State-of-the-Art in Cyber Situational Awareness: A Comprehensive Review and Analysis

Kookjin Kim[1,2], Jaepil Youn[2,3], Hansung Kim[4], Dongil Shin[2,5] and Dongkyoo Shin[2,5*]

[1] Intelligent Network Security Research Team, Cyber Security Research Department, AI Computing Research Division, Electronics and Telecommunications Research Institute,
218 Gajeong-ro, Yuseong-gu, 34129 Daejeon, Republic of Korea
[e-mail : kjkim23@etri.re.kr]

[2] Department of Computer Engineering, Sejong University
209 Neungdong-ro, Gwangjin-gu, 05006 Seoul, Republic of Korea
[e-mail: jpyoun@sju.ac.kr, {dshin,shindk}@sejong.ac.kr]

[3] Joint Forces Military University
1040 Hwangsanbeol-ro, Yangchon-myeon, Nonsan-si, Chungcheongnam-do, Republic of Korea

[4] AI Computing Research Division, Electronics and Telecommunications Research Institute,
218 Gajeong-ro, Yuseong-gu, 34129 Daejeon, Republic of Korea
[e-mail : han_sungkim@naver.com]

[5] Department of Convergence Engineering for Intelligent Drones, Sejong University
209 Neungdong-ro, Gwangjin-gu, 05006 Seoul, Republic of Korea

[*]Corresponding author: Dongkyoo Shin

Received September 29, 2023; revised December 18, 2023; revised Feburary 7, 2024; revised March 11, 2024; accepted April 8, 2024; published May 31, 2024

Abstract

In the complex virtual environment of cyberspace, comprised of digital and communication networks, ensuring the security of information is being recognized as an ongoing challenge. The importance of 'Cyber Situation Awareness (CSA)' is being emphasized in response to this. CSA is understood as a vital capability to identify, understand, and respond to various cyber threats and is positioned at the heart of cyber security strategies from a defensive perspective. Critical industries such as finance, healthcare, manufacturing, telecommunications, transportation, and energy can be subjected to not just economic and societal losses from cyber threats but, in severe cases, national losses. Consequently, the importance of CSA is being accentuated and research activities are being vigorously undertaken. A systematic five-step approach to CSA is introduced against this backdrop, and a deep analysis of recent research trends, techniques, challenges, and future directions since 2019 is provided. The approach encompasses current situation and identification awareness, the impact of attacks and vulnerability assessment, the evolution of situations and tracking of actor behaviors, root cause and forensic analysis, and future scenarios and threat predictions. Through this survey, readers will be deepened in their understanding of the fundamental importance and practical applications of CSA, and their insights into research and applications in this field will be

This work was supported by a National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT) (No. 2022R1F1A1074773).

http://doi.org/10.3837/tiis.2024.05.008 **ISSN : 1976-7277**

enhanced. This survey is expected to serve as a useful guide and reference for researchers and experts particularly interested in CSA research and applications.

Keywords: Cyber Situation Awareness, Cyber Security, Cyber Threat Intelligence, Cyber Intelligence Preparation of the Battlefield, Monitoring

1. Introduction

Cyberspace is defined as a virtual information space based on digital technology and communication networks, especially the internet [1]. Unlike the physical world, cyberspace is constructed through digital data and interactions, comprising interactions among individuals, institutions, and devices in a network-based environment [2-4]. Ensuring the safety of information and data in such a complex and dynamic environment is seen as a significant challenge. The need for CSA, the ability to recognize, understand, and predict various threats in cyberspace, is increasingly highlighted. CSA is described as the capability to recognize, understand, and predict various cyber threats occurring in today's network environment [5-6]. Such situational awareness is not merely limited to protecting information assets from serious cyber threats but is considered a core element of an organization's overall cyber security strategy [6].

Due to the vast influence of cyberspace, awareness of the importance of CSA is progressively being heightened in various industrial sectors. In key sectors such as finance, healthcare, manufacturing, telecommunications, transportation, and energy, this recognition is now being considered as a core competence of enterprises, resulting in extensive research being conducted [7-10]. Technical, organizational, and strategic aspects of CSA are encompassed in such research, with emphasis being placed on the necessity of enhancing cyber security through defensive cyber responses.

Given the importance and complexity of cyberspace, CSA is increasingly being viewed as an essential skill for all modern organizations and individuals. Consequently, this survey aims to emphasize the fundamental significance of CSA and to offer an in-depth analysis of its practical application methods across various industries. Through this, readers will be systematically familiarized with a 5-step CSA-centric approach, laying a foundation for active participation in this research domain. The entire process of CSA, from current situation awareness to future threat predictions, is comprehensively covered by this 5-step methodology. This research is designed to assist all readers whose interests are centralized around CSA and its applications. The main contributions of this research are outlined as follows:

1) A systematic review of recent research trends focused on CSA is conducted, proposing a 5-step methodology for integrating and analyzing them.

2) An overarching overview of contemporary CSA technologies and application solutions is provided.

3) Centering on the proposed methodology, profound discussions on current challenges and future research directions are conducted.

Excluding Chapter 1, the structure of this survey is organized as follows: In Chapter 2, key research strategies for CSA are presented. Chapter 3 contains an in-depth review of research post-2019 and their findings. In Chapter 4, the major challenges encountered in this field and potential directions for future research are explored. The main content and conclusions of this survey are encapsulated in Chapter 5.

2. Research Methodology

CSA is characterized by the ability to perceive and comprehend events and situations in cyberspace in real-time [5-6]. Unlike traditional cybersecurity methods that often react to threats as they arise, CSA proactively analyses security events to enhance decision-making in the digital domain. It plays a pivotal role in contemporary security challenges, incorporating diverse elements such as human factors, Augmented Reality (AR), and Digital Twins (DT) [6]. National cyber capabilities, including CSA, prioritize the resilience of critical infrastructures and emphasize the need for sharing cybersecurity information. As cyber spaces diversify, CSA increasingly integrates concepts like digital twins, artificial intelligence, and big data fusion, distinguishing itself from other cybersecurity techniques by its emphasis on a comprehensive and predictive approach.

This study adopts a structured, step-by-step approach inspired by [11], specifically tailored for the CSA domain. This approach, distinct from the direct application of techniques from [11], adapts its systematic methodology to enhance CSA's effectiveness. The aim is to augment situation awareness systematically and efficiently through a 5-step method. These steps are uniquely formulated to address the complexities of CSA, offering a fresh perspective that diverges from existing CSA research. They include:

1) Identification of the Current Situation and Awareness: This step involves real-time detection and analysis of events in systems like power and naval digital systems, crucial for preventing economic and national losses [12,13]. It includes advanced log analysis, streaming data processing, and anomaly detection using machine learning, differentiating it from later steps by focusing on immediate event detection and analysis.
2) Assessment of Attack Impact and Vulnerabilities: Here, the consequences of a cyber-attack are evaluated, including system vulnerabilities [5]. This phase, distinct from the first, moves from detection to an in-depth assessment, involving vulnerability assessment techniques, attack trees, and impact analysis.
3) Tracking the Evolution of Situations and Attacker Behavior: This phase offers insights into the progress post-attack, emphasizing understanding the motives and methods of attackers [20,21]. It differs from the first step by focusing on the progression and analysis of the attacker's behavior and tactics, rather than initial detection.
4) Root Cause and Forensic Analysis: Post-attack, this phase involves a detailed investigation into the causes and actions involved [15,22,23]. It encompasses memory, network, system, and OS-level forensics, along with malicious code analysis.
5) Future Situation and Threat Prediction: The final step involves predicting future cyber threats based on past incidents [24-26]. It employs machine learning for threat prediction, threat intelligence analysis, and cyber security trend analysis.

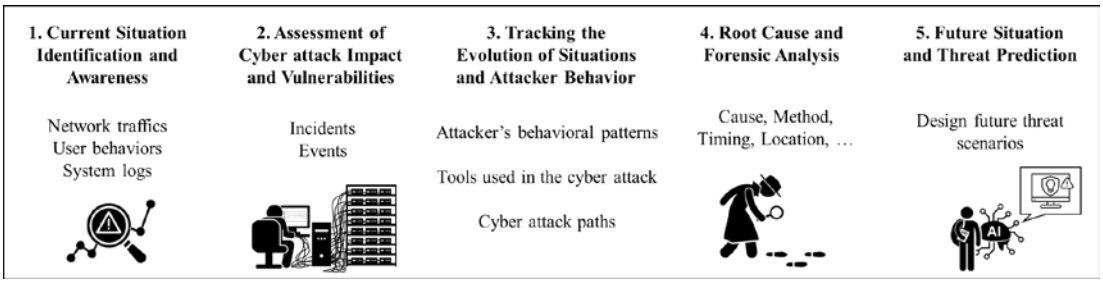

Fig. 1. The CSA-centered approach is considered an essential requirement for understanding events and situations occurring in cyberspace.

Fig. 2 illustrates this CSA-centered approach, highlighting its necessity in understanding cyber events and situations. Each phase of the CSA is differentiated by its unique research issues and techniques, addressing different aspects of cyber situational awareness. This model's effectiveness lies in its comprehensive coverage of various stages of cyber threats, from initial detection to future prediction, offering a more holistic approach than existing CSA research. It recognizes the interconnectedness and potential overlaps of various topics and techniques, underlining the complex nature of CSA. This complexity emphasizes the importance of CSA research as a key tool for addressing security issues in the modern digital environment.

2.1 Current Situation and Identification Awareness

In systems such as power systems and naval on-board digital systems, economic and national losses can be incurred from a single event [12,13]. Consequently, real-time event detection and analysis are essential processes to ensure the system operates safely by informing appropriate actions based on the situation. Although the complexity of systems continues to increase, enhancing situational awareness capabilities can be of significant assistance to system administrators in managing them [14,15]. For executing these processes effectively, various algorithms and systems have been researched:

- **Real-time Log Analysis and Event Detection Techniques**: Logs are records of various activities in the cyber environment. By collecting and analyzing logs in real-time, it is possible to instantly detect anomalies or threatening activities. Advanced log analysis tools require various heuristics and algorithms to detect anomalies with complex patterns.
- **Streaming Data Processing and Analysis Methods**: Data generated in the cyber environment continuously streams in. This streaming data requires a different approach than traditional batch processing. Technologies and algorithms to process streaming data in real-time are central to research and play a crucial role in detecting recent cyber threats in real-time.
- **Cyber Event Processing in Parallel and Distributed Computing Environments**: To process large volumes of data and complex algorithms in real-time, high-performance computing resources are essential. Parallel and distributed computing technologies are among the primary solutions to meet these needs, distributing data and computational tasks across multiple nodes to enhance processing speed.
- **Anomaly Detection Algorithms using Machine Learning and Deep Learning**: Unlike traditional signature-based IDS, machine learning and deep learning detect anomalies based on training data. This enables the effective detection of unknown new threats or highly variant attacks.
- **Comparison and Integration of Signature-based and Behavior-based IDS**: While signature-based IDS detects based on patterns of known attacks, behavior-based IDS

detects anomalies by comparing against the system's normal operational pattern. Considering the strengths and weaknesses of both approaches, an integrated IDS system can possess more potent detection capabilities.

