Cumhuriyet Üniversitesi Fen Fakültesi
Fen Bilimleri Dergisi (CFD), Cilt:36, No: 3 Ozel Sayı (2015)
ISSN: 1300-1949

Cumhuriyet University Faculty of Science
Science Journal (CSJ), Vol. 36, No: 3 Special Issue (2015)
ISSN: 1300-1949

Cyber Situational Awareness using Intelligent Information Fusion Engine (IIFE)

Ali J. RASHİDİ[1], Kourosh D. AHMADİ [1], Mostafa HEİDARPOUR[1,*]

[1]*National Information Fusion Research Center, Malek-Ashtar University of Technology, Tehran, Iran*

Received: 01.02.2015; Accepted: 05.05.2015

Abstract. Situational awareness (SA) represents a knowledge state which is obtained from existing information, and plays an important role in decision making process. Considering the importance of making the best decisions in the shortest time, improving situational awareness, to aim a better perception and comprehension from existing situation, has been a basic topic in recent researches in a variety of domains. In cyber domain, because of its complexity and large amount of data which gathered from different sensors, we need a well suited model for situational awareness to denote all aspects of this domain. In this paper, a new model of situational awareness is proposed which uses intelligent information fusion engine (IIFE) as a main element of situational awareness system. The proposed model is capable of managing large amounts of data and represents a higher abstract level of information. It can also drive knowledge acquisition and evaluates the current situation based on acquired knowledge.

Keywords: Situational Awareness, Cyber Defense, Intelligent Fusion Engine, Information Fusion

1. INTODUCTION

The term “situation awareness” or “situational awareness”, SA is used shortly for both, involves being aware of one's environment and situation. Thus, everyone for his or her efficient activities needs to have an appropriate SA. In other words, this concept is essential for almost all systems and persons activities in all applications (Endsley, 1995; Adams, Tenney, and Pew, 1995). There are several famous definitions for SA in the literatures. Beringer and Hancock (1989) summarized some of these definitions. They also provided a brief history of formation of this concept that we prefer to use it directly: “By the late 1980s, there was a growing interest in understanding how pilots maintain awareness of the many complex and dynamic events that occur simultaneously in flight, and how this information was used to guide future actions. This increased interest was predominantly due to the vast quantities of sensor information available in the modern cockpit, coupled with the flight crew's ‘new’ role as a monitor of aircraft automation.” Starter and Woods (1991) introduced the concept of situation awareness without the support of an accurate definition. Endsley (1988-1995), the chief scientist of the U.S. Air Force, provided a general definition of SA in dynamic environments as follows: “Situation awareness is the perception of the elements of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future”. According to this definition, SA consists of three components that are: perception, comprehension, projection.

In recent years, SA was a challenging research area in many different domains such as security surveillance applications (Franke, and Brynielsson, 2014). In this paper we focused on cyber requirements for situational awareness and proposed a new cyber SA model which is based on intelligent information fusion engine (IIFE). The Proposed IIFE is a well suited means which can be used in many applications. Using this means in cyber domain, can help us to improve our national cyber defense capabilities.

The rest of this paper is organized as follows: Section 2 provides an overview of the SA reference model and outlines primitive definitions needed to introduce our model. Section 3 provides related works and descriptions of cyber SA which is our main scope. Section 4

* Corresponding author. *Email address*: mut.heidarpour@gmail.com

Special Issue: The Second National Conference on Applied Research in Science and Technology

provides a brief overview of information fusion engines and introduces intelligent information fusion engine framework. Section 5 introduces our proposed model and explains its SA levels. Finally, Section 6 concludes the paper with directions for future researches.

2. SITUATIONAL AWARENESS REFERENCE MODEL

According to Endsley's definition, SA begins with perception. Perception provides information about the status, attributes, and dynamics of relevant elements within the environment. It also includes classifying information into understood representations and provides the basic building blocks for comprehension and projection. Without a basic perception of important environmental elements, the odds of forming an incorrect picture of the situation increase dramatically. Comprehension of the situation encompasses how people combine, interpret, store, and retain information. Thus, comprehension includes more than perceiving or attending to information; it includes the integration of multiple pieces of information and a determination of their relevance to an individual's underlying goals and can infer or derive conclusions about the goals. Comprehension yields an organized picture of the current situation by determining the significance of objects and events. Furthermore, as a dynamic process, comprehension must combine new information with already existing knowledge to produce a composite picture of the situation as it evolves. Situational Awareness refers to the knowledge of the status and dynamics of the situational elements and the ability to make predictions based on that knowledge. These predictions represent a Projection of the elements of the environment (situation) into the near future (Tadda, and Salerno, 2010).

