Technology Intercepts for Cyber Security applied to Critical Infrastructures

Mario LA MANNA
Evoelectronics
Rome, Italy

ABSTRACT

The implementation of a cyber security system for critical infrastructures requires the extensive use and the targeted application of the most modern computer and communication technologies. In fact, cyber crime, as many other illegal activities, has gained momentum from the latest expansion and power of the Internet and from the widespread use of the sophisticated tools used in the networks, especially social networks. Combating cyber crime needs the same synergy between human and machine technologies as done by cyberspace hackers to attack their objectives. This paper aims to making a review of these technologies and drawing the guidelines for an efficient design of a cyber security system, with reference to the defense of critical infrastructures.

Keywords: Cyber space, cyber security, cyber crime, environment monitoring, critical infrastructures.

1. INTRODUCTION

A cyber security system for critical infrastructures (Fig. 1) is composed of the following subsystems: a) Sensor subsystem, which collects data coming from the external environment; b) Data and Information Fusion subsystem, which merges data collected by sensors and data and information coming from external intelligence sources; c) Human Agent in the Loop, which performs operations by means of a human operator in the decision loop; d) Core Processor, which combines all the information produced by the previous subsystems with internal data extracted by statistical learning, on the basis of the historical database.

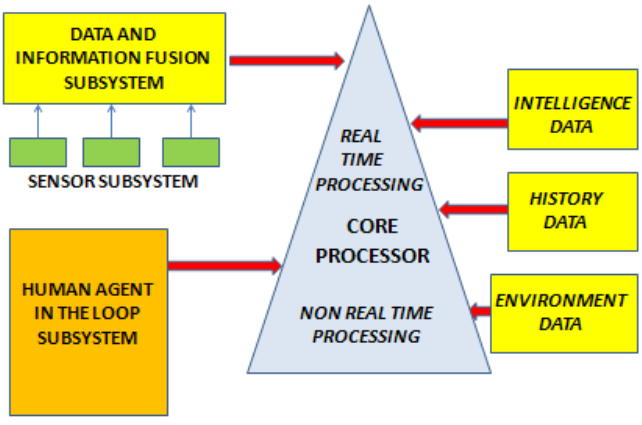

Fig. 1: Cyber Security Architecture for Critical Infrastructures.

The system has to cope with the heterogeneity of the data and information produced by the system itself, those collected by the monitoring tools and secure information coming from different sources. Typically, monitoring data are derived from different types of sensing units, while secure information comes from intelligent external sources, human in the loop agents and internal system intelligence. Most of the data and information for security travel through Internet, by monitoring and analysing specific messages exchanged through the social networks,

In order to apply the proposed architecture to real cases, some key technologies have to be inserted inside the system. The next sections will discuss the main features of these technologies, relying on the work carried out by a large community of researchers and entrepreneurs. The aim of the paper is to give an original contribution in analysing their intercepts for cyber security applied to critical infrastructures.

2. KEY CYBER SECURITY TECHNOLOGIES

Many of the efforts to prevent cyber crime have been put in predicting who might commit illegal actions and to take suitable measures to prevent these actions before they are put into effect. To this end, for example, the high volume of data produced by social networks has been complemented with other data collected by focused crime prevention campaigns, promoted by private and public organizations. Moreover, further sets of live data coming from different sources, based on sensor networks, have been used for detection and geolocalization of cyber criminals. It has been demonstrated that the synergy between different sources of data can help reconstruct a sound picture of a cyber crime scenario.

A correct design of a cyber security system requires the involvement of five key technologies (Fig.2). Regarding these technologies, this paper does not want to introduce any novelty with respect to the state of the art. The original contribution of the paper is instead focused on tailoring these technologies to the applications for the defense of critical infrastructures.

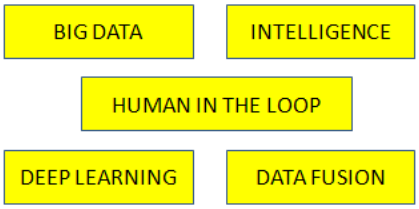

Fig. 2: Key Technologies for Cyber Security.

3. BIG DATA

Big Data [9] represents the information assets characterized by high volume and other specific parameters, so that an ad-hoc technology and management methods are required to transform these data into information to be used by real applications. In particular, Big Data (Fig.3) are characterized by four essential capabilities, namely: Volume, Variety, Velocity and Value.