- **Network Traffic Analysis and Pattern Recognition**: Network traffic fundamentally reflects activities in the cyber environment. By analyzing patterns within the traffic, threatening activities or anomalies can be effectively detected. Pattern recognition algorithms and statistical methodologies play a pivotal role in this analysis.

2.2 Assessment of Attack Impact and Vulnerabilities

In this phase, the consequences of a cyber-attack, including its impact, are understood, and the vulnerabilities of the system are assessed, playing a pivotal role in determining how future threats should be addressed [5]. Such assessments have been discussed in much research long before they became a new concept [16-19]. Topics and techniques that are valuable for research in this area are described as:

- **Vulnerability Assessment Techniques**: Within this category, security flaws within the system are identified, and the potential impact these flaws might have on attackers is evaluated. Exploration of new methodologies and algorithms to enhance the efficiency and accuracy of existing vulnerability scanning tools is required.
- **Attack Trees and Vulnerability Graphs**: This category encompasses tools and methodologies used for visualizing and analyzing cyber-attack pathways. Through this, potential attack routes an attacker might take to access the system and the most vulnerable attack points can be identified.
- **Impact Analysis:** This category deals with analyzing which parts of a system are affected by a cyber-attack, and what consequences this might have for users or organizations. This could include outcomes such as data loss, service interruptions, and financial losses.
- **Simulation and Modeling:** This category is about methodologies for testing system vulnerabilities or evaluating the impact of attacks in simulated scenarios. This allows for proactively addressing threats in actual environments.

2.3 Tracking the Evolution of Situations and Attacker Behavior

This phase provides profound insights into understanding exactly what is happening by tracking the progress after the occurrence of a cyber-attack or threat. Specifically, in this phase, it's important to grasp the motives, methods, and behavioral patterns of the actor [20,21]. Researchers looking to explore topics and techniques related to this should consider papers within the following categories:

- **Behavioral Analysis and Pattern Recognition:** This category covers techniques used to understand and predict the behavioral patterns, tactics, techniques, and procedures (TTPs) of specific attackers or attack groups. Through this, the motives and next moves of the attackers can be inferred.
- **Interaction Analysis with the Victim:** This category is about analyzing interactions between attackers and victims to discern the attacker's objectives and intentions. This can be done through communication patterns, the tools and methods used, among others.
- **Intelligence and Information Sharing:** This category encompasses mechanisms and protocols for integrating and analyzing information from various sources to provide an accurate situational picture.
- **Real-time Data Streaming and Analysis:** This category encompasses methods for monitoring and analyzing the progression of cyber-attacks or threats in real time. Algorithms and tools for rapid processing of large datasets fall under this category.

2.4 Root Cause and Forensic Analysis

After a cyber-attack occurs, it is vital to meticulously analyze the causes and traces, identifying which elements or actors were involved and the specific actions they took during the process [15,22,23]. The categories of topics and technologies that researchers should focus on related to this are as follows:

- **Memory Forensics:** Methods analyzing traces in memory related to the attacker's actions or the activities of malicious code are researched.
- **Network Forensics:** Research that analyzes network traffic to identify attack traces and communication patterns of malicious code.
- **System & OS-level Forensics:** Research conducts analysis of operating systems or system logs, configuration files, etc., to trace the cause of an incident or an attacker's actions.
- **Malicious Code & Virus Analysis:** Research focuses on in-depth analysis of the functionality, behavior, and communication patterns of malicious code or viruses used in an attack.
- **Timeline Analysis:** Research aims to reconstruct all activities in the order they occurred to grasp the entire flow of the attack and the intent of the attacker.
- **Data Recovery & Cryptanalysis:** Research investigates recovering and interpreting deleted or encrypted data to understand the overall context of an incident.

2.5 Future Situation and Threat Prediction

Predicting future situations and threats is a crucial aspect of a holistic view of cyber security. The aim at this stage is to predict potential changes in future threats or the cyber security landscape based on past incidents or the current situation [24-26]. Noteworthy categories of topics and technologies related to this include:

- **Threat Prediction using Machine Learning & Deep Learning:** Research on algorithms that learn from past data and current trends to predict future cyber threats.
- **Threat Intelligence:** Research analyzes information collected from various sources to understand future threats to specific organizations or systems.
- **Predicting Malicious Code Behavior:** This research analyzes the potential evolution and threats posed by various types of malicious code.
- **Risk Management & Evaluation:** This study focuses on methodologies for managing and evaluating future risks, considering the current security posture and potential threats.
- **Scenario-based Prediction:** This research involves constructing various cybersecurity scenarios to anticipate threats in specific future contexts.
- **Cyber Security Trend Analysis:** This study examines future technology trends and industry movements to anticipate changes in cybersecurity.
- **Cyber Strategy & Policy Prediction:** This research aims to predict potential threats arising from changes in national or major organizational cyber strategies and policies.

By exploring these topics and techniques, the essential content and importance of the 'Future Situation and Threat Prediction' phase are understood. Through the fifth step of the CSA, security experts are enabled to perceive threats in the future and to develop effective response strategies accordingly. This plays a pivotal role in protecting an organization's or individual's digital assets. Research on the CSA has drawn the attention of many researchers due to its complexity and diversity. In this chapter, the procedure of CSA was divided into five steps, and research topics and technical categories associated with each step were examined. Through this, the overall structure and operational principles of the CSA can be comprehended. Moreover, it was recognized that various topics and techniques might be interconnected, and

some may have overlapping elements. Such a complex structure and relationship emphasize the importance of CSA research. CSA serves as a key tool for addressing security issues and threats in the modern digital environment. Therefore, such research will greatly assist in establishing future cybersecurity strategies and measures. To conclude this chapter, it is emphasized that research on CSA needs to continually evolve and develop. A deep understanding of each process and category will provide us with better security solutions and equip us with the capability to effectively counter threats in cyberspace.

3. Related Works

In this section, all papers, reports, etc., related to CSA are meticulously reviewed and analyzed based on the approach explained in **Fig. 1**. To reflect the latest trends, all these literatures were constituted of works from 2019 and beyond.

3.1 Current Situation Identification and Awareness

In the initial stages of CSA, the current situation and identification awareness play crucial roles by capturing the current state of the network or system. On this basis, security threats are detected. Depending on the characteristics of each field, these awareness methods and strategies can be applied differently. In the maritime field, due to its nature, computation and communication from remote locations are essential, making it potentially vulnerable to cyber-attacks. To counter this, research was conducted on building a platform to detect cyber-attacks in real-time and refine maritime CSA [13]. In the research below, the authenticity, freshness, completeness, and reliability of logs and threat data were emphasized. It was also proposed that maritime CSA can be achieved through the automatic classification of attack patterns [20]. However, a limitation of this approach is the difficulty in automatically predicting the spread and impact of an attack.

Cyber-Physical Systems (CPS) refer to systems that control and monitor physical processes through computer-based algorithms and networks [27]. These systems interact with the physical environment through real-time data analysis and feedback, playing a pivotal role in various application areas such as automobiles, power grids, medical systems, and smart cities. A digital twin represents a virtual representation of a physical entity or process, collecting information from the real environment to represent, validate, and simulate the current and future behaviors of the physical twin [28]. A prototype of a CSA framework for CPS based on digital twins was introduced in a piece of research [29]. The core of this framework is the virtual environment hosting the digital twin. Data from the physical environment, such as system logs, network traffic, and sensor measurements, is collected, reflecting the program state of the digital twin. Through this state replication mechanism, the operation of the digital twin can be monitored at the program and network layer, and intrusions can be detected. As the digital twin is generated from the specifications of the CPS, it should represent the correct operation of the actual device. The prototype is based on Mininet-WiFi [30], capable of executing International Electrotechnical Commission (IEC) 61131-3 code in the context of the digital twin. This enables emulation or simulation of the device's functions, a crucial element in CSA.

In the field of cyber security and CSA, the importance of data from various fields has been emphasized recently. Research proposing a framework to enhance CSA using various data sources conducted pattern extraction and prediction in data-centric software, focusing on neural networks and machine learning methodologies [31-34]. Serverless computing frameworks were utilized to optimize the cost and speed of machine learning solutions. This

technical approach was based on use cases for public safety solutions. This research explored ways to enhance the efficiency and accuracy of CSA through the integration of machine learning and serverless computing.

There's also research that presented datasets for CSA in the power production sector. In this research, methods correlating the impact of selected Advanced Persistent Threats (APTs) with each stage of the cyber kill chain were explored [35]. As a result of this research, a new dataset called Cyber Situational Awareness System (CYSAS)-S3 was introduced. CYSAS-S3 is a new dataset designed to bridge the gap in the availability of consistent, reliable, and unbiased data for training automation in the context of cyber defense. Most existing network datasets [36-43] do not provide comprehensive information across all communication layers and are synthetically generated in scenarios that do not reflect the unique challenges of cyber defense operations. Furthermore, these datasets overlook the relationship between incidents at the hardware/software level and the impact on military mission assets and objectives, bypassing the chain of dependencies between strategic, operational, tactical, and technical areas. This research presented a technical methodology to evaluate and enhance CSA, focusing on the relationship between APTs and the cyber kill chain.

Due to the countless occurrences of cyber security issues in networks, efforts are actively being made to ensure the safety of networks. As a result, real-time network monitoring and Intrusion Detection Systems (IDS) utilizing machine learning are sometimes being employed. In this context, a novel approach combining Software Defined Networking (SDN) and machine learning to enhance CSA has been introduced in recent research [44]. In this research, network flows were monitored in real-time using SDN, and the vulnerabilities of each entity within the network were evaluated through it. Moreover, an IDS based on Machine Learning (ML) was developed using an enhanced dataset, and a feature to detect ongoing attacks in real-time was implemented. The ML-IDS was trained using neural networks (NN). Considering the existence of multi-class classification problems and following literature [45-48], Rectified Linear Unit (ReLU) was used in the hidden layers of the neural model, while the hyperbolic tangent (Tanh) was used as the activation function. The output layer of the model employed the SoftMax function. Additionally, a method to quantitatively assess the vulnerability status of each entity using the Common Vulnerability Scoring System (CVSS v3.1) was proposed [49].

In reviewing the studies presented in Section 3.1, a clear connection can be observed between these research efforts and the specific techniques detailed in Section 2.1:

- The research on real-time cyber-attack detection in maritime environments, exemplified by Jacq et al. [13], demonstrates an application of real-time log analysis and event detection. This research highlights the necessity for accurate and reliable log data, essential in promptly identifying cyber threats in maritime contexts, resonating with the principles of real-time event detection techniques.
- The development of a CSA framework for CPS incorporating digital twins, as introduced by Eckhart and colleagues [29], aligns with streaming data processing and analysis methods. This innovative approach effectively leverages continuous data streams from the physical environment, showcasing a novel method of data utilization for enhanced situational awareness.
- The proposal of a machine learning-based framework for CSA enhancement, as discussed in the work of Nesen et al. [31], connects directly with the use of anomaly detection algorithms using machine learning and deep learning. This approach underlines the significance of leveraging advanced computational techniques to identify and predict cyber anomalies efficiently.

