was executed, including some early statistics of the research. At section five, the discussion and comparison between methods and systems begins. Finally, the sixth section summarizes the conclusion of this research.

2. Related work

A seemingly related work to this review is this survey [7] that was conducted on six traditional risk assessment frameworks (three institutional standards and three enterprise-wide assessment models) with an emphasis on Critical Infrastructure Systems resulting in the insufficiency of these frameworks in managing the complex nature of such environments and eventually the proposal of a dynamic approach, which is the focus of the current review. The six frameworks described in the survey are:

Institutional standards

1) NIST risk assessment framework (SP800-30/30rev1)
2) ISO/IEC 27005:2008
3) Bs-7799-2006

Enterprise models

1) OCTAVE
2) Fair
3) Microsoft information security risk management

By their nature, these frameworks fail to integrate methods for data gathering and dynamic analysis for predictions of threats in real time, as most dynamic systems encompass. As a response to this situation, the authors propose an alternative dynamic model. The basis of this model is Kaplan's first risk function, and after some modifications from the authors by adding more variables, specifically asset and vulnerability, they deduce their dynamic model that includes four additional constructs in relation to the frameworks mentioned above, which are:

1) Threat/vulnerability pair (TVP),
2) Control assessment (CA),
3) Risk modeling and,
4) Risk policy evaluation.

After performing exhaustive tests of various hypotheses, they conclude that there is the need for traditional methods to take into consideration quantities and qualities that are naturally hard to predict and/or difficult to quantify. More dynamic risk assessment and management methods and systems are presented in the following sections along with their details [7]. These additions attempted to bridge the gap left by traditional models that lack dynamic analysis and real-time data integration.

In another foundational study, the authors of [8] conducted a systematic literature review of 50 dynamic risk assessment (DRA) models, classifying them by analysis method (e.g., AI/ML, Bayesian networks) and domain (e.g., SCADA, healthcare, CAV). They highlighted the importance of real-time risk modeling and adaptation in evolving threat landscapes. However, while the review provided a technical classification, it did not address the governance or compliance integration challenges of these models.

Recent work has begun to address this. For instance, [9] propose a defense-in-depth framework for adapting NIST CSF and ISO RMF to manage frontier AI risks, particularly LLMs. They identify gaps in current frameworks and advocate layered risk modeling to integrate AI safely. This aligns with the present review's goal of understanding how emerging models fit into traditional regulatory scaffolds.

Similarly, this work [10] presents a comprehensive taxonomy of AI techniques in cybersecurity, highlighting research challenges, model limitations, and the emerging role of generative AI in adaptive risk management. While their work maps the technical field well, it does not explicitly align these innovations with ISO/NIST or dynamic compliance architectures.

In addition, the MDPI review on AI Fairness in Data Management [11] provides relevant discussion on bias, accountability, and trust—themes equally important when integrating GenAI into cybersecurity models and aligning them with regulatory expectations.

The authors [12] provide a comprehensive review of AI-driven detection techniques, emphasizing the role of machine learning, deep learning, and metaheuristic algorithms in enhancing cybersecurity measures across various domains. A recent study explores the integration of AI and ML techniques in cyber threat detection, focusing on how these advanced technologies enhance security, automate threat intelligence, and mitigate evolving cyber risks in real-time [13], and a comprehensive review [14] outlines how artificial intelligence techniques—particularly machine learning and deep learning—are being leveraged to enhance

threat detection and prevention across various cybersecurity domains. The review also emphasizes current challenges and proposes research directions for further improving detection efficiency in complex environments.

This current review builds upon these prior efforts by extending the comparison to include Generative AI-specific models and methods, mapping them not only across domains (e.g., ICS, CAV, smart cities) but also across governance and compliance dimensions (e.g., NIST AI RMF, ISO 42001:2023). It focuses on practical applications, recent advances, and case studies in dynamic cyber-risk assessment, particularly in the post-COVID era of accelerated digital transformation. The review also proposes a novel taxonomy of GenAI-enhanced risk models and compares them with traditional rule-based systems.

3. Research method

By definition, a review's goal is to provide a detailed summary of available primary research in answer to a specific research issue. This paper serves as a vital scholarly resource that offers readers an in-depth understanding by synthesizing and summarizing existing literature. By organizing and critically analyzing previous studies, it highlights key patterns, trends, and areas of consensus while also identifying gaps and challenges within the body of knowledge. This approach not only consolidates current understanding but also provides a clear roadmap for future research, guiding scholars and practitioners toward addressing unresolved issues and exploring emerging opportunities in the field. This study is structured as a **qualitative literature review** based on thematic synthesis rather than an experimental or quantitative meta-analysis. Our goal was to consolidate current practices and evolving techniques in dynamic cybersecurity risk assessment, particularly in relation to GenAI. While secondary data from peer-reviewed studies was used, we applied structured selection criteria inspired by PRISMA guidelines to ensure methodological rigor. The diversity of risk models, metrics, and implementation contexts made it infeasible to standardize quantitative variables across all studies. As a result, we focused on **cross-comparative taxonomy development** and **narrative synthesis** rather than formal meta-analytic aggregation. This approach is suitable for fields, like cybersecurity, where experimental control and data uniformity are rarely feasible at scale [15].

A. Research questions.

The objective of this paper is to find methods that have been proposed for a cybersecurity department to be able to calculate/assess the levels of risk/security posture within the organization considering cyber threats and the internal and external environment of the organization in a dynamic manner in all applicable sectors that involve IT activities.

Q1. What methods/architectures have been proposed for an organization to be able to dynamically calculate/assess and manage the levels of risk/security posture?

Q2. What are the latest updates and tools currently existing in the field of GenAI dynamic cybersecurity?

B. Research database.

The database used was Scopus (https://www.scopus.com/ (last accessed on 10th of November 2024)) and Google Scholar, which is a very reliable and up-to-date database. To answer the above questions, the following search query was performed:

TITLE-ABS-KEY (dynamic AND cyber AND security AND risk AND assessment) OR

TITLE-ABS-KEY (dynamic AND cyber AND security AND risk AND management)

TITLE-ABS-KEY (dynamic AND cyber AND security AND risk AND management AND Generative AI)

AND Publication Year > 2010

After searching in Scopus, we exported all of the results to a CSV file and converted it to a spreadsheet file that permitted real-time collaboration with the following columns:

Authors, Title, Status, Review Add to Survey vote, Year, and Link where we applied, after the initial screening, a selection for including (or excluding) a paper to this review based on the relevance and correlation towards this review's target and research question (**Table 1**).

Table 1. Search results.

Search results	**No of Papers**
Papers found	140
Papers included	52
Papers excluded	88

For the storage and organization of the papers, the Zotero application was used, while for the writing and organization of the bibliography, the overleaf online authoring tool was used.

4. Reviewed methods, models, and systems

A dynamic risk management system can collect multiple data from different types of sensors (Wi-Fi, Bluetooth, Work Climate Control, etc.) in real time and detect data anomalies using correlation techniques. It can also predict attacks using mathematical models such as Hidden Markov Models (HMM) and Bayesian networks, trying to assess the intruder's next step [16]. The dynamic risk management system possesses the ability to react to sudden changes in the normal functioning of the organization. It can automatically calculate the best response action to develop the best defense and countermeasures against an attack.

The most common, but not limited to, applications and tools are:

- Identity and access management (IAM).
- Firewalls.
- Endpoint protection.
- Antimalware.
- Intrusion prevention/detection systems (IPS/IDS).
- Data loss prevention (DLP).
- Endpoint detection and response.

- Security information and event management (SIEM).
- Encryption tools.
- Vulnerability scanners.

Analysis of the above tools is out of the scope of this review. Dynamic methods that engulf such tools and techniques are analyzed below and are defined by some similar characteristics that are grouped at the end of this section. The specific domain of application per paper is presented in the table below (**Table 2**).

Table 2. Domain of application.

Category	No of papers
Smart city infrastructure	7
Organizations and Companies	5
Industrial control systems (ICSs)	3
Connected and autonomous vehicles (CAVs)	2
Security automation in government agencies	2
Cyber security products	2
Machine industry	2

4.1. Three layers for dynamic risk assessment and management

A relatively recent publication proposes a system architecture of three layers for dynamic risk assessment and management, each layer providing inputs to the next one, starting from input and data gathering, continuing to data processing and dynamic event prediction resulting in the risk treatment layer that refers to risk assessment and management. Each layer is composed of various software and hardware components [17].

- Input layer.
- Processing and analysis layer.
- Risk treatment layer.

