sensors

MDPI

Review

Survey of Technology in Network Security Situation Awareness

Junwei Zhang [1], Huamin Feng [2,*], Biao Liu [2] and Dongmei Zhao [3]

[1] School of Cyber Engineering, Xidian University, Xi'an 710126, China
[2] School of Cyber Engineering, Beijing Electronic Science and Technology Institute, Beijing 100070, China
[3] College of Computer and Cyber Security, Hebei Normal University, Shijiazhuang 050025, China
* Correspondence: fenghm@besti.edu.cn

Abstract: Network security situation awareness (NSSA) is an integral part of cybersecurity defense, and it is essential for cybersecurity managers to respond to increasingly sophisticated cyber threats. Different from traditional security measures, NSSA can identify the behavior of various activities in the network and conduct intent understanding and impact assessment from a macro perspective so as to provide reasonable decision support, predicting the development trend of network security. It is a means to analyze the network security quantitatively. Although NSSA has received extensive attention and exploration, there is a lack of comprehensive reviews of the related technologies. This paper presents a state-of-the-art study on NSSA that can help bridge the current research status and future large-scale application. First, the paper provides a concise introduction to NSSA, highlighting its development process. Then, the paper focuses on the research progress of key technologies in recent years. We further discuss the classic use cases of NSSA. Finally, the survey details various challenges and potential research directions related to NSSA.

Keywords: situation awareness; situation assessment; situation prediction; NSSA visualization; artificial intelligence

Citation: Zhang, J.; Feng, H.; Liu, B.; Zhao, D. Survey of Technology in Network Security Situation Awareness. *Sensors* **2023**, *23*, 2608. https://doi.org/10.3390/s23052608

Academic Editors: Shaoen Wu, Jinbo Xiong, Periklis Chatzimisios and Mahmoud Daneshmand

Received: 20 January 2023
Revised: 23 February 2023
Accepted: 24 February 2023
Published: 27 February 2023

1. Introduction

Recent years have witnessed the rapid development of emerging technologies, such as big data, cloud computing, the Internet of Things (IoT) [1,2], and blockchain [3]. Computer networks have become the supporting infrastructure for informatization construction, profoundly affecting economic development and human lifestyles [4]. Since the current internet infrastructure is witnessing explosive growth in terms of connected devices and the amount of generated content, despite the networks providing various conveniences for people, some security concerns may arise due to potential attacks [5]. Specifically, most network applications have security vulnerabilities, network attack threats are becoming more and more rampant [6], and network security risks are becoming more and more complex. On a global scale, the internet is frequently attacked, such as Sierra Wireless, an IoT solution provider [7], encountering a ransomware company, which damaged its internal system and made its official website inaccessible. The stock price fell 11.95% that day. Although it did not affect the products and services of the company's other customers, it did affect the company's products and services, and business development also experienced a certain impact.Moreover, the Portuguese energy giant, Energias De Portugal (EDP), suffered a ransomware attack that saw 10 TB of sensitive corporate data stolen and used to blackmail the corporation for nearly EUR 11 million [8].

In recent years, network attacks have gradually shown large-scale, coordinated, and multi-stage characteristics. Network attacks are no longer isolated incidents, and multi-step attacks are emerging one after another. For example, the increasingly widespread Zeus botnet [9], and worm attacks are highly concealed, penetrating and targeted multi-step attacks [10]. Therefore, it is urgent to study the network security situation awareness (NSSA) for multi-step attacks to improve the identification and recognition of multi-step

attacks [11]. The rise of the concept of NSSA has aroused the interest of researchers simultaneously [12–16].

Although there is no uniform definition for NSSA, in general, NSSA extracts the elements which affect the network security, understands, evaluates, and predicts the development trend of the future network. Quantitative analysis and accurate prediction of network security is a means to provide practical decision support for network administrators, to improve the emergency response [17]. With this concept, NSSA can provide various important benefits to network security, as follows:

- The first is to be comprehensive, to perceive the overall situation and all network security events from the perspective of the entire network;
- The second is to be able to accurately and effectively detect network attacks;
- The third is real-time network attacks that break out instantaneously, and real-time detection and real-time evaluation are the core indicators of NSSA.

With these unique advantages, NSSA has become a crucial solution and critical development direction of network security protection since it can change the situation of "active attack by hackers and passive defense by enterprises". Driven by the recent advances of NSSA, several reviews of related work have appeared. For example, the study in [18] provided a survey on the concept and review of research on CSA. It is worth noting that NSSA and CSA are two different expressions, and different authors use them differently, but both refer to network security situational awareness. The author in [19] presented a literature review of NSSA, based on systematic queries in four leading scientific databases. Moreover, the visualizations to support NSSA were investigated in [20]. An overview on the analysis framework of NSSA and comparison of implementation methods was provided in [21]. Another work in [22] presented a systematic explanation for the definition of NSSA and the understanding of the basic concept. Similarly, the authors in [23] discussed the NSSA concept from the architectural perspective, along with the structure and key technology of NSSA. Furthermore, a survey of prediction, and forecasting methods used in NSSA was proposed in [24]. The comparison of the related works and our paper is summarized in Table 1.

Although NSSA has been studied extensively in the literature, there has been no work to conduct a comprehensive and dedicated review of the NSSA technology. The critical contribution of this paper lies in the extensive discussion of NSSA, including the history, model, and taxonomy. Meanwhile, we start from the three functional modules of situation element acquisition, evaluation, and prediction, and introduce the current research situation of each technology in detail. We further discuss the classic use cases of NSSA. Finally, we discuss several important research challenges and future directions in NSSA.

This survey structure is shown in Figure 1. The rest of this survey is outlined as follows. Section 2 introduces the origin, concept, model and the taxonomy of the NSSA. Section 3 discusses the critical technologies of NSSA, including the scientific research literature of the three functional modules in recent years, the technical problems that have been solved, and the technical problems that need to be solved, along with possible directions for future research. Section 4 presents the classic use cases of NSSA. Section 5 concludes the paper and provides an outlook on future research.

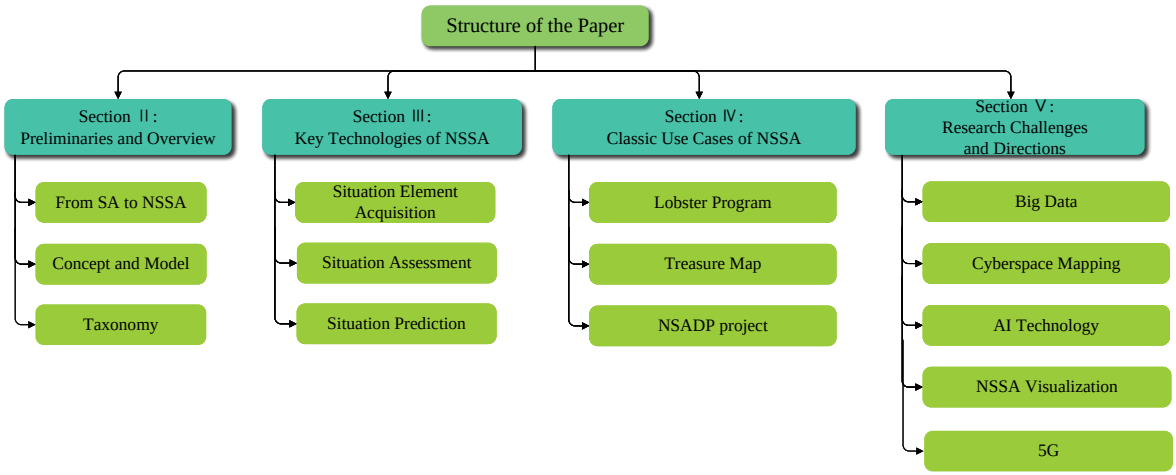

Figure 1. Organization of this survey.

Table 1. Existing surveys on NSSA topics and our new contributions.

Related Works	Key Contributions	Limitations
[18]	A survey on concept and review of research on cyber situation awareness (CSA)	The applications have not been presented.
[19]	A review of CSA, based on systematic queries in four leading scientific databases	The paper only analyzes the research agenda in the area of CSA.
[20]	A survey on the scientific literature on CSA visualizations	The paper only focuses on visualizations.
[21]	A survey on the analysis framework of Network Security Situation Awareness (NSSA) and comparison of implementation methods	The use of NSSA and applications have not been presented.
[22]	A systematic explanation for the definition of NSSA and the understanding of the basic concept	The paper only focuses on discussing the concept and the framework of NSSA.
[23]	A survey on concept, structure and the key technology of NSSA	The analysis of NSSA technologies is limited. Moreover, discussions for use cases are lacking.
[24]	A survey of forecasting methods for NSSA	The paper only focuses on prediction of NSSA, comprehension and assessment are not considered.
Our paper	An extensive survey on the NSSA integration. First, we extensively discuss the concept and the history of NSSA in network security. Second, the critical research works of NSSA technology are also analyzed in detail, including technical classification, technical characteristics, strengths and weaknesses. Third, the classic use cases of NSSA are provided at the national level. Finally, research challenges and directions are also highlighted.	

2. Preliminaries and Overview

The background and history of NSSA are presented in this section. The model and the taxonomy of NSSA are also discussed.

2.1. From Situation Awareness (SA) to NSSA

"Situation" was first used in military warfare to describe large-scale research objects' overall state and changing trends. These research objects are dynamic, affected by many factors, and have relatively complex internal structures. Therefore, a situation is not an illustration of a single situation or state but a comprehensive concept of an entirety that includes a single element.

The early seeds of SA as an area of study were formed in the late 1980s. The foundations of a theory of how people acquired and maintained SA has developed several methods for measuring SA in system design evaluation. The 1990s have expanded this early work to include many other domains and research objectives. From its beginnings in the cockpit realm, more recent work has expanded to include air traffic control, medicine, control rooms, ground transportation, maintenance, space, and education. Research objectives have also grown from one of system design and evaluation to focus on training, selection, and more basic research on the cognitive processes themselves [25].

SA originated from the research of the American military in a military confrontation. In military terms, the goal of situational awareness is to give commanders an understanding of both sides, including the position, current status, and capabilities of the enemy so that they can make quick and correct decisions to know one another. At the International Human Factor Annual Conference, Endsley in [26] first suggested the idea of situational awareness, which is "to identify and grasp environmental aspects in a given location and time, and to predict the future trend".

Tim Bass [27] of the US Air Force Communications and Information Center proposed NSSA and integrated the concept of SA into the field of cyberspace security for the first time. NSSA is designed to provide network security administrators with a basis for decision making to shorten decision-making time, which can effectively improve the network protection awareness of managers. Franke U. [19] believes that the scope of situational awareness is very large, and NSSA is a part of it, which highlights the "network" environment. However, this definition is not clear enough and does not specify whether it is a safe direction for situational awareness. The research of [22] proposes that NSSA is a series of processes for identifying and understanding the state of network security, which mainly includes three steps: Integrate the original data steps measured from the system and realize the extraction of the background state and activity semantics of the system. Second, identify the various types of network activities that exist and the intentions of abnormal movements in them. Finally, the network security situation characterized by this and the influence of the situation on the normal behavior of the network system is obtained.

Then, the research in [28] used a rough set attribute reduction algorithm to extract core attributes and used a particle swarm optimization algorithm to optimize the radial basis function neural network to identify network attacks. In another study, Ref. [29] divided the network situation level, optimized the back propagation (BP) neural network parameters through the simulated annealing algorithm, and determined the network space situation awareness level.