Endsley then extended her concept of SA to include a memory component and a decision/ action taken as a result of the SA. The decision / action is then considered to act upon the environment which produces a circular loop as SA begins again with a perception of the new environment (Figure1).

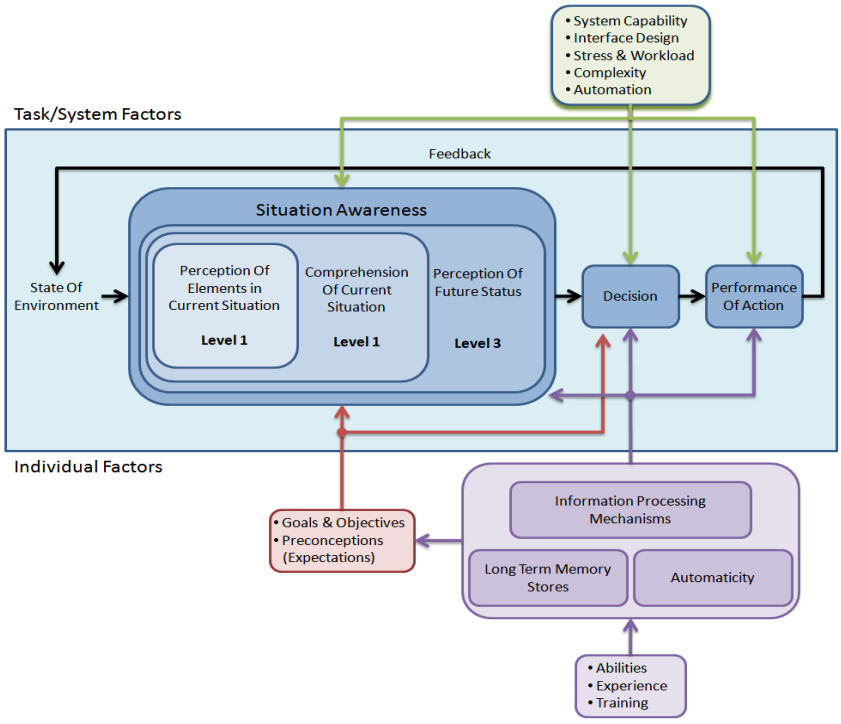

Figure 1. Endsley's situational awareness model (repainted).

McGuinness and Foy (2000) extended Endsley's Model by adding a fourth level, which they called Resolution. This level tries to identify the best path to follow to achieve the desired state change to the current situation. McGuinness and Foy believe that for any fusion system to be successful, it must be resilient and dynamic. In situational Awareness model which is proposed by McGuinness and Foy the following questions are asked in perception, comprehension, projection and resolution modules and is attempted to answer them. In perception module this question is asked: "What are the current facts?" Comprehension asks, "What is actually going on?" Projection asks, "What is most likely to happen if...?" And Resolution asks, "What exactly shall I do?" The answer to the resolution question isn't to tell a decision maker what specific action to perform or what specific decision to make but instead provides options of end actions and how they affect the environment. SA Reference Model is shown in Figure2. This model is built by combining the JDL Data Fusion model and Endsley's SA Model. In addition to presenting the model, definitions of the various components of the model are provided. Therefore, situational awareness is a process which is composed of four levels: perception, comprehension, projection and resolution (Tadda, and Salerno, 2010).

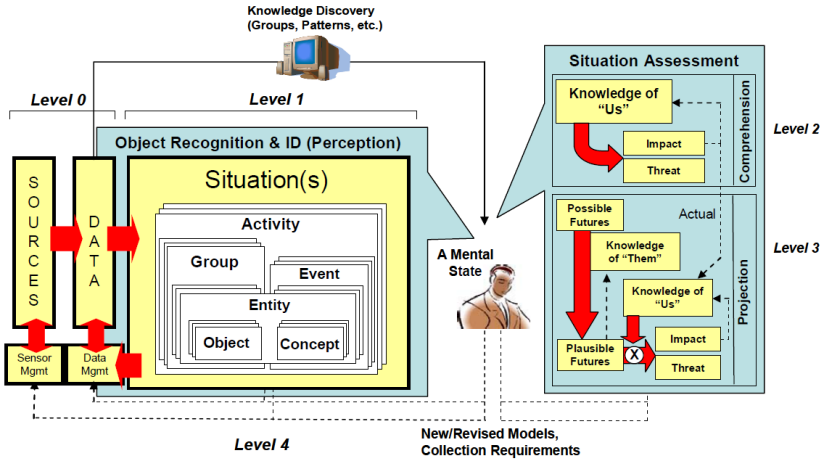

Figure 2. Situational Awareness Reference Model (Salerno, 2008).