Specifically, the input layer refers to both software and hardware equipment like the Intrusion Detection System (IDS) and USB controller, Presence-Asset-Status Controller, Bluetooth and Wi-Fi Controller, etc., that provide raw data for the second layer to work with. The layer in reference adopts Bayesian networks and Hidden Markov Model (HMM) as the two mathematical models to predict attack events. Finally, the third layer, which is not described in detail, the core of the assessment and management efforts, is responsible for compiling metrics and visualizations in real time based on gathered input from the previous layers that will enhance the decision-making process. According to the authors, the proposed system gives an advantage over traditional systems in proactively handling the fast-paced and demanding cyber threats in all kinds of environments. Integrating threat intelligence significantly improves the adaptability of cyber risk models [18]. In a national smart grid infrastructure, the **input layer** collects telemetry from smart meters, SCADA devices, and substations. A **processing layer** using Hidden Markov Models (HMM) identifies anomalies in energy consumption patterns that may indicate stealthy intrusion attempts. The **treatment layer** then quantifies this as a medium-risk incident,

prompting the SOC to issue an automatic configuration update to endpoint devices to block lateral movement.

4.2. Neural network approach to assessing cybersecurity

Dynamic risk management is required in IoT structures and networks [19], since the static models fail to adhere to the demanding and complex nature of such a large number of devices and their interactions. In addition, in general, most of the common risk assessment models evaluate the impact of threats in monetary terms. The author adds the scope of human life and health protection.

Firstly, it distinguishes between qualitative and quantitative risk assessment approaches and presents the reasons why traditional risk analysis techniques (Delphi method, SWIFT, etc.) fail and points out the difficulty in gathering statistical data for modelling calculations (e.g., Monte Carlo, Bayesian networks, etc.) that reasonably lead to the adoption of AI-driven systems and the use of machine learning in measuring the probability of threats and the possible consequences of the realization of such threats. Furthermore, he introduces the use of a three-layered perceptron and the backpropagation algorithm for training. Due to the lack of available data, a simulation of a dynamic network infrastructure of a smart city is performed with the use of the NS-3 dynamic network simulator.

The extracted dataset allowed for the testing of 5 types of network attacks and the implications on a plethora of IoT devices, e.g., smartphones, traffic lights, vehicles, medical doors, and sensors, coming to enlightening conclusions on the ability to operate in quickly changing conditions, high classification accuracy when working with big data, the potential of dynamic risk assessment, and the ability to work in conditions when the state of the complete smart city network is unknown.

4.3. Attack graph and risk analysis

Continuing research on smart cities, the author of the previously presented paper on IoT and AI co-authored the paper on applying an attack graph and risk analysis [19]. This research aimed to develop a method for analyzing the security of smart infrastructure while considering the dynamics of component changes. To achieve this, they initially presented the evaluation and analysis of related works for assessing smart infrastructure security and developed specifications for a new method for dynamic assessment of threats. The proposed method included a calculation of security indicators, risk assessment, and selection of the protective measures. Finally, they implemented and tested their method with interesting results. Based on their initial analysis, the attack graph is depicted as follows: the structure for data storing and analyzing, the construction of which can be done during penetration testing.

Again, in this system, there are several layers, or, as per the authors, modules:

- Data processing module.
- Risk assessment module.
- Countermeasure selection module.
- Visualization module.

The first layer oversees turning the input data as well as data from the countermeasure selection module into a set of classes that implement attack graph

operations. The graph structure in the DOT language is expressed as a list of subgraphs, and the data is in the graph description language (DOT) format. The attack graph is then used from the other layers to dynamically assess security, devise countermeasures, and construct a visual model. E.g., the risk assessment module evaluates the major risk indicators and compares the present condition with the state that existed before one of the existing vulnerabilities was removed.

Finally, the visualization module provides information about the attack graph to a server that visualizes the graph. In conclusion, the created comprehensive method based on the attack graph helps in detecting the most serious vulnerabilities in smart infrastructures and can significantly reduce the security risk posed by an attacker breaking into the smart infrastructure network from any of the system nodes [20].

4.4. Machine learning approach

This article [20] describes an iterative data-driven learning technique for assessing and managing vulnerabilities in complex systems by applying observable indications that can be used to infer time-varying system health features. Multiple sorts of vulnerabilities must be included in an overall system health assessment, according to the method. The designed methods are applied to the Common Vulnerability Scoring System (CVSS) database, which contains thousands of reported cybersecurity flaws. To address dynamic properties of system vulnerabilities, the intent of the authors is to serve as a springboard for further research that explores other data-driven and statistically well-grounded machine learning/artificial intelligence methods. The repetitive steps described in the method are:

- Modeling system properties and evolution using Markov assumptions for the cyber-enabled physical system.
- Learning model parameters from historical observable cyber vulnerabilities.
- Inferring likely system state sequences (referred to as the system posture) to evaluate the state of health for the system.
- Analyzing the sensitivity of the system posture under parametric uncertainties to identify priorities for risk-informed investments.

In addition, to achieve dynamic assessment of threats, four metrics need to be created (**Table 3**).

Table 3. System posture metric.

1	**Stability**	**Probability of staying in a "Good" state.**
2	Antifragility	Probability of not staying in a "Bad" state.
3	Health	Proportion of "Healthy" state in the testing dataset.
4	Dispersion	Gini index measuring statistical dispersion for the categorical hidden system state represented in the HMM.

The overall methodology is a repeatable process that should be updated and refined using results from past iterations combined with new information, such as training parameters, new data, and other decision-making factors that emerge from past use of this methodology.

4.5. Dynamic whitelists

This work [21] demonstrates the importance of not overlooking the power of Whitelists in contrast to Blacklists, which are in general more popular and better designed than Whitelists. By identifying things that should not be banned, Whitelists help to mitigate the risk that large, automated Blacklists carry by blocking access to necessary internet assets. The authors state that Whitelists are sometimes poorly built and poorly maintained, failing to offer the protection that they should as an appropriate counterbalance. The danger of malmaintaned Whitelists leads to compromising the security ecosystem whatsoever. The first published algorithm is described in this publication for the development of an automatic whitelist. The use of Bayesian statistics learning methods and the integration of network and threat data constitute the list to be both defendable and environmentally conscious. In addition, two more whitelisting methods are provided for comparison by evaluating all three throughout the course of a six-week term and the usage of a plethora of data sources.

In conclusion, it is shown how the suggested method may be utilized as a quality assurance mechanism for Blacklists by taking advantage of the threat review capability to find faulty entries in the Blacklist that are difficult to identify (**Table 4**).

Table 4. Methods applied.

Method	Description	Thresholds limits	Conclusions
Max coverage threshold	Simple static threshold based on the assumption that popular domains are benign and ignores threat data.	Max-coverage static threshold using the top 200,000 domains for Alexa and Majestic or the top 95% with respect to density for Farsight.	Whitelists of around 200,000 domains carry a significant risk of threat inclusion.
Min threat threshold	Review of several months of historic threat data and selection of a static threshold that minimized the threat	Min-threat static threshold using either the top 12,000 domains for Alexa and Majestic or the top 75% with respect to density for Farsight.	Includes some threat, and the range overlaps significantly in all cases with the Bayesian model.
Bayesian inference model	A domain is above the threshold if it has a higher rank than the threshold. The whitelist size is defined by the number of domains above the threshold that are not identified as malicious.	Bayesian threshold using the observed threat rank.	The whitelist generated by the Bayesian algorithm adapted to changes in the threat landscape over time.

4.6. Developing a cybersecurity risk analysis system for high tech equipment in machine industry

At this point in the research, it is evident that cybersecurity dynamic risk assessment and management are needed in all aspects of IT activities. Such an area of application is the machine industry [22]. The paper's target, presented herewith, is to develop a system for identifying and assessing cyber risks to support investment decision-making in a machine industry enterprise. After performing a literature review and analysis on traditional methods, FAIR methodology seems the most appropriate to assess cyber-risks in terms of estimating the efficiency of such investment projects due to significant advantages such as:

1) The ability to classify risk factors comprehensively,
2) Presenting quantitative methods for measuring factors and probabilistic computation schemes,
3) The ability to assess the impact of risk factors on the efficiency indicator of investment projects—return on investment given the risks (CyROI).

In contrast to other traditional methods that, according to the authors, have significant flaws, such as:

1) The approaches imply that only a "static" estimate of the average amount of projected losses is possible.
2) They do not take into account the length of time that losses occur.
3) They prevent the correct linking of risk variables, as well as project efficiency indicators.
4) They aren't meant for evaluating the risk correlation.
5) They are difficult to predict usage to figure out the total amount of damage.

