# SoK: Contemporary Issues and Challenges to Enable Cyber Situational Awareness for Network Security

Martin Husák
Institute of Computer Science
Masaryk University
Brno, Czech Republic
husakm@ics.muni.cz

Tomáš Jirsík
Institute of Computer Science
Masaryk University
Brno, Czech Republic
jirsik@ics.muni.cz

Shanchieh Jay Yang
Department of Computer Engineering
Rochester Institute of Technology
Rochester, NY, USA
jay.yang@rit.edu

## ABSTRACT

Cyber situational awareness is an essential part of cyber defense that allows the cybersecurity operators to cope with the complexity of today's networks and threat landscape. Perceiving and comprehending the situation allow the operator to project upcoming events and make strategic decisions. In this paper, we recapitulate the fundamentals of cyber situational awareness and highlight its unique characteristics in comparison to generic situational awareness known from other fields. Subsequently, we provide an overview of existing research and trends in publishing on the topic, introduce front research groups, and highlight the impact of cyber situational awareness research. Further, we propose an updated taxonomy and enumeration of the components used for achieving cyber situational awareness. The updated taxonomy conforms to the widely-accepted three-level definition of cyber situational awareness and newly includes the projection level. Finally, we identify and discuss contemporary research and operational challenges, such as the need to cope with rising volume, velocity, and variety of cybersecurity data and the need to provide cybersecurity operators with the right data at the right time and increase their value through visualization.

## CCS CONCEPTS

• **Security and privacy → Formal security models**; • **Networks → Network security**.

## KEYWORDS

Cyber situational awareness, network security, taxonomy

**ACM Reference Format:**
Martin Husák, Tomáš Jirsík, and Shanchieh Jay Yang. 2020. SoK: Contemporary Issues and Challenges to Enable Cyber Situational Awareness for Network Security. In *The 15th International Conference on Availability, Reliability and Security (ARES 2020), August 25–28, 2020, Virtual Event, Ireland*. ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3407023.3407062


*ARES 2020, August 25–28, 2020, Virtual Event, Ireland*

ACM ISBN 978-1-4503-8833-7/20/08…$15.00
https://doi.org/10.1145/3407023.3407062

## 1 INTRODUCTION

Cyber situational awareness (CSA) is an application of generic situational awareness (SA) into the cyber domain and a frequently discussed topic in cybersecurity research and operations. Perceiving the cyber environment, understanding the current security situation, and being able to project how the situation will evolve is an essential part of cyber defense and a goal of many researchers and practitioners. As computer networks and systems continue to increase in complexity and sophistication, the requirements and demands on a cybersecurity operator increase as well. A concept of CSA aims to provide an operator with a coherent methodology to cope with the networks' and systems' complexity, gather all necessary information, and to comprehend underlying processes in these systems, and anticipate upcoming events. By building and maintaining CSA, an operator is capable of making strategic decisions even in the case of complex and sophisticated systems. The approaches taken to achieve and maintain CSA should be continuously updated and refined to reflect evolving threat landscape and emerging domains and paradigms of computing and networking. Although we focus on network security, there is still a lot of novel phenomena influencing this field. For example, the adoption of cloud computing disrupted the defense of network perimeters, and the boom of IoT increased the number of devices, often vulnerable and unprotected, in the Internet and local networks. There is also a need to take into consideration the world of operational technology as opposed to information technology and take care of the security of ICS and SCADA systems, especially in critical infrastructures.

In this paper, we investigate the current status and challenges of research on CSA. We start from fundamental definitions of SA and CSA to provide a solid base for our work. Subsequently, we proceed with a literature review and revisiting a taxonomy to catch the directions taken by the research on CSA. Finally, we identify the weak spots to set the challenges for future research and development. The contribution of our work can be summarized in four points. First, we put together existing definitions of SA and discuss how they apply to CSA and cope with the cyber environment. Second, we provide brief literature that is focused on trends in publishing on the topic instead of analyzing the content of the publications. The goal is to find if we are still discussing an emerging topic or if the publication counts have culminated. The literature review also enlists major research groups and influential people that contribute or made a significant contribution to the field. Third, we revise an existing taxonomy of CSA and its related tools, techniques, and activities. We also look at the taxonomy from the perspective of the SA and CSA definitions and find common ground. Finally, we

identify and summarize the contemporary challenges of CSA research and development, namely from the perspective of data and tools. The identified challenges pave the way for future work and research directions.

The remainder of this paper is structured as follows. Section 2 presents the basic concepts of situational awareness and its application in the cyber domain. Section 3 presents a brief review of related literature. Section 4 presents an updated taxonomy of CSA. Section 5 identifies research and operational challenges for CSA. Section 6 concludes the paper.

## 2 FROM SITUATIONAL AWARENESS TO CYBER SITUATIONAL AWARENESS

Cyber situational awareness (CSA) is an application of a more general approach, situational awareness (SA). In order to be able to comprehend the cyber situational awareness to all its extends, we need to present the basics background of the underlying situational awareness first. The description of the evolution of SA and explanation of the basic SA definitions will allow for the correct understanding of the concept of the CSA. Hence, this section presents the origins and basic definitions of situational awareness, followed by the description of the cyber situational awareness and its domain-originated specifics.

### 2.1 Situational Awareness

Situational awareness has always been needed in everyday life. A prehistoric hunter undoubtedly needed to observe and understand various inputs from his environment to efficiently hunt down prey bigger and stronger than him, and not to become prey himself at the same time. For many years, SA principles were used in everyday life intuitively. However, the intuitive SA began insufficient as the technology improved, and the complexity of the world increased. People had to start using SA consciously.

The origins of a concept that can be referred to as situational awareness date back to World War I where Oswald Boelke realized the importance of *gaining an awareness of the enemy before the enemy gained a similar awareness and devise methods for accomplishing this* [36]. After the World Wars, the concept of SA did not receive too much attention in literature until the late 1980s [88]. The push came from the aviation domain, where the automation systems were no longer optimized for human operation and even overstepped the human's capability to keep track of the current situation in some cases [83]. The idea of separation between the human operator's understanding of system status and actual system status emerged and became a crux of the definition of SA [97].

The conceptual basis SA had been cloudy before 1990. The main theoretic foundations were laid during the last decade of the 20th century. During the decade, underlying theoretical works were published by Smith and Hancock (1995) [87], Endsley (1995) [29], and Bedny and Meister (1999) [9]. Although SA was already conceptually defined, it was still met with a fair amount of criticism claiming that SA is a *too subjective phenomenon to be measured objectively* [83]. Hence, approaches to objective SA measurement were introduced in a short time (e.g., in [27]), and researchers kept their interest in the topic.

Since then, the application of the concept of SA has quickly spread to other domains than aviation. The most prominent driver of this widespread has been the technology. The complexity of systems and their dynamics and automation has increased rapidly due to introduced technologies, such as IoT and ICS/SCADA systems. The automation of these areas has moved an operator from an active role of searching information in a decision process to a decision maker that consumes information from systems and formulates his decision using the information. SA is being introduced to various areas (power grids, strategic and tactical systems, medicine, and also cyberspace) to ensure that an operator assesses a situation correctly based on received data and can make an informed decision.

*2.1.1 Definitions of SA.* Three main definitions dominate the field of situational awareness [88]. We mention all three definitions with particular attention to Endsley's definition as her definition is widely adopted in the literature and serves as a base ground for further research in CSA. Detailed analysis of all three definitions in the context of CSA can be found in [53].

Smith and Hancock proposed the perceptual cycle definition in [88] that is suitable for explaining the dynamic aspect of SA, such as how the momentary knowledge is updated and how the search for information is initiated. The definition provides a high-level overview of a person interacting with an environment. Bedny and Meister [9] proposed the interactive sub-system definition that is suitable when considering underlying functions and how they interact [88]. This view focuses on the processes that are used by an individual during situation assessment.

