Cyber security situational awareness

Tianfield, Huaglory

Published in:
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)

DOI:
10.1109/iThings-GreenCom-CPSCom-SmartData.2016.165

Publication date:
2017

Document Version
Peer reviewed version

Cyber Security Situational Awareness

Huaglory Tianfield
Department of Computer, Communications and Interactive Systems
Glasgow Caledonian University
Cowcaddens Road, Glasgow G4 0BA, United Kingdom

***Abstract*—Situational awareness in the context of cyber security has been well recognized. In a time cyber-attacks getting increasingly sophisticated and making potentially disruptive impacts, it becomes apparent that a holistic approach is fundamentally needed to handling security data effectively. Cyber Security Situational Awareness (CSSA) emerges timely. In this paper, after revisiting the concept of CSSA, we have aligned the process of CSSA with security data lifecycle and analyzed the requirements of CSSA. Then, we have put forward a multi-level analysis framework for CSSA.**

Keywords—cyber security; situational awareness; data fusion; event processing; event correlation; pattern mining; context inference

I. Introduction

As implied by the terms, awareness is contextual understanding built on intelligence, and situation(al) awareness is to get a grasp of what is happening and how it had evolved in the recent time and how it might trend away in the near future.

From a systemic point of view, situational awareness is applying appropriate mechanisms of assessment, evaluation, and inference, and so forth to generate understanding of the situation and dynamics of the situation.

Cyber security situation refers to the global security status of the monitored network, the cyber-attacks suffered in a certain time window, and the effect to the total objective of network security. Generally, the security situational information consists of two aspects, the time dimension and the space dimension.

To deal with the increased information security threats in large scale networks, many kinds of security devices have been used. These devices produce lots of security events. It is very difficult to obtain the security state of the whole network precisely when overwhelmed with excessive warning information. To address this problem, the concept of situational awareness is introduced into cyber security systems. Bass first introduced the concept of situational awareness into computer networks and put forward the network security perception framework based on multi-sensor data fusion [1] [2]. It helps network administrators to identify, track and measure network attack activities.

This paper studies the concept and frameworks of Cyber Security Situational Awareness (CSSA). The remainder of the paper is arranged as follows. Section II revisits the concept of CSSA by embodying the generic layers of situational awareness with the cyber security contexts. Section III first aligns the process of CSSA with security data lifecycle and analyzes the requirements of CSSA, and then puts forward a multi-level analysis framework for CSSA. Finally, Section IV discusses some insights on the proposed framework of CSSA.

II. Concept of Cyber Security Situational Awareness (CSSA)

Endsley defined situational awareness as the perception of the elements in the environment within an amount of time and space, the comprehension of their meaning and the projection of their status in the near future [5][6][7]. Endsley delineated situation awareness in three layers, namely, Perception, Comprehension and Projection [5] [6], as depicted in Fig. 1.

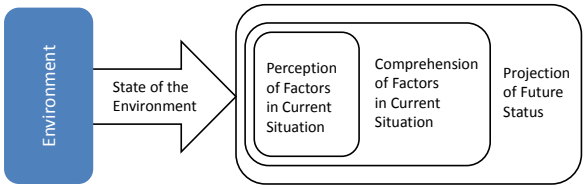

Fig. 1. Three layer of situational awareness

Layer 1 perceives the critical factors in the environment that are important to a particular decision-maker. Perception involves identification and valuation of the status, attributes, and dynamics of the relevant factors over time and space based on the data collected from different sources in the environment.

Layer 2 comprehends what the factors from layer 1 mean. Comprehension involves integration and correlation of disjointed elements that need to be understood in the context of the decision-maker's role to make a sound decision.

Layer 3 projects the understanding of the situation into the future to predict the impact of those elements in the context of the decision-maker's view future decision. Projection involves management of the knowledge of the status and dynamics of the factors and comprehension of the elements characterizing the situation (both layer 1 and layer 2) to predict what will happen in the environment within a period of time.