- The introduction of the CYSAS-S3 dataset, aimed at improving CSA in the power production sector by Medenou Choumanof et al. [35], is particularly relevant to network traffic analysis and pattern recognition. By focusing on the relationship between APTs and the cyber kill chain, this research offers an advanced perspective in network traffic analysis, crucial for understanding and mitigating cyber threats.
- Finally, the innovative research combining SDN with machine learning to enhance CSA, as explored by Nikoloudakis et al. [44], integrates aspects of both anomaly detection algorithms and the combination of signature-based and behavior-based IDS. This study not only utilizes machine learning for real-time threat detection but also proposes a quantitative assessment of network vulnerabilities, embodying a comprehensive approach to modern cyber situational awareness.

3.2 Assessment of Attack Impact and Vulnerabilities

In CSA, the assessment of attack impact and vulnerability evaluation is considered an essential step. In this step, potential attacks and their consequences are assessed, vulnerabilities of the system are analyzed, and response strategies are formulated. By this assessment and analysis, preparation can be made in advance, minimizing damage during actual attacks. As an actual example, a cyber-attack that occurred in Ukraine in 2015 led to a power outage in a CPS environment, resulting in significant social and economic losses [50]. The importance of CPS cyber vulnerabilities was highlighted by this incident. Consequently, vulnerability analysis research centered on a specific attack scenario, False Alarm Attack (FAA), was conducted considering the smart grid as a representative CPS [51]. In this research, the vulnerabilities of CPS were thoroughly analyzed using two primary methodologies: the topology-evaluated method (TEM) [52,53] and the functionality-evaluated method (FEM) [54,55]. The TEM provides an analysis centered on the structural characteristics of the network using indicators like clustering coefficients [56], average path lengths [57], and relative sizes of main components [58]. On the other hand, FEM conducts an analysis focusing on the functional characteristics of the network, identifying vulnerabilities after initial errors by observing congested or disrupted areas in the network.

The stability and security of power systems are regarded as crucial issues, and especially, criteria for evaluating stability when a specific component fails is important. In relation to this, the term N-1 is used in power system operations. N-1 refers to a situation where one of the entire system components has failed, with 'N' representing the total number of system components and '-1' indicating the failure of one component. Thus, the N-1 situation means a scenario where one component in the entire system isn't functioning. Regarding the N-1 security standard, it mandates that the power system continue to operate safely under given circumstances. In power systems that adhere to the N-1 security standard, research has been conducted analyzing the impact of Coordinated Cyber-Physical (CCP) attacks [59] to mitigate Coordinated Cyber-Physical Attack (CCPA) [60]. In this research, the basic principles of CCP [61] and research concerning the most severe CCPA [62] were referenced. The attack model was analyzed using AC-based tri-level optimization [63], and for this, a methodology was proposed to convert tri-level optimization into cone optimization using quasi-governmental integration programming relaxation and primal-dual formalization methods.

Unoccupied aerial vehicles (UAVs) have been progressively developed and are now used in numerous autonomous operations and application areas. Notably, their use in hazardous environments, such as firefighting, has been drawing attention [64-67]. However, UAVs have been widely recognized for their vulnerabilities to cyber-attacks, prompting research to address these issues [68]. A combination of the Petri net model [69-72] and task performance

models has been proposed for modeling and inferring the impacts of attacks and tasks.
In research aimed at identifying and analyzing common cyber vulnerabilities of websites, various techniques and methodologies have been employed [73]. Technologies such as IP-API [74], Port Scan [75,76], Click Jacking [77,78], Host Header Injection [79], and Reverse IP [80] have been utilized to identify and analyze website vulnerabilities.
Profound insights into cyber-attacks and security vulnerabilities for CSA are provided by these studies, which contribute to the establishment of a safer digital environment today. Specifically, CSA for intricate systems like CPS is deemed of high importance, and continued technical and methodological advancements are seen as crucial.
In Section 3.2, the studies contribute significantly to the assessment of attack impact and vulnerabilities, each aligning with the techniques described in Section 2.2:

- The research conducted on FAA in smart grids by Tu et al. [51] aligns closely with the 'Vulnerability Assessment Techniques'. This study employs both the TEM and the FEM for a comprehensive analysis of CPS vulnerabilities. These methodologies exemplify the identification of security flaws and the evaluation of their potential impact, resonating with the principles of vulnerability assessment.
- The examination of CCP attacks in power systems, as explored in the work by Zhou et al. [60], corresponds with 'Impact Analysis'. This research, focusing on the N-1 security standard in power systems, highlights the significance of understanding the effects of cyber-attacks on crucial infrastructure components, thereby providing valuable insights into the consequences of such attacks on system stability and user safety.
- The study on cyber vulnerabilities in UAVs by Soikkeli and colleagues [68] reflects the importance of 'Simulation and Modeling' in CSA. By employing a combination of the Petri net model and task performance models, this research contributes to the simulation and modeling of attack impacts, offering a methodological approach to evaluate and mitigate vulnerabilities in autonomous UAV operations.
- Lastly, the research focusing on common cyber vulnerabilities of websites by Kumar and associates [73] illustrates the application of 'Attack Trees and Vulnerability Graphs'. Utilizing various technologies like IP-API, Port Scan, and others, this study aids in visualizing and analyzing cyber-attack pathways, contributing to the identification of potential vulnerabilities and attack routes in website security.

These studies, by addressing different aspects of vulnerability and impact assessment, reinforce the critical nature of this phase in CSA. They provide a deeper understanding of how to evaluate and mitigate potential cyber threats, underscoring the necessity for continuous advancements in vulnerability assessment and impact analysis methodologies.

3.3 Tracking the Evolution of Situations and Attacker Behavior

In the field of cyber security, various studies have been conducted to enhance CSA by deeply understanding attacker behavior patterns, tools used, and their attack pathways. Among these studies, a method has been proposed to analyze attack graphs to understand attacker activities within the Cyber Kill-Chain and its specifics in a network [82]. This attack graph is generated by collecting vulnerability and access control information from open-source network scanning tools like Nessus [83] and is created using the MulVAL simulation engine [84].
Furthermore, research has been undertaken to precisely model attacker behaviors [85]. The focus of this study is to minimize or prevent potential losses or damages to people, assets, and information, based on a profound understanding of attack mechanisms. A methodology for implementing an attacker agent based on a probabilistic optimization framework has been

introduced and using the adversary view security evaluation (ADVISE) format [86], various attack paths for CPS can be visualized and experimentally tested.

Research is also actively being pursued to enhance security situation awareness using large-scale log data mining. A method has been proposed to apply graph neural networks for security situation awareness, considering interactions between users suitable for graph data structures [87]. This approach mines log data to extract user characteristics and predict user behavior through graph neural networks, representing relationships between users and between users and servers more accurately compared to traditional supervised or unsupervised algorithms.

Recent studies have highlighted the importance of cyber security while pointing out the challenges faced by traditional security systems in detecting zero-day attacks or behavioral changes [88]. As an alternative solution, the Honeynet-Docker (H-DOC) bait deployed in Docker, a hybrid Honeynet model, has been proposed [89]. This method aims to lure attackers and analyze their behavior patterns, with a particular focus on the SSH protocol. This research has made a significant contribution to enhancing the accuracy of attack detection.

In Section 3.3, a series of studies contribute to a deeper understanding of attacker behavior, tools used, and attack pathways, each aligning with the methods detailed in Section 2.3:

- The method for analyzing attack graphs, as proposed in the study by Haque et al. [82], corresponds to the 'Behavioral Analysis and Pattern Recognition' category. By generating attack graphs using open-source network scanning tools and the MulVAL simulation engine, this research offers insights into attacker behavioral patterns, tactics, and procedures within the Cyber Kill-Chain, highlighting the ability to infer attackers' motives and next moves.
- The research focused on modeling attacker behaviors by Gonzalez and colleagues [85] is closely related to 'Interaction Analysis with the Victim'. This study, which implements an attacker agent based on a probabilistic optimization framework and uses the ADVISE format, provides a profound understanding of the interactions between attackers and victims, revealing attackers' objectives and intentions.
- Xu et al.'s approach to enhancing security situation awareness using graph neural networks [87] aligns with the 'Real-time Data Streaming and Analysis' technique. This study's application of graph neural networks to mine large-scale log data and extract user characteristics demonstrates an advanced method for monitoring and analyzing the progress of cyber threats in real-time, emphasizing the importance of rapid data processing.
- The H-DOC bait deployed in Docker, as explored in the work of Amal and associates [89], resonates with the 'Intelligence and Information Sharing' category. This hybrid Honeynet model, focusing on attracting and analyzing attacker behavior, especially regarding the SSH protocol, contributes to the integration and analysis of information from various sources, thus enhancing the accuracy of situational awareness in cybersecurity.

Each of these studies, by addressing different aspects of understanding and tracking attacker behavior, enriches the field of CSA. They provide valuable insights into the methodologies for analyzing attacker interactions, predicting their behavior, and integrating information from various sources for a more accurate and comprehensive situational picture.

3.4 Root Cause and Forensic Analysis

When cyber-attacks occur, it's imperative that the causes and traces of these attacks are analyzed. In the realm of digital forensics, research that addresses situational awareness and time-critical decision-making proposes the Digital Evidence Object (DEO) and aims to

construct a framework for developing digital forensic investigation systems [90]. This research, grounded in the basic principles of the DEO model, analyzes, and conducts digital forensic investigations based on the 5W (Why, When, Where, What, Who).

The operation of Cyber-physical power systems (CPPS) has been widely adopted due to advancements in power grids and information communication technologies [91-93]. To address cyber security issues in these CPPS, it is essential that cyber-attacks are identified and traced [94]. On the physical side, attacks are identified based on network topology and physical location understanding combined with network error location algorithms. On the cyber side, technologies integrating IP tracking, Media Access Control (MAC) layer tracing, and device fingerprint recognition are utilized to trace the source of attacks.

Research has been conducted investigating various literature for implementing security models in UAVs [95]. In this study, techniques were categorized into IP header-based [96], Messages [97], and Traffic patterns. Forensic investigation techniques have been defined in terms of incident handling (e.g., PC, mobile phone usage) [98], identification (e.g., suspect identification, computerized evidence identification) [98], seizure (routine computer evidence storage) [99], imaging (bitwise clone of fragment streams), hashing (MD5, SHA1, SHA25, etc.) [98], analysis (evidence collection, etc.) [98], reporting (providing legal investigation), and preservation (physical and intellectual protection of evidence).

Research exists that utilizes Border Gateway Protocol (BGP) Archive Data to analyze the origins of cyber-attacks [100]. After profiling specific hacking cases of a North Korean cyber-attack group [101], attack techniques were analyzed based on the MITRE ATT&CK framework. Malicious Visual Basic Scripts within document files used in the hacking case [101] were analyzed, from which Command & Control (C2) addresses were obtained. Subsequently, BGP data was preprocessed and analyzed to visualize the network traceback path.