Endsley proposed the three-level model definition: *Situational Awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future.* [26] Definition of SA by Endsley has been widely accepted and is used in a great variety of functional areas, for example, in medicine or vehicle operations [30]. Endsley apprehends SA as a state of knowledge and distinguishes it from the processes used to achieve the state. The definition consists of three ascending primary components referred to as *levels* (see Figure 1).

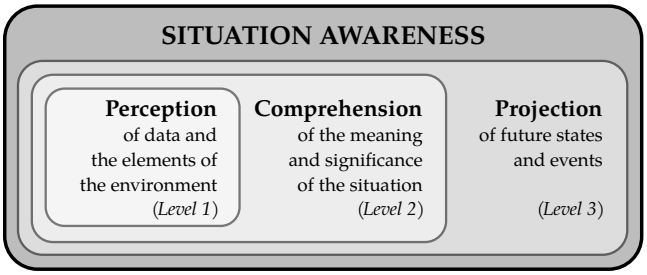


**Figure 1: Three-level model *(adapted from [29]).***

At the first level, the level of perception of the elements in the environment, status attributes and dynamics of relevant attributes of an environment are perceived [26]. The correct perception is crucial for the outcome of SA. If the data obtained at this level are biased, inaccurate, or misleading, the operator gains the notion of

the situation that does not comply with the real world state. Without the correct basic perception of relevant information, the odds of forming an incorrect picture of the situation increases dramatically [28]. No interpretation of the acquired data is performed at this stage. All interpretation is left to the next level. This level is intended to represent to initial reception of information in the raw form. The separation of data capture and data comprehension and interpretation allows identifying discrepancies that might occur when requiring data from senses and sensors. One such a problem solved in SA is the data overload. [60] An operator is overwhelmed with sensors and data, and relevant information is not perceived. Jones et al. [55] found that 76 % of SA errors in pilots could be caused by problems in the perception of relevant information (either failure of the sensors or problems with the cognitive process).

On the second level, the comprehension of the current situation, the SA goes beyond the simple perception of the data. The goal is not only to perceive the situation but to understand the situation correctly. The comprehension of a situation is based on a synthesis of disjoint elements perceived at Level 1 [26]. The elements are combined, interpreted, assigned with significance concerning given goals, and combined with knowledge of an operator to form a holistic picture of an environment. The difference between the levels is analogous to having a reading comprehension (Level 2) and reading individual words (Level 1). For example, an operator of an oil platform needs to put together pieces of information to derive the actual status of the platform's systems. An operator's expertise is a vital requirement at this level. At the perception level, a novice and an experienced operator would reach the same results in situation assessment. At the comprehension level, a lack of expertise would cause the novice's inability to follow basic lines of search coherently for further information or to misinterpretation of the current situation [83].

The projection of future status is the third and highest level of SA. This level is the basis for *being ahead of the plane* [83]. In the majority of fields, where SA is of importance, experienced operators rely heavily on future projection. The future projection based on current events and dynamics enables them to anticipate future events and their implications, which allows them to make decision in time [28]. For example, an experienced driver differs from a common driver. Unlike a common driver, the experienced driver can foresee possible traffic and, thus, prevent collisions more efficiently.

## 2.2 Cyber Situational Awareness

CSA builds upon the Endsley's three-level definition: *Cyber Situational Awareness is the perception of the elements in the **cyber** environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future.* The term environment in the definition refers to the cyber environment or cyberspace. This section discusses the specifics of the application of the general SA concept into the cyber environment.

*2.2.1 Specifics of CSA.* Although a general definition of SA can also be applied to the CSA, there are several specifics of the cyber environment that need to be considered. These specifics have a significant effect on SA and, to some extent, shape the approach to SA and the research efforts for CSA. One of the original applications of SA is in the area of conventional military conflict. Therefore, we demonstrate the specifics of the CSA with a comparison to the SA for military purposes. Although we highlight differences between cyber and military SA, these two types are not contradictory. On the contrary, CSA complements SA for a military operation as both virtual and conventional battlefields are encompassed in the current Information Age conflicts [60]. The specifics of CSA are presented in the following paragraphs.

**Cyber Environment** – There are almost limitless possibilities in the cyber environment. The cyber environment has no borders. This dynamic world is highly malleable and potentially scale-free. The dynamics and limitlessness of such an environment is a challenge for situation assessment compared to the physical world of conventional military conflicts, where the environment is immutable and govern by the law of physics. The conflicts are potentially scale-free [68], an attack can come out of the blue with no warning, and the costs of joining a conflict are low. The spatial properties of the cyber environment are global [20], which makes the determination of the SA boundaries problematic if we do not want to use specification "everything/everywhere." Therefore, the physical location of the network or system is usually used as a spatial boundary for CSA [11].

**Perception** – Information for military SA can be captured both via specifics hardware sensors and by physical observation. The hardware sensors and signal processing techniques play an important but not an essential role; a physical observation can be used in cases hardware sensors are not available. In the CSA, the information is gained solely by sensors. It is not possible to observe the information directly. Each sensor is a complex system that can be misused or deceived to provide false information. The inability to confirm information from a sensor by direct observation limits chances to see through the deception. Similarly to information, anniversaries cannot be directly observed. They can be detected only by an analysis of information captured by sensors, which allows the anniversaries to stay hidden in a network.

**Performance** – The required resources for launching an attack in a cyber environment are relatively small. Compared to a state or organization required in a conventional conflict, the resources needed for starting a cyber conflict may scale down to an individual with a few prerequisites. Another factor to consider concerning the performance is the speed of the events. The speed of the events is orders of magnitude quicker than in case of physical conflicts. The resources needed for the processing of such large volumes of information are significantly higher in the case of CSA.

**Attacker Takes the Advantage** – According to traditional military doctrine, a defender gains numerous advantages, e.g., defensive fortification, information asymmetry) [60]. A cyber-attacker overtakes all advantages in the case of cyber conflicts. The advantages of a cyber-attacker include, but are not limited to, anonymity (it can hide across national sovereignty boundaries), global reach to probe weaknesses, social engineering to exploit human weaknesses, and a possibility to pick a time, place and tools for an attack.

*2.2.2 Entities in CSA.* Entities relevant to CSA are part of a *cyber environment*, as stated in CSA definition. We identified the following major types of entities in the context of CSA based on the above-described definitions: *physical*, *immaterial*, and *human*

entities. Individual entities interact with each other and together influence the creation of CSA. It is important to note that an element that forms the CSA does not necessarily have access to all information on entities.

A group of **physical entities** comprises the physical base of the cyber environment. This group includes computers and their peripherals, network infrastructure formed by wires, switches, routers, and other networking devices. Each device can be described by its properties. The properties can be physical, e.g., number and frequency of computer processing units, random access memory size or volume of the disk space, or describing, e.g., the throughput or packet loss for a wireline. The properties can also cover general characteristics, e.g., the criticality of a computer or line. Besides the characteristics, each element plays a specific role. A computer can be, e.g., a workstation or server. A router can play a role of either a central, vital element of infrastructure or be a low-importance device in the last mile of some insignificant local network.

Next, we introduce a group of **immaterial entities** to capture the virtual essence of the cyber environment. The immaterial entities serve as a "new edge" for communication between humans and computers or between computers themselves. The immaterial entities cover computer programs, services provided in a network, and so forth. Each of the entities can be assigned a set of properties. For example, a service can be characterized by an availability, set of functionalities it offers, confidentiality, and so forth. The immaterial entities had originally a strong relationship with a physical entity (a service was hosted on a given physical server). With advances in cloud computing and virtualization, the relation with a physical entity loosens, though.