Endsley later proposed a model of situation awareness based on its role in dynamic human decision-making [7]. In a dynamic environment, decisions are dependent on an ongoing, up-to-date analysis of the environment and are required over a

fairly narrow interval of time. Thus, decision-making has to be based upon timely, sensible situational awareness.

Although decision-making relies upon and thus poses requirements on situational awareness, it should be pointed out that decision-making itself, however, does not form a part of situational awareness.

The main idea of situational awareness in cyber domain is to analyze the surroundings in cyber infrastructure and to create certain events and visualizations for the purpose of efficient and fast decision-making. In simple words, CSSA can be described as the situational awareness applied for cyber security in a cyber infrastructure.

Cyber infrastructure is a term used broadly to describe computer based networked environments. A typical cyber infrastructure in practice would be an enterprise environment which normally comprises a collection of physical and virtualized infrastructures and both internal corporate network and the external internet. Cyber infrastructure may be divided as system infrastructures and information assets [8]. System infrastructures refer to physical and hardware infrastructures, as well as software infrastructures, including operating systems, virtualization systems, database management systems, middleware, applications, and services.

Embodying the generic concept of situational awareness with the cyber security contexts, CSSA would have the following layers.

Perception involves evidence gathering of the situations in the cyber infrastructure. Perception is to get the knowledge of the elements in the networked environment such as alerts reported by intrusion detection systems, firewall logs, scan reports, as well as the time they occurred. This produces classified information with meaningful representations that offers the foundation for comprehension, projection and resolution.

Security monitoring is involved in the early part of the perception layer of situational awareness [4]. Security monitoring is about acquiring the ongoing phenomenon of computer or network system in which data may continuously change. Whether the security monitoring is passive or active, projection of the future status of the network is not an issue concerned.

Comprehension involves the analysis of the evidences to deduce the exact threat level, type of attack and associated or interdependent risks. Comprehension utilizes a set of relevant techniques and procedures to analyze, synthesize, correlate and aggregate pieces of evidence data perceived in the cyber infrastructure.

Projection involves predictive valuation to address future incidents and resolution to mitigate the network situations. Projection is the ability to make future prediction or forecast based on the knowledge extracted from the dynamics of the network elements and comprehension of the situation.

On top of the three layers in Endsley's situational awareness definition, namely, perception, comprehension and projection, McGuinness and Foy [9] added the fourth layer, i.e., resolution of the perceived situation. Resolution (Layer 4) is about the counter-measure controls required to treat the risks inherent or interdependent in the cyber infrastructure.

CSSA involves the perception of attacks and attack tracks, comprehension of the attack patterns and correlations, and the projection of what will happen in the near future in terms of impact and threat levels towards the infrastructure and information assets [12]. It should be noted that CSSA of an organization ultimately reflects the effectiveness of response to attacks.

III. Process and Framework of Cyber Security Situational Awareness (CSSA)

A. *Process of CSSA*

CSSA can be understood from a systemic point of view, which highlights the process that transforms the various security data into situational patterns. According to such a systemic point of view, CSSA is a process of data transformation and evidence refinement and valuation, as illustrated in Fig. 2.

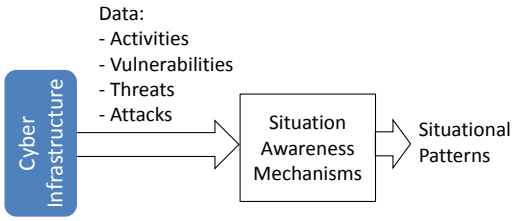

Fig. 2. Process of cyber security situational awareness (CSSA)

The process of CSSA essentially corresponds to the lifecycle that security data should undergo. Along the lifecycle, data take different forms, ranging from the start at the raw sensor data, through cleansed data, fused data, correlated data, perceived events, and formulated contexts, and ending at the situational patterns. The upstream of the security data lifecycle is mainly concerned with data pre-processing, distributed data stores, and data fusion, and event processing, while the downstream of the security data lifecycle is mainly concerned with situational assessment and modeling, sequential pattern mining and pattern analysis, context inference and management, and situational visualization.

