Journal of Systemics, Cybernetics and Informatics (2021) 19(9), 40-45
https://doi.org/10.54808/JSCI.19.09.40

The Role of Human in the Loop in Threat Recognition in Homeland Protection Systems

Mario LA MANNA
Evoelectronics
Rome, Italy

ABSTRACT

Threat Recognition is a primary task in Homeland Protection systems. When performing this task, Human in the Loop is the main part of a multidisciplinary reasoning process, that allows to achieve a high probability of correct classification. This reasoning process relies on two important factors, namely the past recognition history and the threat scenario. The Human in the Loop agent contributes both in controlling the automated process and in acting as a decision support system in different situations, such as dynamic changes in the scenario and occurrence of anomalous conditions. In this paper, we evaluate the performance of a multidisciplinary system, which uses a combination of a multisensory classification algorithm and a multidisciplinary fusion rule. This fusion rule combines the decisions coming from different channels with the reasoning process of a Human in the Loop agent. The performance evaluation of the multidisciplinary threat recognition system is carried out by considering different case studies. The evaluation demonstrates that a multidisciplinary system with a Human in the Loop agent can classify different threats, by using a set of methods and algorithms, with a high probability of correct classification, when compared to a completely automated recognition criterium.

Keywords: homeland protection, threat recognition, machine learning, human in the loop agent, data fusion.

1. INTRODUCTION

A straightforward way to characterize a threat is through the use of a multidimensional threat profile, which describes a threat type and, for each type of threat, a number of specific parameters typical of that type of threat. The use of a multistatic system can exploit the spatial/ capability diversity given by the use of multiple/ heterogeneous channels. In this work we propose the use of threat profiles as fingerprints for identification purposes. The threat recognition is provided by the channels of the system by performing a correlation between the detected profile and a predefined profile data base and is expressed by means of a Confusion Matrix. The Confusion Matrix describes the probabilities associated to the correlation of a new detected profile with each profile contained in the data base. After the above correlation is performed by each channel of the network and the subsequent partial recognition results are provided by different channels, the Data Fusion Engine performs the final choice. The flow diagram of the complete process is reported in Fig.1.

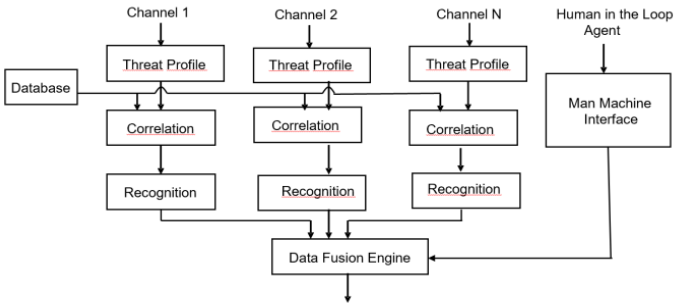

Fig. 1: Flow diagram of the Multidisciplinary Threat Recognition Process.

The Data Fusion Engine (Fig. 2) is composed of two main blocks, namely the Multidisciplinary Data Fusion block, which merges the partial recognitions produced by different channels, and the Machine Learning/ Human in the Loop block, which provides the algorithms used to merge the above recognition results. The algorithms are balanced dynamically by using the data provided by the Machine Learning process and by the interaction with the Human in the Loop agent. The performance of the complete process is enhanced with respect to a traditional one based only on a-priori recognition capability, as it combines the results coming from the different channels with the results produced by Machine Learning and Human in the Loop.

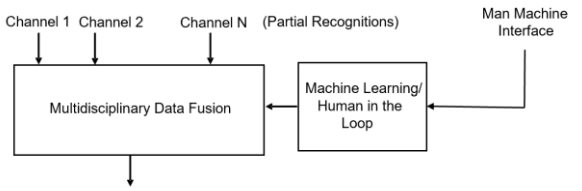

Fig. 2: Flow diagram of the Data Fusion Engine.

