SITUATION AWARENESS IN CRITICAL INFRASTRUCTURES

Abate Vincenza [(a)], Adacher Ludovica [(b)], Pascucci Federica [(c)]

Dip. di Informatica e Automazione
Università degli Studi Roma Tre
Via della Vasca Navale, 79
00146 Roma, Italy

(a) abate@dia.uniroma3.it, (b) adacher@dia.uniroma3.it, (c) pascucci@dia.uniroma3.it

ABSTRACT
The present paper provides a comprehensive review about the main concepts on situation awareness for critical infrastructure. The issues related to models and architectures for data fusion and situation awareness are reported in the framework of Critical Infrastructure Protection.
Both data fusion and situation swareness have been developed in Critical Infrastructure field to merge and integrate data from several heterogeneous sensors. Since Critical Infrastructures are interconnected, the integration of sensor data is mandatory to avoid or mitigate risk of cascading and domino effects. This integration requires the cooperative signal processing of a federation of critical infrastructures.

Keywords: Situation awareness, Critical Infrastructure Protection, Distributed DF, Multi Agent System

1. INTRODUCTION

Situational Awareness (SA) refers to the ability to observe, assimilate and make predictions about relevant elements and attributes of an environment in order to provide a robust survival. SA points at *knowing what is going on around you*. In this perspective, the key idea is to exploit the knowledge acquired in the past to identify, analyze and understand the actual situation. Moreover Sa is able to forecast the evolution of a phenomena and evaluate risks. The ability to predict or model and visualize how the circumstances of a pending or evolving emergency may change over specific times allows emergency managers to allocate resources to priority areas before further damage or loss of life occurs. An effective management of crisis is essential when the emergency occur on a Critical Infrastructure (CI).

Societies are increasingly dependent on a set of products and services including the CIs, i.e. *an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions*. CIs comprise essential components of industry, energy generation, security, defense, transportation and public services. In this sense, an unexpected event on CI has serious consequences to citizens and the society as a whole. The emergency management on a CI should have full situational awareness on the state of CI itself and on the responsibilities to protect them. The main concern with the CI is their growing complexity. This is partially caused by their growing interconnectedness, leading to infrastructural interdependencies with unpredictable consequences and risks. To this end, the integration of sensor data to avoid or mitigate risk due to cascading and domino effects is mandatory. This *process of combining data to refine state estimates and predictions* is known as Data Fusion (DF).

The models and architectures to describe the SA context are recalled in Sec. 2. Section 3 presents a brief background on several computational intelligence techniques applied in CIs domain. A survey on principal concepts and techniques for SA in CIs are also reported. Finally, some concluding remarks are drawn.

2. MODELS AND ARCHITECTURE FOR SITUATION AWARENESS

To describe DF systems, we first highlight the main differences between (Elmenreich 2001):

- *Models* are the description of a set of processes. This set of processes should be undertaken before the system may be regarded as fully operational.
- *Architectures* are the physical structure of the system. Particular attention is devoted to the implementation for information and data communication.
- *Frameworks* are a set of axioms and a reasoning system for manipulating entities. Examples of frameworks currently used in DF are probabilistic reasoning, possibility reasoning and evidential reasoning

2.1. Models

In the following some models proposed in literature are reported (Durrant-Whyte and Henderson 2008).

The Intelligence Cycle involves both information processing and information fusion. It is a conceptual model showing how intelligence operations are conducted.

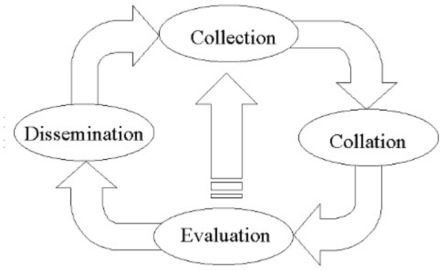

Figure 1: The Intelligence Cycle Model

It consists of four phases:

- *Collection* assets how electronic sensors or human derived sources are deployed to obtain raw intelligence data.
- *Collation* describes how associated intelligence reports are correlated and brought together.
- *Evaluation* explains how the collated intelligence reports are fused and analyzed.
- *Dissemination* clarifies how the fused intelligence is distributed to the users and who use the information to make decisions regarding their own actions and the required deployment of further collection assets.

The Joint Directors of Laboratories Model (JDL) is a layered hierarchical model that identifies fusion processes, processing functions, and processing techniques to accomplish the primary DF functions (Hall and Llinas 2008).