Jia et al. [23] proposed the definition of NSSA in a large-scale network environment. The specific content is as follows: NSSA is to extract, understand, and evaluate the security elements that affect the network security situation, and predict the future security situation based on the assessment results. Moreover, the research in [30] integrated security information from three dimensions, including threat, vulnerability [31], and stability at the decision-making level to measure the security status of the entire network. Zheng et al. used Dempster–Shafer (D-S) evidence theory to integrate host firewall data, web firewall data, and intrusion detection data to evaluate network security.

To our knowledge, academic research on NSSA has increased in frequency and depth. However, as of this writing, a consistent and thorough definition of NSSA has not been developed. Therefore, the systematic and complete definition of NSSA is also an important topic for future research.

2.2. Concept and Model

2.2.1. Model Overview

The earliest and most widely used definition of situational awareness is that of Endsley [32]: Perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in near future. In this definition, situational awareness is divided into three levels as shown in Figure 2.

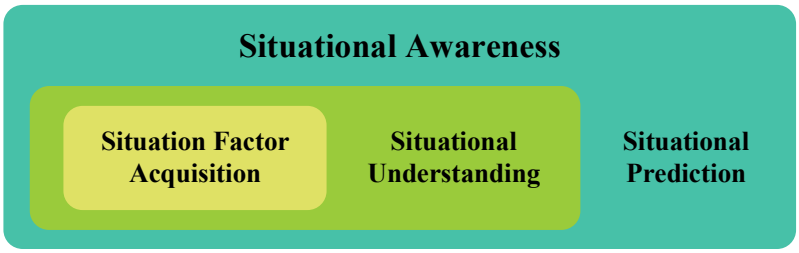

Figure 2. Endsley situational awareness model.

The multi-level model is the earliest situational awareness model, and it consists of three levels. The first level is situation element acquisition, and the most important task is to obtain critical data. The second is situation understanding, which is responsible for analyzing the critical data obtained by the previous level. The last level is situation prediction [18], which uses the data analysis findings from the level before to forecast what may happen in the future.

Additionally, the JDL model is the traditional SA model [33], a data fusion model proposed by the United States Joint Laboratory (JDL). The SA model is broken down into five levels in this concept. The first level is data preprocessing; the main task is to process incomplete data and remove and filter redundant data information. The second level is event extraction, which carries on the relatively structured data and information already processed at the first level, standardizes network events, and prepares for the next level. The third level is the situation assessment, which evaluates the extracted events to form a comprehensive situation map of the network and provides auxiliary information for the administrator to make decisions. The fourth level is impact assessment, which maps the formed situation to the future environment and evaluates the impact of future battlefields or predicted combat behaviors. The fifth level is resource management, process control, and optimization; the major work is to conduct real-time monitoring and evaluation of the whole data fusion process and integrate all levels of information to achieve the optimization of relevant resources [34].

Safety is the major focus of situational awareness in network applications. A multisensory-based intrusion detection framework was presented by Tim Bass [35] (see Figure 3). The model is the prototype for situational awareness in network security, and the reasoning framework includes intrusion detection, intrusion behavior, intrusion identity recognition, scenario assessment, threat assessment, etc. The term NSSA was also discussed by Wang [36] according to the Chinese translation of Endsley.

Additionally, an NSSA model based on netflow was proposed by Lai et al. [37] in their study. Utilizing netflow technology can effectively achieve NSSA, quickly identify weaknesses and potential threats, and graphically convey them to decision makers for thorough network monitoring. Performance optimization concerns must also be further investigated because the system must handle enormous volumes of data and information. The properties of huge data in large-scale networks, as illustrated in Figure 4, led Jia et al. [38] to develop an NSSA model for such networks.

The NSSA system proposed by Kokkonen T. [39] consists of an input interface layer, an information normalization layer, a data fusion layer and a visualization layer. The model emphasizes the role of visualization, which also includes a human–computer interaction interface and an information-sharing interface. By combining and extending the JDL data fusion model and Endsley's situation awareness model, Kokkonen [40] proposed an NSSA model, which consists of four layers, including a recognition layer, understanding layer, prediction layer and measure layer from bottom to top. Compared with the three-tier architecture of the traditional model, this model adds a measured layer, which is more comprehensive, by providing alternative measures and their impacts to assist decision makers in making decisions.

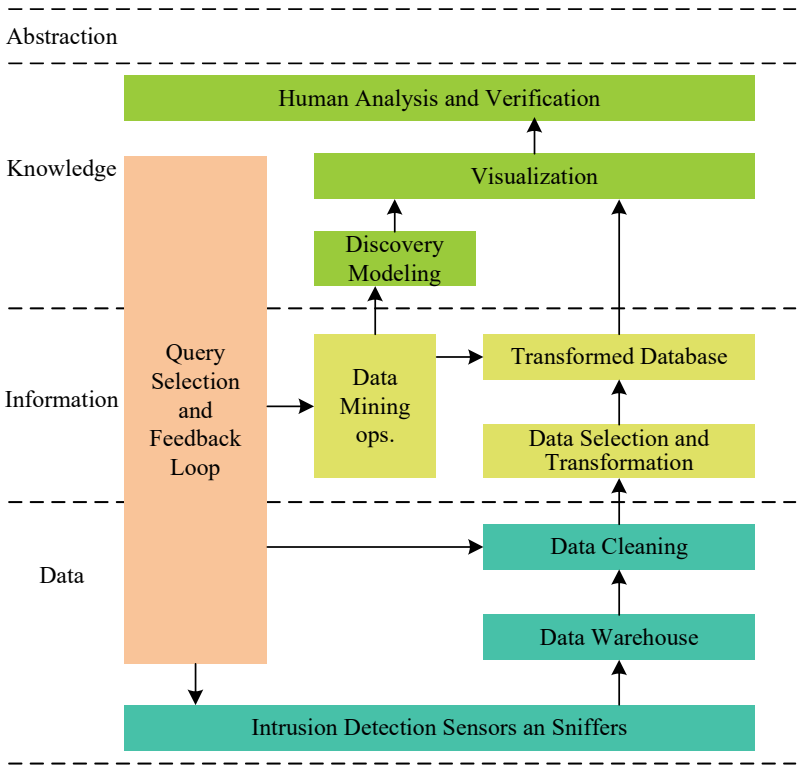

Figure 3. Intrusion detection data fusion model.

Most of the current models are based on the three-tier architecture of the traditional model, supplemented from the perspectives of dynamic circulation, visualization, and automation, and enrich and refine the model according to the needs of different application scenarios.

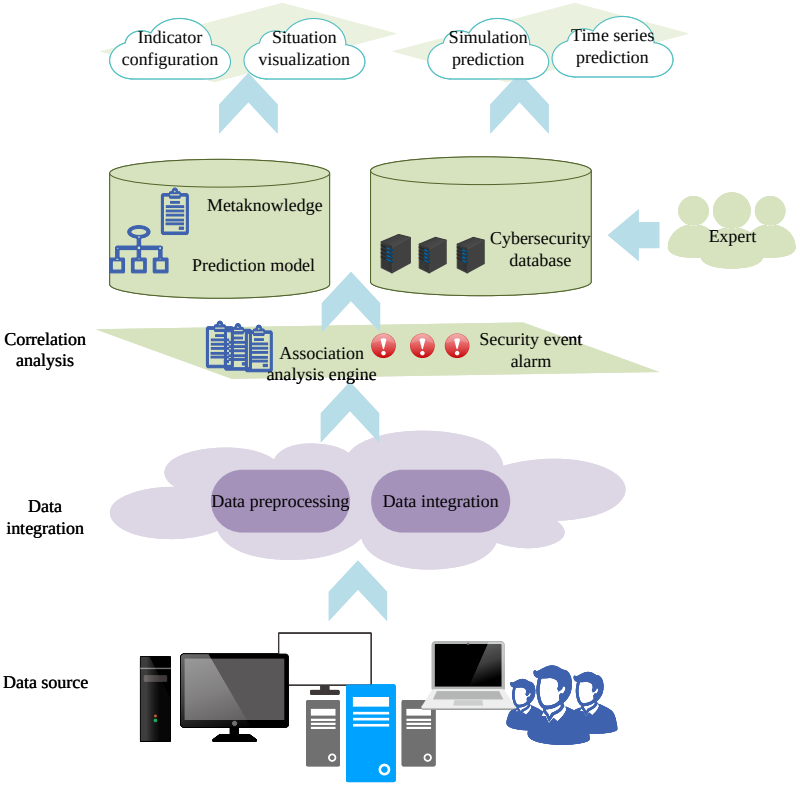

Figure 4. NSSA model for large-scale networks.

2.2.2. Explanation of the Example

Here, we present an example of the operational principles and data processing methods of an NSSA model [38] as shown in the figure. The model consists of four levels. The first level is data integration, which involves preprocessing and integrating multi-source data with different formats. Data are integrated into a unified format by deploying agents to the data sources, and then redundant and noisy data are removed. The second level is correlation analysis, which applies association rules in the network security knowledge base to establish reliability-based correlations among different alarm information and match alarm events. The events are analyzed in conjunction with vulnerabilities, assets, and the events themselves to effectively reduce the false-positive rate of security alarms. The third level is the indicator system and situational display, which calculates network security indicators using scientific methods based on the indicator model and correlation analysis results in the knowledge base, and displays the network security situation visually. Specifically, the basic operation index, network vulnerability index, and network threat index are calculated separately and then integrated to obtain the network security index. Define the network security index at time t as follows:

$$\begin{bmatrix} C(t) \\ I(t) \\ A(t) \end{bmatrix} = \begin{bmatrix} C_1 & C_2 & \cdots & C_n \\ I_1 & I_2 & \cdots & I_n \\ A_1 & A_2 & \cdots & A_n \end{bmatrix} \begin{bmatrix} E_1(t) \\ E_2(t) \\ \vdots \\ E_n(t) \end{bmatrix} \quad (1)$$

In the formula, $E_i(t)$ represents the threat index of security event E_i at time t, n is the number of security event types, and $C(t)$, $I(t)$, and $A(t)$ respectively represent the confidentiality, integrity, and availability indices of T at time t. The fourth layer is situation prediction. Based on the prediction model learned from historical data, a prediction algorithm based on mean and trend features is used to predict network security events.

2.3. Taxonomy

Although considerable work has been conducted on the definitions and associated models of SA and NSSA, little has been conducted to date to classify their constituents. The most representative taxonomy of NSSA is provided by Evesti et al., which includes data collection (actions and policies), analysis, and visualization [41]. What is missing from that taxonomy is a projection-level taxonomy and any associated tools and methods. To overcome the completeness of taxonomy, Martin et al. improved the category [18].

This classification adjusts the category to reflect Endsley's SA three-tier model. Specifically, the perception part mainly uses different tools to obtain network security data, including scanning tools, intrusion detection systems and so on. Comprehension is based on perception, through the calculation and processing of massive data, bypassing complex and difficult appearances, and helping analysts and decision makers understand network status from a higher-dimensional perspective. Projection is based on the perception, comprehension, and processing of historical and current situation data series, through the establishment of mathematical models, exploring the laws of evolution, and reasoning about future development trends and conditions. However, in our opinion, the visualization should be a step after analysis and projection, an essential part of presenting the results of all analysis and projection to administrators, and should not be placed under comprehension. So, the paper moves the visualization to the top level. Figure 5 outlines the improved classification of NSSA, with the most significant changes occurring at the top level, where visualization is considered the final stage of NSSA.

