# A Man-Machine Synergy Integrated Approach for Homeland Protection

**Mario LA MANNA**
**Evoelectronics**
**Rome, Italy**

**ABSTRACT**

A Homeland Protection system is a complex system or, according to a multidisciplinary terminology, a system of systems. Examples of systems of systems are: communication systems, transportation systems, energy grids, border control systems, vessel traffic systems, civilian emergency systems, security systems, etc. A system of systems is made of individual elements with multi-faceted interconnections with each other and with the external environment. Such systems cannot be studied by a simple decomposition into a number of small parts or units, as they present patterns and outcomes, which are not present in individual elements. An advanced security system for Homeland Protection is constituted of a set of sensory elements, enhanced by artificial intelligence, and on human agent/intelligence elements, cooperating with each other. From the examination of some case studies, we demonstrate that a man-machine synergy integrated approach is particularly suited to enhance the security level in Homeland Protection tasks.

**Keywords**: homeland protection, machine learning, human agent, intelligence, environment monitoring, network security.

## 1. INTRODUCTION

An advanced security system [1-4] for homeland protection (Fig. 1) is composed of the following subsystems: a) Data Fusion subsystem, whose function is to collect, merge and process raw data coming from the environment through a sensor subsystem; b) Intelligence subsystem, which processes data and information coming from human agent/ intelligence elements; c) Core Processor, based on artificial intelligence engines, relying on Machine and Man-Machine elements; d) Actuator subsystem, which transfers the final decisions and outputs to the external environment.
The system relies on an interdisciplinary (human/machine) approach, which complies with the heterogeneity of the data processed inside the system and the diversity of the information coming from different sources. This paper focuses on a class of novel algorithms, based on the synergy between automated machine learning and human judgment and demonstrates that the application of these algorithms is effective in enhancing the security in Homeland Protection systems.

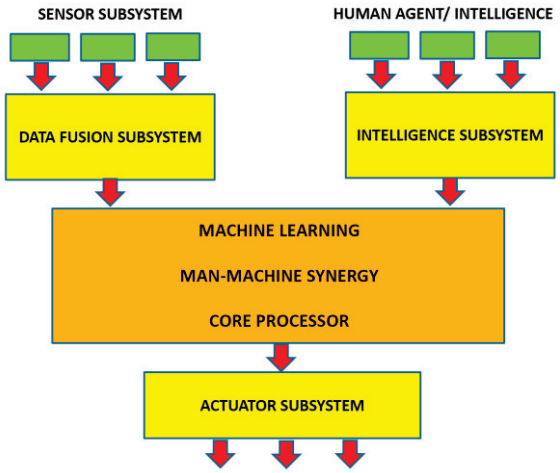


Fig. 1: Advanced Security System Architecture for Homeland Protection.

## 2. THE FULLY AUTOMATED PROCESS BASED ON MACHINE LEARNING

The fully automated process (Fig.2) is based on a set of components, or sub-processes, which transform the external physical stimulation, derived from an external signal, into an internal set of transformations, whose final results depend on a decision process. The stimulation caused by the external signal feeds a sensory process, which has the function to filter the signal and to dispatch the results to the machine learning process. This process combines the real-time input with previous instances of the same input, in order to set-up both the decision process and the thresholding process. The sensory process is assumed to produce a continuous output based on the received signal, whose level is proportional to the external stimulation (Signal, representing the presence of an external threat) and the random Gaussian noise (Noise, representing the presence of false alarms). The decision process has to make a final choice (sent as external response for the actuator subsystem), based on the

Signal/Noise ratio (S/N), the threshold level and the system detection sensitivity. The threshold, calculated by the thresholding process, has to be balanced, in order that the Probability of False Alarms ($P_{fa}$) and the Probability of Detection ($P_d$) are those required by the system as a function of its state (e.g. false alarm reduction, low level of attention, standard level of attention, high level of attention, emergency).