The last group, **human entities**, represents people interacting with the computers. Among the properties of the human entities relevant for CSA belong to experience, attention, determination, perceptual skills, short/long term memory capabilities, and analytic skill [29]. A human entity is also characterized by an assigned role that partially determines the goals of the human and, consequently, the situation assessment process. Each role would require slightly different information, comprehension, and projection to reach CSA. Roles that we consider in this paper relevant for CSA divide into two main groups – attacker and defender roles. The attacker role represent an adversary that intends to do deliberate harm to the object of interest. A defender protects an entrusted asset against the attacker. The defender roles can be, e.g., security analysts (analyze and assess existing vulnerabilities in IT infrastructure), or security architects and engineers (design and utilize technologies to enhance security) [4]. Although all mentioned roles constitute the cyber environment, only human entities usually reach CSA. All three entities form cyberspace, and therefore they are part of the CSA, i.e., are part of the knowledge of the situation. They form the situation and influence its state. However, the actual knowledge of a situation (CSA) is associated with human entities only.

# 3 REVIEW OF RESEARCH ON CSA

Herein, we provide an overview of existing research on CSA. First, we provide an overview of scientific publishing on CSA, namely the numbers of publications on the topic in recent years and identification of the most impactful publications. Second, we introduce leading researchers and research groups and highlight their contributions. Subsequently, we provide a brief overview of available datasets and illustrate how CSA is adopted in national policies.

## 3.1 Publications on CSA

The need and relevance of research on CSA are demonstrated by the increasing numbers of research published on this topic. We queried five scientific databases (ACM Digital Library, IEEE Xplore, Scopus, Springer, and Web of Science) for keywords *cyber situation(al) awareness* for the last ten years, i.e., from 2009 to 2019. The numbers of publications on CSA published thorough the years are presented in Figure 2. We may see that the number of publications on CSA published each year is rising, especially in IEEE Xplore, where we found mostly research papers. Springer database indexes mostly books and their chapters and, thus, thematic publications, such as *Theory and Models for Cyber Situation Awareness* [66] with many chapters on CSA, count multiple times.

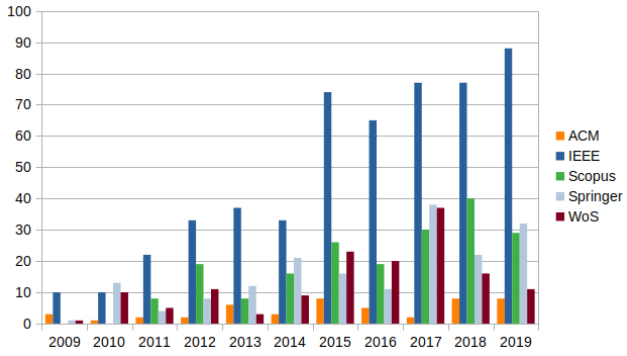


**Figure 2: Number of published papers on CSA.**

According to the survey by Franke and Brynielsson [33] conducted in 2014, the majority of publications covered the design of CSA and attack detection and analysis while application area, thread description, and workflows were covered rather sporadically. In recent years, we see a rising number of applied research and experimental development. Probably the best-known tools were proposed by MITRE [92], such as CyGraph [73]. Applied research and experimental deployment are becoming subject of research by other research groups as well [48, 54, 56, 78, 80].

Most important publications on CSA are these two following collections: *Cyber Situational Awareness: Issues and Research* edited by Jajodia et al. (2010) [49] and *Cyber Defense and Situational Awareness* by Kott et al. (2014) [60]. These collections provide a comprehensive introduction to the topic, an explanation of basic concepts, and a discussion on prevailing open issues. A summary of recent research advances in CSA is summarized in collection *Theory and Models for Cyber Situation Awareness* by Liu et al. from 2017 [66]. An exhausting overview of the literature is provided by Franke and Brynielsson [33]. The authors provide a literature overview for specifics areas of CSA, such as industrial control systems, emergency management, and military. They also list design papers on tools and visualizations for CSA. We were not able to find a similar survey covering the area of CSA published since then. A very brief

survey covering the anomaly detection area of CSA was published in 2015 by Friedberg et al. [34]. The latest review of current CSA models and definitions was published in 2018 by Cooke et al. [19].

## 3.2 Research Groups

Apart from fundamental publications, we also review leading research groups in the CSA field. A strong research group has been established at the Center for Secure Information Systems at George Mason University[1]. The director of this group, prof. Sushil Jajodia, Ph.D., gathered a strong team of scientists and started to research the CSA in the project Computer-aided Human Centric Cyber Situation Awareness. The team's members worth mentioning are Massimiliano Albanese, Ph.D. who is interested in modeling network attack and network hardening, and Steven Noel, Ph.D. whose main research area is attack modeling, graph analytics, and visualizations for information security. The group significantly contributes to the formation of CSA [4, 7], to models underlying CSA [5, 40, 50], and to CSA measurement [35]. Further, the group investigated the concept of attack graphs and their application in CSA [74–76], network hardening [94] along with relevant strategies [6], and cyber deception [3, 51, 52]. The group has also developed a framework for cyber situational awareness that integrates an array of techniques and automated tools [48, 71]. The framework is able among others to represent dependencies in a network or model attack scenarios using attack graphs.

Another research group is led by Alexander Kott at the U.S. Army Research Laboratory (ARL) [2]. They also contributed to the fundamentals of CSA by the formalization of cybersecurity problems [57, 58] and editing a collection that provide an introduction to the basics principles of CSA [60]. The ARL is interested in industrial control system protection; risk modeling and intrusion detection are investigated in [16], metrics of SCADA security in [17], and simulation of the cyber defense in [15]. Other topics under the research focus of the ARL related to CSA are the resilience of the cyber systems and networks [59, 65], modeling of cyber intrusions [14, 15, 64], and attack prediction [81].

Prof. Shanchieh Jay Yang led a research group focusing on several aspects of CSA at Rochester Institute of Technology[3]. The group has contributed to the major publications on CSA with situation assessment research [24, 43, 44]. This group specializes in the area of attack modeling and prediction. They investigate different approaches to attack prediction [98], including Bayesian networks [79], time series forecasting [96], and likelihood estimation using rare-event simulation [61]. They are especially interested in multi-stage cyber attacks. Their research in this area includes the characterization of multi-stage cyber attacks [23, 25] and the creation of a system for multi-stage attack emulation that fuses concepts from computer networks, system vulnerabilities, attack behaviors, and scenarios [70]. More recent works include generating attack models without a priori knowledge [78] and investigating the use of Generative Adversarial Networks to learn and generate synthetic alert scenarios [90].

The next research group investigating CSA has formed in Sweden at Swedish Defense Research Agency[4] and RISE SICS[5]. The group is represented mainly by ass. Prof. Joel Brynielsson, Ulrik Franke, Ph.D., and their students. Their significant contribution is a review of literature on CSA [33] that provides a systematic overview of research areas in CSA and the number of published papers. Further, the group researches CSA testing [11], modeling an attacker via attack persona concept [10], and differences in understanding of CSA between normal and IT skilled employers [91].

Another research group was formed around dr. Florian Skopik at Center for Digital Safety and Security of AIT Austrian Institute of Technology[6]. The researchers at AIT investigates the decision support models in CSA used in cyber operation/security centers [38, 82], CSA in smart grids [85], and network anomaly detection [34]. The design of a system for national situational awareness [86] is also investigated by this group.

Finally, a research group on CSA has been established at the Computer Security Incident Response Team of Masaryk University[7]. The network-wide cyber situational awareness with a focus on the perception and comprehension using IP flows is investigated by Jirsík et al. [53, 54]. Husák et al. focused on the predictive aspects of CSA [46, 47]. Other team members investigated criticality and dependency detection [62] or data models for CSA [56].

## 3.3 Data for CSA Research

The research on CSA is held back by a lack of available datasets that provide solid ground truth. However, this is a concern for the whole cybersecurity. Although there were several frequently used datasets available for research intrusion detection, they were shown to be insufficient for advanced analyses, such as attack projection and intention recognition [47]. The datasets are either artificial or collected from a live environment. The artificial datasets offer ground truth and may include documentation on network topology, intentions of the attackers, and other valuable insights. However, they may lack background traffic, random noise, anomalies, and unknown threats that pose a major challenge for live deployment of any intrusion detection or CSA methodology. Datasets captured in a live environment are closer to the actual needs of cybersecurity operations but lack ground truth and need to be properly anonymized. In addition, all the datasets become obsolete quickly.