2. MULTIDISCIPLINARY CLASSIFICATION

The multidisciplinary classification uses a combination of multistatic classification algorithm and multidisciplinary fusion rule. The multistatic classification employs a likelihood-based algorithm, focused on the evaluation of the correlation of the received threat profile with the threat signatures stored in the database. A normalized version of this correlation function is an approximation of the likelihood function and is the input of a mixed recognition/ data fusion process based on a confusion matrix approach. After the threat estimation is made by each channel of the network, the recognition process delivers the results to the data fusion engine, which transforms the above estimations into a confusion matrix. In particular, the data fusion process combines the elements of the confusion matrix with the data coming from the Machine Learning/ Human in the Loop block and makes the final choice. Each step of the multidisciplinary classification approach is described in the following sections (Threat Profile, Threat Correlation, Threat Recognition and Data Fusion). More sections are dedicated to the description of three case studies (drone swarm, helicopter and clutter). The final two sections contain the conclusions and the references.

3. THREAT PROFILE

In order to characterize different threats, the threat profile can be thought as a vector of N elements, which corresponds to the image of the threat. It includes all the information necessary to distinguish one threat from another. In particular, it describes the threat type (e.g. single intruder, swarm of intruders, cyber threat, etc.) and all the parameters associated to a specific threat, according to its class (e.g. terrestrial threat, maritime threat, airborne threat, composite threat, cyber threat, etc.). The sensor/ device which detects a threat must be able to measure/ estimate its characteristics, in order to match these characteristics with those contained in the data base. The correlation of the features of the discovered threat with the fingerprints of a number of threats contained in the data base is the first step of the classification process. This process is not deterministic. There are different types of errors that can influence the correct correlation. First of all, there is an intrinsic limitation in the definition of the profiles contained in the data base. Then, when comparing the detected object with the data base, different sources of noise can alter some characteristics of an object, thus introducing some errors in the estimation of the threat. In order to minimize the possibility of misinterpreting the threat features, the use of a multistatic system is essential, as the final decision comes from a collective reasoning, not from a single agent.

4. THREAT CORRELATION

As showed in Fig. 1, the received profile is compared with the profiles of all the known threats stored in the database. As mentioned, the dataset contains, for each threat, a set of recorded features, which characterize the specific threat. The correlation is a scalar product given by (1).

$$C_d\left(r(n), g_i(n)\right) = \frac{\left|\sum_{n=1}^{N} r(n)\, g_i(n)^*\right|}{\left|\sum_{n=1}^{N}\left|r(n)\right|^2 \sum_{n=1}^{N}\left|g_i(n)\right|^2\right|^{1/2}} \quad (1)$$

where $r(n)$ and $g_i(n)$ are the functions representative of the received profile (composed of n elements) and of the different stored profiles contained in the data base (i=1,2,…,N). The formula used for the correlation is the classical cross-convolution of the two profile functions.
The value of C_d can be viewed as a likelihood function, that is an approximation of the probability of the received threat profile, given the threat belongs to a specific threat type. Schwartz's inequality insures that $0 \leq C_d \leq 1$ and C=1 $\Leftrightarrow r(n)=\alpha \cdot g_i(n)$, thus the correlation product is always between 0 and 1 and is a direct measure of the resemblance between two profiles.
The correlation formula is applied to all the stored N_a profiles contained in the data base. As a consequence, the output of the correlation process, for each channel, is a vector containing the probabilities $\Pr\{r(n)|\ th=a_i\}$ for i=1,2,…,N_a , where Pr is the probability of the received profile, given the threat belongs to each threat profile a_i stored in the data base, where N_a is the total number of stored profiles. The output of all channels is a matrix (correlation matrix), with N_a rows and N_c columns, whose generic element is the probability that a threat profile belongs to the a_i class (i=1, N_a) with respect to the n_j channel (j=1, N_c).

5. THREAT RECOGNITION

Threat recognition is based on the probability of a determined threat type $Pr\{th=a_i|r\}$ when the received profile is r, which, applying Bayes' rule, is given by (2).

$$Pr\{th = a_i|r\} = \frac{Pr\{r|th{=}a_i\}Pr\{th{=}a_i\}}{\Sigma_{j=1}^{Na} Pr\{r|th{=}a_j\}Pr\{th{=}a_j\}} \qquad (2)$$

The probability $Pr\{th{=}a_i|r\}$ is the output of the recognition block in Fig. 1 for each channel. More precisely, each channel calculates a N_a dimensional vector, whose *i*-th entry is the probability that the detected threat belongs to class *i*. This vector, referred as the recognition vector, depends on the capability of the sensor of a specific channel to identify the threat on the result of matching the identified threat profile with the set of reference profiles stored in the database. The recognition vector is not a deterministic result, but is still a likelihood function, which have to be further correlated with the corresponding functions of the other channels and processed by the machine learning/ human in the loop agent in the data fusion engine. The recognition vectors of all channels can be grouped together, to form a matrix (recognition matrix), whose rows refer to threat classes and columns are constituted by channels. Each element of this matrix corresponds to the probability that a specific channel indicates the threat as belonging to a determined threat class.