B. *Requirements of CSSA*

Cyber security situational patterns will come as the outcomes of CSSA process. Thus, it is necessary to set up specifications on what should be generated through the CSSA process. In particular, the specifications of CSSA should describe what contents of cyber security situation should be generated, e.g., cyber asset assessment, vulnerability assessment, cyber threat/attack assessment, and their evolving trends, and also, how, i.e., in what format, the situational patterns should be prompted to the users for decision support.

Put in to a schema, situation in a cyber infrastructure can be expressed as a description of the valuation of the cyber infrastructure features as below.

```
situation   ::=   <cyber assets, cyber space
                  topologies, activities,
```
(1)

```
actors, vulnerabilities,
threats, known attacks,
adversaries, …>
```

In [3], seven aspects of a cyber security situation are stated, which fall in two groups, that is, (a) static specifications, e.g., current situation, actor behavior, impact of attack, why and how the current situation is caused; and (b) dynamic specifications, e.g., how situations evolve, and plausible future of the current situation.

Requirements of CSSA, functional and system-wise, can be illustrated in Fig. 3. Along the security data lifecycle come the stages through which data are acquired, collected, processed, correlated and extracted for higher level values. Within each stage, the systems, techniques and toolkits are related to the major functional correspondingly needed. Moreover, CSSA is intrinsically born as a distributed data processing infrastructure.

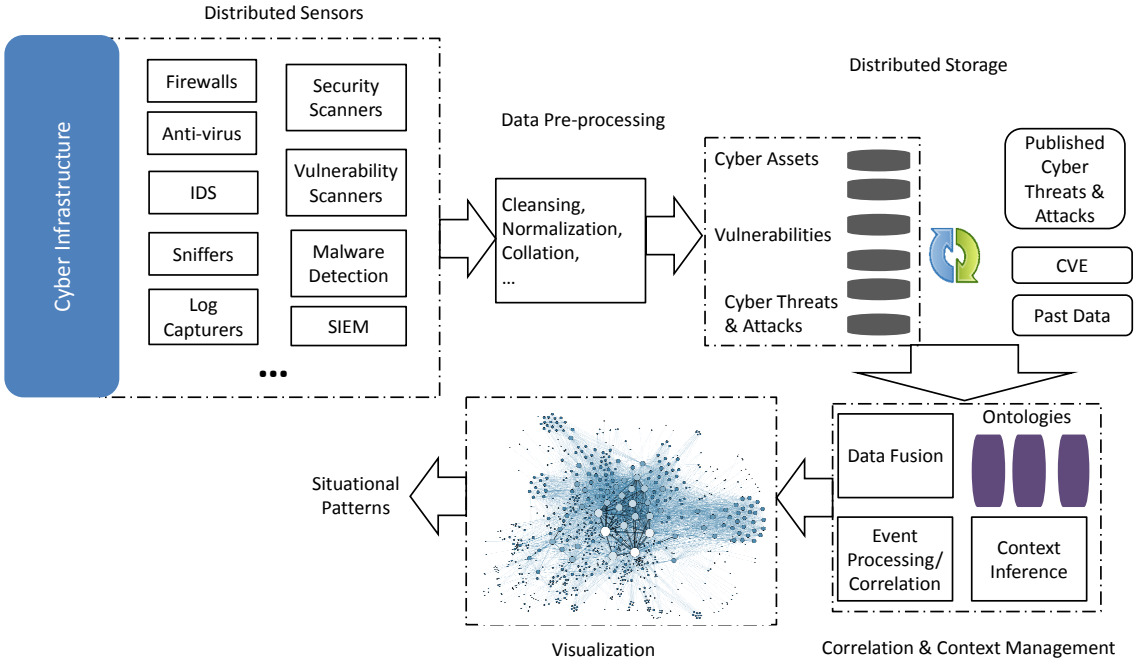

Fig. 3. Requirements of cyber security situational awareness (CSSA)

As a prerequisite, the components of a distributed data storage system have to be deployed in the enterprise so as to provide the collection of static event and instant event logs. Each organizational unit has applications running on its own clients and servers and network devices such as intrusion detection/protection system (IDS/IPS), firewall, etc. information collected across organizational units is sent to a cyber security operation center.