3. CYBER SITUATIONAL AWARENESS

Cyber network threats tend to be highly complex, and attacks may involve internal or external attackers that span varying levels of sophistication—from amateurs to highly organized entities. Cyber networks may be hacked by coordinated, distributed attacks, which are constantly changing to circumvent and exploit cyber defense methodologies. A cyber-attack can have severe consequences in a military network as well as to civilian network infrastructures (Kott, Wang, and Erbacher, 2014).

Therefore, cyber situational awareness is very important to deal with unknown daily growing threats in a national defense. However, cyber situational awareness could be studied in different aspect. For instance, Yu, Xu, Chen, and Moulema (2013) proposed a cloud computing based architecture for conducting cyber security situational awareness. They leveraged the cloud infrastructure with a data-storage and investigate stream processing techniques to reduce operational delays. They presented a parallel cloud based threat detection that integrates both signature-based detection and anomaly-based detection. Liu, Feng, Li, and Wang (2013) proposed cyber security situational awareness based on data mining and state machine. They used the correlation state machine that is a data structure of achieving situational awareness to

assess and predict the threat situation to achieve cyber knowledge. Friedberg, Skopik, and Fiedler (2015) considered network anomaly detection to achieve cyber situational awareness. They proposed the automatic event correlation for incident detection approach for anomaly detection, which aims at extending existing intrusion detection systems. Gundersen (2013) analyzed the relationship between context and situational awareness with the aim to get a better understanding of how context information influences situation assessment.

However, to produce a general cyber defense, several aspects of awareness are needed to form complete cyber situational awareness. Some of these can be listed as follows (Barford et al, 2010):

Be aware of the current situation. This aspect can also be called situation perception. Situation perception includes both situation recognition and identification. Situation identification can include identifying the type of attack (recognition is only recognizing that an attack is occurring), the source (who, what) of an attack, the target of an attack, etc. Situation perception is beyond intrusion detection. Intrusion detection is a very primitive element of this aspect. An IDS (intrusion detection system) is usually only a sensor, it neither identifies nor recognizes an attack but simply identifies an event that may be part of an attack once that event adds to a recognition or identification activity.

Be aware of the impact of the attack. This aspect can also be called impact assessment. There are two parts to impact assessment: 1) assessment of current impact (damage assessment) and 2) assessment of future impact (if the attacker continues on this path or more general if the activity of interest continues - what is the impact?). Vulnerability analysis is also largely an aspect of impact assessment (provides knowledge of us and enables projection of future impact). Assessment of future impact also involves threat assessment.

Be aware of how situations evolve. Situation tracking is a major component of this aspect.

Be aware of actor (adversary) behavior. A major component of this aspect is attack trend and intent analysis, which are more oriented towards the behaviors of an adversary or actor(s) within a situation than with the situation itself.

Be aware of why and how the current situation is caused. This aspect includes causality analysis (via back-tracking) and forensics.

Be aware of the quality (and trustworthiness) of the collected situation awareness information items and the knowledge-intelligence-decisions derived from these information items. The quality metrics include truthfulness (or soundness), completeness, and freshness. This aspect can also be viewed as part of situation perception or more specifically recognition.

Assess plausible futures of the current situation. This involves a multitude of technologies for projecting future possible actions/activities of an adversary, paths the adversary might take, and then constraining the possible futures into those that are plausible. This constraining requires an understanding of adversary intent, opportunity, and capability (knowledge of them) as well as an understanding of blue vulnerabilities, etc. (knowledge of "us"). Plausible futures can also be a part of identifying threats and could be considered part of the threat assessment.

As a result, to produce good cyber situational awareness, in cyber defense, all of these aspects are needed uniformly in a single solution format and using each of them, alone without others, will not work properly. In cyber space we continuously face to different threats which can be random or oriented. Thus an ideal situational awareness system is expected to be self-conscious

and self-protection, working without human intervention. This was the first idea of our researches which finally resulted to this paper.