The datasets, in most cases, contain traces of network traffic that are used to evaluate intrusion detection. Probably the best known are the DARPA datasets[8] that are now considered obsolete but were very popular in the past. More recent and popular datasets are CTU-13[9] and a collection of datasets by the University of New Brunswick[10]. Only some of those datasets are accompanied by intrusion detection rules that allow for generating alerts and network topologies that allow for impact assessment and other CSA-related research. Alert correlation in a collaborative environment can be evaluated using a live dataset from the SABU project[11]. Global CSA

[1] http://csis.gmu.edu/
[2] https://www.arl.army.mil/
[3] https://www.rit.edu/cybersecurity
[4] https://www.foi.se/fusion/
[5] https://www.sics.se/
[6] https://www.ait.ac.at/en/research-topics/cyber-security/
[7] https://csirt.muni.cz/
[8] https://www.ll.mit.edu/r-d/datasets
[9] https://www.stratosphereips.org/datasets-ctu13
[10] https://www.unb.ca/cic/datasets/index.html
[11] https://data.mendeley.com/datasets/p6tym3fghz/1

can be studied using the live data from network telescope and other sensors by CAIDA[12]. MM-TBM dataset[13] is an example of artificial datasets that includes network topology and background noise.

### 3.4 National Strategies

The CSA has been included in the cybersecurity strategies of many nations, which indicates the need and importance of CSA even at the national level. For example, the Australian Cyber Security Operations Centre *provides the Australian Government with all-source cyber situational awareness and an enhanced ability to facilitate operational responses to cybersecurity events of national importance* [18]. The United States of America define their role in cyberspace's future defense as *steady progress towards shared situational awareness of network vulnerabilities and risks among public and private sector networks* [77]. In addition, the National Institute of Standards and Technologies refers to the CSA as a new way to attack and cybersecurity issues rather than using a system defense approach [72]. The German national cybersecurity strategy [32] establishes National Cyber Response Center to *directly inform the crisis management staff headed by the responsible State Secretary at the Federal Ministry of the Interior if the cybersecurity situation reaches the level of an imminent or already occurred crisis.* The United Kingdom aims to *enhance cyber threat awareness, detection, and reaction functions, through the development of a Cyber Security Operations Centre that uses state-of-the-art defensive cyber capabilities to protect the cyberspace and deal with threats* [41]. The Canadian Cyber Incident Response Centre serves *to be the focal point for monitoring and providing advice on mitigating cyber threats, and directing the national response to any cybersecurity incident* as described in Canada's Cyber Security Strategy [37].

## 4 TAXONOMY AND COMPONENTS OF CSA

Given the number of research works on definitions and concepts of SA and CSA, there are surprisingly not many taxonomies or overviews of its components, namely from a more technical or applied perspective. To the best of our knowledge, there is only one work that puts together various components and tools used to achieve and maintain CSA. Evesti et al. [31] provided a taxonomy of cybersecurity situational awareness consisting of data gathering (operational and strategic), analysis, and visualization. We argue that this taxonomy does not conform to the models and definitions of SA and CSA discussed earlier in the paper. However, it may be linked to the three-level model by Endsley [26]. The data gathering is nicely structured and corresponds to the perception level. The analysis and visualization both correspond to the comprehension level and, in our opinion, complement and influence each other. What is missing in this taxonomy is the categorization of projection level and any related tools and approaches.

To overcome the issues of the taxonomy by Evesti et al. [31], we outlined an improved taxonomy of cyber situational awareness in Figure 3. The most important changes happened on the top level, where we adapted the taxonomy to reflect the three-level model of SA by Endsley [26]. The original *Data Gathering* category matches the *Perception* level very well. We moved the remaining two top-level categories, *Analysis* and *Visualization*, under the new *Comprehension* level. Finally, we added the *Projection* level that was missing in the original taxonomy.

We do not propose many changes in the perception level. The operational and strategic subcategories are very convenient and reflect the different needs of cybersecurity operations in day-to-day incident handling as opposed to the needs of cybersecurity analysts, who need more think in longer terms. In the operational subcategory, we added network traffic monitoring [42] as a very important source of data for achieving network-wide SA. In the strategic subcategory, we added OSINT (open-source intelligence) and CTI (cyber threat intelligence) as they both are recent emerging sources of information for cybersecurity analysts. OSINT extends former item of news review and covers any publicly available source of information.

The comprehension level covers analysis and visualization. We perceive the two subcategories as complementing each other as they both increase the comprehension of the situation. We made several changes in these subcategories. First, we moved system log parsing to the operational perception level as it is another source of information, although we acknowledge it is mostly used in the analysis when closely investigating some phenomenon. Subsequently, we replaced clustering with data mining because many more data mining approaches might be used. We also merged it with machine learning as they mostly complement each other. The original taxonomy [31] includes several examples in Metrics. It is indeed advisable to set metrics, although many of them are not transferable to a different environment. However, we would like to add changes in time, such as an increase or decrease of observed values, that provide valuable insights into the evolving situation. Time series are effective models that can be used to further analyze such changes [47]. Finally, anomaly detection is quite confusing because it may fit well in both perception and comprehension, depending on if it is an anomaly detection processing primary data, such as network traffic and system logs, or inferred data, such as security alerts.

The taxonomy of the projection level is borrowed from the survey of attack projection, prediction, and forecasting by Husák et al. [47], who defined use cases for predictive tasks in cybersecurity. The *attack projection* [98] and *intention recognition* [2, 69] are very similar, in essence. They typically use attack models, such as attack graphs, to match observed events to a known scenario and to either project the continuation of an attack, i.e., estimate the most probable next step of an adversary or estimate the adversary's intention by finding a continuation of an attack from which the adversary may profit the most. *Intrusion prediction* [1, 8] covers various methods of predicting particular events, such as particular attacks and exploitations. *Network security situation forecasting* [63] covers various approaches to forecast holistic cybersecurity situation, such as an increase or decrease in the number of expected attacks. The last two categories often rely on time series analysis and other statistical inferences but may also involve predictions based on unconventional sources, such as recent news or sentiment on social media [80].

[12]https://www.caida.org/data/
[13]https://ieee-dataport.org/documents/mm-tbm-evaluation-datasets