Volume is connected to the types of data, generated from different heterogeneous sources, e.g. sensors, communication devices, etc. Gathering large amounts of data allows to discover hidden information and patterns through the detailed analysis of the available data. The examination of a high number of real cases can derive important outputs, useful to prevent the possible occurrence of future cyber crime actions. The results obtainable by the use of data analysis techniques are comparable to those collected from the methodologies to predict the human behaviour patterns.

Variety is an attribute which refers to the different types of data collected by sensors or other devices, or extracted from communications occurring, for example, on the social networks. These types of data include images, video, text, audio and data sets, in different formats and with different structures.

Velocity is about the speed of data transfer. This speed depends on the data sources, which produce the data themselves and on the data treatment, e.g. expansion or compression, by means of the data processing facilities.

Value can be considered the most important characteristics of Big Data in our context, as it is related to the process of discovering hidden features inside large data sets of different types, coming from heterogeneous sources.

The basic methodologies which can be used when designing a cyber security system rely on the previous four capabilities of Big Data. In particular, these methodologies work on the data contained in the messages exchanged by the users of social networks. The same methodologies aim to extract the "metadata", which can be considered a kind of compressed data, containing the useful information carried by the data themselves. Metadata refer, as an example, to the users' language and models, to their geographical location, their attitudes and goals, etc. The metadata, suitably organized and compared, can be a valid tool to forecast the human behavior and the possible occurrence of future criminal actions. Moreover, when the geopolitical information is also present in the analysed data, the physical allocation of cyber crime can be associated to the forecast. When the strength of the four mentioned capabilities of Big Data increases, more significant metadata can be extracted and more accurate can be the forecast regarding future possible cyber crimes.

The use of metadata can be quite effective in discovering the high number of cyber reiterated attacks, happening at a short distance in time. A typical case happened in May 2015, when hackers, believed to be associated with some foreign government, directed their attack against the US Office of Personnel Management.

Fig. 3: Key Technology 1: Big Data.

Only two months later, another cyber attack was directed against the Pentagon, shutting down the unclassified email system for the Joint Staff for nearly two weeks [15].

4. INTELLIGENCE

Intelligence [10] (Fig. 4) refers to different processes, which have the goal to collect, process and interpret information and knowledge relative to a certain topic of interest. When this topic consists of the knowledge of a possible adversary element and the goal is to activate suitable defense actions against possible attacks from that element, the above processes are based both on brain power and experience and on artificial intelligence tools. Artificial intelligence and cognitive computing technologies can hold the key to aggregating and analyzing the data belonging to cyber security strategies and turning this process into actionable intelligence**.** In fact, the rapid expansion of applications, cloud services and mobile devices has brought the focus of cyber attacks from the network and endpoint protection to a more extended attack surface. This wider and deeper attack surface is adding problems in how to manage the volume, velocity and complexity of data to be controlled and critical points to be defended. A traditional approach, based only on human actions, is not any longer conceivable.

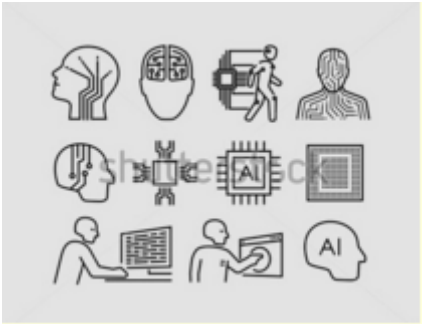

Fig. 4: Key Technology 2: Intelligence.

Artificial intelligence and Machine Learning constitute therefore a strongly needed force multiplier to manage such a complex environment. Additionally, the use of human interactive machine tools can automate the aggregation and analysis of different data and better identify security risks. The efficient coupling of human intelligence and machine intelligence is paramount in cyber security, like in many other areas. In fact, the automated process can produce several benefits in pro-active security incident detection and notification. However, while Machine Learning can help reduce risk and provide fast detection of attacks, it is not able to autonomously protect from cyber crime. In fact, very often, unsupervised Machine Learning contributes to the production of false positives and alerts, resulting in continuous alert activity and decrease of attention. As a consequence, while we have reached a threshold whereby the high volume of security data cannot be handled by human intelligence only, at the same time it becomes risky to delegate all the process of security management to the automated processes. This has led to the conception of a kind of Human Interactive Machine Learning, as a mechanism which complements computer science with the human cognition processes. Human Interactive Machine Learning systems analyze security data and correlate these data with external threat data, in order to trigger human intelligence in discovering anomalies in the analyzed data. Humans then provide feedback to the machine learning system by tagging the most relevant threats. The automated system can then learn from these inputs and adapts its monitoring and analysis based on human cognition. In this way, the Machine Learning system can optimize the likelihood of finding real cyber threats and minimizing false positives. In addition, enlisting machine learning to do the heavy lifting in first line security data assessment enables humans to focus on more advanced investigations of threats rather than performing tactical data crunching. This meeting of the minds, whereby Artificial Intelligence is applied by using a human-interactive approach holds a lot of promise for fighting, detecting, and responding to cyber risks.