4. INTELLIGENT INFORMATION FUSION ENGINE (IIFE)

Information fusion is a rapidly growing research area. In this area, different techniques and means are presented for combining data and information coming from a variety of sensors and resources. Using this techniques and means, results in improved overall system performance and raised capabilities of system operation. One of this means, which has been widely extended recently, is the information fusion engine. An information fusion engine is capable of managing a large amount of data and information; it uses different processing modules and represents a higher abstract level of information, by fusing and analyzing data and information. The most recently proposed fusion engines are INFERD, DAFNE, ORCA and TDFE (Stotz et al, 2007; Ditzel et al, 2011; ORCA Development Team, 2011; Saab group, 2012).

Each of these engines, regarding its own goal and working area, has several specific capabilities and uses specialized modules. Table1 represents a brief overview of basic capabilities and modules existing within mentioned fusion engines. Comparing these fusion engines, we can understand that this technology is growing toward increasing operating capabilities, flexibility, scalability, and containing intelligence. In fact, using different methods, the learning capability and knowledge acquisition process must be implemented within fusion engines. Achieving intelligent information fusion engine has several advantages, including no need to use a priori knowledge which is one of the most challenges in each application.

Our proposed intelligent information fusion engine (IIFE) framework uses machine learning methods and expert system concepts to provide knowledge acquisition capability for information fusion engine. So the information fusion engine is converted to an intelligent means which provides several capabilities such as conceptual modeling, learning and prediction. These capabilities are considered in the architecture of information fusion engine as several distinct modules.

Conceptual modeling represents relations between different entities in a perceptual format and increases overall user and system perception on its own supervising environment. Using this conceptual modeling, the capability of pattern extraction is also provided over existing patterns in data and information. It is clear that the situation and type of the problem must be considered for this operation. For instance, in cyber defense, attack patterns and hacker behavior patterns can be considered for this operation and a distinct knowledge database can be used for each one. After detecting patterns, the learning capability will be provided. Learning and knowledge acquisition process is a main component of IIFE. Our proposed IIFE can learn existing and repeating patterns using one or more knowledge databases, and can use them for the next fusion operation. At the next fusion operation the previous acquired knowledge will be used to predict the next situation. This closed loop will be repeated during the time and finally provides an abstract level of knowledge, which is very important for decision making.

Table 1. Comparing recent Information fusion engines

Row	Fusion Engine	Capabilities	Modules
1	INFERD (2007)	1.Using Several Sensor's Data As Input 2.Using A Conceptual Modeling 3.Ambiguity Detection And Resolution 4.Archiving Tacks For Tracking Process	1.Data Alignment 2.Connotation Elicitation 3.Track Update And Reporting 4.Data Association
2	DAFNE (2011)	1.Using Distributed Fusion 2.Using Different Fusion Levels 3.Using Several Data Stores To Save Settings 4.Using Several Data Stores To Save Histories	1.Tracking 2.Classification 3.Situation Assessment 4.Threat Assessment
3	ORCA (2011)	1.Using Semi Supervised Learning 2.Using Customized Software 3.Creating Database 4.Visualization Interface	1.Feature Extractor 2.Learning 3.Analysis Interface 4.Categorization
4	TDFE (2012)	1.Flexible Architecture 2.Simple Structure 3.Scalability 4.Multi Sensor And Single Sensor Tracking	1.Track Correlation Fusion 2.Multi Sensor Tracker

Figure3 represents an overall view of this framework. In this schema, in addition to previously described conceptual modeling, pattern extraction, learning and prediction modules, there are several more modules. These modules are preprocessing, association, feature extraction and decision making which can be considered as common modules in the architecture of IIFE. Note that these common modules can be customized based on each application. Furthermore, the proposed IIFE framework is a very general model, and as we can see later, it can be implemented in more details for each special application.