The researchers' proposed system is an essential component of the management and evaluation of the effectiveness of an investment project, including the introduction of high-tech equipment. The advantages of this system are:

1) Integration of risk management into the decision-making process.
2) Coordination of all risk management features in a single system.
3) Use of tools with low tolerance to risk and increased attention to quantitative risk assessment.

To implement this system, specific tools were used:

1) A bow-tie diagram for risk identification.
2) Simulation modelling with the use of the Monte Carlo method.
3) A tornado diagram and a chance ratio method for risk analysis.
4) A micromort method for estimating the probability distribution parameters.

A manufacturing plant implementing a FAIR-based approach uses Monte Carlo simulations to estimate cyber-risk exposure for high-value Computer Numerical Control machines. The scenario involves insider threat vectors via USB injection. Risk analysts simulate the potential downtime (in hours) and associated revenue loss. Based on tornado diagram sensitivity results, the control investment is prioritized toward USB port lockdown and role-based access segmentation.

4.7. Quantitative security risk assessment for industrial control systems: Research opportunities and challenges

In relevance to the above-presented paper, which focused on decision-making for investments in industrial machines, this paper [23] focuses on the quantitative security risk assessment for industrial control systems (ICSs). According to the authors' findings, the current state of dynamically analyzing cyber threats for ICSs is characterized by the lack of appropriate (dynamic) security risk assessment methodologies adapted to the unique characteristics of ICSs.

This is made worse by the fact that the threat landscape is becoming increasingly complicated during the era of Industry 4.0, and there is a scarcity of historical data on security events. As a result, asset owners may not be able to quantify their cyber risk exposure, leaving them unsure when making security decisions. In addition, buying cyber insurance to shift the risks of non-Physical Material Damage and Business Interruption, the core problem will remain unresolved since (re)insurers may take on these unassessed risks.

This paper closes by identifying various options for additional study that are worth investigating as a starting step to help those wishing to enhance the estimation

of cyber threats relating to ICSs. The complex environment of industrial plants must be controlled in a holistic and methodical manner to reduce the possible repercussions of cyber assaults. Even though some security recommendations and standards (e.g., VDI/VDE 2182) recommend a qualitative approach (usually based on a scoring system and displayed as a risk matrix or heatmap), there appears to be a rising trend towards quantitative techniques. The reason for this is that qualitative security risk assessment techniques have been heavily criticized due to their inherent ambiguity. Continuing, the authors number the reasons why this field has plenty of room for research, in particular:

1) Physical effects.
2) A changing threat landscape.
3) The importance of threat modelling.
4) The need for cyber risk quantification.
5) Managing complexity through knowledge transfer.
6) The scarcity of historical data.
7) Cyber accumulation.
8) The dynamic nature of security risks.

The authors continue with a synopsis of the literature review for the research reasons presented earlier and an overview of the existing dynamic security risk assessment methods currently applied and evaluated in the ICS domain. Concluding in five main points:

1) An insufficient integration of security modelling languages into PSE (Production Systems Engineering); use of the Semantic Web Rule Language (SWRL) to logically connect engineering and security know-how
2) Poor understanding of potential consequences: The estimation of physical and economic effects caused by potential attacks against ICSs is essential for performing quantitative security risk assessments.
3) The need for automated modelling of sophisticated cyber-physical attacks; threat modelling ought to be mostly automated, allowing security professionals to concentrate on subsequent (sub)processes of risk management.
4) The lack of dynamic risk analysis methods for ICSs; cyber risks cannot be considered as static.
5) Dealing with the paucity of historical data; the absence of data represents a key research challenge for the application of PRA methods.

4.8. Framework for calculating Return on Security Investment (ROSI) for Security-Oriented Organizations

The goal of this study is to provide a complete framework for measuring the Return on Security Investment (ROSI) that fills in the gaps left by traditional methods. The attack dataset from the Common Vulnerability Security System (CVSS) was used to validate the framework. The findings reveal that the yearly loss is quite significant, at $585,553 in the absence of security systems. However, the proposed steps outlined in the study decrease this amount to $146,388 by using a methodical technique. Therefore, the company may save time, money, trust, and its market reputation. The

proposed ROSI framework has six phases with their corresponding sub-phases [24]. The phases are:

1) Asset identification and analysis.
    a) Develop an asset inventory.
    b) Prioritization of assets.
    c) Asset value quantification.
2) Vulnerability and threat identification.
    a) Vulnerability scanning.
    b) Threat modeling.
3) Likelihood and impact determination.
    a) Likelihood determination.
    b) Impact determination.
4) Countermeasure analysis.
5) ROSI calculation.
    a) Cost benefit analysis.
    b) ROSI.
6) Recommendation.

In conclusion, the authors offered a framework for developing cost-effective security measures, which eventually helps companies generate money. In addition, the article examined and contrasted some of the existing ROSI models.

4.9. Attack-defense trees based cyber security analysis for CPSs

A most recent work employs the use of attack-defense trees for Cyber-physical systems analysis. According to the authors, current ideas for risk assessment that use attack trees mostly focus on portraying potential intrusions rather than interactions between threats, vulnerabilities, and defenses.

The use of an attack-defense tree (ADTree) in a system is advocated to show the attack scenarios along with their cost and impact. Considering the impact of both the assault and defense costs. A set of criteria is used to assess the effectiveness of the suggested strategy and metrics such as success likelihood, attack and defensive costs, and the effect of an assault. In addition, two economic aspects are discussed (ROA and ROI) to assess ADTree's performance.

In conclusion, to exemplify their technique, they provide an example of threat risk analysis in a SCADA system. Overall, the proposed method to cyber-physical system security risk assessment and countermeasures evaluation in the evolutionary process of security management is achieved [25].

4.10. A simplified approach for dynamic security risk management in connected and autonomous vehicles [26]

This paper presents a simplified and systematic method for managing cybersecurity risks in connected and autonomous vehicles (CAVs), focusing on adapting to changes in the vehicle's environment. Their approach includes three main modules:

(1) Knowledge-based system (Module A)

This module provides foundational support for identifying critical threats. It includes:

- **Reference architecture**: Outlines the functions of a CAV system, serving as a base for identifying how these functions could be targeted by cyberattacks.
- **Attack surface analysis**: Maps out possible security threats based on components, functions, and communications within the system.
- **Attack goals and trees**: Defines typical attacker objectives and their breakdown into smaller, actionable sub-goals.
- **Threat agent profiles**: Lists possible attackers, their motivations, and capabilities. This information is drawn from existing literature and must be regularly updated.

(2) Context monitoring (Module B)

This module tracks real-time changes in the environment and system state. It:

- Gathers data from the infrastructure and the CAV itself.
- Detects changes in threats, requirements, or system functionalities.
- Forwards relevant changes to Module C for reassessment only when necessary, reducing unnecessary processing.

(3) Risk Management (Module C)

This module performs dynamic risk assessments using inputs from Modules A and B. It follows five key steps:

1) **Identify Potential Attacks**—With help from Module A, assess which attacks could occur.
2) **Identify Essential Components**—Focus on key parts of the CAV, based on both its hardware and software architecture.
3) **Identify Critical Attack Surfaces**—Combine previous steps to highlight high-risk areas needing monitoring.
4) **Conduct Risk Assessment**—Analyze risks based on attack surfaces and data from the Intelligent Transportation System (ITS), which helps estimate the capabilities of threat actors.
5) **Re-evaluate Mitigations**—Update or introduce new mitigation strategies when new risks are detected or when changing road conditions affect the CAV's operation.

An autonomous vehicle traveling through a dynamic urban environment enters a **construction zone** with intermittent 5G signal. The system's **context module** flags the low-signal area as potentially vulnerable to GPS spoofing. The **knowledge layer**, referencing threat intelligence feeds, correlates the environment with recent MITRE ATT&CK techniques related to signal jamming. The **risk treatment module** shifts the control model to manual override and restricts over-the-air firmware updates during this segment. Real-time cyber threat detection in connected autonomous vehicles (CAVs) must operate under tight latency, computational, and power constraints. Traditional cloud-based detection systems are often unsuitable for these environments due to delays and reliance on constant connectivity. To address these challenges, a recent paper [27] proposes the Explainable and Lightweight AI (ELAI) framework, designed specifically for edge-based cyber threat hunting. The framework combines interpretable machine learning models with lightweight deep learning

architectures, allowing high detection accuracy while maintaining low computational overhead. Using datasets such as CICIDS and UNSW-NB15, ELAI demonstrates its ability to detect anomalies in real time with high precision and minimal false positives—making it an ideal solution for deployment within CAVs where transparency and efficiency are both mission-critical.