All collected data are cleansed, normalized and stored in a distributed structurer, which can already be used to support security information management and visualization. The data pre-processing mainly involves cleansing, normalization and collation. Data cleansing may include duplicate elimination, data calibration and filtering of the raw data from security sensors, such as IDS, firewall, network and system log records, SIEM, and NetFlow, etc.

At correlation and context processing, data fusion and event processing and correlation take place. Data fusion is a technique to aggregate sets of evidence regarding a perceived situation. Dempster-Sharer evidence theory is a common technique for data fusion, which synthesizes belief levels of the individual data received from different sources so as to effectively reduce the false positive and false negative of security alerts. Furthermore, data fusion techniques and complex event processing, in which events are detected and correlated, may be utilized to exploit the higher level values out of the data.

At the end, security visualization is the transfer of organized data and information into meaningful patterns or sequence to be visualized. It is part of the comprehension layer of situational awareness. With all the data and events to create an integrated common picture, users can be prompted, immersed and informed by a common operational picture underpinned by CSSA. It is composed of vulnerability, assets, risks and instant status information. Such a consolidated cyber security picture allows decision-makers to make integrated risk analysis and corrective action planning.

As shown in Fig. 3, CSSA builds upon relevant systems and techniques of cyber security, especially at the stage of sensing and acquisition of cyber security data, e.g., Vulnerability Analysis and Risk Management, CVE (Common Vulnerabilities and Exposures) security vulnerability Database, attack tree creation infrastructure, security event logger and correlator in security information and event management (SIEM), etc.

In fact, CSSA can take use of a security operation center where new threats and methods of cyber-attacks that may arise in the future can be tested and counter-measures can be developed. Through the instruments of a security operation center, CSSA can gather network, system and application logs

and sensor alerts in real time all over the cyber infrastructure. Moreover, a cyber security ontology and vulnerability database should be set up.

CSSA integrates and centrally manages vulnerability, network topology and cyber assets information collected from the organizational IT systems. The most effective cyber-attacks to be carried out by cyber-attackers can be analyzed and attack trees can be used to analyze the possible attack vectors (vulnerability, topology, etc.).

C. Multi-Level Analysis Framework of CSSA

From security information acquisition to building the cyber security situation model, it must be an integrated process. To exploit higher level values out of the security data, CSSA will undergo a multi-level analysis process. Fig. 4 illustrates the information flow in the multi-level analysis framework of CSSA. The information flow from security sensors to situational patterns forms an information value chain to achieve CSSA.

At the lowest level, sensors pick up activity, configuration, and topology information from the cyber infrastructure comprising system infrastructures and information assets. Sensor data must be cleansed and normalized when inputted to the distributed data stores. The data is stored in distributed data stores as basic facts about the cyber infrastructure's history and the current state.

For data integration, there is a challenge in integrating the data in different formats from diverse sensors, ranging from network flow records to usage statistics and topology graphs. Though ideal, it is hard and costly to transform data in different formats from heterogeneous sources into a suitable common representational format at the syntactic level. More practical way should turn to data integration at a semantic or service level, e.g., data federation, data virtualization, data as a service. Elements from this common representation are linked in the distributed data store.

After data is processed, the core process of CSSA is situational assessment and projection, which will generate the comprehension and representation of the current situation and then establish a projection on the trend of situation in the near future.

Fig. 5 illustrates the higher levels in the multi-level analysis framework of CSSA, including data fusion, complex event processing, sequential patter mining and pattern analysis, context inference and management, etc., which exploit the higher values out of the data so as to enable the situational assessment and projection.