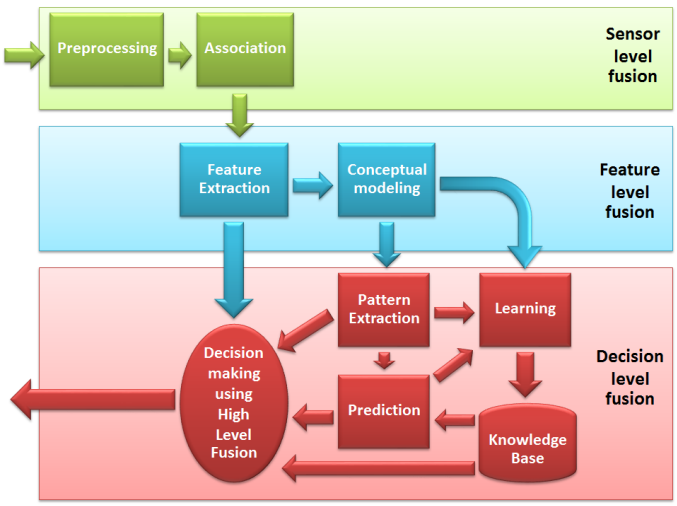

Figure 3. Overall view of IIFE framework.

Moreover, in this framework, the fusion is considered in three levels: sensor, feature and decision, providing the advantages of using different levels of information fusion. In sensor level, first a preprocessing operation over the incoming data and information will be done. Different operations such as data alignment can be considered in this step. Then the association

process which is a famous module specially in tracking applications will be done. In feature level, features will be extracted and conceptual modeling will be done. Finally in decision level, pattern extraction, learning, prediction and decision making will be done.

In addition, several requirements were considered during the extension of IIFE framework. Table2 represents some of these requirements and the advantages obtained using them.

Table 2- IIFE requirements and provided advantages

Row	Requirements	Advantages
1	Minimizing a priori knowledge	Can be used in highly uncertain environments and applications that have not suitable a priori knowledge
2	Scalability	Can be extended to be used in different applications
3	Conceptual modeling	Creating a higher level of perception an comprehension
4	Pattern extraction	Patter recognition and classification and using them for learning
5	Learning capability and knowledge base creation	Knowledge acquisition
6	Using acquired knowledge	Better prediction and estimation

5. PROPOSED CYBER SITUATIONAL AWARENESS MODEL

One of the main, basic and important elements for cyber situational awareness is cyber-attack tracking. Tracking in cyber domain can be defined as identifying the motion trajectory of all attackers in cyber space and up to now, mostly, the tracking is done by correlating IDS alerts (Mirheidari et al, 2013; Elshoush, and Osman, 2011) and generating attack graphs (Khaitan, and Raheja, 2011). According to this definition, would be assumed that cyber tracking is like traditional physical tracking. But, there are many important differences between cyber and physical tracking (Lipson, 2002). For instance, the motion in cyber space, unlike physical space, does not satisfy specific moving equations and originally the tracks in cyber space are based on some virtual concepts and they are very different from physical tracks.

Network configurations that are dynamically changing, is another problem in cyber-attack tracking. This problem causes inconsistency in cyber space and as a result, the tracking process faces to a serious challenge. From the other view, varying and extending data collection systems (sensors), caused data redundancy in this domain and thus resulted in facing a large amount of data and information which mainly contain high uncertainty. Therefore, intelligent information fusion engine (IIFE) can be used as a very useful means for cyber-attack tracking; just we need to extend some of its modules. For instance, extending general IIFE framework showed in Figure3 we got a more detailed IIFE for cyber-attack tracking. The extended IIFE for cyber-attack tracking which is showed in Figure4 is constructed from five different steps. At the first step, row data is collected from different sensors and a preprocessing will be done over them. Since different types of sensors are used in cyber space, so the data and information provided from them are very different. The data and information in this domain are mainly alerts and textual messages which have different formats. Therefore, for using this data and information, we need several processing steps to organize them in a proper format. In this step, three main operations will be done over the data and information: data alignment, feature extraction and concept extraction. Then in the next step called association, must be clear that messages

gathered from sensors are related to which tracks. Furthermore, it must be specified that how these messages must be associated in each tracks. In extended IIFE framework, this is done through three steps: correlation, track estimation and conceptual modeling. Correlation is identifying relations between entities and here this is done in three levels: data, track and concept. After identifying correlations in different levels, it must be specified that each of entities belongs to which of tracks. Also it must be specified whether in this step a new track is generated or not? And if a new track is generated, then which entity is related to it? And finally, a set of estimated tracks with related entities must be represented in a specialized format which this is done using conceptual modeling. Within tracking step, according to the information received from association step, existing knowledge and conceptual modeling, a low level fusion process will be done and real tracks will be identified and reported. In addition, according to existing attack tracks some patterns will be declared that could be used for current situation and the next attack track identification.