The described algorithm matches all the received threat profiles with the same recorded threat profiles and, during the selection/ fusion process, the channels with the best functionalities are highlighted. This solution is scalable and can be used for different types of recognition processes.

6. DATA FUSION

The fusion of data coming from the different channels is performed by using a classification process which uses the Confusion Matrix (CM) as a basic tool.

The generic entry of the CM is the probability that a threat belonging to the class *i* is classified as belonging to class *j*:

$c_{ij}^{(k)}$ =Pr{the k-th channel decides for H_j when H_i is true}

where H_i is the hypothesis that the threat belongs to class *i*. Thus, each row of the CM represents the class of the threat and the *j*-th column of the CM contains the class likelihood functions for each threat class. The diagonal elements of the CM are the conditional correct classification probabilities, while the off-diagonal elements are the conditional error probabilities.

Then the correct classification probability is:

$$P_{CC} = \sum_{i=1}^{N_a} P_{CC}|H_i \cdot \Pr\{H_i\} \qquad (3)$$

where $\Pr\{H_i\}$ is the probability of the *i*-th hypothesis.

The main task of the fusion process is to use the CM tool in order to maximize the correct classification probability, i.e. to highlight the diagonal elements of the CM, and to lower the off-diagonal elements as much as possible. This task is accomplished through a suitable weighting of the estimations coming from different channels. In particular, the role of machine learning and human in the loop is to rely on two important factors, namely the past recognition history and the threat scenario. The past recognition history is included in the data fusion process by the use of machine learning, which selects and highlights those channels with the most favourable capabilities according to the specific scenario. In addition, the human in the loop agent contributes not only to condition and control the machine learning process, but also as a decision support in different situations, such as dynamic changes in the scenario and/or anomalous conditions.

7. CASE STUDY 1: DRONE SWARM

We simulated three case studies. In the first one, the threat consists of a drone swarm. For sake of simplicity, the alternatives that the system can choose have been limited to three different classes of threats, namely 1) drone swarm (a_1), 2) helicopter (a_2) and 3) no threat, i.e. clutter (a_3). In the first simulated case, the system attributes different a-priori probabilities to each possible threat (on the basis of previous threat history), namely $Pr\{th = a_1\}$=60%, $Pr\{th = a_2\}$=20% and $Pr\{th = a_3\}$=20%. The multistatic sensor system was assumed to have three different channels, based on different sensors, namely channel 1 based on a wideband radar (n_1), channel 2 based on an optical sensor (n_2) and channel 3 based on a narrowband radar (n_3), plus an additional channel with machine learning/ human in the loop agent.

The first step applies the correlation formula to the stored profiles contained in the data base, according to the selected scenario, i.e. the three a_i classes (i=1,2,3) corresponding to the three previous possible threats. The output of the correlation process is the matrix containing the probabilities Pr{$r(n)$| $th{=}a_i$} for *i*=1,2,3 for each n_j channel (j=1,2,3), represented in Fig.3.

Correl. Matrix	n_1	n_2	n_3
$\Pr\{r\|th = a_1\}$	0.8	0.5	0.3
$\Pr\{r\|th = a_2\}$	0.1	0.3	0.5
$\Pr\{r\|th = a_3\}$	0.1	0.2	0.2

Fig. 3: Correlation Matrix for Case Study 1.

The second step calculates the recognition matrix, whose generic element is the probability that a threat profile belongs to the a_i class (i=1, N_a) with respect to the n_j channel (j=1, N_c). The matrix obtained, after combining the elements of the correlation matrix with the a-priori probabilities, is represented in Fig. 4.