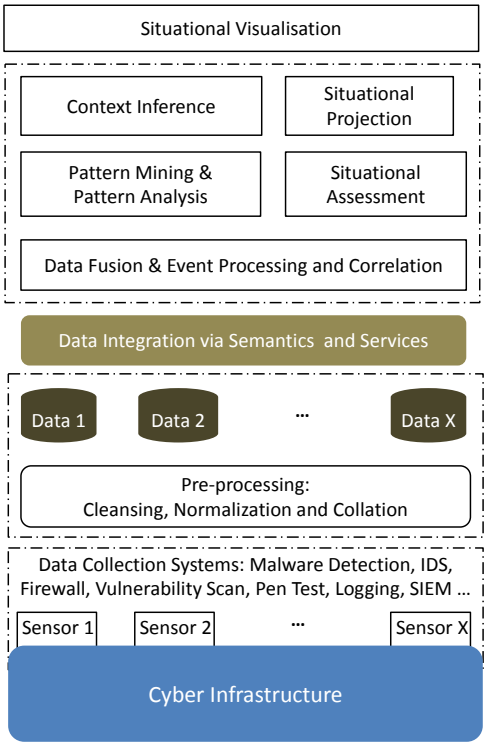

Fig. 4. Multi-level analysis framework of CSSA.

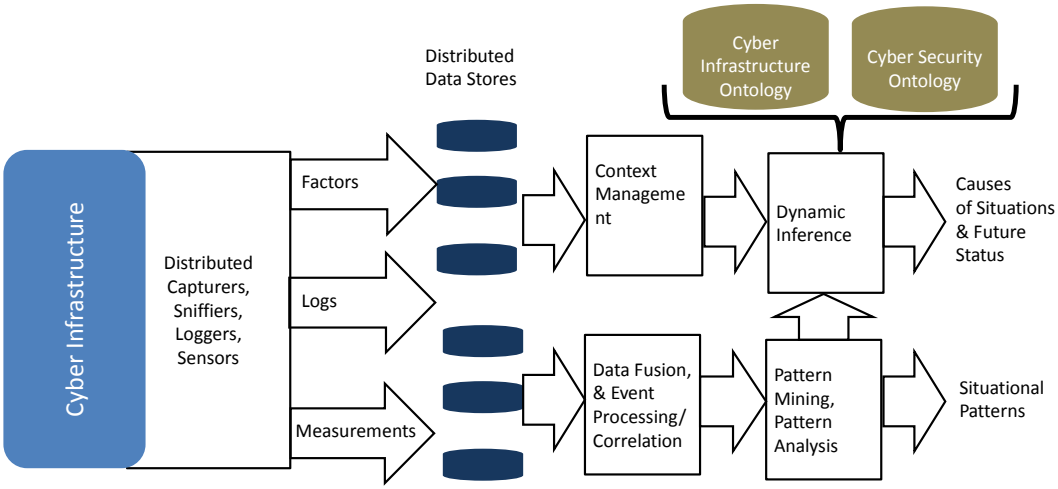

Fig. 5. Higher levels in the multi-level analysis framework of CSSA

Through data fusion and complex event processing, multiple factors are correlated to detect events about the cyber infrastructure components and assets. Using the data in the distributed data store, data fusion therefore creates an overall model of the cyber infrastructure, including the state of and dependencies among its components. For complicated circumstances, data mining is utilized to find frequent patterns in the security events. Situational assessment is based on the analysis of the sequential patterns in the security events.

One point worth noting is that in the multi-level analysis framework of CSSA, data fusion (e.g., based on Dempster-Shafer evidence theory), and event processing and correction should be distinguished from the data cleansing (e.g., duplicate elimination, data calibration and filtering, etc.), normalization and collation. The former are aimed at exploiting higher level values out of the data, whereas the latter are to ensure the data is valid and correct.

Finally, projection into the future is enabled by using the representation of cyber infrastructure model in combination with semantic models. Semantic meaning of data and inference capabilities on the cyber infrastructure components and assets can be established based on context management, cyber infrastructure ontology and cyber security ontology. Further inference capabilities act on incomplete or conflicting information to propagate the components' state to higher levels of dependent services and form a cyber infrastructure model that correctly represents the state and dependencies over time. Visualization of the cyber infrastructure in a cyber operational picture allows stakeholders quick understanding, analysis, and decision-making. [8]

The multi-level analysis framework of CSSA may be generally segmented in line with the upstream and downstream, as illustrated in Fig. 6.