In Section 3.4, various research studies provide significant insights into the forensic analysis of cyber-attacks, aligning with the methodologies described in Section 2.4:

- The study by Grigaliunas et al. [90], focusing on the DEO model for digital forensic investigations, correlates with 'System & OS-level Forensics' and 'Data Recovery & Cryptanalysis'. This research underlines the importance of analyzing system logs and configuration files, as well as recovering and interpreting data to understand the context of cyber incidents, embodying the principles of comprehensive forensic analysis.
- The research addressing cyber security in CPPS by Ni and associates [94] resonates with 'Network Forensics' and 'Timeline Analysis'. It involves the identification of cyber-attacks based on network topology and the tracing of the source of attacks using IP tracking and MAC layer tracing. This approach represents a methodical examination of network traffic and communication patterns, as well as reconstructing the sequence of events to understand the attack flow.
- The study on implementing security models in UAVs by Alsulami [95] aligns with 'Memory Forensics' and 'Malicious Code & Virus Analysis'. This research categorizes techniques such as IP header-based analysis and message patterns, which are crucial for analyzing memory traces and understanding the behavior of malicious code or viruses, providing a detailed perspective on forensic investigation in UAV security.

- Finally, the utilization of BGP Archive Data to analyze cyber-attacks origins, as explored by Youn et al. [100], corresponds with 'Network Forensics' and 'Data Recovery & Cryptanalysis'. This study's profiling of specific hacking cases and the subsequent analysis of BGP data to trace back network paths exemplifies the depth of network forensics and the criticality of data analysis in understanding the origins and progression of cyber-attacks.

Each of these studies contributes significantly to the field of cyber forensics, addressing different aspects of forensic analysis from system and network forensics to the in-depth examination of malicious code and data recovery. They underscore the necessity of comprehensive forensic methodologies to accurately trace, understand, and respond to cyber incidents.

3.5 Future Situation and Threat Prediction

Research has been presented that proposes a model to enhance CSA of Small and Medium-sized Enterprises (SMEs) [102]. This model extended Endsley's situation awareness theory to evaluate the CSA of SMEs [103]. The proposed model was validated using partial least squares structural equation modeling with data collected from an online survey. From this analysis, it was mentioned that SMEs should eliminate outdated password practices and be adjusted under the UK's NCSC to maintain system security [104].

Research has developed an Artificial Intelligence (AI)-based prediction engine that classifies vulnerabilities using various vulnerability reports collected through CyVIA [105], such as NVD [106] [107]. This engine aids cyber defenders by classifying vulnerability reports based on attack types, allowing for rapid analysis of attack types applicable to evaluated infrastructure. The classification was done through AI-based prediction engines developed using K-Means clustering [108], and Zero-Shot learning models (BERT, Flair, Transformer models) [109,110]. Such approaches enable cybersecurity experts to quickly recognize and respond to vulnerabilities, facilitating more effective responses to cyber-attacks.

There are research cases that combine Convolutional Neural Network (CNN) [111] and Bidirectional Gated Recurrent Unit (BiGRU) [112] to improve the accuracy and efficiency of network security situation prediction [113]. By integrating CNN and BiGRU and using the Attention mechanism, weights were variably assigned based on situation attributes. Observing that the results of the model converge to 0.98 indicates highly effective performance.

In research developing tools for Criminal Network Analysis (CNA) [114,115] to halt evolving illicit activities within networks [116], it was demonstrated that models developed with Deep Reinforcement Learning (DRL) [117,118] could exhibit better prediction performance than those developed with conventional supervised learning techniques like GBM [119], RF [120], and SVM [121].

In Section 3.5, the research studies focus on predicting future cyber situations and threats, each aligning with specific categories in Section 2.5:

- The model proposed to enhance CSA for SMEs by Renaud et al. [102] resonates with 'Cyber Strategy & Policy Prediction'. By extending Endsley's situation awareness theory and validating it for SMEs, this study contributes to understanding how changes in cyber strategies and policies can affect the security of smaller organizations, providing insights into future risk management and policy adjustments.
- The development of an AI-based prediction engine for vulnerability classification by Malik and team [107] aligns with 'Threat Prediction using Machine Learning & Deep Learning'. This research, which employs advanced AI techniques like K-

Means clustering and Zero-Shot learning models, demonstrates a method for predicting future cyber threats based on analysis of past data and current vulnerability reports, enhancing the capabilities of cyber defenders in identifying and responding to emerging threats.

- The combination of CNN and BiGRU to improve network security situation prediction, as explored in the study by Hu et al. [113], is closely related to 'Risk Management & Evaluation'. The integration of these advanced neural network models, along with the use of an Attention mechanism, offers an innovative approach to evaluate and manage potential risks in cyber security by accurately predicting future security situations.
- Lastly, the research on CNA tools by Lim and associates [116], which utilizes DRL, aligns with 'Scenario-based Prediction'. This study demonstrates the utility of DRL models in predicting the evolution of criminal networks and illicit activities, thus contributing to the construction of various cybersecurity scenarios for anticipating specific future threats.

Each of these studies advances our understanding of how to predict and prepare for future cyber situations and threats. They emphasize the importance of using advanced data analytics, machine learning, and AI techniques to analyze trends, evaluate risks, and formulate strategies for future cybersecurity challenges.

Table 1 provides a comprehensive overview of CSA research from 2019 to 2023. It categorizes each piece of research by main categories and provides detailed information on their primary objectives, techniques, and methodologies used, limitations, as well as the industry sectors where the research was applied. This table facilitates a quick understanding of the latest research trends and directions in CSA. Additionally, by highlighting each research's limitations, it underscores the necessity and directionality for future research. It is important to note that the references in the 'Technique & Methods' field may differ from those in the 'Research/Year' field. This is because 'Technique & Methods' references are meant to cite the original sources or seminal works where these specific techniques and methods were first introduced or detailed, while the 'Research/Year' references pertain to the specific studies being discussed.

Table 1. CSA Research Overview (2019-2023)

Category	Research / Year	Objective	Technique & Methods	Limitations	Target Area
Current Situation and Identification Awareness	O. Jacq et al. [13] / 2019	Maritime attack detection & CSA refinement	Security ops center logs (Authenticity, freshness, etc.)	Unspecified techniques, only methodology	Marine (Naval)
	M. Eckhart et al. [29] / 2019	CSA via digital twins for CPS	Use of digital twins & Mininet-WiFi [30]	Possible mismatch with real devices	CPS
	A. Nesen et al. [31] / 2021	CSA enhancement with multimodal data	Neural networks, machine learning, and serverless computing [33-34].	Optimal server use if workload unchanged	Public Safety
	R. D. Medenou Choumanof et al [35] / 2022	CYSAS-S3 dataset for power generation sector CSA	Cyber kill chain correlation with selected APTs	Dataset needs isolated environment	Power Generation

	Y. Nikoloudakis et al. [44] / 2021	Machine learning-based situational awareness framework	SDN, machine learning, and CVSS [45-49]	Insufficient real environment validation	Cyber space (Network security)
Assessment of Attack Impact and Vulnerabilities	H. Tu et al. [51] / 2022	CPS vulnerability analysis	FAA [51], TEM [52,53], FEM [54,55]	Assumption on meter readings	CPS
	M. Zhou et al. [60] / 2022	N-1 power system vulnerabilities	AC-based triple optimization [63]	Quasi-static power system operation assumption	Power System
	J. Soikkeli et al. [68] / 2021	UAV team mission survivability analysis	Petri nets [69-72], mission models	UAV damage assumption on attack success	UAV
	B. P. Kumar et al. [73] / 2023	Website security vulnerabilities analysis	IP-API [74], Port Scan [75,76], etc.	80% accuracy due to third-party sites	Cyber space (Web Site)
Tracking the Evolution of Situations and Attacker Behavior	M. A. Haque et al. [82] / 2022	Identifying attack points in graphs	Nessus [83], MulVAL [84]	Absence of labels in attack graph	Cyber space (Threats Analysis)
	S. R. Gonzalez et al. [85] / 2022	Attacker agents' environment for CPS	ADVISE [86]	Model including attacker-defender interaction needed	CPS
	Y. Xu et al. [87] / 2022	Extract user characteristics & predict attacker behavior	Graph neural networks, log analysis	Lack of evaluation on user-server graph effectiveness	Cyber space (Data Mining)
	M. Amal et al. [89] / 2023	Analyze attacker behavior with H-DOC bait	H-DOC, Honeypot, Docker	Focus only on SSH protocol	Cyber space (Pattern Analysis)
Root Cause and Forensic Analysis	S. Grigaliunas et al. [90] / 2020	Digital forensic investigation framework	DEO model for 5W	Focus on limited data, not on big data	Cyber space (Digital forensic)
	M. Ni et al. [94] / 2020	Address cybersecurity in cyber-physical power systems	Cyber-physical event chain	Harmonious design of cyber & physical aspects required	CPPS

	H. Alsulami [95] / 2022	Explore UAV functionality & cybersecurity	Attack detection, traceback [96,97], forensics [98,99]	Not specified	UAV
	J. Youn et al. [100] / 2022	Cyber ISR visualization via BGP data	Hacking case profiles [101], BGP data	Lack of automation in tracking visualization	Cyber space (Visualization)
Future Situation and Threat Prediction	K. Renaud et al. [102] / 2021	Improve CSA for SMEs	Endsley's theory expansion [103]	Focus on SMEs might not apply to large organizations	Small and Medium Enterprises
	A. A. Malik et al. [107] / 2023	Vulnerability report classification	K-Means [108], BERT, Flair, Transformers [109,110]	Data cleaning & manual labeling issues	Cyber Space (Threat Intelligence)
	C. Hu et al. [113] / 2022	Enhance network security prediction accuracy	CNN [111] BiGRU [112]	Need for GRU model optimization	Cyber Space (Situation Prediction)
	M. Lim et al. [116] / 2019	Develop CNA tool against network crime	DRL [117,118]	Incomplete or inconsistent data in crime network prediction	Cyber Space (Network Analysis)

The content examined in this manner addresses the significance of CSA and its application areas, and the implications can be summarized as follows:

1) Significance of research across various domains: CSA is considered an important research topic in various domains, each with its specific challenges and objectives. Through this, one can understand the significance of CSA and the diversity of its application areas.
2) Advancement and limitations of technology: Many research attempts to enhance CSA using the latest technologies and methodologies, yet there remain problems and limitations to be solved. This emphasizes the continuous need for research.
3) Need for an integrated approach: An integrated approach utilizing various technologies and methodologies is essential for enhancing CSA. This is to meet the complexity and diverse requirements of CSA.
4) Difference between research outcomes and real-world application: There may be discrepancies between research findings and their real-world applications. Therefore, thorough validation and testing are required before implementing research results in actual environments.
5) Direction of future research: Research predicting future cyber situations and threats is a crucial aspect of CSA. Through this, strategies can be devised to prepare for future threats and enhance security.