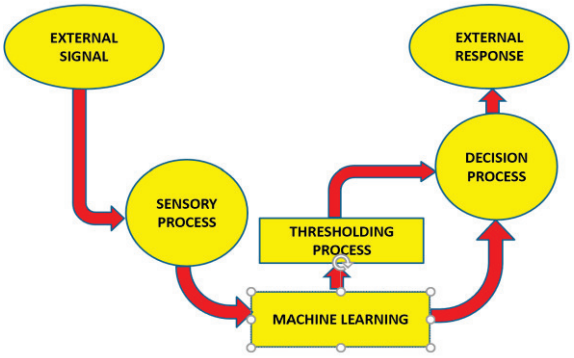


Fig. 2: Flow diagram of the fully automated process.

## 3. THE MAN-MACHINE BASED PROCESS INCLUDING HUMAN JUDGMENT

The man-machine based process (Fig.3) consists of the same components included in the fully automated process, plus a new component, or sub-process, called Human Judgment. The role of this component is twofold, as it influences both the thresholding process and the decision process. In the fully automated process, the thresholding process has the function to calculate a global threshold, which is used to separate two alternative cases, namely presence of threats and absence of threats/presence of false alarms. The threshold is chosen in order to provide a sufficiently high probability of detection of a threat discovered by the sensor process and validated by the machine learning component. The real-time calculation of the threshold level is performed by the machine learning process, on the basis of the data collected and elaborated over time. The introduction of human judgment in the thresholding process is motivated by the practical observation that real-time situation assessment is strongly dependent from the characteristics of the environment. These characteristics can change in an unpredictable way, so that, in order to build a true model of the environment, the support of a human expert and/or intelligence is paramount. In addition, the human expert can also discriminate, in many cases, between quantity and quality of each potentially discovered threat. The same support has to be introduced in the final decision process, where the role of human information increases with the increase of system complexity.

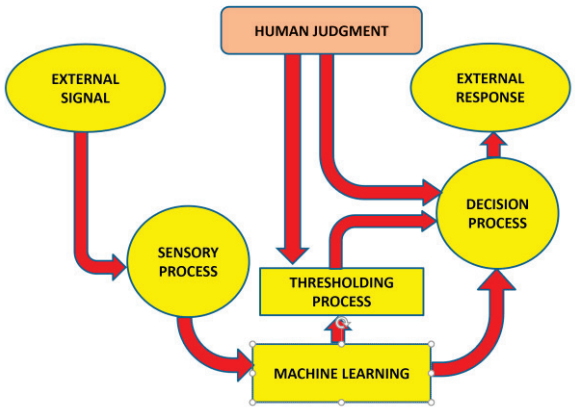


Fig. 3: Flow diagram of the man-machine based process.

## 4. MAN-MACHINE SYNERGY ALGORITHM

The Man-machine Synergy Algorithm is based on a combination of Gaussian signal detection theory on the one hand and decision theory on the other. Taking into account the Gaussian signal detection theory, the sensory process is assumed to have a continuous output based on random Gaussian noise combined with a deterministic signal, when this is present. In our case, the deterministic signal corresponds to a real threat, whose level is generally comparable to a threshold, i.e. likely high enough to require a reaction from the system. The basic variables involved in the detection process are the signal x(t), the Gaussian noise random process, with variance $\sigma_n^2$, the threshold ($x_T$), the Probability of Detection ($P_d$) and the Probability of False Alarms ($P_{fa}$). Based on the Neyman-Pearson criterion [5-6], the Probability of False Alarms is defined as the probability that a sample x of the signal x(t) will exceed the threshold $x_T$ when Gaussian noise alone is present.

$$P_{fa} = \frac{1}{\sqrt{2\pi}\sigma_n}\int_{x_T}^{\infty} e^{-x^2/2\sigma_n^2}dx = \frac{1}{\sqrt{\pi}}\int_{x_T}^{\infty} e^{-y^2}dy$$
$$= \frac{1}{2}erfc\left(\frac{x_T}{\sqrt{2}\sigma_n}\right) \quad (1)$$