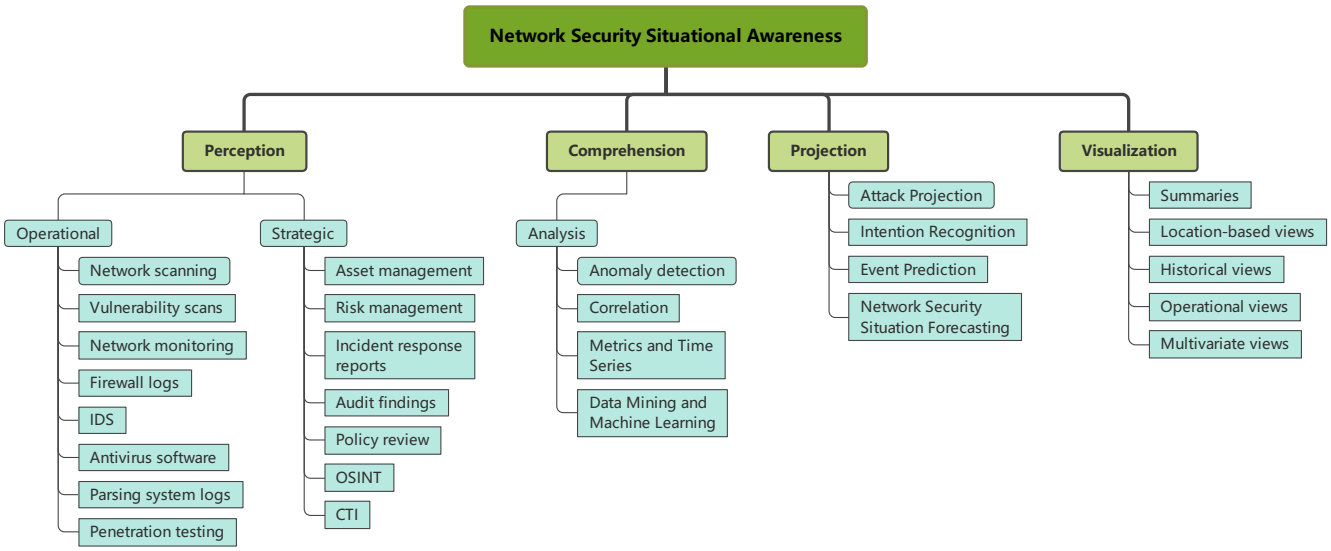

Figure 5. Taxonomy of NSSA tools and components.

3. Key Technologies of NSSA

There are still some issues with researchers' comprehension of the relationship between NSSA in various settings, despite the fact that different researchers have diverse perspectives on how to divide the many stages of NSSA. Researchers most frequently utilize these three functional modules to classify NSSA: situation element acquisition, situation evaluation, and situation prediction. As depicted in Figure 6, this section classifies and introduces the primary NSSA technologies.

3.1. Network Security Situation Element Acquisition

Undoubtedly, situation element acquisition is the premise of NSSA. In most cases, the situational elements mainly include the static configuration and dynamic information of the network [42]. The former contains data about the topology of the network, vulnerabilities, and status. The latter phrase alludes to threat data that have been gathered through log gathering and analysis technologies of various defenses. The efficient integration of this information provides the basis for the high-dimensional abstract understanding of situational awareness. Table 2 summarizes the work on the network security situation elements acquisition.

Table 2. Network security situation elements acquisition.

Ref.	Description	Approach	Strengths	Weaknesses
[43,44]	Obtain vulnerability information	Topological vulnerability analysis (TVA)/ attack graphs	Low evaluation difficulty and high evaluation efficiency	The overall security situation cannot be obtained
[45,46]	Obtain alarm information	Intrusion Detection Systems (IDS) /correlation analysis	Low evaluation difficulty and high evaluation efficiency	The overall security situation cannot be obtained
[47]	Obtain attack information	Honeynets	Low evaluation difficulty and high evaluation efficiency	The overall security situation cannot be obtained
[48]	Obtain multi-source information security data	Index system	Perceive the overall network security situation	High evaluation difficulty and low evaluation efficiency
[49]	Obtain the complex network security information	Botnet detection technology	Perceive the whole network security situation	High time complexity
[50–53]	Obtain multi-source data and information	Multi-source fusion	Perceive the overall network security situation	Reduce the extraction efficiency
[54]	Extract the situation element from multi-source information	Probabilistic neural network	Reduce the system complexity	High time complexity

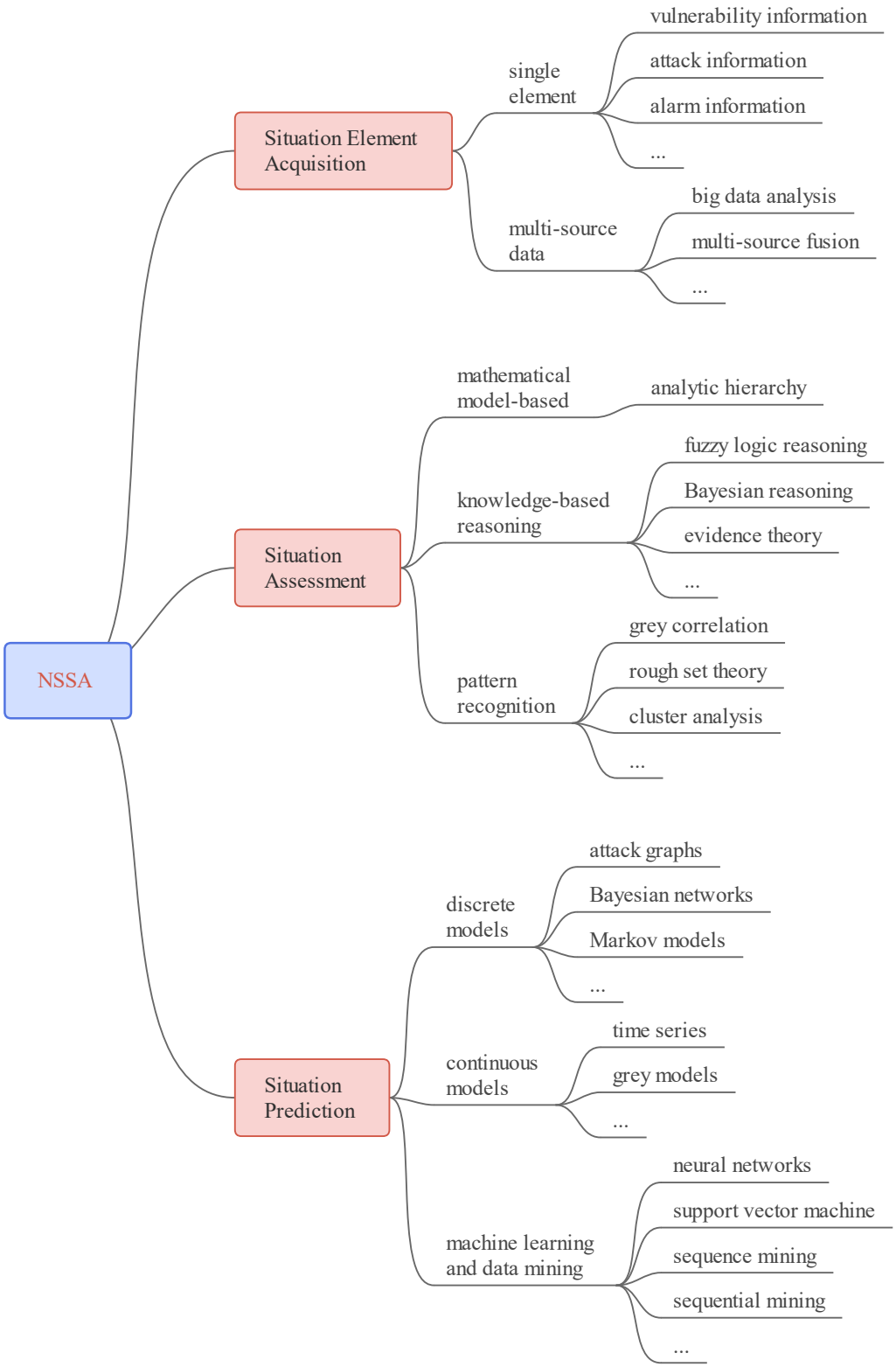

Figure 6. The key technologies of NSSA.

3.1.1. Literature Overview

Researchers mainly extract security data from two levels: single element and multi-source data. Extracting from a single element is mainly used for specific data, such as vulnerability information, warning information, etc., such as the study in [43,44] only gathering network vulnerability information. Barford et al. [47] used attack data and threat information obtained by Honeynet to evaluate the network status, whereas Ning et al. [45,46]

merely collected network alarm information and examined the status of the alarm information to assess the danger of the network. The commonality among the aforementioned studies is that they all gather, examine, and research a single network element, which makes it impossible to gain full information, understand the whole situation or react to the complex and dynamic network environment.

With this in mind, many researchers aim to obtain information from multiple sources and comprehensively evaluate the network security situation from multiple perspectives. For example, Wang Juan's study [48] proposed a layered index model of network security situational awareness based on an index system. The model extracts data from multiple sources of information security following the requirements of hierarchy, information source, and the distinction between structural.

Li et al. proposed a novel multi-source information fusion based heterogeneous network embedding approach [55], for which they jointly modeled the structural proximity, attributed information and labeled information in the framework of non-negative matrix factorization. Additionally, there are many research works on the security extraction of multi-source heterogeneous information network [49–53]. A probabilistic neural network-based technique for extracting security situational elements was suggested by Chang et al. in [54], which addressed the issue of situation element extraction's poor efficiency and accuracy in complex network environments.

3.1.2. Strengths and Weaknesses Analysis

The survey indicates that the majority of researchers concentrate on the single-element acquisition, and the minority of researchers tend to the acquisition of multi-source information. Information data collected from a single source, local network, or a single level have some restrictions and cannot fully describe the current situation of the network; subsequent state analysis and trend prediction require in-depth correlation analysis of multi-source and omnidirectional data. Consequently, the components of a multi-source extraction are necessary. Multi-source data and information, however, do more than only decrease extraction efficiency. However, the multi-source data collection has a lower extraction efficiency due to the severe inconsistency of manufacturers, standards, and targets in current hardware equipment, software systems, and data sources, and inconsistencies in the collective's format, dimension, and semantics. In addition, complex operations, such as the cleaning, integration, specification, and transformation of the collected data, are required. Desultorily data also causes problems with information fusion and redundant processing, and therefore, improving the extraction technique is still a popular area of study.

In addition, the existing information network has grown into a vast, complex, nonlinear system with a high degree of flexibility and dynamics. The generation of secure data is fast, large in scale, and complex in format. For limited communication and computing resources, it is necessary to adopt targeted collection methods, such as on-demand collection and segment collection to reduce the requirements for communication and computing resources for information extraction. There are many theoretical and technical problems in current feature extraction [56]. However, at present, the accuracy of detection results is still insufficient, such as redundant data or error alarm information [57], which still has a great influence on the reconstruction of attack activities. The efficiency of detection is not high. For example, many off-line methods are used for correlating analysis and attack process reconstruction, which cannot meet the requirements of rapid response.

3.2. Network Security Situation Assessment

A crucial part of NSSA is the network security situation evaluation [58]. A network security condition evaluation incorporates several security data sources. Based on a mathematical model and formal logic, the evaluation value of the current network security situation is derived in compliance with the specific requirements of network security assessment. The evaluation value is similar to the stock index, national index and so on to reflect the security state of the network. The mapping from the situation factor to the situation

outcome value is, in essence, what constitutes a network security situation evaluation [59]. In this article, we categorize network security scenario assessment techniques into three groups based on current developments in NSSA: mathematical model-based technique [60], knowledge-based reasoning, and pattern recognition [61]. Table 3 summarizes the work on the network security situation assessment.