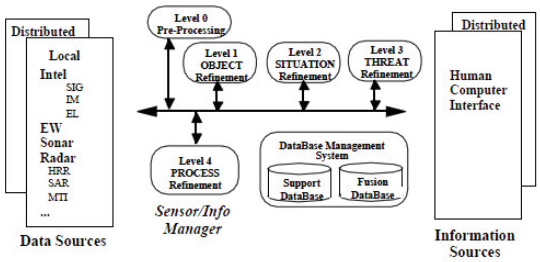

Figure 2: The Joint Directors of Laboratories (JDL) Model

The elements of the model are described in the following:

- *Sources* provide information from a variety of data sources, like sensors, a priori information, databases, human input.
- *Source preprocessing (Level 0):* The task of this element is to reduce the processing load of the fusion processes by prescreening and allocating data to appropriate processes.
- *Object refinement (Level 1):* This level performs data alignment (transformation of data to a consistent reference frame and units), association (using correlation methods), tracking actual and future positions of objects, and identification using classification methods.
- *Situation refinement (Level 2):* The situation refinement attempts to find a contextual description of the relationship between objects and observed events.
- *Threat refinement (Level 3):* This processing level tries to draw inferences about vulnerabilities and opportunities for operation on the basis of a priori knowledge and predictions about the future situation.
- *Process refinement (Level 4):* Level 4 is a meta process that monitors system performance and reallocates sensor and sources to achieve particular mission goals.
- *Database management system:* The task of the database management system is to monitor, evaluate, add, update, and provide information for the fusion processes.
- *Man-machine interaction:* This part provides an interface for human input and communication of fusion results to operators and users.

The Boyd control cycle or OODA loop possesses four phases as shown in Figure 3 (Shahbazian, Blodgett, and Labbé 2001).

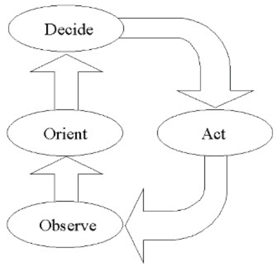

Figure 3: The Boyd (or OODA) Loop

- *Observe:* This stage is broadly comparable to source pre-processing in the JDL model (level 0) and part of the collection phase of the intelligence cycle.
- *Orient:* This stage encompasses the functions of the levels 1, 2 and 3 of the JDL model. It also includes the structured elements of collection and the collation phases of the intelligence cycle.
- *Act:* has no direct analogue in the JDL model and is the only model that explicitly closes the loop by taking account of the effect of decisions in the real world.
- *Decide:* This stage includes JDL level 4 (process refinement and resource management) and the dissemination activities of the intelligence community. It also inclues planning.

A representation of *Waterfall Model* is shown in Fig. 4. It can be seen from this figure that the flow of data operates from the data level to the decision making level. The sensor system is continuously updated with feedback information arriving from the decision-making module. The feedback element advises the multi-sensor system on re-calibration, re-configuration and data gathering aspects

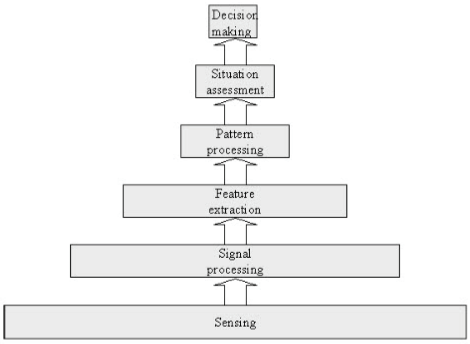

Figure 4: The Waterfall DF Process Model

The Dasaranthy Model is based on fusion functions rather than tasks and it may therefore be incorporated in every fusion activities. Many researchers have identified the three main levels of abstraction during the DF process as being:

- *Decisions* symbols or belief values
- *Features* or intermediate-level information
- *Data* or more specifically sensor data

Bedworth and O'Brien have presented the *Omnibus Model in 1999*. Figure 5 depicts the architecture of the Omnibus Model. It defines a process order and it makes explicit the cyclic nature. The model is intended to be used multiple times in the same application recursively at two different levels of abstraction. First, the model is used to characterize and structure the overall system. Second, the same structure is used to model the single subtasks of the system.