4.11. A profile-driven dynamic risk assessment framework for connected and autonomous vehicles

This paper proposes an approach [28] based on the different data management profiles within CAV systems through a dynamic risk management framework. The framework encourages the search for risks through different risk profiles, in contrast to current risk assessment strategies, each of which represents risk knowledge through a set of risk input assessments, assessment methods, and best response strategies. The benefits of this approach are many:

- Decision-making is made after many data sources. The evaluation will be more accurate, while the training process will become faster and more flexible due to the reduction of data and monitoring capabilities.
- Risk profiles include risks from different categories that interest users and therefore can provide more information and improve the quality of decisions.
- Users get out of the system faster and understand the rating more accurately, which means they are more aware of the risks of the situation and can react better to reduce and manage damage.

4.12. Development of web-based automated system for cyber analytic applications

In this work, the team [29] describes how they have developed a tool that has the ability to gather public data available on the Internet that contains information about cyberattacks that have taken place around the world. Next, they can proceed with the analysis of the data to predict the trends in cyberattacks. The results of the analysis can help organizations take new preventive and effective security measures. In this way, organizations can strengthen cyber risk management programs and therefore avoid similar attacks. The following is a description of the system architecture, which consists of 4 different parts, which are:

1) Collection of links.
2) Scraping of information.
3) Structuring information.
4) Analysis of data.

All modules can run on different operating systems, such as Linux or Windows, by updating the system drivers. In addition, all units operate as a stand-alone unit without any additional assistance.

Next, a detailed description of all the modules of the system is provided.

- Collection of links.

This module is responsible for collecting article links from trusted sources on the web, such as newspaper websites (CNN, CNBC, etc.), with browsers like Google

Chrome, Firefox, etc. It should also be mentioned that the Python 3 programming language with the Selenium module was used for the program automations.

- Scraping of information.

In this module the links collected from the first module are used by the system to access the main article website. The crawler then crawls and checks the entire webpage and then deletes or extracts the entire article containing the information. Only specific data is extracted from the article and stored in sequential files.

- Structuring information.

The specific information is saved into the file and structured in the form of a table. The table includes information like the article's link, the link of the HTML file in which the article is saved, and all the other statistical data. All this data is stored in CSV files for future use.

- Analysis of data.

This last module will analyze the data collected from the previous module. The data will be analyzed based on each category, and we will try to come to possible conclusions from them. This will help us take further security measures in the future to protect our companies.

4.13. Dynamic risk management response system to handle cyber threats [30]

The authors present a system called DRMRS (dynamic risk management response system). Which helps organizations respond more effectively to cyber threats by using software that can assess, predict, and react to attack scenarios automatically.

The DRMRS approach unfolds in three main phases:

The system administrator manually maps out known threats and attack patterns affecting the organization. This involves understanding the current threat environment and anticipating how it might develop. Tools like attack graphs and correlation methods are used to visualize possible scenarios and weak points in the system.

Once potential attacks are identified, the next step is to evaluate their likelihood and possible consequences. The system calculates the business impact and cost of each scenario, as well as the effort required to counter them. This gives a clearer picture of which threats are worth addressing and what resources would be needed.

Here, the system proposes the best course of action to manage the identified risks. It aims to lower the risk to an acceptable level by selecting and deploying the most appropriate countermeasures. The chosen actions are then rolled out across the relevant IT systems.

The structure of DRMRS is organized into three functional layers:

- **Input Data Layer:** This part gathers the data needed for the analysis, including technical details about assets, threat indicators, and business context.
- **Processing Layer:** The core of the system, this layer includes:
  - **Strategic Response Determinant (SRD)**—helps guide high-level decisions.
  - **Attack Graph Generator (AGG)**—visualizes how threats might move through a system.
  - **Operational Response Impact Assessment (ROIA)**—estimates how each

possible response would affect operations.

- **Threat Risk Quantifier (TRQ)**—assigns values to the likelihood and impact of threats.

- **Output Layer:** This layer produces the actual response plans—first drafts and refined versions—detailing the steps to mitigate the risks identified.

4.14. A fuzzy probability Bayesian network approach for dynamic cybersecurity risk assessment in industrial control systems

Because of the lack of sufficient historical data [31], it is difficult to build a risk propagation model for industrial control systems (ICSs). In this paper, a fuzzy probability Bayesian network (FPBN) approach is presented for dynamic risk assessment. An FPBN is used to analyze and predict cybersecurity risks. It uses a probabilities approach to replace the precise probabilities required in a typical BN model. Then a dynamic algorithm is developed for dynamic assessment of industrial control systems (ICSs) cybersecurity risk.

The network architecture contains two types of input data: attack evidence and anomaly evidence. Anomaly evidence can be generated by cyberattacks or system errors. In addition, system failures can lead to a risk assessment error, so attack evidence and anomaly evidence must be filtered. The FPBN can know information about attacks, system operations, hazards, and system assets. After training the FPVN network with evidence, the network can calculate the chances of assets being destroyed. It then assesses the potential cybersecurity risk with asset losses. The "X" symbol means that the value of the cybersecurity risk is equal to the product of the asset damage and the corresponding probabilities.

4.15. Dynamic framework for assessing cyber security risks in a changing environment

Nowadays, [32] an organization or business can easily be exposed to cyber threats due to the fact that all businesses now have a global presence or even a digital footprint on the internet. Generally, threats may occur because of different changes happening internally or externally to the organization. In this work, the authors propose a new method of applying a system dynamics approach for designing a dynamic risk assessment framework.

They propose a dynamic framework for understanding how risk vectors change and the exposure of organizations to these risks over time. This framework will allow companies to assess how changes in an organization's internal and external environment affect priorities, threats, and risks. The results will allow information and security managers to review risk assessment frameworks in a timely manner and make the necessary changes to identify high-priority risks.

The framework can be used to provide information on when the relevant changes needed to record and address the relevant high-priority risks will be implemented. The dynamics of the system are used to understand how risk vectors change and the exposure of organisms to these hazards over time.

4.16. Cybersecurity risk assessment in smart city infrastructures

The authors proposed [33] a new approach to cyber risk management based on object typing, data mining, and quantitative risk assessment for smart city infrastructure. In their work, they studied how an artificial neural network allows us to automatically evaluate cyberspace for various types of objects in the dynamic digital infrastructure of the smart city. The first step in the operation of the artificial neural network should be to identify the risks of cybersecurity breaches. The technique consists of four stages:

1) Preparatory stage.
2) Training sample formation, the basis of scenarios (BS) of dynamic network modes.
3) Classification.
4) Cyber security risk assessment.

Neural network training is a very important step in preparing the data set. To properly assess cyber risks, they need data sets that are collected in smart city networks and contain various types of assets, network traffic, and the level of cybersecurity risks. To test the model, the team simulated network attacks such as black hole (BH), grey hole (GH), DoS, DDoS, and wormhole (WH). Of course, all of these types of attacks have to do with the type of device they can affect.

Generally, the cybersecurity risk assessment is a classification problem, and a regression tree either classifies the current cybersecurity risk level as acceptable or unacceptable or predicts classes based on past data. In addition, the artificial neural network models are more capable of modeling more complex nonlinear functions than classical statistical models such as linear discriminant analysis and logistic regression.

Finally, it should be noted that machine learning technology has proven its effectiveness in tasks that require working with big data. Using the network simulator, it was possible to recreate the dynamic network infrastructure of a smart city. From the data collected during the modelling, a data set was prepared, which contains elements of the network as well as the economic characteristics.

4.17. Enhancing risk-based decisions by leveraging cybersecurity automation

Al Sadhan and Park, in their paper [34], propose the addition of risk management, real-time information, and threat detection to the automation activities in the management of cybersecurity environments due to their complex nature and exponential growth. Information Security Continuous Monitoring (ISCM) objectives and capabilities in heterogeneous systems ask for a plethora of measures, activities, and analyses to be carried out constantly to achieve a system of situational awareness engulfed in an Information Security Continuous Monitoring Framework.

This framework takes into consideration regulations and standards and business mission and risk aspects that go through various stages in order to create risk-based decisions when it comes to cybersecurity. It is ongoing research.

4.18. MITIGATE: An innovative cyber-security maritime supply chain risk management system [35]

It is a project funded by the EU's Horizon 2020 program. Its goal is to strengthen cybersecurity in ports and maritime infrastructure. To achieve this, it offers services like collaborative risk management, cyberattack simulation and visualization, and open-source threat intelligence.