It is frequently required to create a network security indication system before performing a network security scenario evaluation. The indicator system is defined as a unified whole composed of a number of interconnected and complementary indicators to evaluate and reflect a certain situation in a certain field. Many scholars have established a network security index system with their own rationality on the premise of a large number of summaries. Wang Juan et al. [48] proposed a layered index model and 25 candidate indicators based on comprehensive security assessment and large-scale network research results and established an index system for situational awareness. On the basis of this achievement, Yue [62] proposed an NSSA system model based on the index system. According to functional requirements, the system is divided into seven modules: "situation data collection-index extraction-index system establishment-data storage-situation assessment-situation prediction-visualization". It briefly introduces the function of each module and its key technical implementation. The construction of the network security index system is the core of the entire network security situation assessment. Its main goal is to establish the mapping relationship between the situation assessment factor and the final situation value. It must also be improved. Just like the above-mentioned representative index system, it has the characteristics of the stage at that time, so the construction of the index system is a process of dynamic evolution.

Table 3. Researchers on the network security situation assessment of relevant work.

Ref.	Approach/Model	Description	Shortcomings
[63]	Analytic hierarchy process (AHP)	Quantitative evaluation at four levels	High time complexity
[64–66]	AHP	Hierarchical analysis of multi-source data	High time complexity
[67]	AHP	Multi-layered methodology for situation assessment	Poor real-time performance
[68]	AHP and fuzzy evaluation method	AHP combined with fuzzy evaluation	Low accuracy
[69]	Fuzzy inference model	Generate risk assessment results using fuzzy inference models	Poor real-time performance
[70,71]	Rough set theory	Build decision tables for assessment	Low precision and high time complexity
[72]	Rough set and fuzzy rough set	Mix information processing improves output accuracy	High time complexity
[73]	Deep learning	Adaptive momentum into the training process of the neural network	Over-dependence on parameter selection
[74]	Deep neural network	Combine Deep Autoencoder (DAE) with Deep Neural Network (DNN)	High time complexity

3.2.1. Literature Overview

The analytic hierarchy process (AHP) is the most common situation assessment method based on mathematical models. The representative research results are the quantitative assessment model of the network system security threat situation proposed by Chen in [63]. The model is divided into four levels from top to bottom—system, host, service, and attack—as shown in Figure 7. However, the model has some shortcomings: only intrusion detection systems (IDSs) alarm information is used in the evaluation method. In real network system deployment, security factors, such as firewalls and system logs, are indispensable. If security information from multiple sources is not included, the situation

assessment will be lost. For this reason, the research in [64–66] all optimized the above-mentioned hierarchical model, and the purpose of optimization is to make the hierarchical analysis of more sources more accurate. Others, such as Jia [67], suggested a multi-layered methodology for evaluating the security of a network, which can reflect the security state of the information system at a certain stage but also has shortcomings, which is that it cannot analyze the state of network security in real time.

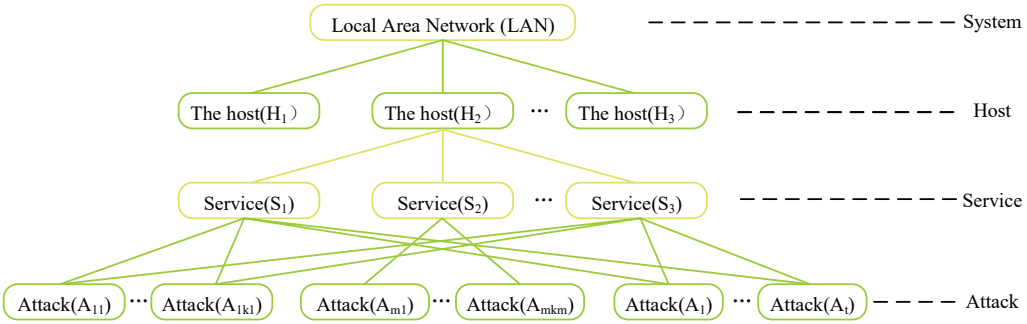

Figure 7. Hierarchical network system security threat situation quantitative assessment model.

The knowledge-based reasoning method mainly relies on the knowledge and experience of experts in the process of constructing the evaluation model, and analyzes the current network security situation according to the experience of the experts. Common knowledge-based reasoning methods include fuzzy logic reasoning, Bayesian reasoning, and evidence theory. To assess the network security situation, for instance, Kong et al. suggested a fuzzy comprehensive assessment model that combines AHP and the fuzzy evaluation method [68]. Alali et al. proposed to use a fuzzy inference model to generate risk assessment results based on the four risk factors of vulnerability, threat, likelihood and impact, designate the scope of risk that can threaten any entity, and try to address such issues to the proposed entity. Afterward, various analyses of these factors were carried out to verify the feasibility of the method [69]. The grey correlation approach, rough set theory, and cluster analysis method are examples of pattern recognition techniques. Reference [70] provided a detailed analysis of the decision table construction process as applied to the rough set approach of situation appraisal. A mixture of the rough set and the fuzzy rough set was utilized for information processing in reference [72], which increases the accuracy of calculation outputs to address the drawback of accuracy loss when using rough set theory for situational awareness. A network scenario assessment approach based on rough set analysis was developed in reference [71] by fusing conditional attribute reduction and decision rule reduction.

Moreover, because of its powerful learning capabilities, versatility, and broad coverage, deep learning has effectively been implemented in numerous industries, including anomaly detection in medical images [75], target monitoring and recognition [76,77], and feature learning [78]. Therefore, many researchers have recently used deep learning in network situation assessment [73]. For example, the study in [74] proposed a network security situation assessment method based on deep adversarial learning, which establishes a new model that combines deep autoencoder (DAE) with the deep neural network (DNN), as shown in Figure 8. They compared the results of other models to show that the proposed model is more accurate for identifying network attacks and can evaluate the network situation more comprehensively and flexibly.

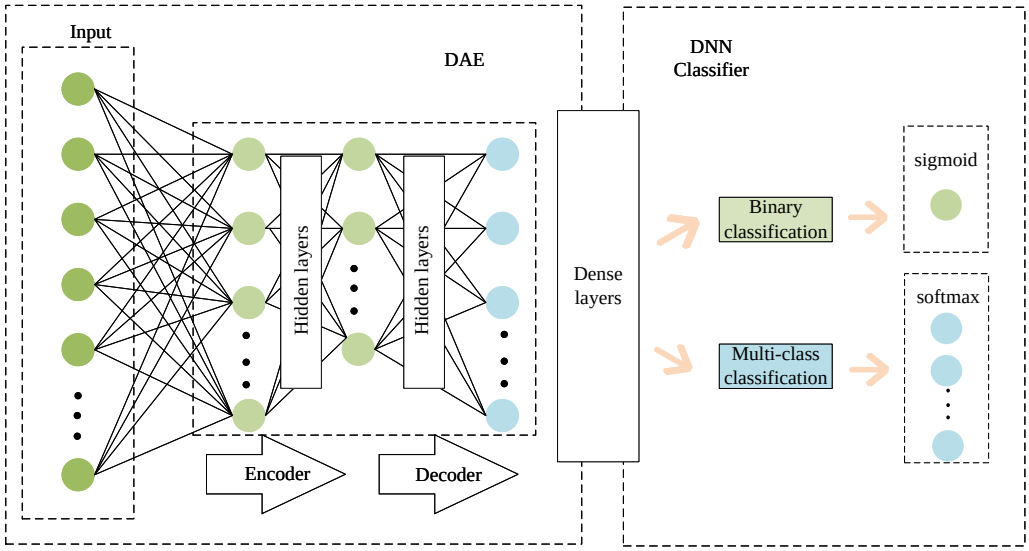

Figure 8. A classification model combining DNN and DAE.

3.2.2. Strengths and Weaknesses Analysis

Although the knowledge reasoning-based approach to assessing network security has some artificial intelligence (AI), it is hampered by the difficulties of gathering inference rules and previous information. Even though the evidence theory has the benefit of being simple to obtain and integrating a variety of expert knowledge and data sources, when there is conflicting evidence, it is likewise bad to have excessive computational complexity.

The complete network state may be integrated to some extent using conventional methods based on the mathematical logic model and knowledge reasoning model, which also provide network management with decision-making advice. It is difficult to evaluate the situation in light of the network's real-time state because some traditional methods, which typically rely excessively on expert assessments and logical reasoning, are not equipped to handle the demands of dealing with a large volume of network traffic and attacks as the network enters the big data era [74].

The pattern recognition approach divides situations using pattern matching and mapping by first applying machine learning (ML) to construct a situation template. It is more complex than knowledge reasoning and depends less on specialized information and expertise. The pattern recognition assessment method has the advantages of being highly efficient, having an enormous processing capacity, and not relying too heavily on expert knowledge. The drawback is that it is challenging to deal with increasingly complicated data during the pattern extraction step, which reduces the effectiveness of the evaluation. In addition, fuzzy theory paired with ML can better reflect changes in network state. A fuzzy neural network (FNN) can also be useful in scenario evaluation [79].

3.3. Network Security Situation Prediction

The ultimate goal of the assessment is to predict and use historical data to provide a management framework for future network security, making network security management change from passive to active. Network security situation prediction (NSSP) is based on historical information and network security conditions to predict the development trend in the future. It is the highest level of full situational awareness and plays an essential role in network security defense [80].

3.3.1. Literature Overview

Network attacks are random and uncertain, and the change in the security situation is bound to be a complex nonlinear process [81], so traditional prediction models are difficult to apply. In previous studies, researchers classified NSSP methods into the following stages. First, Wei et al. [82] divided NSSP into neural networks, time series forecasting

methods, and support vector machine (SVM) methods. Second, Liu et al. surveyed several existing cybersecurity situational prediction techniques and classified them according to their theoretical backgrounds [83], including ML, Markov models [84], and grey theory. Third, Abdlhamed et al. published two classification methods successively. The prediction methods are divided into methods using hidden Markov models, methods based on Bayesian networks, and genetic algorithms in the research [85]. A survey was then released to categorize forecasting methods as well as forecasting systems, arguing that forecasting methods could be based on alert correlations, action sequences, statistical and probabilistic methods, and feature extraction, among others [86].

This section summarizes the research progress of network security situational prediction according to the classification in [24]. It categorizes methods according to the theoretical background on which the forecast is based. Typically, predictive methods in network security use models to represent an attack or network security situation. Table 4 summarizes the researchers' work on network security situation prediction.

The first category is discrete models, including graph models and game-theoretical models; graph models include attack graphs, Bayesian networks, and Markov models. An attack graph is a graphical representation of an attack scenario introduced in 1998 by Phillips and Swiler [87], which quickly became a popular method of the formal expression of attacks. A technique for creating attack graphs utilizing information from the infrastructure of the maritime supply chain was presented by Nikolaos [88]. This approach provides all potential access points that could be used. A recommender system then foretells how the network will be attacked in the future. The approach in [89] employs a Bayesian network to describe the assault propagation process and extrapolate the likelihood of compromised sensors and actuators. The study in [90] examined the weaknesses of conventional attack prediction algorithms and proposed to set up a hidden Markov model based on the alteration of the host's security status with the alteration of the observation sequence to more accurately reflect the network security state. To more accurately calculate the projected attack probability and decrease the frequency of false alarms, the parameters of the hidden Markov model (HMM) were improved. Quantitative analysis was performed to determine the security posture across the entire network.