Recogn. Matrix	n_1	n_2	n_3
$Pr\{th = a_1 \mid r\}$	0.48	0.30	0.18
$Pr\{th = a_2 \mid r\}$	0.02	0.06	0.10
$Pr\{th = a_3 \mid r\}$	0.02	0.04	0.04

Fig. 4: Recognition Matrix for Case Study 1.

The final step, i.e. data fusion, consists of maximizing the correct classification probability through the use of the CM. In order to perform this process, the estimations coming from the three different channels are suitably weighted, relying on the past recognition history and the threat scenario. In particular, the estimation given by channel 1, which is based on a wideband radar, is further highlighted with respect to the other channels, due to its favourable capability of working in the given scenario. The CM produced by the system is reported in Fig. 5. The final choice results the one with the higher probability, i.e. the drone swarm (threat a_1), with a probability of 78%. The higher probability of recognition would have been 48% (the one scored by channel 1, see Fig. 4) without the use of the multidisciplinary data fusion process.

CM	$Pr\{th = a_1\}$	$Pr\{th = a_2\}$	$Pr\{th = a_3\}$
$th = a_1$	**0.78**	0.05	0.02
$th = a_2$	0.05	0.01	0.04
$th = a_3$	0.02	0.04	0.01

Fig. 5: Confusion Matrix (CM) for Case Study 1.

The correct classification probability is a function of time, due to the adaptive nature of the process. With reference to the specific case study, we can observe that, when we run the CM simulation vs. time, the probability $Pr\{th = a_1\}$ tends to increase, as long as time grows. In general, the collection of a number of time lags can increase or decrease the probability of correct classification, with respect to the first observation, depending on the reliability of the first observation, due to the intrinsic learning capability of the recognition/ data fusion process. The graphic of the probability of the simulated correct classification vs. time for the considered case study is reported in Fig. 6.

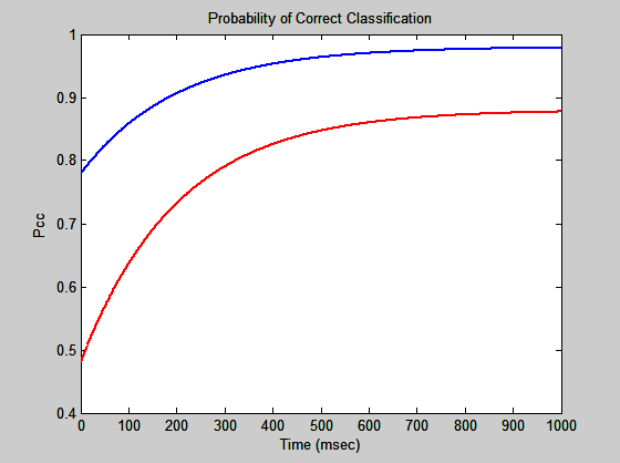

Fig. 6. Probability of correct classification vs. time , Case Study 1, with multidisciplinary data fusion (upper diagram) and automated recognition (lower diagram) .

8. CASE STUDY 2: HELICOPTER

We simulated a second scenario, with a threat consisting of a helicopter. The alternatives were still the above three different classes of possible threats, namely drone swarm (a_1), helicopter (a_2) and no threat, i.e. clutter (a_3). For this case, we assumed different a-priori probabilities for each possible threat, namely $Pr\{th = a_1\}$=10%, $Pr\{th = a_2\}$=70% and $Pr\{th = a_3\}$=20%. The multistatic sensor system was constituted of the same channels as the previous case study.
The correlation process applied to this case, considering the stored profiles contained in the data base, produced the matrix represented in Fig.7.

Correl. Matrix	n_1	n_2	n_3
$\Pr\{r \mid th = a_1\}$	0.4	0.2	0.3
$\Pr\{r \mid th = a_2\}$	0.5	0.7	0.5
$\Pr\{r \mid th = a_3\}$	0.1	0.1	0.2

Fig. 7: Correlation Matrix for Case Study 2.

The recognition matrix for case study 2, after combining the elements of the correlation matrix with the a-priori probabilities, is represented in Fig. 8.

Recogn. Matrix	n_1	n_2	n_3
$Pr\{th = a_1 \mid r\}$	0.04	0.02	0.03
$Pr\{th = a_2 \mid r\}$	0.35	0.49	0.35
$Pr\{th = a_3 \mid r\}$	0.02	0.02	0.04

Fig. 8: Recognition Matrix for Case Study 2.