Using the expert capability of system in fusion process is one of the capabilities considered in proposed model. This expert capability can be raised through the time. In learning steps, based on existing parameters, the engine itself will learn the reported patterns automatically and will save the acquired knowledge in rule formats in knowledge base. For this reason, two separated knowledge base are considered, one for attack patterns and the other for attacker behavior patterns. Each of these knowledge bases, stores new patterns like a long time memory, and even uses saved patterns for learning new patterns.

In prediction step, based on generated knowledge and existing information, probabilistic attack tracks and feasible attacker behavior will be predicted, and then, a high level fusion will be done. This prediction can be used as either probabilistic knowledge or extra conceptual information in the next step.

According to what expressed in previous section, we can conclude that an IIFE is capable of representing several levels of situational awareness using different processes. In fact, at first it preprocesses the data and information and then identifies the relations among entities and does a sensor level fusion. Doing this, a proper perception from current situation will be generated. In the second step, different entities and the features of them are specified and a conceptual model is generated and a feature level fusion will be done. In this stage a considerable comprehension will be created from current situation. In the next step, existing patterns in the model will be identified and concurrently the operation of learning, prediction and decision fusion will be done. In learning stage, for each of existing pattern types in operation environment, a separate knowledge base will be considered. The learning operation will update knowledge bases by means of creating some rules, based on expert systems. Also a specific weight measure is considered for each rule. The value of these weights will be changed considering pattern repetition frequency. The prediction operation, according to the acquired knowledge and existing information, identifies that existence of which pattern is more probably. This, results in creating a proper projection from the next possible situations.

Figure4 represents an overall view of cyber situational awareness levels within an intelligent information engine (IIFE). According to this figure, cyber situational awareness levels, have a close relationship with each other and couldn't be separated.

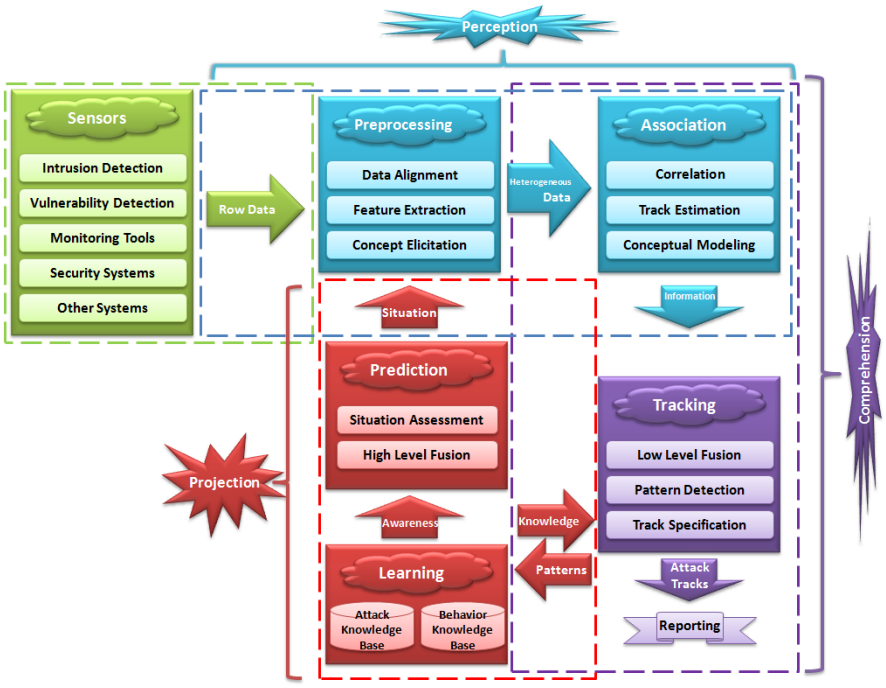

Figure 4. Situational awareness levels within IIFE.

From the other point of view, these cyber situational awareness levels, like a closed loop showed in Figure5, are continuously updating during the time.

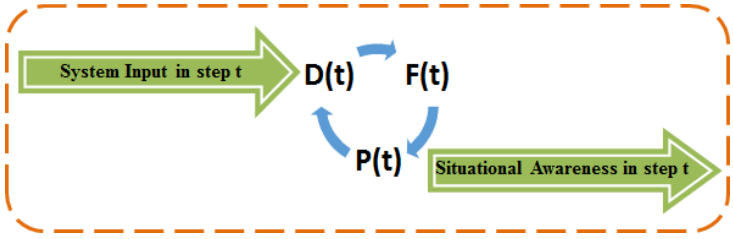

Figure 5. The relationship of situational awareness levels within IIFE.