Additionally, a weighted HMM-based technique was presented [91] to predict the security condition of the mobile network to address the problem that traditional HMM based algorithms for predicting network security are not accurate. To overcome the slow data training speed in mobile networks, multiscale entropy was applied, and the parameters of the HMM situation transition matrix were also improved. Game-theoretical methods seek to identify the optimal strategy for the players rather than the most frequent attack progression shown in historical data, in contrast to graphical model-checking approaches. Therefore, game-theoretical approaches appear promising, particularly for forecasting the behavior of sophisticated attackers. For instance, the study in [92] suggested using game theory in opposition to nature to choose the best bid estimate variant.

Table 4. Researchers on the network security situation prediction of relevant work.

Ref.	Approach/Model	Description	Shortcomings
[88]	Attack graph	Identify attack paths	High time complexity
[89]	Bayesian models	Infer the probabilities of sensors and actuators to be compromised	Easy to produce overfitting and reduce the prediction accuracy
[93]	Fuzzy Markov chain	Combines historical data with the level of threat, predict the next threat by value using fuzzy Markov chains	Low prediction accuracy
[92]	game theory	Based on the use of game theory against nature to identify the optimal variant of a bid estimate	Algorithmic complexity is too high
[94–97]	BP neural network	Adjust and optimize parameters in time through continuous learning	Slow convergence and easy to fall into local optimal solution

Table 4. *Cont.*

Ref.	Approach/Model	Description	Shortcomings
[98]	Wavelet neural network	Optimized by genetic algorithms	Low prediction accuracy
[99,100]	RBF neural network	Through training the RBF neural network, find out the nonlinear mapping relationship	Low learning accuracy and poor generalization ability
[101]	Cyclic neural network	Based on recurrent neural network with gated recurrent unit	Only valid for data with sequence properties
[102]	SVM	Use mapreduce to perform distributed training on SVMs to improve training speed	too sensitive to parameters
[103]	SVM	Optimize SVM parameters based on grey wolf optimization algorithm	Can't handle massive data
[104–107]	deep learning/Stacked Denoising Auto-Encoders (SAE) /association rules mining	Improve prediction accuracy and reduce algorithm complexity	Overfitting of low-dimensional data High complexity of high-dimensional data

The second category is continuous models, including time-series and grey models. Lai [108], for example, developed a prediction model based on gray theory and provided an NSSP technique based on simple weighting and grey theory. Zhang et al. [109] utilized the grey correlation model and grey prediction algorithm as an additional NSSP technique. To forecast network security issues, Deng et al. suggested combining neural networks and gray theory, which also produced positive results [110].

The third category is ML and data mining. ML is gaining popularity in a widely explored field in the research community, and network security is no exception. It contains a large number of methods, such as neural networks and support vector machines. Generally, the BP neural network is a very classic neural network model, combined with the network security situation. Lin et al. [94] proposed an NSSP method based on the BP neural network, and Tang [95] proposed an NSSP method based on the dynamic covariance BP neural network. Zhang et al. proposed a network security situation prediction algorithm based on the BP neural network. By adjusting the weights and thresholds, Zhang et al. [97] compared the actual output value of the network with the expected value, and they proposed an NSSP method based on the optimized BP neural network. Previous studies have demonstrated that the BP neural network's slower convergence speed is a limitation. As a result, it is prone to fluctuation during the learning process and to settle into the best local answer. To improve the network security condition's forecasting accuracy, the research in [98] created a parametric optimized wavelet neural NSSP model utilizing an upgraded niche genetic algorithm. The radial basis function (RBF) neural network can approximate any nonlinear function with arbitrary precision and is capable of global approximation. A generalized RBF neural network-based approach to network security situation prediction is proposed in order to address the issue of prediction accuracy in network situational awareness [111]. Simulation studies demonstrate that this strategy may more precisely predict situations and enhance network security through active security protection. In addition, the study in [112] optimized the RBF neural network with the hybrid hierarchy genetic algorithm and the simulated annealing (SA) technique.

Furthermore, Feng et al. [101] introduced an NSSP method based on cyclic neural networks in their paper. For the first time, this technique extracts internal and external information features from the initial time-series network data. The deep recurrent neural network (RNN) model is then trained and validated using the extracted features. The well-trained model will produce accurate NSSA predictions after iteration and optimization, and the model is stable for erratic network data.

According to the theoretical basis of SVM, the security situation prediction method based on SVM is very sensitive to the selection of parameters, and the prediction result

depends on whether the parameter selection is reasonable. At present, various parameter optimization algorithms are usually used to optimize the model parameters. Hu et al. proposed a MapReduce–support vector machine (MR-SVM) model based on the big data processing framework MapReduce and SVM in 2019, using the cuckoo search algorithm to optimize the SVM parameters and using MapReduce to train the SVM model in parallel, improving the model training accuracy and reducing the training time cost [102]. In the same year, Lu et al. established a kind of NSSP model, which makes it more generalized, and also effectively improves the prediction effect of SVM [103].

The fourth category contains methods that are very specific or difficult to classify. There are many medium prediction methods that will not be introduced one by one here [104–107].

3.3.2. Strengths and Weaknesses Analysis

Generally speaking, each prediction method has its advantages and limitations. The outstanding self-learning and adaptive capabilities of ML can offer quick convergence and great fault tolerance. To acquire parameters, however, there must be enough training data, and creating neurons that are self-learning and adaptable is challenging. Even though the Markov model may predict different time series, it still requires a set of training data. Additionally, especially in large networks, it is very hard to distinguish all potential states and their transitions. In the short-term prediction, grey theory can offer a sparse sample of data, improving prediction without any training. However, the number of network samples is large and complex, so the limitations of grey theory are also evident. Compared with neural networks, SVM has many advantages, such as strong generalization ability, good adaptability, fast convergence speed, and strong mathematical theory support. It is an excellent security situation prediction algorithm at present.

4. Classic Use Cases of NSSA

Because network security is directly related to national security, NSSA has been incorporated into the cybersecurity strategies of many countries. In this section, we will cover some classic use cases of NSSA.

4.1. Lobster Program

The full name of the Lobster Program [113] is large-scale monitoring of broadband internet infrastructures. The program was undertaken by the Hellenic Research and Technology Foundation, in conjunction with Alcatel, Symantec, Greek Telecom, Czech National Education and Research Network, European Research and Education Network Association, Vrije Universiteit Amsterdam, and other companies and institutions and schools, aiming at European establishment of a passive monitoring infrastructure for internet traffic, improving the monitoring capabilities of the basic internet, providing early warnings for security incidents, and providing accurate and meaningful performance measurement methods to improve the performance of the internet and the ability to deal with security issues. The Lobster Project lasted more than three years, from January 2004 to June 2007. Its functions include monitoring network performance and availability, which can be directly or indirectly applied to NSSA as core supporting technologies. Although the project has been phased out, the original relevant participants and later service beneficiaries continue their respective research and application work based on this plan. The essential purpose of this plan is to perceive the situation of the network, especially the security situation.

4.2. Treasure Map

The National Security Agency (NSA) deployed the Deep Network Surveillance Program also known as the Treasure Map Program in 2011. The research goal of this program is to dynamically incorporate all devices in the entire network into monitoring at any location and at any time to achieve a quasi-real-time, interactive global internet map. In other words,

the main task of this plan is network situational awareness. Users of this system include the U.S. National Security Agency, the U.S. Department of Defense, and the Five Eyes Alliance (FVEY), which consists of intelligence agencies in the United States, the United Kingdom, Australia, Canada, and New Zealand. The intelligence and espionage alliance formed by these five countries realizes the interconnection and exchange of intelligence information.

4.3. NSADP Project

The British Defense Science and Technology Laboratory (DSTL) and the British Mood company jointly launched the "Network Situational Awareness, Display, and Prediction (NSADP)" project. Through network data collection, analysis, and security situational awareness, the program utilizes a causal modeling approach to support military commanders in taking appropriate proactive actions to respond to adversary cyberattacks.

Except for the above few typical cases, many others have not been introduced one by one, including the Centaur system of the US Department of Defense, the US Eyesight System, the EU's Wombat Program, the UK Shared Network Security Information Platform, etc.

In short, building an NSSA system aims to achieve active defense against attacks. Many existing critical technical difficulties still need to be further broken through, such as how to accurately and efficiently predict the development trend of the situation, how to judge the attacker's intention, etc. The breakthrough of difficult points will be essential to realizing active defense.

5. Research Challenges and Directions

NSSA is a popular area of study. There are numerous open research fields with significant obstacles that require sophisticated approaches to overcome. New solutions must adhere to a set of constraints and requirements, such as low complexity and reliability. Several possible research directions for these challenges are also discussed.

5.1. Big Data

Situational awareness may dynamically reflect the state of network security as a whole and forecast its future course. However, the complexity of the network environment is rising, and the variety of data types and formats is expanding quickly. Massive security data cannot be used directly as an analysis item for determining how secure a network is. Consequently, the use of big data technology opens up possibilities for innovations in extensive network security situational awareness research. Researchers have provided some of the new solutions for this topic [114,115]. A future work proposed in [116] can be improved the recognition rate and reduce the error rate. According to [116], the scheme can seamlessly integrate fuzzy cluster-based association analysis, game theory, and reinforcement learning. Finally, network situational assessment and situational security prediction can be realized. Additionally, several academic studies [117–119] demonstrated how big data's enormous storage, parallel processing, and fusion analysis can help with the NSSA research challenges. Big data technology's debut presents a chance for big advances in this area. However, the big data-based approach for NSSA still requires a lot of work and careful consideration.

5.2. Cyberspace Mapping

To realize an accurate, real-time, and intelligent NSSA system, the first thing to do is to understand the network, which is impossible without cyberspace mapping [120] technology. The application of situational awareness technology is to establish an "immune" system in cyberspace, through all-weather and all-round awareness of cyber threats, especially for deep-level threats that are difficult to detect and defend against traditional security equipment.

In this way, it is possible to respond promptly, deal with it on time, achieve maximum stop loss, eliminate the impact as quickly as possible, carry out necessary countermeasures as needed, break the enemy at the source, and realize the transformation from passive defense to active defense.

Therefore, cyberspace mapping technology is the first link of the network situational awareness system, and it is also essential data support in the cyberspace situational awareness system [121]. In the network situational awareness system, comprehensive and multi-dimensional network asset mapping is indispensable. In today's country, the concept of cyberspace security has been elevated to a critical level, and it is even more important.

5.3. AI Technology

The paper [122] discovered that the majority of the suggested ways are realized through the transformation of the fundamental AI techniques by summarizing papers about AI in network security. These fundamental techniques serve as the cornerstone and demonstrate the viability and superiority of cyber security solutions. To achieve network situational awareness, for instance, Zhao [29] developed a wavelet neural network (WNN) based on a particle swarm algorithm. The study in [123] used the RBF neural network to accurately quantify the network security situation to predict the power information network security situation. Yang et al. [74] established the deep autoencoder-deep neural network (AEDNN) model based on DAE and DNN to offer an NSSA approach based on DNN. By conducting comparative experiments, they demonstrated that the proposed model can improve the ability to identify network attacks. On the other hand, changing only one pixel of the image [124] or just a few bytes in the sample [125] can cause the neural network to misclassify. Furthermore, edge intelligence emerged as a promising solution to leverage massive data distributed at the network edge for training various machine learning models at the edge server [126]. As a "double-edged sword", AI technology has shortcomings and good performance. Once the information is "infected", the AI system can be easily deceived, leaving the network in an insecure state. Moreover, the AI models consume more time because they need huge data to complete the training. Therefore, a future research topic is how to use AI technology to improve network security situational awareness while further overcoming its shortcomings.