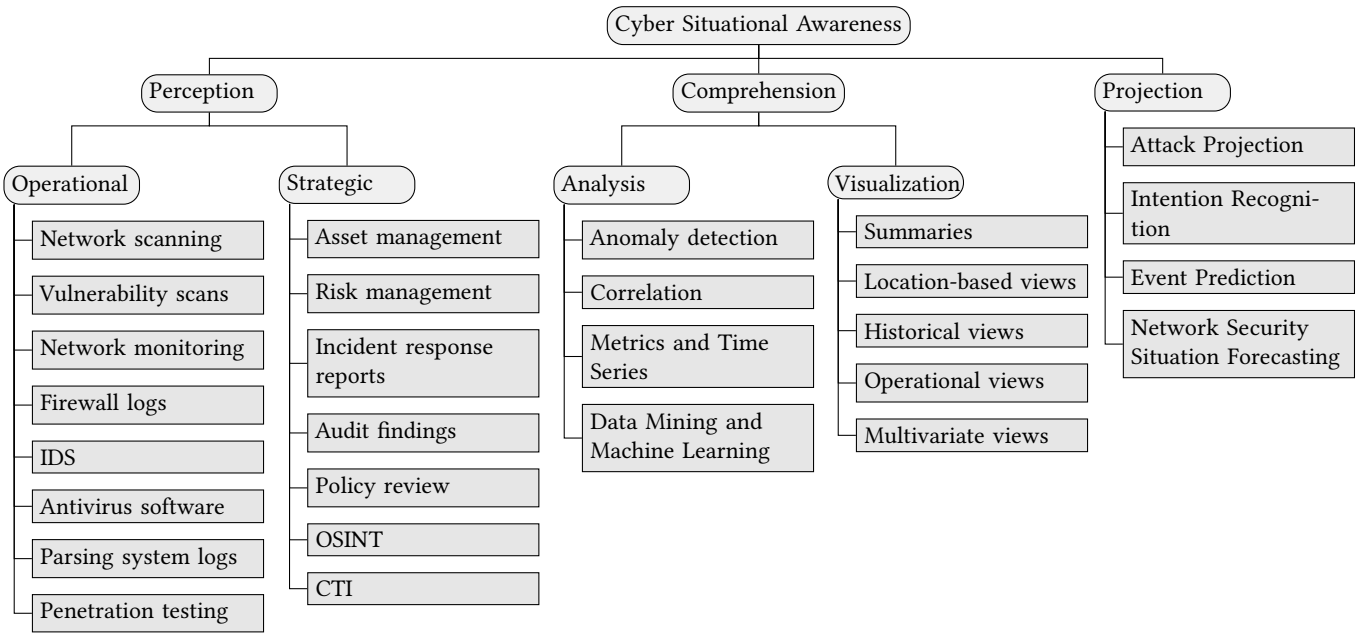


**Figure 3: Taxonomy of Cyber Situational Awareness tools and components.**

## 5 CONTEMPORARY CHALLENGES FOR CSA

Adaptation of Situational Awareness to the cyber domain is not straightforward, due to several characteristics in its operations, adversaries, and the observability of the activities. Earlier works, including [22, 44, 60], discussed several challenges that are unique in enabling CSA. This section extracts prior works as well as our renewed perspectives, and present a summary of the contemporary challenges for CSA. We consider the challenges from the perspectives of *Data* and *Toolsets*, respectively, that are specific to the cyber domain.

### 5.1 The Data Perspective

Analogous to the *big data* challenges [21, 95], CSA shares many and exhibits some unique characteristics in *volume*, *velocity*, *veracity*, *variety*, and *volatility*. According to the Cisco report on IP traffic forecast [13], the volume of global IP traffic was 96 EB per month in 2016 and is expected to rise to 278 EB per month by 2021. The velocity of the network traffic is forecast to nearly double by 2021. The variety of the network traffic will increase too as new applications and protocols are continuously developed (e.g., the number of applications in Apple App Store increased from 585 thousand in 2012 to 2.2 million in 2017 [89]). The value of the information in network traffic can be demonstrated by the market value of the network security segment that is estimated to reach 11,669 million USD at the end of 2018 [93]. Each of the demonstrated *big data* characteristics of CSA data opens new challenges for CSA.

**Volume with Velocity and Veracity** – The volume of the data captured and produced by sensors in cyberspace provides an operator with a massive amount of available information. However, information and data are usually in a raw form that brings little understanding to an operator. An operator is overloaded with data with no meaning to him/her. This challenge can be appropriately summarized as *Data overload – meaning underload*, as mentioned in [60]. To make things worse, the velocity of incoming data combined with a demand for real-time analyses and results delivery puts challenging requirements on the data processing. Tools for data processing and analysis need to provide sufficient throughput to process all data at high-speeds. Moreover, the real-time data processing puts an emphasis on correct time ordering of data as events occur at millisecond or faster rates in cyberspace. Correct time ordering of the events is required for data analyses where causality is of interest (*e.g.*, root-cause analyses, advanced persistent threat detection). With a large volume of data coming in at high speed, the actual critical and malicious activities may only trigger a very small number of intrusion alerts, resulting in an extremely high noise-to-signal ratio that requires intelligent systems that can recognize rare yet contextually critical events.

**Variety and Volatility** – The variety of data opens challenges in homogenizing data from different sources and of different types, as well as due to the heterogeneous attack behaviors/tactics and network protocol and system configurations. In term of homogenization, typical security operations desire central processing, *e.g.*, in a data cloud, which require proper metrics and alert thresholds [22]. Data refinement and normalization is necessary to transform into a common format for effective data synthesis [22] while maintaining the original characteristics and dealing with data duplication, unreliable sources, and errors. The complexity and rapidly evolving network protocols and services, as well as cyberattack behaviors, aggravates the already challenging problem of variety by introducing the volatility into the meanings of information retrieved from past data. New nodes are added or removed, systems are updated, new technologies are introduced, and entities are entering or leaving with mobile technologies. Models and patterns learned in

recent months, weeks, or even days, may not be applicable tomorrow. According to Symantec 2017 Internet Security Threat Report, 375 M of new malware variants were discovered in 2017 [12]. At any given point in time, security analysts must deal with a large variety of user, system, and adversary behaviors, most of which may not be quite dependent on what has been observed in the past. This requires an intelligent system that not only can homogenize the variety of cyber sensors but also quickly adapt to the complex and changing environment and adversary behaviors.

## 5.2 The Toolset Perspective

The cyber big data challenges are tightly coupled with those present in the contemporary toolsets. A toolset used by an operator significantly influences his/her level of CSA. An operator observes cyberspace using different monitoring tools, considers standardized threat models, comprehends data via tools for data analysis, and presents results utilizing various visualization tools. The properties, functions, and performance of available toolset determine an understanding of the current situation and its assessment. Many tools are under rapid development [93] and research. Yet many improvements and additional features are desired. We continue to present the toolset challenges by referencing to the big data V's.

**Variety with Veracity and Volatility** – A CSA operator needs various information from different data sources (network traffic, logs, ADS and IDS systems, antivirus tools, threat intelligence reports, and so forth). A special tool is needed to process data from each different source, and an operator is forced to switch between the tools and utilize a number of different analysis workflows to retrieve needed information. These create a highly manually intensive process that hampers current cyber operations. Cybersecurity vendors are racing to introduce new tools for network visibility, attack detection, and cyber defense to ease complex network comprehension and to reduce a workload on a human operator. This creates a tension for specialized tools versus integrated and unified platform for CSA data analytics. In addition, many industry standards and taxonomies, such as the various attack reference models and tools of similar functions present interoperability issues across organizations and countries. The variety of toolsets and standards causes unnecessary overhead while the same cyber adversary can attack many places at once – creating an increasingly asymmetric cyber warfare. To make things worse, the trend in cyber defense requires shared threat intelligence; yet, the fidelity in these intelligence reports are still low, causing concern of trust for applicability and usability of supposedly advance warnings. The variety in toolsets, compounded with the fidelity in the analytics and threat intelligence as well as the need to adapt to new toolsets and standards, pose unprecedented challenges for the cyber operators to ever become effective.

**Value through Visualization** – The value of data is determined by the *value of information* (as defined in [45]) carried in data for an operator of CSA. The information carried in data is, however, devaluated by the presence of a high noise-to-signal ratio. Anomalous events are common in a cyber world, systems might not work properly, users behave unexpectedly, protocols are not used according to standards, and so forth. Such disruptions to a 'normal' behavior complicate relevant information retrieval and introduce a noise into data, which reduces its value. A plausible solution to overcome the high noise-to-signal ratio is through visualization of intelligent system outputs – visual analytics. It is not news that visualization plays a crucial role in situation comprehension. Several past works [39, 67, 84] have discussed visualization approaches for cybersecurity. Nevertheless, many issues remain open for research, including big data visualization, SDN networks, and human-centered evaluation [39]. One open issue related directly to CSA is a visualization of large-scale complex and dynamically changing networks [60]. The visualization of the networks should be able to scale across levels of detail and across time so that an operator has an instant approach to both overview and detailed information. Additionally, as CSA moves into 'anticipation,' visualization of projected or predicted scenarios with traceable evidence is a new challenge to bring actionable intelligence to the cyber operators. This may present uncharted scientific challenges as cyber predictions may involve novel events that have rarely occurred or never happened yet for the operator.