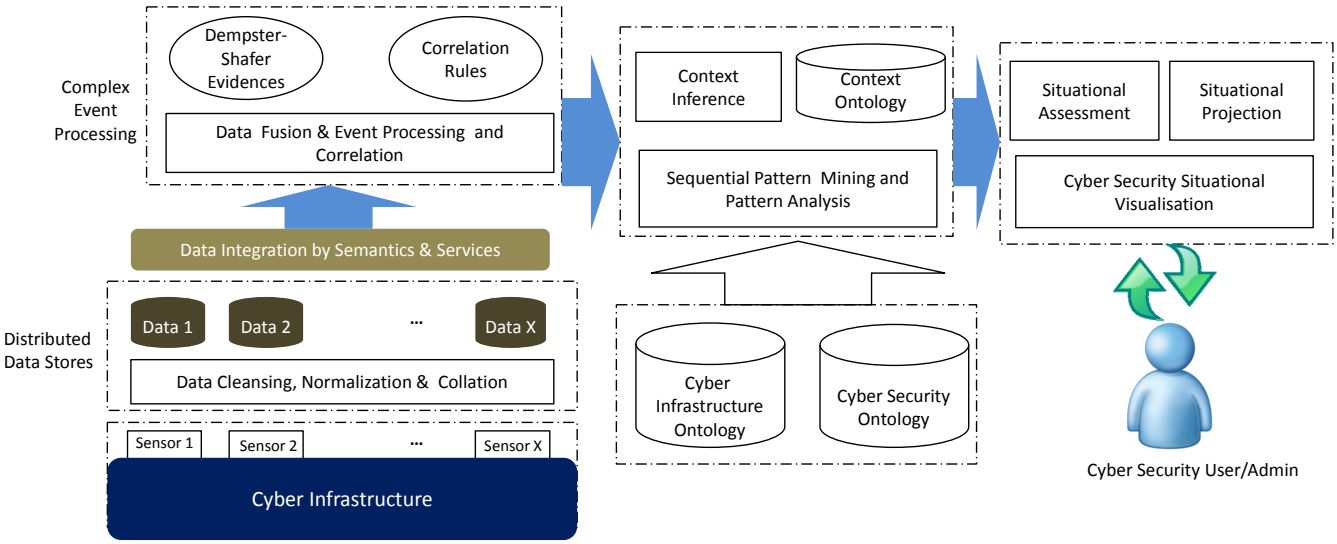

Fig. 6. Upstream and downstream in the multi-level analysis framework of CSSA

CSSA at the upstream is concerned with data pre-processing and the distributed data stores alongside constructing the information models, including data fusion based on Dempster-Sharer evidence theory for the delineation of cyber security situations.

At the start of the upstream is data pre-processing. Data pre-processing is designed to collect security data from different sensors, which are mostly embedded in cyber security toolkits, e.g., anti-virus, malware detection, IDS/IPS, log management, SIEM, etc. Pre-processing may include cleansing (e.g., duplicate elimination, data calibration, filtering/validation, etc.), normalization, collation, etc. Data validation mechanism is adopted to determine whether there is a successful attack. By comparing the conditions and the system configuration (e.g., OS version, services running, etc.) necessary for a successful attack, non-impact attack alert could simply be removed. Finally, the security data will be normalized into a uniform format so as to be usable in the later stages of CSSA.

Data fusion is one of the advanced stages in the upstream, which may be carried out according to Dempster-Sharer evidence theory.

CSSA at the downstream is concerned with the general processes of event processing and correlation analysis of various types of alert events from security sensors, sequential pattern mining and pattern analysis, and context inference and situational assessment and projection, and situational visualization.

For sequential pattern mining and pattern analysis, first, attack patterns are acquired through interactive knowledge discovery by applying frequent pattern mining algorithm, which helps discover the knowledge hidden in an event sequence. Then, the discovered frequent patterns and sequential patterns are transformed to the correlation rules of alert events. Finally, cyber security situation graph is dynamically generated.

IV. Discussions

At present, most of the work is focused on the fusion of the security events, and work in visualization is focused on visualizing network traffic flows, rather than being deeply incorporated into Cyber Security Situational Awareness (CSSA).