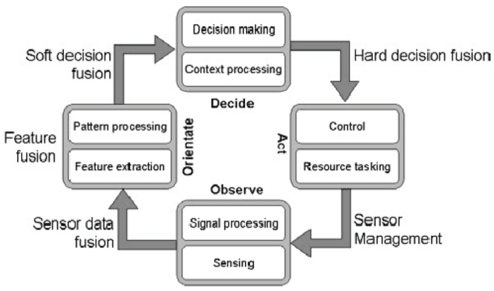

Figure 5: The Omnibus Model: A Unified DF Process Model

The Extendend OODA Model for DF systems developed at Lockheed Martin Canada (LMC) synthesizes some of the useful features of the models described previously, moreover provides a mechanism for multiple concurrent and potentially interacting DF processes. The details of the Extended OODA model are depicted in Fig. 6.

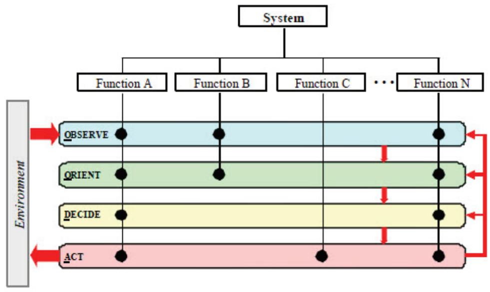

Figure 6: The Extended OODA Model for DF

A system using DF for decision-making is decomposed into a meaningful set of high-level functions (Figure 6 shows a set of N functions). These functions are examined in terms of the *Observe*, *Orient*, *Decide*, and *Act* decision loop that constitute the OODA model.

Endsley's Model defines SA as a state of knowledge resulting from a process. Situation Awareness is formally defined as *the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and projection of their status in the near future*. The model proposed by Endsley is graphically described as follows:

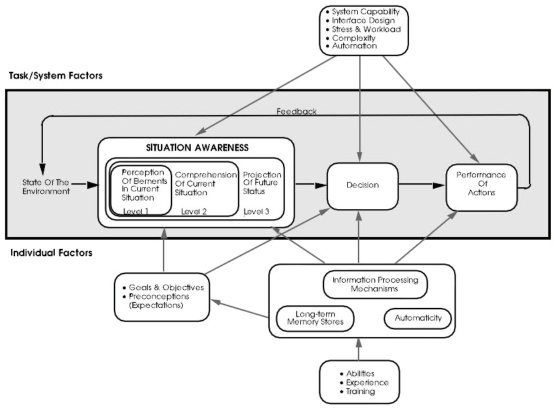

Figure 7: Endsley's Situation Awareness Model

The core portion follows Endsley's proposition that SA has three levels of mental representation:

- *Level 1 SA - Perception of the elements in the environment.* The first step in achieving SA is the perception of the status, attributes, and dynamics of relevant elements in the environment.
- *Level 2 SA - Comprehension of the current situation.* Comprehension of the situation is based on a synthesis of disjointed Level 1 elements.
- *Level 3 SA - Projection of future status* is the ability to project the future actions of the elements in the environment, at least in the

near future. It is the third and highest level of situation awareness.

The Boyd Control Loop was first used for modeling the military command process, but has since been widely used for DF. The Boyd and JDL models show distinct similarities, although the Boyd model makes the iterative nature of the problem more explicit.

The Waterfall Model emphasizes the processing functions on the lower levels. The stages relate to the levels 0, 1, 2, and 3 of the JDL model as follows: sensing and signal processing correspond to source preprocessing (level 0), feature extraction and pattern processing match object refinement (level 1), situation assessment is similar to situation refinement (level 2), and decision making corresponds to threat refinement (level 3).

In literature the JDL model is adopted to solve the SA problem. In fact, the JDL model is a suitable manner to model, describe and understand various activities in the SA community. Although the JDL provides a functional model for the DF process, it does not model it from a human perspective. Endsley provides an alternative to the JDL model that addresses SA from this viewpoint.

2.1.1. Architectures

Different architecture has been proposed in literature for DF and SA (Salerno 2001).

Centralized DF (CDF) is characterized by a hierarchy of nodes: all information is passed up the hierarchy to a centralized fusion node. An example of this kind of architecture is given in the Fig. 8.