4. Challenges and Future Opportunities

With the rapid progression of the digital environment, the importance of CSA is escalating. From 'current situation and identification awareness' to 'future situation and threat prediction', there are various challenges and opportunities. These challenges and opportunities were identified based on the key elements from Section 3: Related Works. This section systematically explores these challenges and opportunities, providing a deeper understanding of CSA and suggesting directions for future research. **Fig. 2** visually summarizes these challenges and opportunities. These serve as vital guidelines in planning and implementing CSA research and strategies and will be a useful reference for researchers and experts.

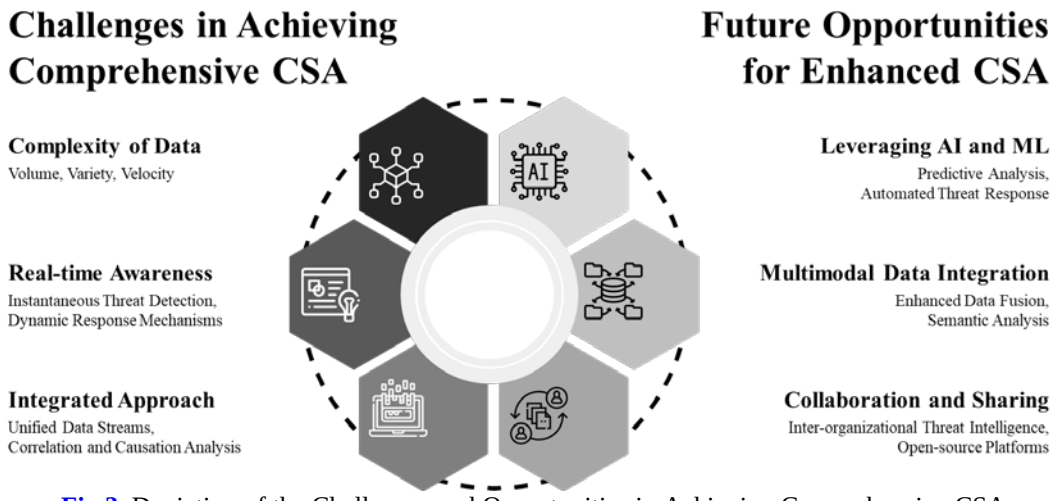

Fig 3. Depiction of the Challenges and Opportunities in Achieving Comprehensive CSA

4.1 Challenges in Achieving Comprehensive CSA

Firstly, in 'current situation and identification awareness', there's a challenge related to the 'complexity of data' where massive amounts of data are continuously generated and need real-time processing. In 'evaluation of attack impact and vulnerabilities', the need for 'real-time awareness' is highlighted due to the rapid detection and response to various threats as they emerge. Furthermore, in 'tracking the progression of situations and attacker behaviors', the importance of an 'integrated approach' is emphasized, necessitating connections and integrations between diverse data sources and platforms.

4.1.1 Complexity of Data

- **Volume of Data:** It has been observed that the volume of data in cyberspace is increasing exponentially [122]. This burgeoning amount of data necessitates the employment of sophisticated real-time processing solutions. Technologies in big data analytics and cloud computing are being leveraged to handle this data efficiently.
- **Diversity:** The data in cyberspace, noted for its inconsistency [123], ranges from structured formats to unstructured data like social media posts, images, and videos. Advanced algorithms for extracting actionable insights from this diverse data are being explored, with techniques in data mining and natural language processing being employed.
- **Speed:** The speed of data generation and processing in cyberspace is unparalleled [124]. High-performance and edge computing technologies are being considered to meet the need

for rapid data analysis and threat detection.

4.1.2 Real-time Awareness

- **Immediate Threat Detection:** The need for immediate detection of cyber threats, owing to their frequent occurrence, is emphasized [125]. The integration of AI and ML for rapid analysis and identification of cyber threats is being pursued to improve immediate threat detection capabilities.
- **Dynamic Response Mechanism:** The development of systems capable of initiating immediate responses upon threat detection is being prioritized. This involves the creation of self-adaptive cybersecurity systems that autonomously react to threats in real-time.

4.1.3 Integrated Approach

- **Integrated Data Stream:** The integration of data from diverse sources, such as network logs, user activity, and external threat feeds into a single platform, is being advocated [126]. This approach aims to provide a holistic view of the cyber environment.
- **Correlation and Causal Analysis:** The capability of systems to link different data points after data integration is being enhanced [127]. This includes the refinement of correlation and causal analysis tools to establish relationships between various events in the cyber realm.

4.2 Future Opportunities for Enhanced CSA

Potential future opportunities include leveraging artificial intelligence and machine learning in "Cause & Forensic Analysis" to predict potential future threats based on past data ("Utilization of AI & ML"). "Future Situation & Threat Prediction" offers the opportunity for "Multimodal Data Integration", merging data in forms like text, images, and audio for a more in-depth and comprehensive understanding of CSA. Lastly, emphasizing collaboration and sharing in all research areas, opportunities for "Collaboration & Sharing" are presented, including inter-organizational threat intelligence sharing and the development of open-source platforms.

4.2.1 Leveraging Artificial Intelligence and Machine Learning

- **Predictive Analysis:** The use of AI and ML for predictive analysis to foresee potential future threats based on historical data is being investigated [128].
- **Automated Threat Response:** Training machine learning models to initiate automated responses upon threat detection is a focus area [129].

4.2.2 Multimodal Data Integration

- **Enhanced Data Fusion:** Efforts are being made to integrate different forms of data, such as text, images, and audio, to achieve a more comprehensive understanding of the cyber environment [130].
- **Semantic Analysis:** Technologies like NLP are being utilized to derive deeper insights from text data, enhancing the understanding of user behavior and potential threats [131].

4.2.3 Collaboration and Sharing

- **Inter-organizational Threat Intelligence Sharing:** The sharing of threat intelligence among organizations is being promoted to enhance CSA [132].
- **Open-source Platforms:** The development of open-source platforms for CSA is being

encouraged to provide broader access to advanced tools and techniques, benefiting a wider range of organizations.

The path to achieving comprehensive CSA is laden with challenges, but it also offers significant opportunities for advancement through technology and collaboration. The future direction of CSA research should focus on these specific areas, leveraging the latest technological innovations to create a safer, more secure cyberspace.

5. Conclusion

The exploration of CSA within this study highlights the evolving complexity of information security in the digital and communication networks of cyberspace. The significance of CSA has been underscored, establishing it as a pivotal component of cyber security strategies. It focuses on the identification, understanding, and response to a wide array of cyber threats, a capability deemed essential, particularly from a defensive perspective.

This research introduced a systematic five-step approach to CSA, aiming to systematically enhance situational awareness. It segments the CSA process into stages encompassing current situation identification, attack impact assessment, tracking situational evolution, forensic analysis, and future threat prediction. The application of this approach is vital across various industries, such as finance, healthcare, manufacturing, communication, transportation, and energy, highlighting its increasing relevance and the need for deeper insights into these sectors.

From the survey and analysis of recent CSA research works, as detailed in **Table 1**, several key implications have emerged:

- Diversity in Application Areas: The research surveyed demonstrates CSA's applicability across different sectors, each presenting unique challenges and necessitating tailored approaches. This diversity underscores the flexibility and wide-ranging impact of CSA strategies.
- Technical Challenges and Innovations: The studies reveal ongoing challenges in processing vast data volumes, achieving real-time awareness, and integrating diverse data sources. Concurrently, they showcase innovative solutions and technologies addressing these challenges, underscoring the dynamic nature of CSA.
- Future Directions and Opportunities: The advancements in artificial intelligence, machine learning, and multi-modal data integration present promising avenues for further enhancing CSA. Additionally, the potential for expanded effectiveness through cross-organizational collaboration and information sharing is evident.

The comprehensive understanding of CSA provided by this research aims to fuel active pursuit in its research and development. The findings and recommendations serve as foundational references for implementing CSA in real-world cyber security scenarios.

In future studies, it is to be recommended that the integration of detailed case studies, which demonstrate the application of CSA in real-world scenarios, will be undertaken, alongside the exploration of specific implementation strategies and advanced technologies. Through these additions, deeper insights into the implementation and impact of CSA strategies are to be gained. Moreover, the proposed CSA methodologies are to be subjected to comparative analysis against other existing frameworks or approaches. This analysis is expected to elucidate the relative strengths and weaknesses of the methodologies, thereby assessing the unique contributions of this research within the broader context of CSA studies. Such ongoing research and development are essential for strengthening cyberspace safety and security, and for proactively protecting organizations and individuals from emerging cyber threats.

References

[1] M. Castells, "The Rise of the network society Volume 1 With a new preface," *The Rise of the network society*, vol. 1, p. 91, 2009. Article (CrossRef Link).

[2] L. Lessig, *Code: And other laws of cyberspace*, Basic Books, Inc.Division of HarperCollins 10 E. 53rd St. New York, NYUnited States, 1999. [Online]. https://dl.acm.org/doi/10.5555/555000

[3] J. P. Barlow, "A Declaration of the Independence of Cyberspace," *Duke L. & Tech. Rev.*, vol. 18, p. 5, 2019. [Online]. Available: https://wac.colostate.edu/rhetnet/barlow/barlow_declaration.html. Accessed on: Sep 27, 2023.

[4] U. Department of Defense, "Quadrennial defense review report," ed: Department of Defense Washington, DC, 2010. [Online]. Available: https://dod.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf. Accessed on: Sep 27, 2023.

[5] M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," *Human factors*, vol. 37, no. 1, pp. 32-64, 1995. Article (CrossRef Link)

[6] P. Liu, V. Swarup, and C. Wang, *Cyber Situational Awareness: Issues and Research*, Springer-Verlag US, 2010. Article (CrossRef Link)

[7] T. Bass, "Intrusion detection systems and multisensor data fusion," *Communications of the ACM*, vol. 43, no. 4, pp. 99-105, 2000. Article (CrossRef Link)

[8] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Leading Issues in Information Warfare & Security Research*, vol. 1, no. 1, p. 80, 2011. Article (CrossRef Link).

[9] E. D. Matthews, H. J. Arata III, and B. L. Hale, "Cyber situational awareness," *The Cyber Defense Review*, vol. 1, no. 1, pp. 35-46, 2016. [Online]. Available: https://www.jstor.org/stable/26267298. Accessed on: Sep 27, 2023.

[10] S. C. Sundaramurthy, A. G. Bardas, J. Case, X. Ou, M. Wesch, J. McHugh, and S. R. Rajagopalan, "A human capital model for mitigating security analyst burnout," in *Proc. of Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pp. 347-359, 2015. [Online]. Available: https://www.usenix.org/conference/soups2015/proceedings/presentation/sundaramurthy. Accessed on: Sep 27, 2023.