In other words, if we show perception, comprehension and projection, respectively, with D, F and P; then the following relation will be satisfied:

$$\text{Input}(t)+P(t-1) \rightarrow D(t) \rightarrow F(t) \rightarrow P(t) \quad (1)$$

Thus, situational awareness within IIFE is a continuous process, created during the time, and will be improved, proportional to the learning operation and completing knowledge bases. Now regarding what was mentioned up to now, we can propose a new cyber situational awareness model that is constructed from an intelligent information fusion engine. To do this, we just need to add some more modules to construct final level of situational awareness i.e. resolution level. Although, different aspects could be considered for this work; Here, we only considered capability, opportunity and intention. Figure6 represents the proposed cyber situational awareness model.

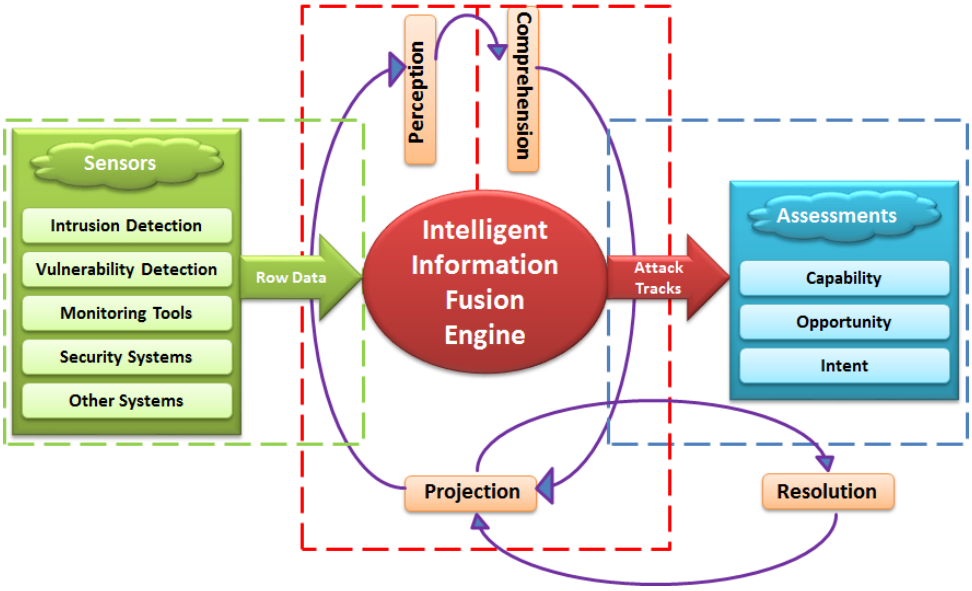

Figure 6. Cyber situational awareness model using an IIFE

As we can see in this figure, situational awareness levels in the proposed model, against previous models, does not have a hierarchical structure and like a continuous chain thought the time leads to increased knowledge and improved situation awareness.

5. CONCLUSIONS

One of the most novel topics in the information fusion domain which got a great attention recently, is the information fusion engine. An information fusion engine is composed of different means, techniques and levels of information fusion and uses several modules to perform its commission. In fact, an information fusion engine, like a uniform process, drives all operations needed to fusing data and information and finally provides a higher abstract level of information. This abstract level of information, increases users and systems perception and comprehension, in their own observable environments, and as a result, along with situational awareness, improves the decision making process.

An intelligent information fusion engine (IIFE), provides knowledge acquisition capability for information fusion, by mens of continuous learning and expert systems concepts. Then, information fusion engine is converted to an intelligent means which represents several capabilities such as conceptual modeling, pattern extraction, learning and prediction. However, perception, comprehension and projection levels of situational awareness are formed within IIFE and leads to improvement of cyber situational awareness.

In this paper, using the concept of IIFE, a novel model is proposed for situational awareness. The proposed model, continuously through the time, results in upgrading the situational awareness. The proposed model is very flexible and simply can be used in a variety of domains.

There are many researches that should be done to continue this activity. For example, the IIFE framework can be extended for other applications more than the only cyber application. Also, a network of distributed IIFEs can be considered for each application which concurrently can improve the situational awareness from different aspects. Moreover, embedding assessment related modules within the IIFE can be resulted in a more general framework for IIFE which

contains all of the situational awareness levels. We are now working on this model, and it will be reported as soon as possible.