5.4. NSSA Visualization

Franke et al. [19] specifically highlighted the need for going beyond technical aspects of the visualizations to obtain a more comprehensive understanding of NSSA. Although various visualizations have been proposed to support NSSA, there is no clear understanding of the different stakeholders for those visualizations, different types of information visualized, data sources employed, visualization techniques used, levels of NSSA that can be achieved, and the maturity levels of the visualizations, challenges, and practices for NSSA visualizations. Due to the heterogeneity and complexity of network security data, often with multidimensional attributes, sophisticated visualization techniques are needed to achieve NSSA [127]. On this issue, Tamassia et al. [128] provided a crystal-clear statistical finding. The analysis procedure and data in IDS were successfully filtered by Beaver et al. [129], who then visually presented them to administrators. NSSA visualization can be portrayed in two ways [130], emphasizing both interactivity and visualization. However, the most recent work just presents the raw data from real-time data without any analysis, instead emphasizing the cooperative interaction between humans and technology. The flexible analysis of network security situational awareness in general settings still has a long way to go.

5.5. 5G

New technologies will bring new security problems, which may be the security problems existing in the technology itself, or the technology may cause other security problems [131]. Since risks can have serious repercussions, security has emerged as the top priority in many telecommunications sectors today [132]. Confidential information will transit at all layers in the future wireless system as the 5G network's core, and enabling technologies will be included [133,134]. As a result, modern security attacks have be-

come more sophisticated and powerful, making it more difficult to identify them and stop their sabotage.

6. Conclusions

This paper presents a state-of-the-art study on the NSSA that can help bridge the current research status and future large-scale application. We first discussed the history of the NSSA. Subsequently, we provided a brief overview of the model and concept of NSSA and introduced the most impactful NSSA models. Then, we combined the previous classification and Endsley's three-layer model and proposed a new method for the taxonomy of NSSA to overcome the taxonomy issues. Meanwhile, the paper summarized the research progress of NSSA in recent years. It analyzed in detail the critical technologies of situation element acquisition, situation assessment, and situation prediction of three functional modules. We also showed several examples of each technology, illustrating the broad interest in the topic.

The research on NSSA is of great significance to the field of information security. As a branch of computer research that started relatively late, there are still many problems to be solved. The Internet of Things technology and cloud computing technology related to situational awareness are still in their infancy, so mass data acquisition and the high-speed processing technology need to be further improved, and the artificial intelligence machine learning method combined with neural networks and deep learning needs to be further integrated. Moreover, security visualization is a very young term; however, as the number of security-related events generated in modern networks is on the rise, the need for network security visualization systems is felt more than ever.

Even though NSSA is still in its infancy, it will continue to thrive and will be an active and essential research area in the foreseeable future. We believe that this survey will stimulate more attention in this emerging area and encourage more research efforts to absolve the existing technical deficiencies.

Author Contributions: Conceptualization, J.Z. and H.F.; methodology, J.Z. and H.F.; writing—original draft preparation, J.Z.; writing—review and editing, J.Z. and H.F.; supervision, B.L. and D.Z.; project administration, B.L.; funding acquisition, H.F. and D.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the "High-precision" Discipline Construction Project of Beijing Universities (No.20210071Z0403) and Hebei Science Supported Planning Projects Under Grant (No.20310701D).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence
AVS	Antivirus Software
BP	Back Propagation
CSA	Cyber Situation Awareness
DAE	Deep Autoencoder
DNN	Deep Neural Network
D-S	Dempster–Shafer
FNN	Fuzzy Neural Network
HMM	Hidden Markov Models

IDS	Intrusion Detection Systems
IoT	Internet of Things
JDL	Joint Directors of Laboratories
ML	Machine learning
NSSA	Network Security Situation Awareness
NSSP	Trusted Execution Environments
RBF	Radial Basis Function
RNN	Recurrent Neural Network
SA	Situation Awareness
SVM	Support Vector Machine
WNN	Wavelet Neural Network

References

1. Zarei, S.M.; Fotohi, R. Defense against flooding attacks using probabilistic thresholds in the internet of things ecosystem. *Secur. Priv.* **2021**, *4*, e152. [CrossRef]
2. Wu, S.; Guo, H.; Xu, J.; Zhu, S.; Wang, H. In-band full duplex wireless communications and networking for iot devices: Progress, challenges and opportunities. *Future Gener. Comput. Syst.* **2019**, *92*, 705–714. [CrossRef]
3. Zhou, Z.; Tian, Y.; Xiong, J.; Ma, J.; Peng, C. Blockchain-enabled Secure and Trusted Federated Data Sharing in IIoT. *IEEE Trans. Ind. Inform.* 2022, *Early Access*. [CrossRef]
4. Prvan, M.; Ožegović, J. Methods in Teaching Computer Networks: A Literature Review. *ACM Trans. Comput. Educ.* **2020**, *20*, 1–35. [CrossRef]
5. Nour, B.; Mastorakis, S.; Ullah, R.; Stergiou, N. Information-Centric Networking in Wireless Environments: Security Risks and Challenges. *IEEE Wirel. Commun.* **2021**, *28*, 121–127. [CrossRef]
6. Khan, R.; Asif, R. Reflective In-Band Full Duplex NOMA Communications for Secure 5G Networks. In Proceedings of the International Conference on Smart Applications, Communications and Networking, SmartNets 2021, Glasgow, UK, 22–24 September 2021; pp. 1–6.
7. Wang, L.; Tian, Y.; Xiong, J. Achieving reliable and anti-collusive outsourcing computation and verification based on blockchain in 5G-enabled IoT. *Digit. Commun. Netw.* **2022**, *8*, 644–653. [CrossRef]
8. Barak, I. Critical infrastructure under attack: Lessons from a honeypot. *Netw. Secur.* **2020**, *2020*, 16–17. [CrossRef]
9. Aanjankumar, S.; Poonkuntran, S. An efficient soft computing approach for securing information over GAMEOVER Zeus Botnets with modified CPA algorithm. *Soft Comput.* **2020**, *24*, 16499–16507. [CrossRef]
10. Mondal, A.; Das, A.K.; Nath, S.; Goswami, R.T. Review Study on Different Attack Strategies of Worm in a Network. *Webology* **2020**, *17*, 363–375. [CrossRef]
11. Xosanavongsa, C. Heterogeneous Event Causal Dependency Definition for the Detection and Explanation of Multi-Step Attacks. Ph.D. Thesis, Centrale Supélec, Gif-sur-Yvette, France, 2020.
12. Zhang, Y.; Zhang, J.; Zhang, B. Visual Analysis of Cybersecurity Situational Awareness. In Proceedings of the 2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 18–20 October 2019; pp. 685–688.
13. Chen, C.; Ye, L.; Yu, X.; Ding, B. A Survey of Network Security Situational Awareness Technology. In Proceedings of the International Conference on Artificial Intelligence and Security, New York, NY, USA, 26–28 July 2019; pp. 101–109.
14. Gutzwiller, R.; Dykstra, J.; Payne, B. Gaps and Opportunities in Situational Awareness for Cybersecurity. In *Digital Threats: Research and Practice*; Association for Computing Machinery: New York, NY, USA, 2020; pp. 1–6.
15. Zhang, D.; Qian, K.; Wang, W.; Fang, F.; Wang, C.; Luo, X. Network Security Situation Awareness Technology Based on Multi-source Heterogeneous Data. In Proceedings of the 2020 International Conference on Cyberspace Innovation of Advanced Technologies, Guangzhou, China, 4–6 December 2020; pp. 420–424.
16. Azhagiri, M.; Rajesh, A.; Karthik, S. A multi-perspective and multi-level analysis framework in network security situational awareness. *Int. J. Comput. Netw. Commun. Secur.* **2017**, *5*, 71.
17. Li, J.; Yi, X.; Wei, S. A study of network security situational awareness in Internet of Things. In Proceedings of the 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 15–19 June 2020; pp. 1624–1629.
18. Husák, M.; Jirsík, T.; Yang, S.J. SoK: Contemporary issues and challenges to enable cyber situational awareness for network security. In Proceedings of the 15th International Conference on Availability, Reliability and Security, Online, 25–28 August 2020; pp. 1–10.
19. Franke, U.; Brynielsson, J. Cyber situational awareness–a systematic review of the literature. *Comput. Secur.* **2014**, *46*, 18–31. [CrossRef]
20. Jiang, L.; Jayatilaka, A.; Nasim, M.; Grobler, M.; Zahedi, M.; Babar, M.A. Systematic Literature Review on Cyber Situational Awareness Visualizations. *arXiv* **2021**, arXiv:2112.10354.
21. Li, Y.; Huang, G.Q.; Wang, C.Z.; Li, Y.C. Analysis framework of network security situational awareness and comparison of implementation methods. *EURASIP J. Wirel. Commun. Netw.* **2019**, *2019*, 205. [CrossRef]
22. Gong, J.; Zang, X.; Su, Q.; Hu, X.; Xu, J. Overview of Network security Situational Awareness. *J. Softw.* **2017**, *28*, 17.