The final step, i.e. data fusion, produced the CM reported in Fig. 9.

CM	$Pr\{th = a_1\}$	$Pr\{th = a_2\}$	$Pr\{th = a_3\}$
$th = a_1$	0.04	0.05	0.04
$th = a_2$	0.05	**0.72**	0.04
$th = a_3$	0.04	0.04	0.01

Fig. 9: Confusion Matrix (CM) for Case Study 2.

The probability of the simulated correct classification vs. time for case study 2 (Fig. 10) resulted similar to the previous case, i.e. outperforming automated recognition and growing towards 100% as long as time grows.

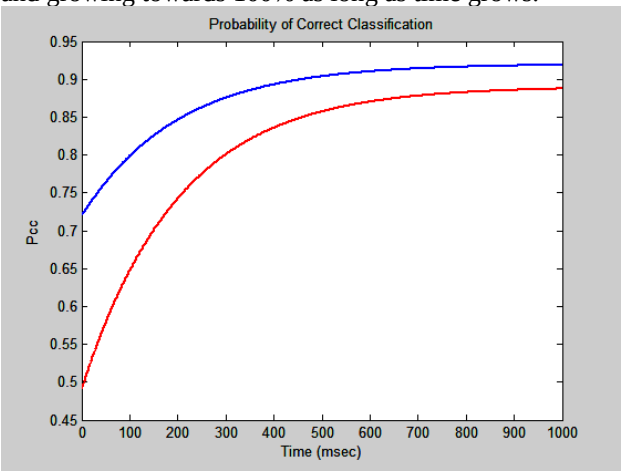

Fig. 10. Probability of correct classification vs. time, Case Study 2, with multidisciplinary data fusion (upper diagram) and automated recognition (lower diagram).

9. CASE STUDY 3: CLUTTER

In the last scenario, we simulated no real threat but only presence of clutter. The possible alternatives for recognition were the same classes as before. According to the scenario, the system attributed the following a-priori probabilities: $Pr\{th = a_1\}$=20%, $Pr\{th = a_2\}$=30% and $Pr\{th = a_3\}$=50%. The multistatic sensor system was constituted of the same channels as in the previous cases. The correlation matrix, obtained after considering the stored profiles of the data base, is represented in Fig.11.

Correl. Matrix	n_1	n_2	n_3
$Pr\{r\|th = a_1\}$	0.2	0.1	0.1
$Pr\{r\|th = a_2\}$	0.2	0.1	0.3
$Pr\{r\|th = a_3\}$	0.6	0.6	0.8

Fig. 11: Correlation Matrix for Case Study 3.

The recognition matrix for case study 3, obtained after combining the elements of the correlation matrix with the a-priori probabilities, is represented in Fig. 12.

Recogn. Matrix	n_1	n_2	n_3
$Pr\{th = a_1\|r\}$	0.04	0.02	0.02
$Pr\{th = a_2\|r\}$	0.06	0.03	0.09
$Pr\{th = a_3\|r\}$	0.30	0.30	0.40

Fig. 12: Recognition Matrix for Case Study 3.

The final step, i.e. data fusion, produced the CM reported in Fig. 13.

CM	$Pr\{th = a_1\}$	$Pr\{th = a_2\}$	$Pr\{th = a_3\}$
$th = a_1$	0.04	0.02	0.10
$th = a_2$	0.06	0.03	0.10
$th = a_3$	0.10	0.10	**0.70**

Fig. 13: Confusion Matrix (CM) for Case Study 3.

The probability of the simulated correct classification vs. time for case study 3 (Fig.14) resulted similar to the previous case studies and demonstrates that the multidisciplinary recognition algorithm always outperforms automated recognition.