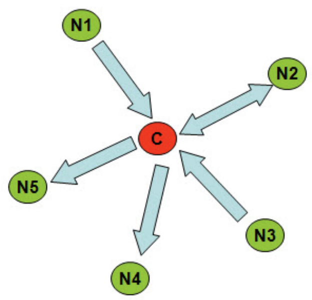

Figure 8: An Example of a Centralized DF system. The central node, C, receives information from three sensor nodes, N1, N2 and N3. It fuses information about the tracking object, thereafter it propagates back the results of DF to every node (including N2).

Unfortunately, this kind of architecture presents several disadvantages. For these reasons it is less used. Indeed,

- It imposes a latency on the availability of the fused picture at the lower level nodes;
- It also imposes a single point of failure in the system: if the fusion node is lost or loses communications, the overall situation awareness of the system is compromised;
- It limits the ability of the individual participants to operate independently or as part of a much smaller group;
- It requires significant communications bandwidth.

Decentralized DF (DDF) architectures are fully decentralized structures, without any central processor and/or common communication system. In this architecture, nodes can operate in a fully autonomous fashion, only coordinating through the anonymous communication information. Referring to Fig. 9, a DDF system consists of a network of agents, each one having its own processing capabilities, not requiring any central fusion or central communication facility.

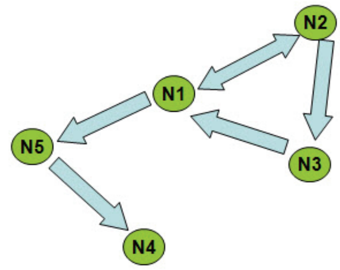

Figure 9: An example of Decentralized DF System. The agents communicate information among each other

A DDF system is characterized by three constraints:

1. There is no single central fusion center;
2. There is no common communication facility;
3. Sensor nodes do not have any global knowledge of sensor network topology.

The above constraints provide a number of important characteristics for DDF systems.

Hierarchical DF (HDF) architecture is a hybrid architecture mixing together the centralized and decentralized architectures.

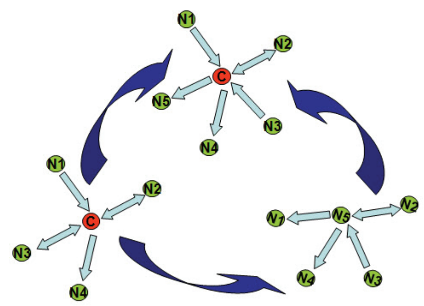

Figure 10: An Example of Hierarchical DF System. The agents are grouped in cliques and they share information about the environment with their neighbors. Communication with other groups ensures the spread of knowledge within all nodes.

In the hierarchical architecture there are often several hierarchical levels where the top level contains a

Proceedings of the International Defense and Homeland Security Simulation Workshop 2012
ISBN 978-88-97999-08-9; Bruzzone, Buck, Longo, Sokolowski and Sottilare Eds.

single centralized fusion node and last level is made up of several decentralized (local) fusion nodes. Each local fusion node receives inputs either from a small group of sensors or from an individual sensor. The hierarchical approach has been employed in a number of DF systems and has resulted in a variety of useful algorithms for combining information at different levels of a hierarchical structure.

3. SITUATION AWARENESS IN INTERDEPENDENT SYSTEMS

Modern CI systems utilize intelligent embedded devices, communication capability, and distributed computing to streamline and fortify their operation (Kokar, Matheus and Baclawski 2009). Identifying, understanding, and analyzing such interdependencies are significant challenges (Pederson, Dudenhoeffer, Hartley and Permann 2006; Rigole and Deconinck, 2006). These challenges are greatly magnified by the breadth and complexity of transnational critical infrastructures. Examples include smart grids and intelligent water distribution networks. The increasing prevalence and complexity of this intelligent control brings its dependability into question. In this section we present several of the most established methodologies for the aggregation of multiple information sources necessary to describe a situational awareness problem for CI system.

Evidence Theory: Dempster-Shafer Theory (DST) is a mathematical theory of evidence. In a finite discrete space, Dempster-Shafer theory can be interpreted as a generalization of probability theory where probabilities are assigned to sets as opposed to mutually exclusive singletons. In traditional probability theory, evidence is associated with only one possible event. It has uncertainty management and inference mechanisms analogous to our human reasoning process.