23. Jia, Y.; Han, W.; Yang, H. Research status and development trend of network security situational awareness. *J. Guangzhou Univ.* **2019**, *18*, 1–10.
24. Husák, M.; Komárková, J.; Bou-Harb, E.; Čeleda, P. Survey of attack projection, prediction, and forecasting in cyber security. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 640–660. [CrossRef]
25. Endsley, M.R.; Garland, D.J. *Situation Awareness Analysis and Measurement*; CRC Press: Boca Raton, FL, USA, 2000.
26. Endsley, M.R. Design and evaluation for situation awareness enhancement. In Proceedings of the Human Factors Society Annual Meeting, Anaheim, CA, USA, 24–28 October 1988; Sage Publications: Los Angeles, CA, USA, 1988; Volume 32, pp. 97–101.
27. Bass, T.; Gruber, D. A glimpse into the future of id. *Mag. Usenix Sage* **1999**, *24*, 40–49.
28. Chen, W.; Ao, Z.; Guo, J.; Yu, Q.; Tong, J. Research on cyberspace situation awareness security assessment based on improved BP neural network. *Comput. Sci.* **2018**, *45*, 335–337.
29. Zhao, D.; Liu, J. Study on network security situation awareness based on particle swarm optimization algorithm. *Comput. Ind. Eng.* **2018**, *125*, 764–775. [CrossRef]
30. Rongrong, X.; Xiaochun, Y.; Zhiyu, H. Framework for risk assessment in cyber situational awareness. *IET Inf. Secur.* **2019**, *13*, 149–156. [CrossRef]
31. Ziems, N.; Wu, S. Security Vulnerability Detection Using Deep Learning Natural Language Processing. In Proceedings of the IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Online, 2–5 May 2021; pp. 1–6.
32. Endsley, M.R. Situation awareness global assessment technique (SAGAT). In Proceedings of the IEEE 1988 National Aerospace and Electronics Conference, Dayton, OH, USA, 23–27 May 1988; pp. 789–795.
33. Giacobe, N.A. Application of the JDL data fusion process model for cyber security. In Proceedings of the Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications, Orlando, FL, USA, 7–8 April 2010; International Society for Optics and Photonics: Bellingham, WA, USA, 2010; Volume 7710, p. 77100R.
34. Zhigang, A. *Cyberspace Operations Situational Awareness': 'Cyberspace Operations: Mechanism and Planning*; Publishing House of Electronics Industry: Beijing, China, 2018; p. 1.
35. Bass, T. Intrusion detection systems and multisensor data fusion. *Commun. ACM* **2000**, *43*, 99–105. [CrossRef]
36. Huiqiang, W.; Jibao, L.; Liang, Z.; Ying, L. Survey of Network Situation Awareness System. *Comput. Sci.* **2006**, *33*, 5–10.
37. Jibao, L.; Huiqiang, W.; Shuang, J. Study of network security situation awareness system based on Netflow. *Comput. Appl. Res.* **2007**, *24*, 167–169.
38. Yan, J.; Xiaowei, W.; Weihong, H.; Aiping, L.I.; Wencong, C. YHSSAS: Large-scale Network Oriented Security Situational Awareness System. *Comput. Sci.* **2011**, *38*, 4–8.
39. An, J.; Li, X.; You, C.; Zhang, L. The research of cyber situation awareness model. In Proceedings of the International Conference on Intelligent and Interactive Systems and Applications, Shanghai, China, 25–26 June 2016; pp. 232–238.
40. Kokkonen, T. Architecture for the cyber security situational awareness system. In *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 294–302.
41. Evesti, A.; Kanstrén, T.; Frantti, T. Cybersecurity situational awareness taxonomy. In Proceedings of the 2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), London, UK, 19–20 June 2017; pp. 1–8. [CrossRef]
42. Vaarandi, R.; Pihelgas, M. Using security logs for collecting and reporting technical security metrics. In Proceedings of the 2014 IEEE Military Communications Conference, Washington, DC, USA, 6–8 October 2014; pp. 294–299.
43. Jajodia, S.; Noel, S.; O'berry, B. Topological analysis of network attack vulnerability. In *Managing Cyber Threats*; Springer: Berlin/Heidelberg, Germany, 2005; pp. 247–266.
44. Wang, L.; Singhal, A.; Jajodia, S. Toward measuring network security using attack graphs. In Proceedings of the 2007 ACM Workshop on Quality of Protection, Alexandria, VA, USA, 29 October 2007; pp. 49–54.
45. Ning, P.; Cui, Y.; Reeves, D.S.; Xu, D. Techniques and tools for analyzing intrusion alerts. *ACM Trans. Inf. Syst. Secur. (TISSEC)* **2004**, *7*, 274–318. [CrossRef]
46. Xu, D.; Ning, P. Alert correlation through triggering events and common resources. In Proceedings of the 20th Annual Computer Security Applications Conference, Washington, DC, USA, 6–10 December 2004; pp. 360–369.
47. Barford, P.; Chen, Y.; Goyal, A.; Li, Z.; Paxson, V.; Yegneswaran, V. Employing honeynets for network situational awareness. In *Cyber Situational Awareness*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 71–102.
48. Juan, W.; Fengli, Z.; Chong, F.U.; Lisha, C. Study on index system in network situation awareness. *Comput. Appl.* **2007**, *27*, 1907–1909.
49. Hailong, W.; Zhenghu, G. Heterogeneous multi-sensor information fusion model for botnet detection. In Proceedings of the 2010 International Conference on Intelligent Computation Technology and Automation, Changsha, China, 11–12 May 2010, Volume 2; pp. 428–431.
50. Liu, X.; Wang, H.; Yu, J.; Cao, B.; Gao, Z. Network security situation awareness model based on multi-source fusion. *Adv. Sci. Lett.* **2012**, *5*, 775–779. [CrossRef]
51. Heyi, W.; Aiqun, H.; Yubo, S.; Ning, B.; Xuefei, J. A new intrusion detection feature extraction method based on complex network theory. In Proceedings of the 2012 Fourth International Conference on Multimedia Information Networking and Security, Nanjing, China, 2–4 November 2012; pp. 852–856.

52. Tsang, C.H.; Kwong, S. Multi-agent intrusion detection system in industrial network using ant colony clustering approach and unsupervised feature extraction. In Proceedings of the 2005 IEEE international conference on industrial technology, Hong Kong, China, 14–17 December 2005; pp. 51–56.
53. Lai, J.; Wang, H.; Zheng, F.; Feng, G. Network Security Situation Element Extraction Method based on DsimC and EWDS. *Comput. Sci.* **2010**, *37*, 64–69.
54. Chang, Y.; Ma, Z.; Li, X.; Gong, D. Security situation element extraction based on probabilistic neural network. *Cyberspace Secur.* **2020**, *11*, 6.
55. Li, B.; Pi, D.; Lin, Y.; Khan, I.A.; Cui, L. Multi-source information fusion based heterogeneous network embedding. *Inf. Sci.* **2020**, *534*, 53–71. [CrossRef]
56. Jia, Y.; Fang, B. *Network Security Situation Awareness*; Publishing House of Electronics Industry: Beijing, China, 2020; p. 47.
57. Lan, L.; Jun, L. Some special issues of network security monitoring on big data environments. In Proceedings of the 2013 IEEE 11th International Conference on Dependable, Autonomic and Secure Computing, Chengdu, China, 21–22 December 2013; pp. 10–15.
58. Wang, H.; Chen, Z.; Feng, X.; Di, X.; Liu, D.; Zhao, J.; Sui, X. Research on network security situation assessment and quantification method based on analytic hierarchy process. *Wirel. Pers. Commun.* **2018**, *102*, 1401–1420. [CrossRef]
59. Zhang, J. Research on some key technologies of network security situation assessment. Ph.D. Thesis, National University of Defense Technology, Changsha, China, 2013.
60. Zhang, H.; Kang, C.; Xiao, Y. Research on Network Security Situation Awareness Based on the LSTM-DT Model. *Sensors* **2021**, *21*, 4788. [CrossRef]
61. Xiaolu, H.; Yun, L.; Zhenjiang, Z.; Xin, L.; Yang, L. Network Security Situation Awareness Theory and Technology Overview and Research on Difficult Issues. *Inf. Secur. Commun. Confidentiality* **2019**, 61–71.
62. Li, Y. Research on Network Security Situational Awareness Technology Based on Indicator System. Ph.D. Thesis, Tianjin University of Technology, Tianjin, China, 2016.
63. Xiuzhen, C.; Qinghua, Z.; Xiaohong, G.; Chenguang, L. Quantitative Hierarchical Threat Evaluation Model for Network Security. *J. Softw.* **2006**, *17*, 885–897.
64. Lai, J. Research on Several Key Technologies of Network Security Situational Awareness Based on Heterogeneous Sensors. Ph.D. Thesis, Harbin Engineering University, Harbin, China, 2009.
65. Zhang, Y. Research and System Implementation of Network Security Situational Awareness Model. Ph.D. Thesis, University of Science and Technology of China, Hefei, China, 2010.
66. Meng, J. Research on Key Technologies of Network Security Situation Assessment and Forecast. Ph.D. Thesis, Nanjing University of Science and Technology, Nanjing, China, 2012.
67. Jia, Y.; Wu, H.; Jiang, D. A Hierarchical Framework of Security Situation Assessment for Information System. In Proceedings of the 2015 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Xi'an, China, 17–19 September 2015; pp. 23–28.
68. Kong, D.; Li, H.; Dong, H. Research on Network Security Situation Assessment Technology Based on Fuzzy Evaluation Method. *J. Phys. Conf. Ser. IOP* **2021**, *1883*, 012108. [CrossRef]
69. Alali, M.; Almogren, A.; Hassan, M.M.; Rassan, I.A.; Bhuiyan, M.Z.A. Improving risk assessment model of cyber security using fuzzy logic inference system. *Comput. Secur.* **2018**, *74*, 323–339. [CrossRef]
70. Zhao, G.; Wang, H.; Wang, J. Research on survivability situation assessment of network based on grey relational analysis. *Small Microcomput. Syst.* **2006**, *27*, 4.
71. Zhuo, Y.; He, M.; Gong, Z. Rough set analysis model for network situation assessment. *Comput. Eng. Sci.* **2012**, *34*, 1–5.
72. Li, X.; Li, X.; Zhao, Z. Combining deep learning with rough set analysis: A model of cyberspace situational awareness. In Proceedings of the 2016 6th International Conference on Electronics Information and Emergency Communication (ICEIEC), Beijing, China, 17–19 June 2016; pp. 182–185.
73. Zhang, L.; Zhu, Y.; Shi, X.; Li, X. A situation assessment method with an improved fuzzy deep neural network for multiple UAVs. *Information* **2020**, *11*, 194. [CrossRef]
74. Yang, H.; Zeng, R.; Xu, G.; Zhang, L. A network security situation assessment method based on adversarial deep learning. *Appl. Soft Comput.* **2021**, *102*, 107096. [CrossRef]
75. Hossain, M.S.; Amin, S.U.; Alsulaiman, M.; Muhammad, G. Applying deep learning for epilepsy seizure detection and brain mapping visualization. *ACM Trans. Multimed. Comput. Commun. Appl. (TOMM)* **2019**, *15*, 1–17. [CrossRef]
76. Ahmad, K.; Mekhalfi, M.L.; Conci, N.; Melgani, F.; Natale, F.D. Ensemble of deep models for event recognition. *ACM Trans. Multimed. Comput. Commun. Appl. (TOMM)* **2018**, *14*, 1–20. [CrossRef]
77. Tian, Y.; Lee, G.H.; He, H.; Hsu, C.Y.; Katabi, D. RF-based fall monitoring using convolutional neural networks. *Proc. ACM Interactive Mobile Wearable Ubiquitous Technol.* **2018**, *2*, 1–24. [CrossRef]
78. Zhang, Q.; Yang, L.T.; Chen, Z.; Li, P. Dependable deep computation model for feature learning on big data in cyber-physical systems. *ACM Trans. Cyber-Phys. Syst.* **2018**, *3*, 1–17. [CrossRef]
79. Li, C.; Li, X.M. Cyber performance situation awareness on fuzzy correlation analysis. In Proceedings of the 2017 3rd IEEE International Conference on Computer and Communications (ICCC), Chengdu, China, 13–16 December 2017; pp. 424–428.