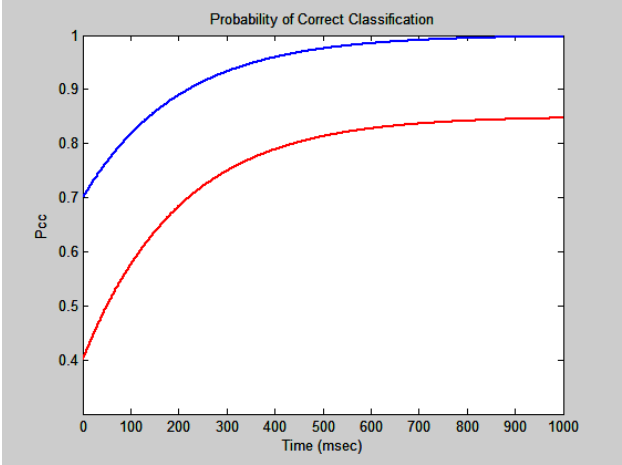

Fig. 14. Probability of correct classification vs. time, Case Study 3, with multidisciplinary data fusion (upper diagram) and automated recognition (lower diagram).

10. CONCLUSIONS

We evaluated a multidisciplinary threat recognition system, based upon a combination of a multisensor classification algorithm and a multidisciplinary data fusion

rule. The basic concept of the fusion rule is to combine the decisions coming from different channels with the reasoning process of a machine learning/human in the loop agent. The multidisciplinary data fusion rule merges the different channel decisions, taken by different sensors and/or devices, with the intelligence data provided by the machine learning/ human in the loop channel. The purpose of the multidisciplinary data fusion rule is to highlight the channels which, inside the machine learning process and through the interaction with the human in the loop agent, show better performance in terms of recognition capabilities in the specific scenario. The performance evaluation is carried out by considering three different case studies. We demonstrate that a multidisciplinary threat recognition system can outperform a traditional system, based on a completely automated recognition, in terms of higher probability of correct classification.

11. REFERENCES

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

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

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

[4] M. LaManna "Man-Machine Synergy in Systems for Critical Infrastructure Protection" WMSCI 2019, 6-9 July 2019, Orlando, FL.

[5] M. LaManna "A Man-Machine Synergy Integrated Approach for Homeland Protection" WMSCI 2020, 13-16 September 2020, Orlando, FL.

[6] Papoulis, A., Probability, Random Variables, and Stochastic Processes, 2nd edition, McGraw-Hill, New York, 1984.

[7] B. Kamiński, M. Jakubczyk, P. Szufel "A framework for sensitivity analysis of decision trees". Central European Journal of Operations Research, 2017.

[8] R.J. Urbanowicz, J.H.Moore "Learning Classifier Systems: A Complete Introduction, Review, and Roadmap". Journal of Artificial Evolution and Applications. 2009.

[9] N.Friedman, D. Geiger, M. Goldszmidt "Bayesian Network Classifiers". Machine Learning, Nov. 1997.

[10] H.Zhang "The Optimality of Naive Bayes", Florida Artificial Intelligence Research Society Conference, 2004.

[11] W. Daelemans, A. Van den Bosch, "Memory-Based Language Processing". Cambridge University Press, 2005.

[12] M. L. Minsky, S. A. Papert "Perceptrons, Expanded Edition". MIT Press, 1988.

[13] M.Hahsler "Introduction to arules, a computational environment for mining association rules and frequent item sets", Journal of Statistical Software, 2005.

[14] E. Achtert, C. Böhm, P. Kröger, A. Zimek "Mining Hierarchies of Correlation Clusters", International Conference on Scientific and Statistical Database Management, 2006.

[15] P.A.Gagniuc "Markov Chains: From Theory to Implementation and Experimentation", John Wiley & Sons, 2017.

[16] S.Skiena, "The Algorithm Design Manual", Springer Science and Business Media, 2010.

[17] S.Haykin "Neural networks : a comprehensive foundation", Prentice Hall, 1999.

[18] V. Novak, I. Perfilieva, J. Močkoř "Mathematical principles of fuzzy logic", Dordrecht: Kluwer Academic, 1999.

[19] L.N.de Castro, J. Timmis "Artificial Immune Systems: A New Computational Intelligence Approach". Springer, 2002.

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

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

[22] 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.

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

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

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

[26] Andler, S. F. Information Fusion from Databases, Sensors and Simulations, Annual Report 2005, June 2006.

[27] Hall, D. & Llinas, J. Handbook of multisensor data fusion. CRC Press.

[28] Hughes, T.J. "Sensor Fusion in a Military Avionics Environment." Measurement and Control. Sept. 1989.