[11] J. Zhang, L. Pan, Q. -L. Han, C. Chen, S. Wen and Y. Xiang, "Deep Learning Based Attack Detection for Cyber-Physical System Cybersecurity: A Survey," *IEEE/CAA Journal of Automatica Sinica*, vol. 9, no. 3, pp. 377-391, March 2022. Article (CrossRef Link)

[12] A. Iqbal and T. Jain, "Real-time event detection based on Weibull distribution using synchrophasor measurements for enhanced situational awareness," *IEEE Transactions on Power Systems*, vol. 37, no. 2, pp. 1425-1436, 2022. Article (CrossRef Link)

[13] O. Jacq, D. Brosset, Y. Kermarrec, and J. Simonin, "Cyber attacks real time detection: towards a cyber situational awareness for naval systems," in *Proc. of 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, pp. 1-2, 2019. Article (CrossRef Link)

[14] C. Sandom, "Operator situational awareness and system safety," in *Proc. of IEE One-day Seminar on Systems Dependency on Humans (Ref. No. 2000/020)*, pp. 5/1-5/8, 2000. Article (CrossRef Link)

[15] P. Barford et al., "Cyber SA: Situational awareness for cyber defense," *Cyber Situational Awareness: Issues and Research*, pp. 3-13, 2010. Article (CrossRef Link)

[16] M. Liggins II, D. Hall, and J. Llinas, *Handbook of multisensor data fusion: theory and practice*, CRC press, 2017. [Online]. Available: https://doi.org/10.1201/9781420053098. Accessed on: Sep 27, 2023.

[17] A. Stotz, "Advancements in computational situation assessment with dynamic graph-based procedures," *State University of New York at Buffalo*, 2009. [Online]. Available: https://www.proquest.com/openview/ad6f91961a3eb74a9fcf559c155e1157/1?cbl=18750&pq-origsite=gscholar#. Accessed on: Sep 27, 2023.

[18] J. Salerno, "Measuring situation assessment performance through the activities of interest score," in *Proc. of 2008 11th International Conference on Information Fusion*, pp. 1-8, 2008. Article (CrossRef Link).
[19] D. A. Lambert, "Grand challenges of information fusion," in *Proc. of the 6th International Conference on Information Fusion*, vol. 1, pp. 213-220, 2003. Article (CrossRef Link)
[20] G. P. Tadda and J. S. Salerno, "Overview of cyber situation awareness," in *Cyber Situational Awareness: Issues and Research*: Springer, 2009, pp. 15-35. Article (CrossRef Link)
[21] H. Tianfield, "Cyber security situational awareness," in *Proc. of 2016 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)*, pp. 782-787, 2016. Article (CrossRef Link)
[22] S. Varga, J. Brynielsson, and U. Franke, "Information requirements for national level cyber situational awareness," in *Proc. of 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, pp. 774-781, 2018. Article (CrossRef Link)
[23] S. Grigaliunas, J. Toldinas, A. Venckauskas, N. Morkevicius, and R. Damaševičius, "Digital evidence object model for situation awareness and decision making in digital forensics investigation," *IEEE Intelligent Systems*, vol. 36, no. 5, pp. 39-48, 2021. Article (CrossRef Link)
[24] G. Ioannou, P. Louvieris, and N. Clewley, "A Markov multi-phase transferable belief model for cyber situational awareness," *Ieee Access*, vol. 7, pp. 39305-39320, 2019. Article (CrossRef Link)
[25] A. P. Moore, R. J. Ellison, and R. C. Linger, "Attack modeling for information security and survivability," 2001. [Online]. Available: https://apps.dtic.mil/sti/citations/ADA388771. Accessed on: Sep 27, 2023.
[26] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1836-1846, 2008. Article (CrossRef Link)
[27] R. Baheti and H. Gill, "Cyber-physical systems," *The impact of control technology*, vol. 12, no. 1, pp. 161-166, 2011. Article (CrossRef Link).
[28] D. M. Botín-Sanabria, A.-S. Mihaita, R. E. Peimbert-García, M. A. Ramírez-Moreno, R. A. Ramírez-Mendoza, and J. d. J. Lozoya-Santos, "Digital twin technology challenges and applications: A comprehensive review," *Remote Sensing*, vol. 14, no. 6, p. 1335, 2022. Article (CrossRef Link)
[29] M. Eckhart, A. Ekelhart, and E. Weippl, "Enhancing cyber situational awareness for cyber-physical systems through digital twins," in *Proc. of 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, pp. 1222-1225, 2019. Article (CrossRef Link)
[30] R. R. Fontes, S. Afzal, S. H. Brito, M. A. Santos, and C. E. Rothenberg, "Mininet-WiFi: Emulating software-defined wireless networks," in *Proc. of 2015 11th International Conference on Network and Service Management (CNSM)*, pp. 384-389, 2015. Article (CrossRef Link)
[31] A. Nesen and B. Bhargava, "Towards situational awareness with multimodal streaming data fusion: serverless computing approach," in *Proc. of the International Workshop on Big Data in Emergent Distributed Environments*, pp. 1-6, 2021. Article (CrossRef Link)
[32] M. Crane and J. Lin, "An exploration of serverless architectures for information retrieval," in *Proc. of the ACM SIGIR International Conference on Theory of Information Retrieval*, pp. 241-244, 2017. Article (CrossRef Link)
[33] L. Feng, P. Kudva, D. Da Silva, and J. Hu, "Exploring serverless computing for neural network training," in *Proc. of 2018 IEEE 11th international conference on cloud computing (CLOUD)*, pp. 334-341, 2018. Article (CrossRef Link)
[34] M. Zhang, Y. Zhu, C. Zhang, and J. Liu, "Video processing with serverless computing: A measurement study," in *Proc. of the 29th ACM workshop on network and operating systems support for digital audio and video*, pp. 61-66, 2019. Article (CrossRef Link)
[35] R. D. Medenou Choumanof et al., "Introducing the CYSAS-S3 Dataset for Operationalizing a Mission-Oriented Cyber Situational Awareness," *Sensors*, vol. 22, no. 14, p. 5104, 2022. Article (CrossRef Link)

[36] B. Laboratory, "LBNL Dataset,". [Online]. Available: http://powerdata.lbl.gov/download.html. Accessed on: Sep 27, 2023.
[37] C. UCSD, "DDoS Attack 2007 Dataset," [Online]. Available: http://www.caida.org/data/passive/ddos-20070804_dataset.xml. Accessed on: Sep 27, 2023.
[38] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proc. of 2015 military communications and information systems conference (MilCIS)*, pp. 1-6, 2015. Article (CrossRef Link)
[39] K. Cup, "KDD Cup Dataset,". [Online]. Available: https://kdd.org/kdd-cup/view/kdd-cup-1999/Data. Accessed on: Sep 27, 2023.
[40] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Proc. of 2009 IEEE symposium on computational intelligence for security and defense applications*, pp. 1-6, 2009. Article (CrossRef Link)
[41] Canadian Institute for Cybersecurity (CIC), "Intrusion Detection Evaluation Dataset (ISCXIDS2012),". [Online]. Available: https://www.unb.ca/cic/datasets/ids-2017.html. Accessed on: Sep 27, 2023.
[42] DARPA, "DARPA Intrusion Detection Evaluation,". [Online]. Available: https://www.ll.mit.edu/r-d/datasets/1998-darpa-intrusion-detection-evaluation-dataset. Accessed on: Sep 27, 2023.
[43] J. McHugh, "Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory," *ACM Transactions on Information and System Security (TISSEC)*, vol. 3, no. 4, pp. 262-294, 2000. Article (CrossRef Link)
[44] Y. Nikoloudakis, I. Kefaloukos, S. Klados, S. Panagiotakis, E. Pallis, C. Skianis, and E. K. Markakis, "Towards a machine learning based situational awareness framework for cybersecurity: an SDN implementation," *Sensors*, vol. 21, no. 14, p. 4939, 2021. Article (CrossRef Link)
[45] J. Brownlee, *Better deep learning: train faster, reduce overfitting, and make better predictions*. Machine Learning Mastery, 2018. [Online]. Available: https://machinelearningmastery.com/better-deep-learning/. Accessed on: Sep 27, 2023.
[46] J. Brownlee, "Master Machine Learning Algorithms Discover How They Work and Implement Them From Scratch i Master Machine Learning Algorithms," Technical report, 2016. [Online]. Available: https://datageneralist.files.wordpress.com/2018/03/master_machine_learning_algo_from_scratch.pdf. Accessed on: Sep 27, 2023.
[47] J. Brownlee, "Supervised and unsupervised machine learning algorithms," *Machine Learning Mastery*, vol. 16, no. 03, 2016. [Online]. Available: https://machinelearningmastery.com/supervised-and-unsupervised-machine-learning-algorithms/. Accessed on: Sep 27, 2023.
[48] J. Brownlee, *Deep learning with Python: develop deep learning models on Theano and TensorFlow using Keras*, Machine Learning Mastery, 2016.
[49] First.org, "CVSS V3.1,". [Online]. Available: https://www.first.org/cvss/. Accessed on: Sep 27, 2023.
[50] J. E. Sullivan and D. Kamensky, "How cyber-attacks in Ukraine show the vulnerability of the US power grid," *The Electricity Journal*, vol. 30, no. 3, pp. 30-35, 2017. Article (CrossRef Link)
[51] H. Tu, Y. Xia, and X. Chen, "Vulnerability analysis of cyber physical systems under the false alarm cyber attacks," *Physica A: Statistical Mechanics and its Applications*, vol. 599, p. 127416, 2022. Article (CrossRef Link)
[52] D. Xia, Q. Li, Y. Lei, X. Shen, M. Qian, and C. Zhang, "Extreme vulnerability of high-order organization in complex networks," *Physics Letters A*, vol. 424, p. 127829, 2022. Article (CrossRef Link)
[53] H. Tu, Y. Xia, J. Wu, and X. Zhou, "Robustness assessment of cyber–physical systems with weak interdependency," *Physica A: Statistical Mechanics and its Applications*, vol. 522, pp. 9-17, 2019. Article (CrossRef Link)