5. HUMAN IN THE LOOP

Traditional information security systems are based either on unsupervised Machine Learning or on analyst-driven solutions. Analyst-driven solutions rely on rules determined by fraud and security experts, and usually lead to high rates of undetected attacks and delays between attack detection and implementation of countermeasures. Moreover, hackers often figure out current rules and design different types of attacks that can avoid detection. On the other hand, unsupervised Machine Learning can improve early attack detection, but at the same time it may trigger more false positive alerts, which can require substantial investigative efforts before they are dismissed. Such false alarms can cause alarm fatigue and distrust and, over time, can cause reversion to analyst-driven solutions.

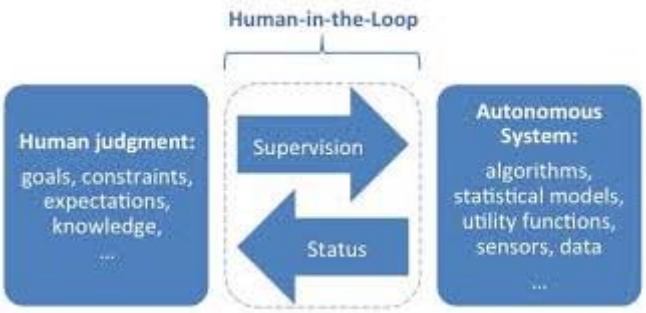

Fig. 5: Key Technology 3: Human in the Loop.

Human in the Loop [11] (Fig. 5) is a processing model requiring human interaction inside an automated process. This model is required when the result of an automated process leads to a critical decision. Such decision consists, quite often, in estimating how malicious the discovered threats are. Current Machine Learning systems, which use anomaly detection, are usually not able to discriminate about the level of anomaly. As a consequence, the role of the human analyst is paramount in judging if the suspicious events are real attacks and defining the rank of the attack. In addition, the analyst's feedback goes into the automated system, improving constantly its performance. A specific project, carried out by the Computer Science and Artificial Intelligence Laboratory (CSAIL) of MIT in 2016 [12], in cooperation with PatternEx, has shown that early discovery of cyber attacks is much more efficient when using Human in the Loop techniques. The research team designed a system, named AI2 (Artificial Intelligence and Analyst Intuition), which performs an automatic scan of a large data base by means of Machine Learning techniques and then reports the results to human analysts, who have to discriminate events linked to cyber attacks. The outputs from analysts are forwarded to the Machine Learning system, to be used for the processing of the new logs. The AI2 system was tested on three billion pieces of data, generated by millions of users over a period of three months. According to the MIT experts, the AI2 system performance resulted three times better than modern automated cyber attack detection systems, while reducing the false alerts by a factor of five.

Independently from the improvement that can be measured after the introduction of the Human in the Loop techniques, they are certainly advantageous when in presence of new threats or threats whose characteristics have not yet been clearly identified.

6. DEEP LEARNING

Deep Learning [13] is a branch of Machine Learning, consisting of a set of algorithms, which model non linear data transformation by using multiple processing layers (Fig. 6). At each layer, data are transformed by a processing unit, like an artificial neuron, whose parameters are learned through training. The overall structure of a deep learning network is inspired by a biological model of the human brain.