80. Wu, S.; Rendall, J.B.; Smith, M.J.; Zhu, S.; Xu, J.; Wang, H.; Yang, Q.; Qin, P. Survey on prediction algorithms in smart homes. *IEEE Internet Things J.* **2017**, *4*, 636–644. [CrossRef]
81. Ebazadeh, Y.; Fotohi, R. A reliable and secure method for network-layer attack discovery and elimination in mobile ad-hoc networks based on a probabilistic threshold. *Secur. Priv.* **2022**, *5*, e183. [CrossRef]
82. Wei, X.; Jiang, X. Comprehensive analysis of network security situational awareness methods and models. In Proceedings of the 2013 2nd International Symposium on Instrumentation and Measurement, Sensor Network and Automation (IMSNA), Toronto, ON, Canada, 23–24 December 2013; pp. 176–179.
83. Leau, Y.B.; Manickam, S. Network security situation prediction: A review and discussion. In Proceedings of the International Conference on Soft Computing, Intelligence Systems, and Information Technology, Chennai, India, 12–13 November 2015; pp. 424–435.
84. Ioannou, G.; Louvieris, P.; Clewley, N. A Markov multi-phase transferable belief model for cyber situational awareness. *IEEE Access* **2019**, *7*, 39305–39320. [CrossRef]
85. Abdlhamed, M.; Kifayat, K.; Shi, Q.; Hurst, W. A system for intrusion prediction in cloud computing. In Proceedings of the International Conference on Internet of Things and Cloud Computing, Dalian, China, 22–23 October 2016; pp. 1–9.
86. Abdlhamed, M.; Kifayat, K.; Shi, Q.; Hurst, W. Intrusion prediction systems. In *Information Fusion for Cyber-Security Analytics*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 155–174.
87. Phillips, C.; Swiler, L.P. A graph-based system for network-vulnerability analysis. In Proceedings of the 1998 Workshop on New Security Paradigms, Charlottesville, VA, USA, 22–26 September 1998; pp. 71–79.
88. Polatidis, N.; Pimenidis, E.; Pavlidis, M.; Papastergiou, S.; Mouratidis, H. From product recommendation to cyber-attack prediction: Generating attack graphs and predicting future attacks. *Evol. Syst.* **2018**, *11*, 479–490. [CrossRef]
89. Huang, K.; Zhou, C.; Tian, Y.C.; Yang, S.; Qin, Y. Assessing the physical impact of cyberattacks on industrial cyber-physical systems. *IEEE Trans. Ind. Electron.* **2018**, *65*, 8153–8162. [CrossRef]
90. Jing, S.; Li, M.; Sun, Y.; Zhang, Y. Research on Prediction of Attack Behavior Based on HMM. In Proceedings of the 2021 IEEE 4th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Chongqing, China, 18–20 June 2021; Volume 4; pp. 1580–1583.
91. Liang, W.; Long, J.; Chen, Z.; Yan, X.; Li, Y.; Zhang, Q.; Li, K.C. A security situation prediction algorithm based on HMM in mobile network. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 5380481. [CrossRef]
92. Rzepecki, Ł.; Jaśkowski, P. Application of game theory against nature in supporting bid pricing in construction. *Symmetry* **2021**, *13*, 132. [CrossRef]
93. Wang, Y.; Li, W.; Liu, Y. A forecast method for network security situation based on fuzzy Markov chain. In *Proceedings of the Advanced Technologies, Embedded and Multimedia for Human-Centric Computing: HumanCom and EMC 2013*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 953–962.
94. Lin, Z.; Chen, G.; Guo, W.; Liu, Y. PSO-BPNN-based prediction of network security situation. In Proceedings of the 2008 3rd International Conference on Innovative Computing Information and Control, Dalian, China, 18–20 June 2008; p. 37.
95. Tang, C.; Xie, Y.; Qiang, B.; Wang, X.; Zhang, R. Security situation prediction based on dynamic BP neural with covariance. *Procedia Eng.* **2011**, *15*, 3313–3317. [CrossRef]
96. Zhang, R.; Liu, M.; Yin, Y.; Zhang, Q.; Cai, Z. Prediction Algorithm for Network Security Situation based on BP Neural Network Optimized by SA-SOA. *Int. J. Perform. Eng.* **2020**, *16*, 1171–1182.
97. Zhang, Y.; He, C.; Wu, H. Network security situation prediction based on optimized BP neural network. In Proceedings of the 2021 IEEE International Conference on Electronic Technology, Communication and Information (ICETCI), Changchun, China, 27–29 August 2021; pp. 682–686. [CrossRef]
98. Zhang, H.; Huang, Q.; Li, F.; Zhu, J. A network security situation prediction model based on wavelet neural network with optimized parameters. *Digit. Commun. Netw.* **2016**, *2*, 139–144. [CrossRef]
99. Ren, W.; Jiang, X.; Sun, Y. Network security situation prediction method based on RBF neural network. *Comput. Eng. Appl.* **2006**, *42*, 4.
100. Jiang, Y.; Li, C.H.; Yu, L.S.; Bao, B. On network security situation prediction based on RBF neural network. In Proceedings of the 2017 36th Chinese Control Conference (CCC), Dalian, China, 26–28 July 2017; pp. 4060–4063.
101. Feng, W.; Wu, Y.; Fan, Y. A new method for the prediction of network security situations based on recurrent neural network with gated recurrent unit. *Int. J. Intell. Comput. Cybern.* **2018**, *13*, 25–39. [CrossRef]
102. Hu, J.; Ma, D.; Liu, C.; Shi, Z.; Yan, H.; Hu, C. Network security situation prediction based on MR-SVM. *IEEE Access* **2019**, *7*, 130937–130945. [CrossRef]
103. Lu, H.; Zhang, G.; Shen, Y. Cyber security situation prediction model based on GWO-SVM. In Proceedings of the International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Asan, Republic of Korea, 1–3 July 2019; pp. 162–171.
104. Dong, Z.; Su, X.; Sun, L.; Xu, K. Network security situation prediction method based on strengthened LSTM neural network. *J. Phys. Conf. Ser. IOP Publ.* **2021**, *1856*, 012056. [CrossRef]
105. Xue, R.; Tang, P.; Fang, S. Prediction of Computer Network Security Situation Based on Association Rules Mining. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 2794889. [CrossRef]

106. Chen, L.; Zheng, M.; Liu, Z.; Chen, F.; Zhou, K.; Liu, B. SAE+ Bi-GRU Based Security Situation Prediction for Smart Grid. In Proceedings of the International Conference on Emerging Internetworking, Data & Web Technologies, Okayama, Japan, 2–4 March 2022; pp. 21–30.
107. Lin, Z.; Yu, J.; Liu, S. The prediction of network security situation based on deep learning method. *Int. J. Inf. Comput. Secur.* **2021**, *15*, 386–399. [CrossRef]
108. Jibao, L.; Huiqiang, W.; Liang, Z. Study of network security situation awareness model based on simple additive weight and grey theory. In Proceedings of the 2006 International Conference on Computational Intelligence and Security, Alexandria, VA, USA, 16–17 October 2006, Volume 2; pp. 1545–1548.
109. Zhang, F.; Wang, J.; Qin, Z. Using gray model for the evaluation index and forecast of network security situation. In Proceedings of the 2009 International Conference on Communications, Circuits and Systems, Milpitas, CA, USA, 23–25 July 2009; pp. 309–313.
110. Deng, Y.; Wen, Z.; Jiang, X. Network Security Situation Prediction Method Based on Grey Theory. *J. Hunan Univ. Technol.* **2015**, *29*, 5.
111. Chen, G. Multimedia Security Situation Prediction Based on Optimization of Radial Basis Function Neural Network Algorithm. *Comput. Intell. Neurosci.* **2022**, *2022*, 6314262. [CrossRef] [PubMed]
112. Chen, Z. Research on Internet Security Situation Awareness Prediction Technology based on Improved RBF Neural Network Algorithm. *J. Comput. Cogn. Eng.* **2022**, *1*, 103–108.
113. Maintz, S.; Deringer, V.L.; Tchougréeff, A.L.; Dronskowski, R. LOBSTER: A tool to extract chemical bonding from plane-wave based DFT. *J. Comput. Chem.* **2016**, *37*, 1030–1035. [CrossRef] [PubMed]
114. Qian, W.; Lai, H.; Zhu, Q.; Chang, K.C. Overview of network security situation awareness based on big data. In Proceedings of the International Conference on Advanced Machine Learning Technologies and Applications, Cairo, Egypt, 20–22 March 2021; pp. 875–883.
115. Zhu, B.; Chen, Y.; Cai, Y. Three Kinds of Network Security Situation Awareness Model Based on Big Data. *Int. J. Netw. Secur.* **2019**, *21*, 115–121.
116. Wu, J.; Ota, K.; Dong, M.; Li, J.; Wang, H. Big Data Analysis-Based Security Situational Awareness for Smart Grid. *IEEE Trans. Big Data* **2018**, *4*, 408–417. [CrossRef]
117. Chandarana, P.; Vijayalakshmi, M. Big data analytics frameworks. In Proceedings of the 2014 International Conference on Circuits, Systems, Communication and Information Technology Applications (CSCITA), Mumbai, India, 4–5 April 2014; pp. 430–434.
118. Fischer, F.; Keim, D.A. NStreamAware: Real-time visual analytics for data streams to enhance situational awareness. In Proceedings of the Eleventh Workshop on Visualization for Cyber Security, Paris, France, 10 November 2014; pp. 65–72.
119. Chen, X.; Zeng, X.; Wang, W. Big data analytics for network security and intelligence. *Adv. Eng. Sci.* **2017**, *39*, 112–129.
120. Shao, S.; Satam, P.; Satam, S.; Al-Awady, K.; Ditzler, G.; Hariri, S.; Tunc, C. Multi-Layer Mapping of Cyberspace for Intrusion Detection. In Proceedings of the 2021 IEEE/ACS 18th International Conference on Computer Systems and Applications (AICCSA), Tangier, Morocco, 30 November–3 December 2021; pp. 1–8.
121. Gao, C.; Guo, Q.; Jiang, D.; Wang, Z.; Fang, C.; Hao, M. The theoretical basis and technical path of cyberspace geography. *J. Geogr. Sci.* **2019**, *29*, 5–20.
122. Zhang, Z.; Ning, H.; Shi, F.; Farha, F.; Xu, Y.; Xu, J.; Zhang, F.; Choo, K.K.R. Artificial intelligence in cyber security: Research advances, challenges, and opportunities. *Artif. Intell. Rev.* **2021**, *55*, 1029–1053. [CrossRef]
123. Xiaofei, Z.; Daoyin, Z.; Luolin, Z.; Decheng, C.; Rong, F. Research on Power Information Network Security Situation Awareness Based on LDA-RBF. *Low Volt. Appar.* **2021**, *8*, 16–23.
124. Su, J.; Vargas, D.V.; Sakurai, K. One pixel attack for fooling deep neural networks. *IEEE Trans. Evol. Comput.* **2019**, *23*, 828–841. [CrossRef]
125. Kolosnjaji, B.; Demontis, A.; Biggio, B.; Maiorca, D.; Giacinto, G.; Eckert, C.; Roli, F. Adversarial malware binaries: Evading deep learning for malware detection in executables. In Proceedings of the 2018 26th European Signal Processing Conference (EUSIPCO), Rome, Italy, 3–7 September 2018; pp. 533–537.
126. Zhang, T.; Wang, S.; Li, G.; Liu, F.; Zhu, G.; Wang, R. Accelerating edge intelligence via integrated sensing and communication. In Proceedings of the ICC 2022-IEEE International Conference on Communications, Seoul, Republic of Korea, 16–20 May 2022; pp. 1586–1592.
127. Giles, K.; Hagestad, W. Divided by a common language: Cyber definitions in Chinese, Russian and English. In Proceedings of the 2013 5th International Conference on Cyber Conflict (CYCON 2013), Tallinn, Estonia, 4–7 June 2013; pp. 1–17.
128. Tamassia, R.; Palazzi, B.; Papamanthou, C. Graph drawing for security visualization. In Proceedings of the International Symposium on Graph Drawing, Crete, Greece, 21–24 September 2008; pp. 2–13.
129. Beaver, J.M.; Steed, C.A.; Patton, R.M.; Cui, X.; Schultz, M. Visualization techniques for computer network defense. In Proceedings of the Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense X, Orlando, FL, USA, 15–17 April 2011; SPIE: Bellingham, WA, USA, 2011; Volume 8019; pp. 18–26.
130. Sharma, S.; Bodempudi, S.T.; Reehl, A. Real-Time Data Visualization to Enhance Situational Awareness of COVID pandemic. In Proceedings of the 2020 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 16–18 December 2020; pp. 352–357.
131. Zaminkar, M.; Fotohi, R. SoS-RPL: Securing internet of things against sinkhole attack using RPL protocol-based node rating and ranking mechanism. *Wirel. Pers. Commun.* **2020**, *114*, 1287–1312. [CrossRef]

132. Khan, R.; Kumar, P.; Jayakody, D.N.K.; Liyanage, M. A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 196–248. [CrossRef]
133. Khan, R.; Tsiga, N.; Asif, R. Interference management with reflective in-band full-duplex NOMA for secure 6G wireless communication systems. *Sensors* **2022**, *22*, 2508. [CrossRef] [PubMed]
134. Khan, R.; Jayakody, D.N.K. Full Duplex Component-Forward Cooperative Communication for a Secure Wireless Communication System. *Electronics* **2020**, *9*, 2102. [CrossRef]