REFERENCES

[1] Adams, M. J., Tenney, Y. J., & Pew, R. W. (1995). Situation awareness and the cognitive management of complex systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 37(1), 85-104.

[2] Barford, P., Dacier, M., Dietterich, T. G., Fredrikson, M., Giffin, J., Jajodia, S. ... & Yen, J. (2010). Cyber SA: Situational awareness for cyber defense. In *Cyber Situational Awareness* (pp. 3-13). Springer US.

[3] BERINGER, D., & HANCOCK, P. (1989). Exploring situational awareness- A review and the effects of stress on rectilinear normalization ((aircraft pilot performance)). In *International Symposium on Aviation Psychology, 5th, Columbus, OH* (pp. 646-651).

[4] Ditzel, M., van den Broek, S., Hanckmann, P., & van Iersel, M. (2011). DAFNE–a distributed and adaptive fusion engine. In *Hybrid Artificial Intelligent Systems* (pp. 100-109). Springer Berlin Heidelberg.

[5] Elshoush, H. T., & Osman, I. M. (2011). Alert correlation in collaborative intelligent intrusion detection systems—A survey. *Applied Soft Computing*, 11(7), 4349-4365.

[6] Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 37(1), 32-64.

[7] Franke, U., & Brynielsson, J. (2014). Cyber situational awareness–A systematic review of the literature. *Computers & Security*, 46, 18-31.

[8] Friedberg, I., Skopik, F., & Fiedler, R. (2015). Cyber situational awareness through network anomaly detection: state of the art and new approaches. *E&I Elektrotechnik und Informationstechnik*, 132(2), 101-105.

[9] Gundersen, O. E. (2013). Situational awareness in context. In *Modeling and Using Context* (pp. 274-287). Springer Berlin Heidelberg.

[10] Khaitan, S., & Raheja, S. (2011). Finding optimal attack path using attack graphs: a survey. *International Journal of Soft Computing and Engineering*, 1(3), 2231-2307.

[11] Kott, A., Wang, C., & Erbacher, R. (2014). *Cyber Defense and Situational Awareness*. Springer.

[12] Lipson, H. F. (2002). *Tracking and tracing cyber-attacks: Technical challenges and global policy issues* (No. CMU/SEI-2002-SR-009). CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

[13] Liu, J., Feng, X. W., Li, J., & Wang, D. X. (2013). Cyber Security Situation Awareness Based on Data Mining. *Advanced Materials Research*, *756*, 4336-4342.

[14] McGuinness, B., & Foy, L. (2000, October). A subjective measure of SA: the Crew Awareness Rating Scale (CARS). In *Proceedings of the first human performance, situation awareness, and automation conference, Savannah, Georgia*.

[15] Mirheidari, S. A., Arshad, S., & Jalili, R. (2013). Alert Correlation Algorithms: A Survey and Taxonomy. In *Cyberspace Safety and Security* (pp. 183-197). Springer International Publishing.

[16] ORCA Development Team. (2011). ORCA Fusion Engine, *http://orca.ornl.gov/Fusion_Engine.html.*

[17] Saab group. (2012, January). Track data fusion engine adaptable to your demands, Security and Defense Solutions, Sweden. *http://saab.com/air/air-c4i-solutions/data-information-fusion/Track-Data-Fusion-Engine*.

[18] Salerno, J. (2008, June). Measuring situation assessment performance through the activities of interest score. In *Information Fusion, 2008 11th International Conference on* (pp. 1-8). IEEE.

[19] Sarter, N. B., & Woods, D. D. (1991). Situation awareness: A critical but ill-defined phenomenon. *The International Journal of Aviation Psychology*, 1(1), 45-57.

[20] Stotz, A., & Sudit, M. (2007, July). Information fusion engine for real-time decision-making (INFERD): A perceptual system for cyber-attack tracking. In *Information Fusion, 2007 10th International Conference on* (pp. 1-8). IEEE.

[21] Tadda, G. P., & Salerno, J. S. (2010). Overview of cyber situation awareness. In *Cyber situational awareness* (pp. 15-35). Springer US.

[22] Yu, W., Xu, G., Chen, Z., & Moulema, P. (2013, October). A cloud computing based architecture for cyber security situation awareness. In *Communications and Network Security (CNS), 2013 IEEE Conference on* (pp. 488-492). IEEE.