It is based on two ideas: the idea of obtaining degrees of belief for one question from subjective probabilities for a related question, and Dempster's rule for combining such degrees of belief when they are based on independent items of evidence (Rakowsky 2007). Principally we can define three important functions in Dempster-Shafer theory:

- *the basic probability assignment function (bpa)* defines a mapping m of the power set to the interval between 0 and 1, where the bpa of the null set is 0 and the summation of the bpa's of all the subsets of the power set is 1.

$$m : P(X) \to [0,1]$$

$$m(\emptyset) = 0$$

$$\sum_{A \in P(X)} m(A) = 1$$

where $P(X)$ represents the power set of X, ∅ is the null set, and A is a set in the power set ($A \in P(X)$).

- *the Belief function (Bel)* is defined as the sum of all the basic probability assignments of the proper subsets (B) of the set of interest (A) ($B \subseteq A$)

$$Bel(A) = \sum_{B|B \subseteq A} m(B)$$

- *the Plausibility function (Pl)* is the sum of all the basic probability assignments of the sets (B) that intersect the set of interest (A) ($B \cap A \neq \emptyset$)

$$Pl(A) = \sum_{B|B \cap A \neq \emptyset} m(B)$$

Hidden Markov Model is a technique suitable for situation awareness (Thyagaraju 2010). SA is a process that comes to a conclusion based on the events that take place over a period of time across a wide area. Hence, since the situational awareness is achieved based on the sequence of events observed, Hidden Markov model (HMM) is ideally suited. The formal definition of a HMM consists of a compact notation to indicate the complete parameter set of the model:

$$\lambda = (A, B, \pi)$$

where:

$A=\{a_{ij}\}$ is the transition array, storing the probability of state j following state i

$$a_{ij} = P(q_t = s_j \mid q_{t-1} = s_i), \quad 1 \le i \quad , j \le N$$

$B=\{b_j(k)\}$ is the observation array, storing the probability of observation k being produced from the state j, independent of t

$$b_j(k) = P(x_t = v_k \mid q_t = s_j), \quad 1 \le j \le N, \quad 1 \le k \le M$$

$\pi=\pi_i$ is the initial state distribution

$$\pi_i = P(q_1 = s_i), \quad 1 \le i \le N,$$

The model il based on two assumptions:

Markov assumption: the current state is dependent only on the previous state, this represents the memory of the model:

$P(q_t \mid q_1^{t-1}) = P(q_t \mid q_{t-1})$

Independence assumption: the output observation at time t is dependent only on the current state, it is independent of previous observations and states:

$P(o_t \mid o_1^{t-1}, q_1^t) = P(o_t \mid q_t)$

There are three fundamental problems that we can solve using HMMs:

Evaluation: Given the observation sequence $O=O_1 O_2 \cdots O_T$ and a model $\lambda=(A,B,\pi)$, how do we efficiently compute $P(O|\lambda)$, the probability of the observation sequence?

Decoding: Given the observation sequence $O=O_1 O_2 \cdots O_T$ and the model $\lambda=(A,B,\pi)$, how do we choose a corresponding optimal state sequence $Q=q_1 q_2 \cdots q_T$ (i.e., the best "explains" the observations)?

Learning: How to maximize $P(O|\lambda)$ by the model parameter $\lambda=(A,B,\pi)$ (transitional probabilities, observation probabilities, initial probabilities))?

Artificial Neural Network (ANN) constitutes a well-established computational model, which is inspired by the biological neural system (Yao and Islam, 2008). A set of *neurons* or *processing elements,* interconnected by a network with a certain topology, has limited or local computation capability. The underlying idea is to train the network by a suitable set of known inputs and associated outputs. Thereafter, the trained network, in a "black-box" perspective, evaluates the function. Formally, an Artificial Neural Network can be defined as follow:

Definition 1 *ANN is a network of n interconnected neurons described by a directed graph* $\mathcal{G}=\{\mathcal{V},\xi,\mathcal{W}\}$ *where* $\mathcal{V}=\{1,\cdots,n\}$ *is the set of nodes/neurons and* $\xi\xi=\{e_{ij}\}\in\mathcal{V}\times\mathcal{V}$ *is the set of links; the weight of the link* e_{ij} *is described by the entry* w_{ij} *of the adjacency matrix* $\mathcal{W}$.

The structure of an ANN is typically composed by four sets:

- The set of processing units or neurons;
- The weighted links between the processing units;
- The activation rule, that converts the neuron's inputs into its outputs;
- The learning mechanisms to adjust the weights.

The focus is on the learning procedure used to train the ANN. Several methodologies are used, according to a supervised or unsupervised learning approach.