The Deep Learning technology undergoes a constant learning process and performs a suitable learning activity on the basis of a specific training through massive data sets from different sources. The result is a continuously updated model of prediction for real time cyber intelligence, which is forwarded to the cyber security system controlling the customer's premises. Deep Learning involves training a large network of simulated neurons and synapses to recognize complex patterns in large data bases. After analysing a sufficiently large number of examples, such a network can correctly identify new patterns, with different characteristics with the ones already known. Due to the presence of multiple processing layers, Deep Learning is extremely resistant to noise and can detect much more malware than other machine learning systems. According to the Israeli startup Deep Instinct, which uses Deep Learning in its security systems [28], the use of Deep Learning can improve detection performance of cyber threats by more than 20% with respect to the most advanced security software. Deep Learning is particularly efficient for the detection of automatically generated malware. Analysts are able to manually investigate a small number of unknown files, but the best large scale defense for detecting malware is automated malware classification. Malware classifiers often use sparse binary features, and the number of potential features can be on the order of tens or hundreds of millions. Feature selection reduces the number of features to a manageable number for training simpler algorithms such as logistic regression, but this number is still too large for more complex algorithms such as neural networks. To overcome this problem, random projections can be used to further reduce the dimensionality of the original input space and a Deep Learning network can be trained to detect new instances of malware with "state-of-the-art performance [14].

The emergence of Deep Learning have already brought many large tech companies and startups to pursuing this approach. According to the point of view of the researchers in this field, the introduction of the Deep Learning techniques will bring a breakthrough into the area of computer security. Even if the results of this new technology have not been yet very well assessed, with respect to cyber security, as in other areas such as voice recognition and language interpretation, Deep Learning has to be considered one of the key technologies to better explore in the future.

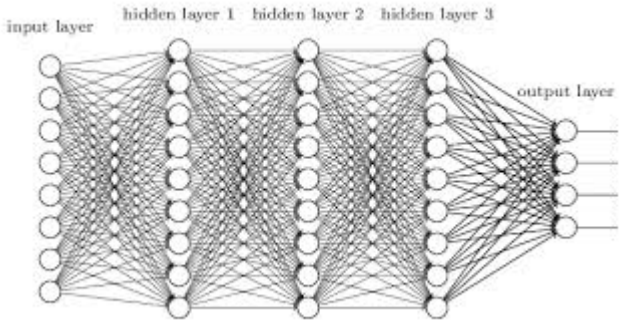

Fig. 6: Key Technology 4: Deep Learning.

7. DATA FUSION

Data Fusion [15] (Fig.7) is the process of integrating and merging multiple data and knowledge, representing the same real world object into a consistent and practical data object. The whole process is usually implemented by means of several subsequent steps, in order to transform raw data into more organized data structures, that provide effective support for human or automated decision making. The successful application of data fusion techniques is present in a wide variety of fields ranging from transportation optimisation to military situational awareness.

The most accepted definition of data fusion has been provided by the Joint Directors of Laboratories (JDL) workshop [18] (Fig. 8). According to this definition, Data Fusion is a multi-level process dealing with the association, correlation, combination of data and information from single and multiple sources to achieve refined position, identify estimates and complete and timely assessments of situations, threats and their significance.

Five different levels of Data Fusion are defined (see also Fig.8).

Level 0, Source Preprocessing: includes fusion at the signal and pixel levels. In the case of text sources, this level also includes the information extraction process. This level reduces the amount of data and maintains useful information for the high-level processes.

Level 1, Object Refinement: employs the processed data from the previous level. Common procedures of this level include space-time alignment, association, correlation, clustering or grouping techniques, state estimation, removal of false positives, identity fusion, and the combining of features that were extracted from images. The output results of this stage are the object discrimination (classification and identification) and object tracking (state of the object and orientation). This stage transforms the input information into consistent data structures.

Level 2, Situation Assessment: aims to identify the likely situations given the observed events and obtained data. It establishes relationships between the objects (i.e., proximity, communication), to determine the significance of the entities or objects in a specific environment. The aim of this level includes performing high level inferences and identifying significant activities and events (patterns in general). The output is a set of high-level inferences.

Level 3, Impact Assessment: evaluates the impact of the detected activities in order to perform a future projection and identify possible risks, vulnerabilities, and operational opportunities. This level includes an evaluation of the risk or threat and a prediction of the logical outcome.

Level 4, Process Refinement: provides resource and sensor management. The aim is to achieve efficient resource management while accounting for task priorities, scheduling, and the control of available resources.