The system's architecture includes several key components:

- **Asset Modeling and Visualization**: This lets users define cyber assets and their relationships in a structured format.
- **Maritime Supply Chain Service (MSCS) Modelling**: Analysts can model their organization's maritime processes and link them to existing cyber assets, making it easier to assess how these processes depend on digital infrastructure.
- **Simulation and Game Theory**: This module helps identify possible attack paths and calculates the most effective defense strategies using principles from game theory.
- **Collaborative Risk Assessment**: Guides analysts through the risk assessment process based on the MITIGATE methodology, focusing on specific MSCSs.
- **Open Intelligence and Big Data Analytics**: Gathers and processes real-time data from public sources like Twitter, Reddit, and RSS feeds to alert organizations about emerging vulnerabilities.
- **Notification and Reporting**: Sends alerts and updates to analysts when key activities occur, such as completing a vulnerability scan or calculating risks.
- **Administrative Component**: Maintains key system definitions and categories (e.g., types of vulnerabilities or business partners) that other components rely on.
- **Access Control and Privacy**: Ensures security and privacy across the entire system.

The platform also includes a data storage layer with two types of databases:

- A **relational database** for storing structured data.
- A **NoSQL database** for frequently updated, semi-structured data like vulnerability reports.

Communication between components is handled through a **publish/subscribe (pub/sub) system**, which allows them to operate independently and prevents delays caused by direct communication.

4.19. GenAI disruption

The following papers present the latest research on how GenAI and LLMs have already disrupted cybersecurity risk management.

The authors of [36] present the opportunities and threats in cybersecurity by arguing that GenAI is a double-edged sword in cybersecurity, capable of enhancing defense mechanisms such as vulnerability scanning and threat intelligence while also enabling new attack vectors, like automated phishing and malware generation. They highlight the need for ethical norms and defense mechanisms to counter these challenges.

Another study [37] explores the integration of GenAI in the public sector, emphasizing its transformative potential in efficiency and decision-making. However,

they point to critical risks like data privacy breaches and the erosion of public trust. Their qualitative content analysis across national guidelines reveals commonalities in risk perceptions, urging more robust governance frameworks to address these issues. Recent studies have highlighted the misuse of generative AI models in crafting sophisticated social engineering attacks, emphasizing the need for robust countermeasures [38].

In this paper [39], focus is put on GenAI's dual role in securing Cyber-Physical Systems (CPS). While it excels in intrusion detection and defensive deception, its potential misuse in creating sophisticated attack payloads highlights significant vulnerabilities. The importance of advancing defensive strategies alongside GenAI's adoption to mitigate threats is underscored.

Another recent work [40] illustrates GenAI's potential to revolutionize Governance, Risk, and Compliance (GRC) through automated policy enforcement, predictive analytics, and real-time compliance tracking. Despite these benefits, the author cautions about the challenges of ensuring transparency and accountability in GenAI-driven decision-making processes.

For example, a financial institution deploys a GenAI-powered system trained on internal email, behavior logs, and transaction patterns. When an employee attempts to download unusually large datasets after midnight and sends an encrypted zip file externally, the GenAI system flags the activity. Unlike rule-based DLPs, the model contextualizes the employee's behavior within job role history, previous anomaly scoring, and risk posture trends, prompting an automatic escalation to human investigators before data exfiltration occurs.

In conclusion, GenAI has a great impact on cybersecurity professionals [41]. The authors investigate the implications of GenAI and LLMs for cybersecurity roles. Their qualitative study highlights professionals' cautious adoption due to ethical and security concerns. The interviews reveal a critical need for a balanced approach that embraces GenAI's capabilities while mitigating risks. Further research proposes a framework for ensuring secure and ethically aligned deployment of GenAI in critical systems [42].

GenAI-enabled cybersecurity models represent a significant advancement over traditional models by offering dynamic, proactive, and scalable solutions to address evolving threats. Traditional cybersecurity models rely on rule-based approaches with predefined heuristics and static patterns, limiting their adaptability to new and complex attack vectors. These models primarily handle structured datasets, focus on known attack signatures, and require significant human oversight for operations and psychological resilience of cybersecurity staff, which is a critical dimension of risk response layers [43]. In contrast, GenAI-enabled models utilize AI-driven frameworks capable of generating dynamic responses and analyzing both structured and unstructured data in real-time. They predict and mitigate unseen threats, adapt rapidly through continuous learning, and automate compliance and policy enforcement. While traditional models emphasize static regulatory adherence and simpler use cases, GenAI excels in handling multi-layered, complex threats and provides high customization through adaptive learning models. However, the integration of GenAI introduces ethical challenges, such as the potential misuse for malicious activities, and

requires cybersecurity professionals to develop advanced skills in AI, machine learning, and GenAI-specific technologies.

Case studies of GenAI enhancements in cybersecurity

Recent empirical studies demonstrate how GenAI models are not only theoretically robust but also practically superior to traditional systems in threat detection, prediction, and compliance. For instance, Abo Sen proposed an Attention-GAN framework that achieved **99.69% accuracy** on the KDD dataset for intrusion detection, significantly outperforming classical algorithms like support vector machines and decision trees [44]. This result highlights GenAI's strength in learning complex attack behaviors from high-dimensional input.

In another case, Tallam et al. developed **CyberSentinel**, a real-time cybersecurity detection system powered by transformer-based architectures [45]. Their evaluation of enterprise-grade traffic logs showed a **34% faster incident response time** and a **22% reduction in false positives** compared to commercial SIEM systems. These gains were attributed to the system's generative learning component that synthesized attack patterns and response strategies in real time.

In the domain of regulatory compliance, Deloitte Insights [46] reports that GenAI applications are being used to automate documentation for ISO 27001 and NIST 800-53 audits [47], reducing manual effort by **up to 65%**. These systems automatically cross-reference security logs, access policies, and threat intelligence to pre-fill compliance checklists and generate risk reports.

Together, these case studies illustrate that GenAI is not only complementary to traditional cybersecurity models but can also redefine best practices in detection accuracy, real-time response, and audit automation.

5. List of dynamic risk assessment methods

The above presented papers are summarized in **Table 5** below, grouped under some defining characteristics.

- **Number of Papers**: Number of research references in the present work.
- **Domain of Application**: Scope of application of this method.
- **Inputs**: The type of data entered as inputs in the method for risk assessment and management, e.g., threats, vulnerabilities, assets.
- **Risk Calculation Method**: In this column the mathematical models or the method for risk assessment is presented.
- **Integrations with other systems**: In this column the cooperation and integration of the method with other technologies and systems is presented.
- **Outputs**: Record of the output given by the system after calculating the risks.

To enable a more rigorous comparison across dynamic risk assessment models, several recent studies provide empirical performance metrics. For instance, Abo Sen's Attention-GAN achieved 99.69% detection accuracy on the KDD dataset, surpassing traditional models like decision trees and SVMs in precision and recall [44]. Similarly, the CyberSentinel system reduced false positives by 22% and improved threat response times by 34% over baseline SIEM tools [45].

Other systems apply well-defined security posture metrics such as Gini index dispersion, antifragility scores, and posture stability—particularly in Bayesian or

HMM-based architectures [16,20]. These metrics quantify how likely a system is to remain in a "Good" or "Healthy" state under evolving threat conditions.

In the compliance domain, GenAI-powered documentation tools reportedly reduce manual effort by up to 65% during ISO/NIST audit processes [46]. Similarly, FAIR-based investment frameworks calculate Cyber ROI (CyROI) and use tornado diagrams and micromort estimations to quantify risk exposure in monetary terms [22].

6. Discussion

While this review does not introduce a new model or conduct primary experiments, it provides a novel contribution by offering a comprehensive, cross-sector taxonomy of dynamic cybersecurity risk assessment methods. Specifically, it is among the first to systematically map traditional models (e.g., FAIR, Bayesian, whitelisting) alongside emerging GenAI-based models, using a common comparison structure. **Table 5** consolidates 22 distinct methods by sector (e.g., ICS, smart cities, autonomous vehicles), inputs, processing frameworks, outputs, and performance metrics.

Table 5. Risk assessment methods comparison.