Agent-based Modeling A new emerging modeling paradigms is Multi Agent Systems (Dianne, Barton and Stamber 2000). These agent-based systems try to tackle a variety of complex problems using a fully distributed, bottom-up approach using a society of autonomous, interconnected, intelligent agents. Agent-based models are frequently used in interdependency and infrastructure analysis. Infrastructure or physical components are modeled as agents, allowing analysis of the operational characteristics and physical states of infrastructure. The agents are able to capture rational and non-rational behavior. We can define an agent as

Definition 2 *An autonomous agent is a system situated within and a part of an environment that senses that environment and acts on it, over time, in pursuit of its own agenda and so as to affect what it senses in the future.*

A CI is characterized by its location, its behaviour, interaction capabilities and its internal state. Then a CI can be modeled as an autonomous agent. The system composed by interdependent CI can be modeled as interacting agents cooperating and/or competing to realize a common or an individual goal.

Interactions between agents are the following:

- Agents have the ability to co-operate or to act against the interest of other agents
- Agents can interact whilst having different level of information about each other ;
- Agents may interact in singular encounters, or their interactions and negotiations may take place over multiple rounds of engagement;
- Decisions and actions of agents can be reached simultaneously, or can occur sequentially.

4. CONCLUSION

As we have seen there is a growing interest in critical infrastructure protection, situation awareness, and the risks related to the increasing interconnection of these infrastructures. To assess these risks new modeling and simulation tools are needed; many modeling frameworks have been proposed in the recent years. This paper proposes a descriptive survey on this great variety of approaches, considering both high-level macroscopic models and microscopic models. These two different perspectives meet in the agent-based approach that seems to be a promising technique, even if its practical use in the field of critical infrastructures is yet to be proven. In the field of SA for CI the techniques adopted should be considering the "man in the loop" problem, by modeling reasoning about ignorance, spatial-temporal reasoning capabilities, and social ability for acquiring information, hence HMM, ANN, and Evidence Theory seems to be suitable approaches.

According with these remarks, future work will address a theoretical foundation of situation awareness and its measurement based on dynamic decision networks and information value theory.

REFERENCES

Dianne, C. Barton, K., Stamber, L., 2000. An Agent-Based Microsimulation of Critical Infrastructure Systems, *Proceedings of the 8th International Energy Forum*, Las Vegas.

Durrant-Whyte, H.F., Henderson, T.C., 2008. Multisensor Data Fusion. In *Springer Handbook of Robotics*, Siciliano, B, and Kathib H. Eds, 585-610.

Elmenreich, W., 2001. *An Introduction to Sensor Fusion Research.* Report 47/2001, Institut fur Technische Informatik.

Hall, D.L., Llinas, J., 2008. *Handbook of Multisensor Data Fusion*, CRC press. Lopez, J., Setola, R., Wolthusen, S.D., (Eds), 2012. *Critical Infrastructure Protection, Information Infrastructure Models,* Lecture Notes in Computer Science, Analysis and Defence, Springer.

Kokar, M.M., Matheus, C.J., Baclawski, K., 2009. Ontology-based situation awareness. *Inf. Fusion*, 10(1), 83-98.

Pederson, P., Dudenhoeffer, D., Hartley, S., Permann, M., 2006. *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*. Rep.No INL/EXT-06-11464, Critical Infrastructure Protection Division, INEEL.

Rakowsky, U., 2007. *Fundamentals of Dempster-Shafer theory and its applications to system safety and reliabilitymodeling*. RTA, No. 3-4.

Rigole, T., Deconinck, G., 2006. A Survey on Modeling and Simulation of Interdependent Critical Infrastructures, *Proceeding of the 3rd IEEE BENELUX Young Researchers Symposium in Electrical Power Engineering*, Ghent, Belgium.

Salerno, J., 2002. Information Fusion: A High-level Architecture Overview*, Proceedings of the Fusion-2002*, pp. 680-686, Annapolis, MD.

Shahbazian, E., Blodgett, D.E., Labbé, P., 2001. The Extended OODA Model for Data Fusion Systems. *Proceedings of the 4th International Conference on Information Fusion*, pp.1-19, Montréal.

Thyagaraju, D., 2010. *Hidden Markov Model as a Framework for Situational Awareness, Sensor Fusion and its Application*s, Ciza Thomas (Ed.).

Yao, X., Islam, Md.M., 2008. Evolving artificial neural network ensembles, *IEEE Computational Intelligence Magazine*, 3(1), 31-42.