Ontologies of cyber infrastructure and cyber security are important for context inference and management. There is work on is cyber security ontology [10] [11], but it is practically not incorporated into CSSA, yet.

Majority of the existing work is concerned with network security situational awareness. Also security sensors are in network security toolkits, e.g., IDS/IPS. Furthermore, network security situational awareness presents a very clear instance for multi-sensor information fusion. However, when moving into general CSSA, there will be broader issues. Basically, there is no boundary on data sources, whether it is network related or otherwise. There is a need to deal with data in a holistic manner. On the hand, the specifications on situational awareness should be much broader than network security situational awareness simply because cyber infrastructure is much beyond just network.

In all cases there is lack of an integrated situational awareness framework for cyber infrastructures.

Our proposed multi-level analysis framework of CSSA is essentially based on aligning the CSSA process with the security data lifecycle. The proposed multi-level analysis framework of CSSA has expanded Endsley's three layer model of situational awareness in the following aspects. At the overall level, multi-level analysis framework highlights the explicit treatment of data and data flows in CSSA, and has opened it up that CSSA is a process, aligned with the security data lifecycle, which may undergo any multiple levels as needed in exploiting higher level values out of the security data, whereas Endsley's three layer model suggests it that each layer is more or less a separate conception of situational awareness.

Another point, in the multi-level analysis framework, data acquisition and storage follows a distributed structure, that is, every kind of data should have a processing corresponding to the data that is acquired with the monitored cyber infrastructure.

References

[1] T. Bass (1999). Intrusion detection systems and multisensor data fusion: creating cyberspace situational awareness. Communications of the ACM, 1999, vol. 43, no. 4, pp. 99-105.

[2] T. Bass (1999). Multisensor data fusion for next generation distributed intrusion detection systems. 1999 IRIS National Symposium on Sensor and Data Fusion, May 1999, pp. 24-27.

[3] L. D. Cumiford (2006). Situation awareness for cyber defense. 2006 CCRTS: The State of the Art and State of the Practice, 11 pages.

[4] A. D'Amico and M. Kocka (2015). Information assurance visualizations for specific stages of situational awareness and intended uses: lessons learned. IEEE Workshop on Visualization for Computer Security (VizSEC'05), Chicago, IL, USA, 25 Oct 2015.

[5] M. Endsley (1988). Design and evaluation for situation awareness enhancement. Proceedings of the Human Factors Society 32nd Annual Meeting, Human Factors Society, 1988, pp. 97-101.

[6] M. Endsley (1988). Situation awareness global assessment technique (SAGAT). Proceedings of the IEEE 1988 National Aerospace and Electronics Conference, 23-27 May 1998, vol. 3, pp. 789-795.

[7] M. R. Endsley (1995). Toward a theory of situation awareness in dynamic systems: situation awareness. Human Factors, vol. 37, no. 1, 1995, pp. 32-64.

[8] V. Lenders, A. Tanner, A. Blarer (2015). Gaining an edge in cyberspace with advanced situational awareness. IEEE Security & Privacy, March/April 2015, pp. 65-74.

[9] B. McGuinness and L. Foy (2000). A subjective measure of SA: the crew awareness rating scale (CARS). Proc. of Human Performance, Situation Awareness and Automation: User-Centered Design for the New Millenium, 2000, pp. 286-291.

[10] L. Obrst, P. Chase and R. Markeloff (2012). Developing an ontology of the cyber security domain. Seventh International Conference on Semantic Technologies for Intelligence, Defense, and Security, 2012, pp. 49-56.

[11] A. Oltramari and L. F. Cranor, R. J. Walls and P. McDaniel (2014). Building an ontology of cyber security. Proc. Intl. Conference on Semantic Technologies for Intelligence, Defense, and Security (STIDS), Nov 2014. Fairfax, VA, USA.

[12] G. P. Tadda, J. S. Salerno (2010). Overview of cyber situation awareness. In: S. Jajodia et al, eds, Cyber Situational Awareness - Issues and Research, vol. 46, Springer, 2010, pp. 15-35.