# of Paper	Domain	Inputs	Risk Calculation Method	Integrations with other systems	Outputs
[16]	Organizations and Companies	The system is collecting multiple data from different types of sensors (presence, environmental, WiFi, Bluetooth, network anomaly, work climate, etc.) and detecting anomalies in such data using correlation techniques. Threats, Vulnerabilities	Hidden Markov Models (HMM) and Bayesian networks	Intrusion prediction techniques with Hidden Markov Model (HMM) and Bayesian networks. In order to model the activity of an incident, attack graphs are proposed, specifically Directed Acyclic Graphs (DAG) formed by nodes connected with arcs.	Event Prediction (Tries to estimate the next step of the attacker), Anomaly Detection, Event Correlation
[17]	Large-scale dynamic networks of smart city	Assets: Smartphone, Laptop Vehicle, Traffic light Roadside unit, Smart door lock, medical sensor Temperature sensor, Database server, Smart robot. Two datasets were generated: a training one, consisting of 10000 vectors, and a test one, consisting of 10000.	Artificial Neural Network	A three-layer perceptron was chosen as a model of a neural network, and datasets were generated synthetically using a network simulator NS-3. TensorFlow and Keras frameworks were used.	Experimental results showed that the neural network model proposed by the author allows for rapidly changing conditions to unambiguously and reasonably assess the risks of cybersecurity
[19]	Smart infrastructure	Cyber-physical systems like robots, sensors, IoT devices. Assets	Attack graph and risk analysis	Data processing module, risk assessment module, countermeasure selection module, visualization module.	The visualization module provides information about the attack graph to a server that visualizes the graph
[20]	Physical infrastructure systems	Vulnerabilities,(CVSS) database, Threats	Machine learning/artificial intelligence methods	Common Vulnerability Scoring System (CVSS) database Markov assumptions Machine learning	The overall methodology is a repeatable process that should be updated and refined using results from past iterations combined with new information
[21]	Cyber security products	Large, automated Blacklists Vulnerabilities, Threats	Bayesian statistics learning methods Machine learning algorithms	Algorithm for automated whitelist creation, Malware sandboxes, Machine learning algorithms	Algorithm for automated whitelist creation
[22]	Investment decision-making in a machine industry	Threat, Asset, and Vulnerability	FAIR methodology	A bow-tie diagram for risk identification, Monte Carlo method, A tornado diagram and a chance ratio method for risk analysis, A micromort method for estimating the probability distribution parameters	Support investment decision-making in a machine industry enterprise
[23]	Industrial control systems (ICSs)	Threat, Asset, and Vulnerability	Quantitative risk assessments Data flow diagrams	Risk identification, Risk analysis, Risk evaluation CPS threat modeling methodology	Effective decision-making process for security investments. Quantitatively assessing cyber risks for ICSs

Table 5. (*Continued*).

# of Paper	Domain	Inputs	Risk Calculation Method	Integrations with other systems	Outputs
[24]	Organizations and Companies	Attack dataset from the Common Vulnerability Security System (CVSS)Assets Vulnerability and threat identification	ROSI framework	1) Asset identification and analysis2) Vulnerability and threat identification3) Likelihood and impact determination4) Countermeasure analysis5) ROSI calculation6) Recommendation	Cost-benefit analysis ROSI Recommendation
[25]	Cyber-physical system (CPS)	Real-time data from the physical system	Attack-defence tree (ADTree)	The ADTree model is used as a framework to derive the attack scenarios and attack-countermeasure scenarios.	Overall, the proposed method to cyber-physical system security risk assessment and countermeasures evaluation in the evolutionary process of security management is achieved
[26]	Connected and autonomous vehicles (CAVs)	Driving software supported by many embedded sensors (such as GPS, radar, LIDAR, ultrasonic) to sense the driving environments combined with actuators. Communicating with other entities, such as transportation infrastructure (V2I) and surrounding vehicles (V2V), to provide a shared understanding.	Intelligent Transportation System (ITS)	Module A: Knowledge-Based System Module B: Context Monitoring Module C: Risk Management	We use knowledge regarding the attack trees to predict the relevant attacks and system withstands to estimate attacker capabilities.
[28]	Connected and autonomous vehicles (CAVs)	IoT cloud—collected data Risk profile of an object, Threats, Vulnerabilities	Dynamic Risk Management Framework BN inference Machine Learning FTAFAIR	Managing big data gathered from different IoT sources. The gathered data can be used to obtain the risk assessment. The framework manages risks through profiles, each containing risk information of a specific aspect	Adaptive models Decision-making support Situational awareness Reaction System Feedback Manage training data
[29]	Organizations and Companies	Available public data on the Internet containing information about cyberattacks	Python, HTML, SQL, CSV files	The system is divided into 4 different modules collection of links, scraping of data, structuring of data and analysis of data	Predict trends in the cyber breaches. Obtained results from the analysis can help organizations in deriving new proactive and effective security measures.
[30]	Critical infrastructure	List of all pieces of equipment in the infrastructure with the exhaustive list of its current vulnerabilities. The DRMRS consists of over 13,000 nodes categorized as entry points.	Dynamic risk management response system (DRMRS) consisting of proactive and reactive management software aimed at evaluating threat scenarios in an automated manner	Attack graph generation, Threat risk quantification, Operational, Financial impact assessments	Automated response plan generation of all possible combinations of mitigation actions Automated selection of the best response plan for a given threat scenario. Attack Graph Proactive Risk Profile

Table 5. (*Continued*).

# of Paper	Domain	Inputs	Risk Calculation Method	Integrations with other systems	Outputs
[31]	Industrial Control Systems (ICSs)	Attack evidence Anomaly evidence	Fuzzy probability Bayesian network (FPBN) for dynamic risk assessment	Fuzzy Probability Bayesian Network Inference Engine	After training the FPVN network with evidence, the network can calculate the chances of assets being destroyed. It then assesses the potential cybersecurity risk with asset losses.
[32]	Organizations and Companies(Large energy management company)	Threats, Risks relevance, Vulnerabilities	Simplified causal-loop diagrams of key risk drivers	System dynamics to understand how the vectors of risk and the exposure of organizations to these risks change over time	The results will allow information and security managers to review risk assessment frameworks in a timely manner and make the necessary changes to identify high-priority risks.
[33]	Smart city infrastructure	Data sets that are collected in smart city networks and contain various types of assets	Artificial Neural Network	Preparatory stage, Training sample formation, Classification, Cyber security risk assessment	Evaluation of the cyberspace for various types of objects in the dynamic digital infrastructure of the smart city
[34]	Security automation in government agencies	Data that is accurate, near real-time and represents risk factors: threat, vulnerability, impact of the threat exploiting the vulnerability and likelihood that harm would occur	Information Security Continuous Monitoring (ISCM)	Real-time threat detection, incident response and risk-based decision-making capabilities	ISCM and risk-based decision-making in relation to security automation in government agencies
[35]	Safeguard the cybersecurity of ports and maritime infrastructure facilities	Asset Modelling and Visualization component, where users can designate cyber assets.	Collaborative Risk Management, advanced Simulation and visualization of cyberattacks, and open intelligence services	Web-based Access & Collaboration Layer, Big Data Threat Analysis, Risk/Vulnerability Visualization Open Simulation Environment Relational DB NoSQL DB	Calculations of the best defensive strategy regarding the protection of a specific cyber asset. Real-time notifications regarding potential vulnerabilities related to a cyber asset

Furthermore, the review introduces a practical model-to-framework alignment, showing how each method could potentially integrate with NIST 800-30, ISO 27001, or AI RMF controls. This synthesis enables practitioners to benchmark not only the techniques but also the governance readiness and auditability of each approach.

To our knowledge, no prior study has organized these models across technical, strategic, and compliance layers while incorporating GenAI-specific risks and benefits into the comparative analysis. This positions the review as a foundation for both practitioners seeking model selection guidance and researchers aiming to build hybrid frameworks that combine AI capabilities with formalized governance standards.

Dynamic risk assessment and management go hand in hand with the dynamically changing cybersecurity environment and the constant emergence of new threats, i.e., GenAI and LLMs' latest developments. Thus, continuous research and development of new mechanisms is crucial and mandatory. The present review, which was carried out to record current methods, techniques, software, and hardware in the arsenal of cybersecurity dynamic risk assessment and management, constitutes a complete set of possible solutions and alternatives for security policy and strategy designers and human or AI actuators that require contemporary approaches. Research space under the prism of financial decisions and investment risks in the domain of dynamic cyber-physical security is existent.

GenAI enhances defensive capabilities through real-time anomaly detection, predictive modeling, and automated compliance tracking while also introducing risks such as its potential misuse for sophisticated attacks like phishing and malware generation. The dual nature of GenAI highlights the need for stringent ethical frameworks, robust governance models, and adherence to regulations like GDPR and ISO to ensure transparency and accountability.