Data fusion in the cyber domain has been conducted previously with Intrusion Detection Systems and Intrusion Prevention Systems and achieved good results. More recent work aimed to incorporate soft fusion techniques that integrate

the human component in the data fusion process. The reliability aspect of data fusion has been discussed at length with a variety of proposed solutions offered, such as Dempster Shafers method and derivatives such as the Transferable Belief Model [19]. To achieve reliable data fusion, it is critical to assess the data sources in a complete and uniform manner. Traditionally, information sources can be classified according to three main characteristics, namely the quality of the source, quality of the information and quality of presentation. To address the complexities involved in cyber data fusion, a structured approach is required, e.g. an adapted JDL model for data fusion.

The JDL model was first adapted to the cyber defence domain when the benefits of data fusion were explored to obtain a more reliable Intrusion Detection System. The JDL model has been extended to merge cyber information in Intrusion Detection System and Intrusion Prevention System [20]. Data fusion techniques have been extensively employed on multisensor environments with the aim of merging and aggregating data from different sensors. The goal of using data fusion in multisensor environments is to obtain a lower detection error probability and a higher reliability by using data from multiple distributed sources. The available data fusion techniques can be classified into three main categories: data association, state estimation, and decision fusion. All these techniques have to be introduced in implementing cyber security systems for critical infrastructures.

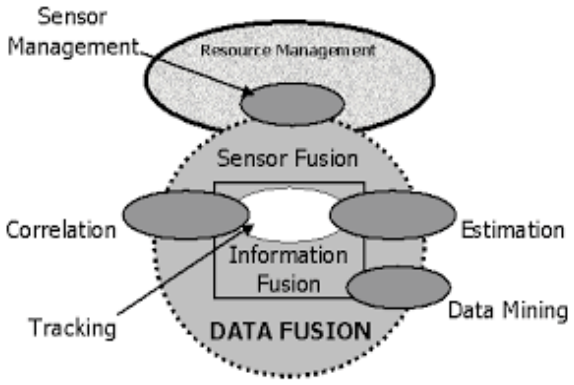

Fig. 7: Key Technology 5: Data Fusion.

8. CONCLUSIONS

The importance of critical infrastructures in modern life requires their continuous protection against cyber crime. An efficient cyber security system dedicated to critical infrastructures must be based on the most modern computer and communication technologies. This paper defines a general architecture for such a system and analyses the key perspectives and limits of the key technologies to be applied in order to implement the proposed architecture. Five key technologies are described and analysed with respect to their potential application to cyber security.

Big Data represents the information assets characterized by such a high volume of data to require that these data are transformed into compressed information to be used by real applications.

Intelligence consists of those processes, which have the goal to collect, process and interpret information and knowledge relative to a certain topic of interest. These processes are based both on brain power and experience and on artificial intelligence tools.

Human in the Loop consists of human interaction inside an automated process. This model is required when the result of an automated process leads to a critical decision, which cannot be taken by an automated system.

Deep Learning is a branch of machine learning, consisting of a set of algorithms, which model non linear data transformation by using multiple processing layers. The overall structure of a deep learning network is inspired by a biological model of the human brain.

Data Fusion is the process of integrating and merging multiple data and knowledge, representing the same real world object into a consistent and practical data object. The whole process is usually implemented by means of several subsequent steps, in order to transform raw data into more organized data structures, that provide effective support for human or automated decision making.

The analysis carried out aims to define a guideline for the efficient design of a cyber security system for the defense of critical infrastructures. The discussion about the intercepts of each of the technologies, with relation to the cyber security of critical infrastructures, shows that, in order to design efficiently this kind of systems, a strong synergy between human and machine technologies is necessary.

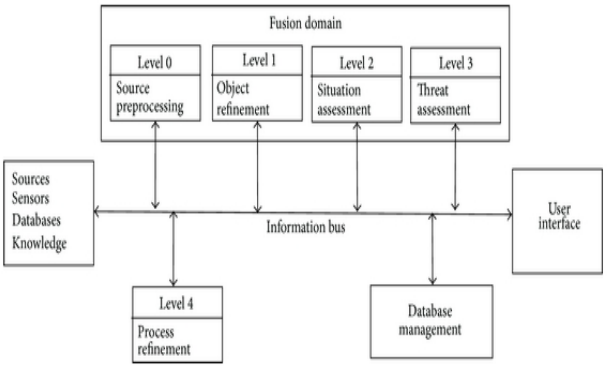

Fig. 8: The JDL Data Fusion Framework.

9. REFERENCES

[1] S. Asur and B. A. Huberman: "Predicting the future with social media", 2010 IEEE/WIC/ACM Intl.Conference on Web Intelligence and Intelligent Agent Technology.