[54] M. Tian, Z. Dong, and X. Wang, "Reinforcement learning approach for robustness analysis of complex networks with incomplete information," *Chaos, Solitons & Fractals*, vol. 144, p. 110643, 2021. Article (CrossRef Link)
[55] S.-G. Liao and S.-P. Yi, "Modeling and analysis knowledge transmission process in complex networks by considering internalization mechanism," *Chaos, Solitons & Fractals*, vol. 143, p. 110593, 2021. Article (CrossRef Link)
[56] J. Saramäki, M. Kivelä, J.-P. Onnela, K. Kaski, and J. Kertesz, "Generalizations of the clustering coefficient to weighted complex networks," *Physical Review E*, vol. 75, no. 2, p. 027105, 2007. Article (CrossRef Link)
[57] Y. Hayashi and J. Matsukubo, "Geographical effects on the path length and the robustness in complex networks," *Physical Review E*, vol. 73, no. 6, p. 066113, 2006. Article (CrossRef Link)
[58] Z. Li and X. Tang, "Robustness of complex networks to cascading failures induced by Poisson fluctuating loads," *Physica A: Statistical Mechanics and its Applications*, vol. 536, p. 120848, 2019. Article (CrossRef Link)
[59] Y. Xiang, L. Wang, and N. Liu, "Coordinated attacks on electric power systems in a cyber-physical environment," *Electric Power Systems Research*, vol. 149, pp. 156-168, 2017. Article (CrossRef Link)
[60] M. Zhou, C. Liu, A. A. Jahromi, D. Kundur, J. Wu, and C. Long, "Revealing vulnerability of n-1 secure power systems to coordinated cyber-physical attacks," *IEEE Transactions on Power Systems*, vol. 38, no. 2, pp. 1044-1057, 2023. Article (CrossRef Link)
[61] R. Deng, P. Zhuang, and H. Liang, "CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2420-2430, 2017. Article (CrossRef Link)
[62] J. Zhang and L. Sankar, "Physical system consequences of unobservable state-and-topology cyber-physical attacks," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 2016-2025, 2016. Article (CrossRef Link)
[63] X. Liu and Z. Li, "Trilevel modeling of cyber attacks on transmission lines," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 720-729, 2017. Article (CrossRef Link)
[64] H. Shakhatreh et al., "Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges," *Ieee Access*, vol. 7, pp. 48572-48634, 2019. Article (CrossRef Link)
[65] B. Nassi, R. Bitton, R. Masuoka, A. Shabtai, and Y. Elovici, "SoK: Security and privacy in the age of commercial drones," in *Proc. of 2021 IEEE Symposium on Security and Privacy (SP)*,. 1434-1451, 2021. Article (CrossRef Link)
[66] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," *Internet of Things*, vol. 11, p. 100218, 2020. Article (CrossRef Link)
[67] K. L. Best et al., "How to analyze the cyber threat from drones," *RAND ARROYO CENTER SANTA MONICA CA SANTA MONICA United States*, vol. 328, 2020. [Online]. Available: https://view.ckcest.cn/AllFiles/ZKBG/Pages/316/RAND_RR2972.pdf. Accessed on: Sep 27, 2023.
[68] J. Soikkeli, C. Perner, and E. C. Lupu, "Analyzing the Viability of UAV Missions Facing Cyber Attacks," in *Proc. of 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 103-112, 2021. Article (CrossRef Link)
[69] B. B. Madan and K. S. Trivedi, "Security modeling and quantification of intrusion tolerant systems using attack-response graph," *Journal of High Speed Networks*, vol. 13, no. 4, pp. 297-308, 2004. Article (CrossRef Link).
[70] B. Li, R. Lu, K.-K. R. Choo, W. Wang, and S. Luo, "On reliability analysis of smart grids under topology attacks: A stochastic petri net approach," *ACM Transactions on Cyber-Physical Systems*, vol. 3, no. 1, pp. 1-25, 2018. Article (CrossRef Link)
[71] O. M. Dahl and S. D. Wolthusen, "Modeling and execution of complex attack scenarios using interval timed colored petri nets," in *Proc. of Fourth IEEE International Workshop on Information Assurance (IWIA'06)*, pp. 12 pp.-168, 2006. Article (CrossRef Link)

[72] D. H. Collins and A. V. Huzurbazar, "Petri net models of adversarial scenarios in safety and security," *Military Operations Research*, vol. 24, no. 3, pp. 27-48, 2019. Article (CrossRef Link).
[73] B. P. Kumar, K. S. Vaishnavi, K. G. P. S. Nitya, P. P. Durga, K. B. Prakash, and G. P. S. Varma, "Analysing Cyber Security Vulnerabilities using Click Jacking and HostHeader Injection," in *Proc. of 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*, pp. 1-5, 2023. Article (CrossRef Link)
[74] V. N. Padmanabhan and L. Subramanian, "An investigation of geographic mapping techniques for Internet hosts," in *Proc. of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications*, pp. 173-185, 2001. Article (CrossRef Link)
[75] M. De Vivo, E. Carrasco, G. Isern, and G. O. De Vivo, "A review of port scanning techniques," *ACM SIGCOMM Computer Communication Review*, vol. 29, no. 2, pp. 41-48, 1999. Article (CrossRef Link)
[76] S. Panjwani, S. Tan, K. M. Jarrin, and M. Cukier, "An experimental evaluation to determine if port scans are precursors to an attack," in *Proc. of 2005 International Conference on Dependable Systems and Networks (DSN'05)*, pp. 602-611, 2005. Article (CrossRef Link)
[77] U. U. Rehman, W. A. Khan, N. A. Saqib, and M. Kaleem, "On detection and prevention of clickjacking attack for osns," in *Proc. of 2013 11th International Conference on Frontiers of Information Technology*, pp. 160-165, 2013. Article (CrossRef Link)
[78] G. Rydstedt, E. Bursztein, D. Boneh, and C. Jackson, "Busting frame busting: a study of clickjacking vulnerabilities at popular sites," *IEEE Oakland Web*, vol. 2, no. 6, p. 24, 2010. Article (CrossRef Link).
[79] I. Simic, "HTTP Host Header Attack: Explanation and Examples," Crashtest Security, Mar 7, 2022. [Online]. Available: https://crashtest-security.com/invalid-host-header/. Accessed on: Sep 27, 2023.
[80] S. Nakrani and C. Tovey, "From honeybees to Internet servers: biomimicry for distributed management of Internet hosting centers," *Bioinspiration & biomimetics*, vol. 2, no.4, pp. S182, 2007. Article (CrossRef Link)
[81] B. Strickson, C. Worsley, and S. Bertram, "Human-centered Assessment of Automated Tools for Improved Cyber Situational Awareness," in *Proc. of 2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)*, pp. 273-286, 2023. Article (CrossRef Link)
[82] M. A. Haque, S. Shetty, C. A. Kamhoua, and K. Gold, "Attack Graph Embedded Machine Learning Platform For Cyber Situational Awareness," in *Proc. of MILCOM 2022-2022 IEEE Military Communications Conference (MILCOM)*, pp. 464-469, 2022. Article (CrossRef Link)
[83] H. Anderson, "Introduction to nessus," *SecurityFocus*, 2003. [Online]. Available: http://cryptomex.org/SlidesSeguRedes/TutNessus.pdf. Accessed on: Sep 27, 2023.
[84] X. Ou, S. Govindavajhala, and A. W. Appel, "MulVAL: A logic-based network security analyzer," in *Proc. of USENIX security symposium*, vol. 8, Baltimore, MD, pp. 113-128, 2005. [Online]. Available: https://www.usenix.org/event/sec05/tech/full_papers/ou/ou_html. Accessed on: Sep 27, 2023.
[85] S. R. Gonzalez et al., "Modeling attacker behavior in cyber-physical-systems," in *Proc. of the 11th Latin-American Symposium on Dependable Computing*, pp. 117-124, 2022. Article (CrossRef Link)
[86] E. LeMay, M. D. Ford, K. Keefe, W. H. Sanders, and C. Muehrcke, "Model-based security metrics using adversary view security evaluation (advise)," in *Proc. of 2011 Eighth International Conference on Quantitative Evaluation of SysTems*, pp. 191-200, 2011. Article (CrossRef Link)
[87] Y. Xu, P. Yu, W. Shen, and Z. Li, "Security attack situation awareness based on massive log data mining," in *Proc. of 2022 5th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE)*, pp. 567-570, 2022. Article (CrossRef Link)
[88] N. El Kamel, M. Eddabbah, Y. Lmoumen, and R. Touahni, "A smart agent design for cyber security based on honeypot and machine learning," *Security and Communication Networks*, vol. 2020, pp. 1-9, 2020. Article (CrossRef Link)

[89] M. Amal and P. Venkadesh, "Hybrid H-DOC: A bait for analyzing cyber attacker behavior," *International journal of electrical and computer engineering systems*, vol. 14, no. 1, pp. 37-44, 2023. Article (CrossRef Link)
[90] S. Grigaliunas, J. Toldinas, A. Venckauskas, N. Morkevicius, and R. Damaševičius, "Digital evidence object model for situation awareness and decision making in digital forensics investigation," *IEEE Intelligent Systems*, vol. 36, no. 5, pp. 39-48, 2021. Article (CrossRef Link)
[91] Q. Guo, S. Xin, H. Sun, and J. Wang, "Power system cyber-physical modelling and security assessment: motivation and ideas," *Proceedings of the CSEE*, vol. 36, no. 6, pp. 1481-1489, 2016. Article (CrossRef Link)
[92] D. Liu, W. Sheng, Y. Wang, Y. Lu, and C. Sun, "Key technologies and trends of cyber physical system for power grid," *Proceedings of the CSEE*, vol. 35, no. 14, pp. 3522-3531, 2015. Article (CrossRef Link)
[93] K.-D. Kim and P. R. Kumar, "Cyber–physical systems: A perspective at the centennial," *Proceedings of the IEEE*, vol. 100, no. Special Centennial Issue, pp. 1287-1308, 2012. Article (CrossRef Link)
[94] M. Ni, M. Li, Y. Wu, and Q. Wang, "Concept and research framework for coordinated situation awareness and active defense of cyber-physical power systems against cyber-attacks," *Journal of Modern Power Systems and Clean Energy*, vol. 9, no. 3, pp. 477-484, 2021. Article (CrossRef Link)
[95] H. Alsulami, "Implementation analysis of reliable unmanned aerial vehicles models for security against cyber-crimes: Attacks, tracebacks, forensics and solutions," *Computers and Electrical Engineering*, vol. 100, p. 107870, 2022. Article (CrossRef Link)
[96] H. Akrout and G. Nagy, "Trust and commitment within a virtual brand community: The mediating role of brand relationship quality," *Information & Management*, vol. 55, no. 8, pp. 939-955, 2018. Article (CrossRef Link)
[97] Y. Zeng and R. Zhang, "Energy-efficient UAV communication with trajectory optimization," *IEEE Transactions on wireless communications*, vol. 16, no. 6, pp. 3747-3760, 2017. Article (CrossRef Link)
[98] S. R. Selamat, R. Yusof, and S. Sahib, "Mapping process of digital forensic investigation framework," *International Journal of Computer Science and Network Security*, vol. 8, no. 10, pp. 163-169, 2008. Article (CrossRef Link).
[99] S. E. Prastya, I. Riadi, and A. Luthfi, "Forensic analysis of unmanned aerial vehicle to obtain GPS log data as digital evidence," *IJCSIS*, vol. 15, no. 3, 2017. Article (CrossRef Link). \
[100] J. Youn, K. Kim, D. Kang, J. Lee, M. Park, and D. Shin, "Research on Cyber ISR Visualization Method Based on BGP Archive Data through Hacking Case Analysis of North Korean Cyber-Attack Groups," *Electronics*, vol. 11, no. 24, p. 4142, 2022. Article (CrossRef Link)
[101] J. C. Advisory, "North Korean Advanced Persistent Threat Focus: Kimsuky," *Cybersecurity and Infrastructure Security Agency (CISA): Arlington*, VA, USA, 2020. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-301a. Accessed on: Sep 27, 2023.
[102] K. Renaud and J. Ophoff, "A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs," *Organizational Cybersecurity Journal: Practice, Process and People*, vol. 1, no. 1, pp. 24-46, 2021. Article (CrossRef Link)
[103] M. Ward, "Business statistics. briefing paper number 06152," *House of Commons Library*, 22nd January, 2021. [Online]. Available: https://commonslibrary.parliament.uk/research-briefings/sn06152/. Accessed on: Sep 27, 2023.
[104] N. C. S. Centre, "Password administration for system owners,". [Online]. Available: https://www.ncsc.gov.uk/collection/passwords. Accessed on: Sep 27, 2023.
[105] A. A. Malik and D. K. Tosh, "Robust cyber-threat and vulnerability information analyzer for dynamic risk assessment," in *Proc. of 2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*, pp. 168-173, 2021. Article (CrossRef Link)
[106] N. I. o. S. a. Technology, "National Vulnerability Database,". [Online]. Available: https://nvd.nist.gov/general/news. Accessed on: Sep 27, 2023.