Despite the promising potential of GenAI in cybersecurity, practical integration with established governance frameworks like NIST and ISO introduces both opportunities and implementation challenges. For example, NIST's AI Risk Management Framework (AI RMF) encourages the alignment of AI systems with principles such as transparency, reliability, and privacy preservation [48]. Similarly, ISO/IEC 42001:2023 focuses on AI management system requirements, aiming to harmonize AI outputs with compliance goals and lifecycle governance [49].

However, aligning GenAI-generated insights with these frameworks is not trivial. GenAI systems often produce probabilistic, non-deterministic outputs (e.g., risk narratives or control recommendations) that lack standardized structure or explainability, making integration with rigid compliance controls (e.g., ISO 27001:2022 or NIST SP 800-53 Rev. 5) difficult [50]. This disparity complicates auditability, traceability, and accountability in cybersecurity management.

Mitigation strategies include the use of **structured GenAI output schemas**, such as JSON-based compliance mappers, which translate natural language risk assessments into NIST control labels (e.g., AC-2, SI-4). Techniques like **prompt engineering** and **rule-based post-processing** can help constrain GenAI outputs to follow taxonomies compatible with control frameworks. Moreover, incorporating **Explainable AI (XAI)** methods—such as SHAP or LIME—enables model transparency, helping risk managers justify GenAI-driven actions in regulated

environments. Integrating explainable AI into dynamic risk frameworks enhances transparency in high-stakes environments [51].

To bridge the gap further, hybrid systems are emerging where GenAI assists rather than replaces traditional tools. For instance, GenAI might synthesize audit evidence narratives while deterministic systems handle final control validation. Such co-functionality enables organizations to leverage GenAI's generative power without sacrificing formal alignment with ISO/NIST-based cybersecurity governance.

Dynamic risk assessment methods, leveraging tools such as Bayesian networks, neural networks, and attack graphs, enable organizations to anticipate and mitigate threats proactively by analyzing data from diverse sources in real-time. These advancements, however, demand a significant adaptation of skills among cybersecurity professionals, who must balance the potential of GenAI with its associated risks. Maintaining public trust through transparent systems and ethical AI-driven decision-making is paramount, particularly as organizations employ these tools to optimize security postures. As demonstrated in recent literature [52], deep learning techniques such as CNNs and RNNs play a pivotal role in advancing proactive cybersecurity strategies, especially where real-time pattern recognition is critical.

Overall, while GenAI and dynamic methodologies hold immense promise for revolutionizing cybersecurity practices, their effective implementation requires a careful balance of innovation, governance, and skill adaptation to navigate the complex challenges of a rapidly changing threat landscape.

In conclusion, this review presented definitions, tools, and modern methods for dynamic risk management. Most of the papers focus on and elaborate on machine learning and attack graph models. Most of the models follow a layered architecture and try to predict attacks through the threats' vulnerabilities and calculate the financial cost of damage to the organization and its assets through dynamic analysis and assessment. Despite their strengths, these methods face limitations, such as dependency on quality data and the need for skilled professionals to interpret results.

Dynamic risk assessment models are instrumental in diverse domains, from critical infrastructure protection to connected and autonomous vehicles (CAVs). For example:

- In **smart cities**, neural networks enable rapid adaptation to changing conditions, ensuring the safety of IoT-based systems.
- In **industrial control systems (ICSs)**, quantitative methods support investment decisions by evaluating the financial and operational impact of cyber risks.

These examples demonstrate the versatility and applicability of dynamic models across industries. The systems collect multiple data from different types of sensors. The most popular methodologies for dynamic risk assessment for attack predictions are found in mathematical models (e.g., Hidden Markov Model (HMM) and Bayesian networks). Other machine learning algorithms have been used, such as K-Nearest Neighbors, but Bayesian networks seem to provide the best results under the conditions applied. Both ICT systems and the threat landscape continuously evolve. At the average organization, cyber-physical security management is a novel term based on purely technical processes and vendor tools, performed by administrators who are not necessarily aware of the organization's business and strategic aspects.

This gap between technical and managerial levels calls for dynamic risk assessment and management methods. Dynamic cybersecurity risk management is paramount to tackling potential breaches and putting up guardrails while navigating through the maze that unfolds.

The dual-edged nature of GenAI necessitates robust ethical frameworks and adherence to regulations like GDPR and ISO standards. Ensuring transparency and accountability in AI-driven decision-making processes is critical to maintaining public trust.

Although there are **challenges and research gaps** that persist and should be investigated further:

1) **Data scarcity**: Many models require extensive historical data, which may not always be available, particularly in ICSs.
2) **Interdisciplinary integration**: Bridging the gap between technical and managerial domains remains a challenge, as cybersecurity professionals must adapt to both.
3) **Ethical risks of GenAI**: Misuse of generative models for sophisticated attacks highlights the need for proactive governance.

To advance the field, future research should focus on:

- Enhancing interoperability between dynamic models and existing frameworks like NIST and ISO standards.
- Developing adaptive training datasets for AI models to improve predictive accuracy.
- Exploring the application of GenAI in under-researched areas such as maritime cybersecurity and healthcare systems.

Dynamic risk management is indispensable in navigating the complexities of modern cybersecurity. While GenAI and advanced methodologies hold immense promise, their effective implementation requires a careful balance of innovation, governance, and skill adaptation. By addressing the identified gaps and challenges, organizations can optimize their security postures and safeguard against an ever-evolving threat landscape.

Institutional review board statement: Not applicable.

Informed consent statement: Not applicable.

Conflict of interest: The authors declare no conflict of interest.

References

1. Taherdoost H. Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. Electronics. 2022; 11(14). doi: 10.3390/electronics11142181
2. Marchal N, Xu R, Elasmar R, et al. Generative AI Misuse: A Taxonomy of Tactics and Insights from Real-World Data. Available online: http://doi.org/10.48550/arXiv.2406.13843 (accessed on 5 April 2025).
3. Blake H. Generative AI in Cyber Security: New Threats and Solutions for Adversarial Attacks. 2024. Available online: https://www.researchgate.net/profile/Harrison-Blake-2/publication/387136288_Generative_AI_in_Cyber_Security_New_Threats_and_Solutions_for_Adversarial_Attacks/links/6761c8fb2d60b863e276c9b4/Generative-AI-in-Cyber-Security-New-Threats-and-Solutions-for-Adversarial-Attacks.pdf (accessed on 5 April 2025).