**Performance amid Volume, Velocity, Veracity, and Volatility** – The performance challenge is closely related to data challenges described above, namely the big data characteristics of data processed in CSA. The volume and speed of the processed data impose a demanding requirement for data processing and computational powers of current CSA tools. Namely, scalability and throughput of the tools are currently trending challenges for CSA toolset. The scalability challenge could potentially be met by the development of cloud-based distributed solutions. The throughput is increased by an extensive parallelization of computations and data processing tasks. A novel approach to scalability and throughput challenges that is gaining attention is distributed data stream processing. Other challenges of CSA related to performance are the reduction of analysis time and response time. The operator needs new information as soon as possible to be able to react in time. The approaches to the analysis of CSA data are subjects to delay, partially by their design and by the big data processed. The data processing workflows and analysis methods need to be improved and optimized to reduce delays caused by data analysis. The above performance gains must be maintained (or suffer minimal degradation) even in the presence of high noise-to-signal ratio and rapidly evolving nature of adversary behaviors and network environments.

# 6 CONCLUSION

In this paper, we discussed the current state of research on cyber situational awareness, an essential concept in cyber defense. We first discussed the way from generic situational awareness to cyber situational awareness and pinpointed unique features of situational awareness in the cyber environment. Subsequently, we provided a brief overview of research on CSA, introduced the most impactful researchers and research groups, identified fundamental works, and provided an insight into trends in publishing on the topic. The number of new publications on CSA per year is still rising and may see a move of attention from fundamental research on principles of CSA towards applied research and experimental development. We may expect that this trend will continue, and we will see more applied research works, tools, and reports from their experimental or operational deployment. We also showed several examples of

CSA in national cybersecurity strategies, which illustrate the wide interest in the topic. Further, we proposed an updated taxonomy of CSA tools and components that are used for achieving and maintaining CSA. Finally, we identified and summarized open research and operational challenges for CSA that we see as the most important and prospective in the near future. First, we need to cope with rising volume, variety, and velocity of the data as cybersecurity data has effectively become big data. Second, there is a need to propose novel tools to support CSA operators with the right data at the right data, visualize the data in a meaningful manner, and maintain sufficient performance.

## ACKNOWLEDGMENTS

This research was supported by ERDF "CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence" (No. CZ.02.1.01/0.0/0.0/16_019/0000822), RIT Global Cybersecurity Institute, and US NSF Award # 1742789.

## REFERENCES

[1] Mohamed Abdlhamed, Kashif Kifayat, Qi Shi, and William Hurst. 2017. *Intrusion Prediction Systems.* Springer International Publishing, 155–174.
[2] Abdulghani Ali Ahmed and Noorul Ahlami Kamarul Zaman. 2017. Attack Intention Recognition: A Review. *IJ Network Security* 19, 2 (2017), 244–250.
[3] Massimiliano Albanese, Ermanno Battista, and Sushil Jajodia. 2015. A Deception Based Approach for Defeating OS and Service Fingerprinting. In *IEEE Conference on Communications and Network Security (CNS).* IEEE, Florence, Italy, 317–325.
[4] Massimiliano Albanese and Sushil Jajodia. 2014. Formation of awareness. *Advances in Information Security* 62 (2014), 47–62.
[5] Massimiliano Albanese and Sushil Jajodia. 2017. A Graphical Model to Assess the Impact of Multi-Step Attacks. *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology* (apr 2017).
[6] Massimiliano Albanese, Sushil Jajodia, and Steven Noel. 2015. Methods and systems for determining hardening strategies. Patent No. US 9,203,861 B2, Filed Jun 21, 2013, Issued Dec 1, 2015.
[7] Paul Barford, Marc Dacier, Thomas G. Dietterich, Matt Fredrikson, Jon Giffin, Sushil Jajodia, Somesh Jha, Jason Li, Peng Liu, Peng Ning, Xinming Ou, Dawn Song, Laura Strater, Vipin Swarup, George P. Tadda, Cliff Wang, and John Yen. 2010. Cyber SA: Situational awareness for cyber defense. *Advances in Information Security* 46 (2010), 3–13.
[8] Václav Bartoš, Martin Žádník, Sheikh Mahbub Habib, and Emmanouil Vasilomanolakis. 2019. Network entity characterization and attack prediction. *Future Generation Computer Systems* 97 (2019), 674 – 686.
[9] G. Bedny and D. Meister. 1999. Theory of Activity and Situation Awareness. *International Journal of Cognitive Ergonomics* 3, 1 (1999), 63–72.
[10] Joel Brynielsson, Ulrik Franke, Muhammad Adnan Tariq, and Stefan Varga. 2016. Using cyber defense exercises to obtain additional data for attacker profiling. In *IEEE International Conference on Intelligence and Security Informatics: Cybersecurity and Big Data, ISI 2016.* IEEE, 37–42.
[11] Joel Brynielsson, Ulrik Franke, and Stefan Varga. 2016. Cyber Situational Awareness Testing. In *Combatting Cybercrime and Cyberterrorism.* Springer, Cham, 209–233.
[12] Kavitha Chandrasekar, Gillian Cleary, Orla Cox, Hon Lau, Benjamin Nahorney, Brigid O Gorman, Dick O'Brien, Scott Wallace, Paul Wood, and Candid Wueest. 2017. *Internet Security Threat Report.* https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf
[13] Cisco. 2017. *Cisco Visual Networking Index: Forecast and Methodology, 2016-2021.* https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.pdf
[14] Edward Colbert, Alexander Kott, Lawrence P Knachel, and Daniel T Sullivan. 2017. *Modeling Cyber Physical War Gaming.* Technical Report. US Army Research Laboratory Aberdeen Proving Ground United States. 46 pages. http://www.dtic.mil/docs/citations/AD1038105
[15] Edward Colbert, Daniel T Sullivan, and Alexander Kott. 2017. Cyber-Physical War Gaming. (2017). arXiv:1708.07424
[16] Edward J. M. Colbert and Alexander Kott. 2016. *Cyber-security of SCADA and Other Industrial Control Systems.* Advances in Information Security, Vol. 66. Springer International Publishing.
[17] Zachary A. Collier, Mahesh Panwar, Alexander A. Ganin, Alexander Kott, and Igor Linkov. 2016. Security Metrics in Industrial Control Systems. In *Cybersecurity of SCADA and Other Industrial Control Systems, Advances in Information Security.* Vol. 66. Springer, Cham, 167–185.
[18] Commonwealth of Australia. 2009. *Cyber Security Strategy.*
[19] Ian A. Cooke, Alexander Scott, Kasia Sliwinska, Novia Wong, Soham V. Shah, Jihun Liu, and David Schuster. 2018. Toward Robust Models of Cyber Situation Awareness. In *Advances in Intelligent Systems and Computing*, Vol. 782. Springer, Cham, 127–137.
[20] Department of the Army. 2014. *FM 3-38: Cyber Electromagnetic Activities.*
[21] Jean-Pierre Dijcks. 2012. *Oracle: Big data for the enterprise.* http://www.oracle.com/us/products/database/big-data-for-enterprise-519135.pdf
[22] Judson Dressler, Calvert L. Bowen, William Moody, and Jason Koepke. 2014. Operational data classes for establishing situational awareness in cyberspace. In *2014 6th International Conference On Cyber Conflict (CyCon 2014).* IEEE, 175–186.
[23] Haitao Du, Daniel F Liu, Jared Holsopple, and Shanchieh Jay Yang. 2010. Toward Ensemble Characterization and Projection of Multistage Cyber Attacks. In *2010 Proceedings of 19th International Conference on Computer Communications and Networks.* IEEE.
[24] Haitao Du, Changzhou Wang, Tao Zhang, Shanchieh Jay Yang, Jai Choi, and Peng Liu. 2015. Cyber Insider Mission Detection for Situation Awareness. In *Studies in Computational Intelligence.* Vol. 563. Springer, Cham, 201–217.
[25] Haitao Du and Shanchieh Jay Yang. 2014. Probabilistic Inference for Obfuscated Network Attack Sequences. In *Proceedings of IEEE/ISIF International Conference on Dependable Systems and Networks.*
[26] Mica R. Endsley. 1988. Situation awareness global assessment technique (SAGAT). In *Aerospace and Electronics Conference, 1988. NAECON 1988., Proceedings of the IEEE 1988 National.* IEEE, 789–795.
[27] Mica R. Endsley. 1995. Measurement of Situation Awareness in Dynamic Systems. *Human Factors* 37, 1 (1995), 65–84.
[28] Mica R. Endsley. 1995. Theoretical underpinnings of situation awareness: A critical review. In *Proceedings of the International Conference on Analysis and Measurement of Situation Awareness.* 24.
[29] Mica R. Endsley. 1995. Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors* 37, 1 (1995), 32–64.
[30] Mica R. Endsley. 2015. Situation Awareness Misconceptions and Misunderstandings. *Journal of Cognitive Engineering and Decision Making* 9, 1 (2015), 4–32.
[31] Antti Evesti, Teemu Kanstrén, Tapio Frantti, Teemu Kanstren, and Tapio Frantti. 2017. Cybersecurity Situational Awareness Taxonomy. In *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA).* IEEE.
[32] Federal Ministry of the Interior. 2011. *Cyber Security Strategy for Germany.* https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile
[33] Ulrik Franke and Joel Brynielsson. 2014. Cyber situational awareness – A systematic review of the literature. *Computers & Security* 46 (2014), 18–31.
[34] Ivo Friedberg, Florian Skopik, and Roman Fiedler. 2015. Cyber situational awareness through network anomaly detection: state of the art and new approaches. *e & i Elektrotechnik und Informationstechnik* 132, 2 (mar 2015), 101–105.
[35] Rajesh Ganesan, Ankit Shah, Sushil Jajodia, and Hasan Cam. 2017. A Novel Metric for Measuring Operational Effectiveness of a Cybersecurity Operations Center. In *Network Security Metrics.* Springer International Publishing, 177–207.
[36] Richard D. Gilson. 1995. Special Issue Preface. *Human Factors* 37, 1 (1995), 3–4.
[37] Government of Canada. 2010. *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada.* http://publications.gc.ca/collections/collection_2010/sp-ps/PS4-102-2010-eng.pdf
[38] Roman Graf, Florian Skopik, and Kenny Whitebloom. 2016. A decision support model for situational awareness in National Cyber Operations Centers. In *2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA).* IEEE, London, UK.
[39] Vinicius Tavares Guimaraes, Carla Maria Dal Sasso Freitas, Ramin Sadre, Liane Margarida Rockenbach Tarouco, and Lisandro Zambenedetti Granville. 2016. A Survey on Information Visualization for Network and Service Management. *IEEE Communications Surveys & Tutorials* 18, 1 (2016), 285–323.
[40] William Heinbockel, Steven Noel, and James Curbo. 2016. Mission Dependency Modeling for Cyber Situational Awareness. In *NATO IST-148 Symposium on Cyber Defence Situation Awareness.*
[41] HM Government. 2016. *National Cyber Security Strategy 2019-2020.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
[42] Rick Hofstede, Pavel Čeleda, Brian Trammell, Idilio Drago, Ramin Sadre, Anna Sperotto, and Aiko Pras. 2014. Flow monitoring explained: From packet capture to data analysis with netflow and ipfix. *IEEE Communications Surveys & Tutorials* 16, 4 (2014), 2037–2064.
[43] Jared Holsopple, Moises Sudit, Michael Nusinov, Daniel Liu, Haitao Du, and Shanchieh Yang. 2010. Enhancing situation awareness via automated situation assessment. *IEEE Communications Magazine* 48, 3 (mar 2010), 146–152.
[44] Jared Holsopple, Moises Sudit, and Shanchieh Jay Yang. 2014. Impact Assessment. In *Cyber Defense and Situational Awareness.* Springer, Cham, 219–238.
[45] Ronald Howard. 1966. Information Value Theory. *IEEE Transactions on Systems Science and Cybernetics* 2, 1 (1966), 22–26.