[107] A. A. Malik and D. K. Tosh, "Dynamic Vulnerability Classification for Enhanced Cyber Situational Awareness," in *Proc. of 2023 IEEE International Systems Conference (SysCon)*, pp. 1-8, 2023. Article (CrossRef Link)
[108] scikit-yb, "Elbow Method,". [Online]. Available: https://www.scikit-yb.org/en/latest/api/cluster/elbow.html. Accessed on: Sep 27, 2023.
[109] N. Reimers and I. Gurevych, "Sentence-bert: Sentence embeddings using siamese bert-networks," *arXiv preprint arXiv:1908.10084*, 2019. Article (CrossRef Link)
[110] A. Akbik, T. Bergmann, D. Blythe, K. Rasul, S. Schweter, and R. Vollgraf, "FLAIR: An easy-to-use framework for state-of-the-art NLP," in *Proc. of the 2019 conference of the North American chapter of the association for computational linguistics (demonstrations)*, pp. 54-59, 2019. Article (CrossRef Link)
[111] L. O. Chua and T. Roska, "The CNN paradigm," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 40, no. 3, pp. 147-156, 1993. Article (CrossRef Link)
[112] D. Bahdanau, K. Cho, and Y. Bengio, "Neural machine translation by jointly learning to align and translate," *arXiv preprint arXiv:1409.0473*, 2014. Article (CrossRef Link)
[113] C. Hu, G. Liu, and M. Li, "A Network Security Situation Prediction Method Based on Attention-CNN-BiGRU," in *Proc. of 2022 IEEE 25th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, pp. 257-262, 2022. Article (CrossRef Link)
[114] J. Xu and H. Chen, "Criminal network analysis and visualization," *Communications of the ACM*, vol. 48, no. 6, pp. 100-107, 2005. Article (CrossRef Link)
[115] A. Potgieter, K. April, R. J. Cooke, and I. O. Osunmakinde, "Temporality in link prediction: Understanding social complexity," 2008. [Online]. Available: https://aisel.aisnet.org/sprouts_all/195/. Accessed on: Sep 27, 2023.
[116] M. Lim, A. Abdullah, N. Jhanjhi, and M. K. Khan, "Situation-aware deep reinforcement learning link prediction model for evolving criminal networks," *IEEE Access*, vol. 8, pp. 16550-16559, 2019. Article (CrossRef Link)
[117] H. Li, N. Kumar, R. Chen, and P. Georgiou, "A deep reinforcement learning framework for Identifying funny scenes in movies," in *Proc. of 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 3116-3120, 2018. Article (CrossRef Link)
[118] D. Bahdanau, J. Chorowski, D. Serdyuk, P. Brakel, and Y. Bengio, "End-to-end attention-based large vocabulary speech recognition," in *Proc. of 2016 IEEE international conference on acoustics, speech and signal processing (ICASSP)*, pp. 4945-4949, 2016. Article (CrossRef Link)
[119] J. Lao, Y. Chen, Z.-C. Li, Q. Li, J. Zhang, J. Liu, and G. Zhai, "A deep learning-based radiomics model for prediction of survival in glioblastoma multiforme," *Scientific reports*, vol. 7, no. 1, p. 10353, 2017. Article (CrossRef Link)
[120] G. Biau and E. Scornet, "A random forest guided tour," *Test*, vol. 25, pp. 197-227, 2016. Article (CrossRef Link)
[121] C. Schuldt, I. Laptev, and B. Caputo, "Recognizing human actions: a local SVM approach," in *Proc. of the 17th International Conference on Pattern Recognition, 2004. ICPR 2004.*, vol. 3, pp. 32-36, 2004. Article (CrossRef Link)
[122] M. Husák, T. Bajtoš, J. Kašpar, E. Bou-Harb, and P. Čeleda, "Predictive cyber situational awareness and personalized blacklisting: a sequential rule mining approach," *ACM Transactions on Management Information Systems (TMIS)*, vol. 11, no. 4, pp. 1-16, 2020. Article (CrossRef Link)
[123] M. Husák, T. Jirsík, and S. J. Yang, "SoK: Contemporary issues and challenges to enable cyber situational awareness for network security," in *Proc. of the 15th International Conference on Availability, Reliability and Security*, pp. 1-10, 2020. Article (CrossRef Link)
[124] T. Jirsik and P. Celeda, "Toward real-time network-wide cyber situational awareness," in *Proc. of NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium*, pp. 1-7, 2018. Article (CrossRef Link)

[125] K. Kim, J. Youn, S. Yoon, J. Kang, K. Kim, and D. Shin, "Study on Cyber Common Operational Picture Framework for Cyber Situational Awareness," *Applied Sciences*, vol. 13, no. 4, p. 2331, 2023. Article (CrossRef Link)

[126] G. Doukas et al., "An Intuitive Distributed Cyber Situational Awareness Framework Within a Healthcare Environment," *CYBER-PHYSICAL THREAT INTELLIGENCE FOR CRITICAL INFRASTRUCTURES SECURITY*, p. 433, 2021. [Online]. Available: https://www.nowpublishers.com/article/Chapter/9781680838220?cId=978-1-68083-823-7.ch20. Accessed on: Sep 27, 2023.

[127] P. Rajivan and N. Cooke, "Impact of team collaboration on cybersecurity situational awareness," *Theory and Models for Cyber Situation Awareness*, pp. 203-226, 2017. Article (CrossRef Link)

[128] R. Vinayakumar, K. Soman, P. Poornachandran, V. S. Mohan, and A. D. Kumar, "ScaleNet: scalable and hybrid framework for cyber threat situational awareness based on DNS, URL, and email data analysis," *Journal of Cyber Security and Mobility*, vol. 8, no. 2, pp. 189–240, 2019. Article (CrossRef Link).

[129] M. Husák, L. Sadlek, S. Špaček, M. Laštovička, M. Javorník, and J. Komárková, "CRUSOE: A toolset for cyber situational awareness and decision support in incident handling," *Computers & Security*, vol. 115, pp. 102609, 2022. Article (CrossRef Link)

[130] J. Komárková, M. Husák, M. Laštovička, and D. Tovarňák, "Crusoe: Data model for cyber situational awareness," in *Proc. of the 13th International Conference on Availability, Reliability and Security*, pp. 1-10, 2018. Article (CrossRef Link)

[131] T. Schaberreiter et al., "A cybersecurity situational awareness and information-sharing solution for local public administrations based on advanced big data analysis: the CS-AWARE project," in *Challenges in Cybersecurity and Privacy–the European Research Landscape*, 2019, pp. 149-180. Article (CrossRef Link).

[132] C. Sánchez-Zas, V. A. Villagrá, M. Vega-Barbas, X. Larriva-Novo, J. I. Moreno, and J. Berrocal, "Ontology-based approach to real-time risk management and cyber-situational awareness," *Future Generation Computer Systems*, vol. 141, pp. 462-472, 2023. Article (CrossRef Link)

Kookjin Kim received a B.S. degree in computer science from Seoul Hoseo Occupational Training College, Seoul, Republic of Korea in 2017. He received a Ph.D. degree in Computer Engineering at Sejong University, Seoul, Republic of Korea in 2023. From 2017 to 2019 he developed mobile applications and back-end software at M2Soft, Republic of Korea. He is currently working in the Intelligent Networks Lab at Electronics and Telecommunications Research Institute (ETRI). His research interests include machine learning, neural networks, cyberspace, cyber warfare, cyber targeting.

Jaepil Youn received a B.S. degree in computational information processing from the Korea Army Academy at Yeongcheon (KAAY), Republic of Korea, in 2008, and an M.S. degree in cybersecurity from Ajou University at Suwon, Republic of Korea, in 2017. He received a Ph.D. degree in Computer Engineering at Sejong University, Seoul Republic of Korea in 2023. From 2018 to 2020, he was a researcher with the Agency for Defense Development (ADD), Republic of Korea. From 2021 to 2023, he was an officer for cyber operations planning and cyber operations training at the Army Cyber Operations Center (ACOC). He currently conducts research at the Joint Forces Military University (JFMU), where he studies advancements in defense policy, military strategy, defense planning, and joint coalition operations. His research interests include cyber intelligence surveillance and reconnaissance (ISR) and cybersecurity.

Hansung Kim received a B.Sc. degree in computer science from Korea Military Academy (KMA), Seoul, Republic of Korea in 1990, an M.Sc. degree in computer science from the University of Western Ontario, London, ON, Canada in 1995 and a Ph.D. in computer science from Korea Advanced Institute of Science and Technology (KAIST), Republic of Korea in 2005. He is currently working as a visiting researcher in the Artificial Intelligence Computing Research Lab at Electronics and Telecommunications Research Institute (ETRI). His research interests include information security, cyber warfare, cyber operation and software engineering.

Dongil Shin received a B.S. degree in computer science from Yonsei University, Seoul, South Korea in 1988, an M.S. degree in computer science from Washington State University, Pullman, WA, USA in 1993, and a Ph.D. from the University of North Texas, Denton, TX, USA in 1997. He was a Senior Researcher with the System Engineering Research Institute, Deajun, South Korea in 1997. Since 1998, he has been with the Department of Computer Engineering, Sejong University, South Korea, where he is currently a Professor. His research interests include information security, bio-signal data processing, data mining and machine learning.

Dongkyoo Shin received a B.S. degree in computer science from Seoul National University, Republic of Korea in 1986, an M.S. degree in computer science from the Illinois Institute of Technology, Chicago, IL, USA in 1992, and a Ph.D. in computer science from Texas A&M University, College Station, TX, USA in 1997. He is currently a Professor with the Department of Computer Engineering, Sejong University, Republic of Korea. From 1986 to 1991, he was with the Korea Institute of Defense Analyses, where he developed database application software. From 1997 to 1998, he was a Principal Researcher with the Multimedia Research Institute, Hyundai Electronics Co., Republic of Korea. His research interests include machine learning, ubiquitous computing, bio-signal data processing and information security