4. Parker J. Generative AI (GAI) Use for Cybersecurity Resilience: A Scoping Literature Review. International Journal of Applied Science. 2025; 8(2). doi: 10.30560/ijas.v8n2p1
5. Mizrak F. Integrating cybersecurity risk management into strategic management: A comprehensive literature review. Research Journal of Business and Management. 2023; 10(3): 98–108. doi: 10.17261/Pressacademia.2023.1807
6. CNSS-Glossary|CSRC. Available online: https://csrc.nist.gov/glossary/term/CNSS (accessed on 5 April 2025).
7. Tweneboah-Koduah S, Buchanan W. Security Risk Assessment of Critical Infrastructure Systems: A Comparative Study. The Computer Journal. 2018; 61(9): 1389–1406. doi: 10.1093/comjnl/bxy002
8. Cheimonidis P, Rantos K. Dynamic Risk Assessment in Cybersecurity: A Systematic Literature Review. Future Internet. 2023; 15(10). doi: 10.3390/fi15100324
9. Ee S, O'Brien J, Williams Z, et al. Adapting cybersecurity frameworks to manage frontier AI risks: A defense-in-depth approach. 2024; Available online: http://doi.org/10.48550/arXiv.2408.07933 (accessed on 5 April 2025).
10. Kaur R, Gabrijelčič D, Klobučar T. Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion. 2023; 97: 101804. doi: 10.1016/j.inffus.2023.101804
11. Chen P, Wu L, Wang L. AI Fairness in Data Management and Analytics: A Review on Challenges, Methodologies and Applications. Applied Sciences. 2023; 13(18). doi: 10.3390/app131810258
12. Salem AH, Azzam SM, Emam OE, Abohany AA. Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. Journal of Big Data. 2025.
13. Sivakumar J, Salman NR, Salman FR, et al. Ai-Driven Cyber Threat Detection: Enhancing Security Through Intelligent Engineering Systems. Journal of Information Systems Engineering and Management. 2025; 10(19s). doi: 10.52783/jisem.v10i19s.3116
14. Khanna S. AI in Cybersecurity: A Comprehensive Review of Threat Detection and Prevention Mechanisms. International Journal of Sustainable Devlopment in Field of IT. 2025; 17(17).
15. Petticrew M, Roberts H. Systematic Reviews in the Social Sciences: A Practical Guide. John Wiley & Sons; 2008.
16. Larriva-Novo X, Vega-Barbas M, Villagrá VA, et al. 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; 25–28 August 2020; New York, NY, United States. p. 9.
17. 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; 4–7 November 2020; New York, NY, United States. pp. 1–8.
18. El Amin H, Samhat AE, Chamoun M, et al. An Integrated Approach to Cyber Risk Management with Cyber Threat Intelligence Framework to Secure Critical Infrastructure. Journal of Cybersecurity and Privacy. 2024; 4(2): 357–381. doi: 10.3390/jcp4020018
19. 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); 27–28 July 2020; London, UK. pp. 295–300.
20. Chatterjee S, Thekdi S. An iterative learning and inference approach to managing dynamic cyber vulnerabilities of complex systems. Reliability Engineering & System Safety. 2020; 193. doi: 10.1016/j.ress.2019.106664
21. Burton R, Rocha L. Whitelists that Work: Creating Defensible Dynamic Whitelists with Statistical Learning. In: Proceedings of the 2019 APWG Symposium on Electronic Crime Research (eCrime); 13–15 November 2019; Pittsburgh, PA, USA.
22. Suloyeva S, Grishunin S, Burova E. Developing a Cybersecurity Risk Analysis System for High-Tech Equipment in Machine Industry. In: Proceedings of the 2019 International SPBPU Scientific Conference on Innovations in Digital Economy; 24–25 October 2019; New York, NY, United States. pp. 1–6.
23. Eckhart M, Brenner B, Ekelhart A, Weippl E. Quantitative security risk assessment for industrial control systems: Research opportunities and challenges. Journal of Internet Services and Information Security. 2019; 9(3): 52–73. doi: 10.22667/JISIS.2019.08.31.052
24. Yaqoob T, Arshad A, Abbas H, et al. Framework for Calculating Return on Security Investment (ROSI) for Security-Oriented Organizations. Future Generation Computer Systems. 2019; 95: 754–763. doi: 10.1016/j.future.2018.12.033
25. 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); 30 May–1 June 2016; Shanghai, China. pp. 693–698.

26. Le A, Maple C. A simplified approach for dynamic security risk management in connected and autonomous vehicles. In: Proceedings of the Living in the Internet of Things (IoT 2019); 1–2 May 2019; London, UK.
27. Rahmati M. Towards Explainable and Lightweight AI for Real-Time Cyber Threat Hunting in Edge Networks. Available online: http://doi.org/10.48550/arXiv.2504.16118 (accessed on 5 April 2025).
28. Le A, Maple C, Watson T. A profile-driven dynamic risk assessment framework for connected and autonomous vehicles. In: Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT—2018; 28–29 March 2018; London, UK.
29. Pillai A, Schnebly J, Sengupta S. Development of Web-based Automated System for Cyber Analytic Applications. In: Proceedings of the 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON); 8–10 November 2018; New York, NY, USA. p. 871.
30. Gonzalez-Granadillo G, Dubus S, Motzek A, et al., Dynamic risk management response system to handle cyber threats. Future Generation Computer Systems. 2018; 83: 535–552. doi: 10.1016/j.future.2017.05.043
31. Zhang Q, Zhou C, Tian YC, et al. A Fuzzy Probability Bayesian Network Approach for Dynamic Cybersecurity Risk Assessment in Industrial Control Systems. IEEE Transactions on Industrial Informatics. 2018; 14(6): 2497–2506. doi: 10.1109/TII.2017.2768998
32. 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); 2–4 November 2016; Tashkent, Uzbekistan.
33. Kalinin M, Krundyshev V, Zegzhda P. Cybersecurity risk assessment in smart city infrastructures. Machines. 2021; 9(4). doi: 10.3390/machines9040078
34. AlSadhan T, Park JS. Enhancing risk-based decisions by leveraging cyber security automation. In: Proceedings of the 2016 European Intelligence and Security Informatics Conference (EISIC); 17–19 August 2016; Uppsala, Sweden. pp. 164–167.
35. Duzha A, Gouvas P, Canepa M. MITIGATE*: An Innovative Cyber-Security Maritime Supply Chain Risk Management System. In: Proceedings of the 1st Italian Conference on Cyber Security (ITASEC'17); 17–20 January 2017; Venice, Italy. p. 5.
36. Yigit Y, Buchanan WJ, Tehrani MG, Maglaras L. Review of Generative AI Methods in Cybersecurity. Available online: http://arxiv.org/abs/2403.08701 (accessed on 5 April 2025).
37. Beltran MA, Ruiz Mondragon MI, Han SH. Comparative Analysis of Generative AI Risks in the Public Sector. In: Proceedings of the 25th Annual International Conference on Digital Government Research; 11–14 June 2024; New York, NY, USA. pp. 610–617.
38. Falade PV. Decoding the Threat Landscape: ChatGPT, FraudGPT, and WormGPT in Social Engineering Attacks. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2023; 9(5): 185–198.
39. Mavikumbure HS, Cobilean V, Wickramasinghe CS, et al. Generative AI in Cyber Security of Cyber Physical Systems: Benefits and Threats. In: Proceedings of the 2024 16th International Conference on Human System Interaction (HSI); 8–11 July 2024; Paris, France. pp. 1–8.
40. Chandrasekaran AS. Harnessing the Power of Generative Artificial Intelligence (GenAI) in Governance, Risk Management, and Compliance (GRC). International Research Journal of Engineering and Technology. 2024; 11(5).
41. Capodieci N, Sanchez-Adames C, Harris J, Tatar U. The Impact of Generative AI and LLMs on the Cybersecurity Profession. In: Proceedings of the 2024 Systems and Information Engineering Design Symposium (SIEDS); 3 May 2024; Charlottesville, VA, USA. pp. 448–453.
42. Radanliev P, Santos O, Ani UD. Generative AI Cybersecurity and Resilience. Frontiers in Artificial Intelligence. 2025; 8. doi: 10.3389/frai.2025.1568360
43. Fatima F, Hyatt JC, Rehman SU, et al. Resilience and risk management in cybersecurity: A grounded theory study of emotional, psychological, and organizational dynamics. Journal of Economy and Technology. 2024; 2: 247–257. doi: 10.1016/j.ject.2024.08.004
44. Sen MA. Attention-GAN for Anomaly Detection: A Cutting-Edge Approach to Cybersecurity Threat Management. Available online: http://doi.org/10.48550/arXiv.2402.15945 (accessed on 5 April 2025).
45. Tallam K. CyberSentinel: An Emergent Threat Detection System for AI Security. Available online: https://arxiv.org/abs/2502.14966v1 (accessed on 5 April 2025).

46. How can tech leaders manage emerging generative AI risks today while keeping the future in mind. Available online: https://www2.deloitte.com/us/en/insights/topics/digital-transformation/four-emerging-categories-of-gen-ai-risks.html (accessed on 5 April 2025).
47. Alshar'e M. CYBER SECURITY FRAMEWORK SELECTION: COMPARISION OF NIST AND ISO27001. Applied Computing Journal. 2023; 3(1): 245–255. doi: 10.52098/acj.202364
48. Tabassi E. Artificial Intelligence Risk Management Framework (AI RMF 1.0). Available online: https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-ai-rmf-10 (accessed on 5 April 2025).
49. ISO/IEC 42001:2023. Available online: https://www.iso.org/standard/81230.html (accessed on 5 April 2025).
50. McIntosh TR, Susnjak T, Liu T, et al. From COBIT to ISO 42001: Evaluating Cybersecurity Frameworks for Opportunities, Risks, and Regulatory Compliance in Commercializing Large Language Models. Computers & Security; 2024; 144: 103964. doi: 10.1016/j.cose.2024.103964
51. Islam S, Basheer N, Silvestri S, et al. Intelligent Dynamic Cybersecurity Risk Management Framework with Explainability and Interpretability of AI models for Enhancing Security and Resilience of Digital Infrastructure. 2024. Preprint. doi: 10.21203/rs.3.rs-4796809/v1
52. Ubeysinghe R. AI-Powered Threat Detection in Cybersecurity: A Comprehensive Review. 2024. Available online: https://www.researchgate.net/publication/387271355_AI-Powered_Threat_Detection_in_Cybersecurity_A_Comprehensive_Review (accessed on 5 April 2025).