[46] Martin Husák. 2020. *Prediction of Network Attacks in Collaborative Environment.* Doctoral thesis. Masaryk University, Faculty of Informatics. https://is.muni.cz/th/dmpga/

[47] Martin Husák, Jana Komárková, Elias Bou-Harb, and Pavel Čeleda. 2019. Survey of Attack Projection, Prediction, and Forecasting in Cyber Security. *IEEE Communications Surveys Tutorials* 21, 1 (Firstquarter 2019), 640–660.

[48] Sushil Jajodia and Massimiliano Albanese. 2017. An integrated framework for cyber situation awareness. In *Theory and Models for Cyber Situation Awareness. Lecture Notes in Computer Science.* Vol. 10030. Springer, Cham, 29–46.

[49] Sushil Jajodia, Peng Liu, Vipin Swarup, and Cliff Wang. 2010. *Cyber situational awareness: Issues and Research.* Springer US.

[50] Sushil Jajodia, Steven Noel, Pramod Kalapa, Brian C O'Berry, Michael A Jacobs, Eric B. Robertson, and Robert G. Weierbach. 2011. Network attack modeling, analysis, and response. Patent No. US 7,904,962 B1, Filed Mar 10, 2006, Issued Mar 8, 2011.

[51] Sushil Jajodia, Noseong Park, Fabio Pierazzi, Andrea Pugliese, Edoardo Serra, Gerardo I. Simari, and V. S. Subrahmanian. 2017. A Probabilistic Logic of Cyber Deception. *IEEE Transactions on Information Forensics and Security* 12, 11 (2017), 2532–2544.

[52] Sushil Jajodia, V. S. Subrahmanian, Vipin Swarup, and Cliff Wang. 2016. *Cyber deception: Building the scientific foundation.* Springer International Publishing.

[53] Tomáš Jirsík. 2019. *Cyber Situation Awareness via IP Flow Monitoring.* Doctoral thesis. Masaryk University, Faculty of Informatics. https://is.muni.cz/th/ejynv/

[54] Tomáš Jirsík and Pavel Čeleda. 2018. Toward Real-time Network-wide Cyber Situational Awareness. In *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium.* IEEE, Taipei, Taiwan.

[55] Debra G. Jones and Mica R. Endsley. 1996. Sources of situation awareness errors in aviation. *Aviation Space and Environmental Medicine* 67, 6 (jun 1996), 507–512.

[56] Jana Komárková, Martin Husák, Martin Laštovička, and Daniel Tovarňák. 2018. CRUSOE: Data Model for Cyber Situational Awareness. In *Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES 2018).* ACM, Article 36, 10 pages.

[57] Alexander Kott. 2014. Towards fundamental science of cyber security. *Advances in Information Security* 55 (2014).

[58] Alexander Kott. 2015. Science of Cyber Security as a System of Models and Problems. Lemnios 2011 (nov 2015). arXiv:1512.00407

[59] Alexander Kott and Tarek Abdelzaher. 2014. *Resiliency and Robustness of Complex Systems and Networks.* Vol. 67. CRC Press, Chapter 5, 67–86.

[60] Alexander Kott, Cliff Wang, and Robert F. Erbacher. 2014. *Cyber defense and situational awareness.* Vol. 62. Springer.

[61] Alexander L. Krall, Michael E. Kuhl, Stephen F. Moskal, and Shanchieh J. Yang. 2016. Assessing the likelihood of cyber network infiltration using rare-event simulation. In *2016 IEEE Symposium Series on Computational Intelligence (SSCI).* IEEE.

[62] Martin Laštovička and Pavel Čeleda. 2017. Situational Awareness: Detecting Critical Dependencies and Devices in a Network. In *Security of Networks and Services in an All-Connected World.* Springer International Publishing, 173–178.