[2] James Vlahos: "The Department of Pre-Crime", Scientific American 306, January 2012.

[3] Sharon Weinberger: "Terrorist Pre.Crime Detector Field Tested in the US", Nature, May 2011.

[4] Paul J. Croft et al. "UrbanNet: Urban Environment Monitoring and Modeling with a Wireless Sensor Network", 90th American Meteorological Society Annual Meeting, Atlanta, 2010.

[5] M. LaManna "Urban Environment Monitoring: System and Technology Issues", IMCIC 2012, 25-28 March 2012, Orlando, FL.

[6] M. LaManna "Data Fusion of Heterogeneous Sensors in Urban Environment Monitoring" IMCIC 2013, 9-12 July 2013, Orlando, FL.

[7] M. LaManna "Cost-Benefit Analysis of Automated Systems for the Control of Urban Critical Infrastructures" WMSCI 2015, 12-15 July 2015, Orlando, FL.

[8] T. Armending: "Cybercrime: much more organized", CSO Report, 23 June 2015.

[9] I. Hashem et al. "The rise of Big Data on Cloud Computing: review and open research issues", Information Systems, Vol. 47, January 2015.

[10] B. Berkowitz "Intelligence for the Homeland." SAIS Review of International Affairs 24, no. 1, 2004.

[11] W.Karwowski "International encyclopedia of ergonomics and human factors", CRC Press, 2006.

[12] Kalyan Veeramachaneni, CSAIL,MIT et al. "AI2: Training a big data machine to defend." AI2 IEEE International Conference on Big Data Security, April 2016, New York.

[13] I. Arel, D. C. Rose, and Thomas P. Karnowski "Deep Machine Learning. A New Frontier in Artificial Intelligence Research" IEEE Computational Intelligence Magazine, 2013.

[14] G. Dahl, W. Stokes, Li Deng, Dong Yu, "Large-Scale Malware Classification using Random Projections and Neural Networks", IEEE Conference on Acoustics, Speech, and Signal Processing, 2013.

[15] E. Blasch, et al. "High-Level Information Fusion Management and System Design". Norwood, MA: Artech House Publishers, 2012.

[16] P. Shinkman: "Reported Russian Cyber Attack Shuts Down Pentagon Network", US News, 6 August 2015.

[17] M. LaManna, "Architecture and Data Fusion Strategies for a Wireless Sensor Network for Urban Environment Monitoring" IASTED International Conference on Wireless Communications, Vancouver, Canada, June 2011.

[18] JDL, Data Fusion Lexicon. Technical Panel For C3, F.E. White, San Diego, Calif, USA, Code 4^{20}, 1991.

[19] P. Smets, Belief functions: The disjunctive rule of combination and the generalized bayesian theorem. International Journal of Approximate Reasoning, 1993.

[20] S. Schreiber-Ehle, W. Koch "The JDL model of data fusion applied to cyber-defence - A review paper", Workshop on Sensor Data Fusion: Trends, Solutions, Applications, Bonn, 4-6 September 2012.

[21] C.H. Baker "A vulnerability assessment methodology for critical infrastructure sites", DHS Symposium R&D Partnerships in Homeland Security, 2005.

[22] R.Blundell, M. Costa-Dias "Alternative approaches to evaluation in empirical macroeconomics", Journal of Human Resources, 2009.

[23] M. Kears, L.E.Ortiz "Algorithms for interdependent security games", Neural Information Processing Systems, 2003.

[24] R. Lazarick "Airport vulnerability assessment. A methodology evaluation.", IEEE International Carnahan Conference on SecurityTechnology, 1999.

[25] A. Roecker, and C.D. McGillem, "Comparison of Two-Sensor Tracking Methods Based on State Vector Fusion and Measurement Fusion", *IEEE Trans. On Aerospace and Electronic Systems*, vol. 24, no. 4, July 1988, pp. 447-449.

[26] G. Ferrari, M. Martalo', R. Pagliari, "Decentralized detection in clustered sensor networks", IEEE Transactions on Aerospace and Electronic Systems, Vol.47, N.2, April 2011.

[27] M. LaManna, "Future Trends for Cyber Security for Critical Infrastructures", WMSCI 2016, 5-9 July 2016, Orlando, FL.

[28] E. David, "Deep Learning for Automatic Malware Signatture Generation and Classification", IEEE Intl. Conference on Neural Networks, Killarney, Ireland, July 2015.