[63] Yu-Beng Leau and Selvakumar Manickam. 2015. *Network Security Situation Prediction: A Review and Discussion.* Springer Berlin Heidelberg, 424–435.

[64] Nandi O Leslie, Richard E Harang, Lawrence P Knachel, and Alexander Kott. 2017. Statistical models for the number of successful cyber intrusions. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology* (jun 2017), 154851291771534.

[65] Igor Linkov, Daniel A. Eisenberg, Kenton Plourde, Thomas P. Seager, Julia Allen, and Alexander Kott. 2013. Resilience metrics for cyber systems. *Environment Systems and Decisions* 33, 4 (dec 2013), 471–476.

[66] Peng Liu, Sushil Jajodia, and Cliff Wang. 2017. *Theory and Models for Cyber Situation Awareness.* Springer International Publishing.

[67] William J. Matuszak, Lisa DiPippo, and Yan Lindsay Sun. 2013. CyberSAVe: Situational Awareness Visualization for Cyber Security of Smart Grid Systems. In *Proceedings of the Tenth Workshop on Visualization for Cyber Security (VizSec '13).* ACM, 25–32.

[68] James Moffat. 2006. Mathematical modelling of information age conflict. *Journal of Applied Mathematics and Decision Sciences* 2006 (jul 2006).

[69] Stephen Moskal and Shanchieh Jay Yang. 2020. Cyberattack Action-Intent-Framework for Mapping Intrusion Observables. arXiv:cs.CR/2002.07838

[70] Stephen Moskal, Shanchieh Jay Yang, and Michael E. Kuhl. 2018. Extracting and Evaluating Similar and Unique Cyber Attack Strategies from Intrusion Alerts. In *2018 IEEE International Conference on Intelligence and Security Informatics (ISI).* 49–54.

[71] Arun Natarajan, Peng Ning, Yao Liu, Sushil Jajodia, and Steve E Hutchinson. 2012. NSDMiner: Automated discovery of network service dependencies. In *Proceedings - IEEE INFOCOM.* IEEE, 2507–2515.

[72] NIST. 2017. *Situational Awareness a New Way to Attack Cybersecurity Issues Rather Than Using a System Defense Approach.* Technical Report. NIST. http://csrc.nist.gov/cyberframework/rfi_comments/tri-county_electric_cooperative_part2_032613.pdf

[73] S. Noel, E. Harley, K. H. Tam, M. Limiero, and M. Share. 2016. CyGraph: Graph-Based Analytics and Visualization for Cybersecurity. In *Handbook of Statistics.* Vol. 35. 117–167.

[74] Steven Noel and Sushil Jajodia. 2014. Metrics suite for network attack graph analytics. In *Proceedings of the 9th Annual Cyber and Information Security Research Conference on - CISR '14.* ACM, 5–8.

[75] Steven Noel and Sushil Jajodia. 2017. A Suite of Metrics for Network Attack Graph Analytics. In *Network Security Metrics.* Springer International Publishing, 141–176.

[76] Steven Noel, Sushil Jajodia, Lingyu Wang, and Anoop Singhal. 2010. Measuring Security Risk of Networks Using Attack Graphs. *International Journal of Next Generation Computing* 1, 1 (2010), 135–147.

[77] Barack Obama. 2011. *International Strategy for Cyberspace.* https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[78] Ahmet Okutan and Shanchieh Jay Yang. 2019. ASSERT: attack synthesis and separation with entropy redistribution towards predictive cyber defense. *Cybersecurity* 2, 1 (2019), 15.

[79] Ahmet Okutan, Shanchieh Jay Yang, and Katie McConky. 2017. Predicting Cyber Attacks with Bayesian Networks Using Unconventional Signals. In *Proceedings of the 12th Annual Conference on Cyber and Information Security Research (CISRC '17).* ACM, Article 13, 4 pages.

[80] Ahmet Okutan, Shanchieh Jay Yang, Katie McConky, and Gordon Werner. 2019. CAPTURE: Cyberattack Forecasting Using Non-Stationary Features with Time Lags. In *2019 IEEE Conference on Communications and Network Security (CNS).* 205–213.

[81] Michael Ownby and Alexander Kott. 2016. Predicting Enemy's Actions Improves Commander Decision-Making. (jul 2016). arXiv:1607.06759

[82] Timea Pahi, Maria Leitner, and Florian Skopik. 2017. Analysis and Assessment of Situational Awareness Models for National Cyber Security Centers. In *Proceedings of the 3rd International Conference on Information Systems Security and Privacy.* 334–345.

[83] Nadine B. Sarter and David D. Woods. 1991. Situation Awareness: A Critical But Ill-Defined Phenomenon. *The International Journal of Aviation Psychology* 1, 1 (1991), 45–57.

[84] Hadi Shiravi, Ali Shiravi, and Ali A. Ghorbani. 2012. A Survey of Visualization Systems for Network Security. *IEEE Transactions on Visualization and Computer Graphics* 18, 8 (2012), 1313–1329.

[85] Yegor Shovgenya, Florian Skopik, and Klaus Theuerkauf. 2015. On demand for situational awareness for preventing attacks on the smart grid. In *2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA).* IEEE.

[86] Florian Skopik, Zhendong Ma, Paul Smith, and Thomas Bleier. 2012. Designing a cyber attack information system for national situational awareness. In *Communications in Computer and Information Science*, Vol. 318. Bonn, Germany, 277–288.

[87] Kip Smith and Peter A. Hancock. 1995. Situation Awareness Is Adaptive, Externally Directed Consciousness. *Human Factors* 37, 1 (1995), 137–148.

[88] Neville A. Stanton, Peter R. G. Chambers, and John Piggott. 2001. Situational awareness and safety. *Safety Science* 39, 3 (2001), 189 – 204.

[89] Statista. 2017. *Apple App Store: number of available apps 2017.* https://www.statista.com/statistics/263795/number-of-available-apps-in-the-apple-app-store/

[90] Christopher Sweet, Stephen Moskal, and Shanchieh Jay Yang. 2019. Synthetic Intrusion Alert Generation through Generative Adversarial Networks. In *Proceedings of IEEE MILCOM.*

[91] Muhammad Adnan Tariq, Joel Brynielsson, and Henrik Artman. 2014. The security awareness paradox: A case study. In *ASONAM 2014 – Proceedings of the 2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining.* 704–711.

[92] The MITRE Corporation. 2015. An Overview of MITRE Cyber Situational Awareness Solutions. https://www.mitre.org/sites/default/files/publications/pr-15-2592-overview-of-mitre-cyber-situational-awareness-solutions.pdf

[93] Rob van der Meulen and Christy Pettey. 2017. *Gartner Forecasts Worldwide Security Spending Will Reach $96 Billion in 2018, Up 8 Percent from 2017.* https://www.gartner.com/en/newsroom/press-releases/2017-12-07-gartner-forecasts-worldwide-security-spending-will-reach-96-billion-in-2018

[94] Lingyu Wang, Massimiliano Albanese, and Sushil Jajodia. 2014. *Attack Graph and Network Hardening.* Springer International Publishing, 15–22.

[95] Jonathan Stuart Ward and Adam Barker. 2013. Undefined By Data: A Survey of Big Data Definitions. *Commun. ACM* 58, 7 (jun 2013), 56–68. arXiv:1309.5821

[96] Gordon Werner, Shanchieh Yang, and Katie McConky. 2017. Time series forecasting of cyber attack intensity. In *Proceedings of the 12th Annual Conference on Cyber and Information Security Research - CISRC '17.* ACM.

[97] David D. Woods. 1988. Tasks, Errors, and Mental Models. Taylor & Francis, Chapter Coping with Complexity: The Psychology of Human Behaviour in Complex Systems, 128–148.

[98] Shanchieh Jay Yang, Haitao Du, Jared Holsopple, and Moises Sudit. 2014. *Attack Projection.* Springer International Publishing, 239–261.