The Probability of Detection is defined as the probability that a sample x of the signal x(t) will exceed the threshold $x_T$ when both a deterministic signal A and a random Gaussian noise are present. The whole mechanism is represented in Fig. 4.

$$P_d = \frac{1}{\sqrt{2\pi}\sigma_n}\int_{x_T}^{\infty} e^{-(x-A)^2/2\sigma_n^2}dx = \frac{1}{\sqrt{\pi}}\int_{\frac{x_T-A}{\sqrt{2}\sigma_n}}^{\infty} e^{-y^2}dy$$
$$= \frac{1}{2}erfc\left(\frac{x_T-A}{\sqrt{2}\sigma_n}\right) \quad (2)$$

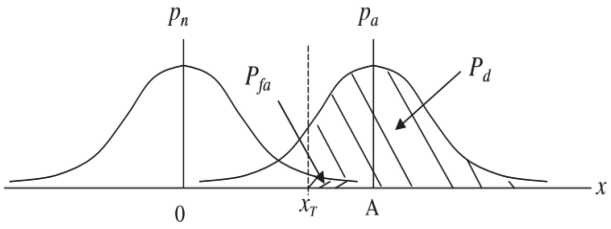


Fig. 4: Probability of False Alarms and Probability of Detection.

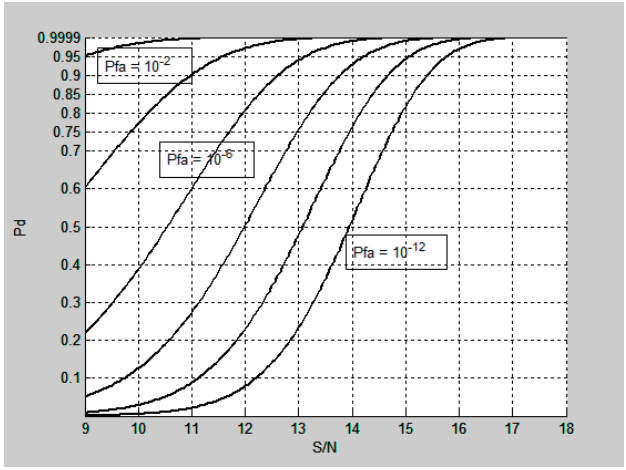


Fig. 5. Relation between S/N (dB), $P_d$ and $P_{fa}$ ($P_{fa}$ values ranging from $10^{-2}$ to $10^{-12}$).

In the Man-machine Synergy Algorithm, the choice of the threshold depends on the machine learning output and by the output of the human judgment process. The machine learning process has the function to maintain the threshold level compatible with a limited false alarm rate, i.e. low Probability of False Alarms ($P_{fa}$). On the other hand, human judgment has the function to provide a suitable Probability of Detection ($P_d$), especially in difficult and unpredictable conditions. The synergy of the two processes has been demonstrated to offer the best performance in terms of Probability of False Alarms ($P_{fa}$) and Probability of Detection ($P_d$), independently from the system state. In fact, from direct experience during the operativity of the network, while the machine learning process works better when the system operates in normal conditions, the support of human judgment is decisive in critical situations, such as anomalous conditions or emergencies. According to the above observation, the Man-Machine Synergy Algorithm has to be suitably designed to calculate the threshold $x_T$ as a function of the system state, the level of the discovered threat and the risk level envisaged for the network. We model the external signal as the combination of a deterministic signal S, which is proportional to the level A of the threat discovered by the data fusion subsystem and a random Gaussian noise N present in the network (Signal to Noise ratio = S/N). Any change in the threshold $x_T$, according to the Neyman-Pearson criterion, has a direct impact on the Probability of False Alarms and on the Probability of Detection. The relation between S/N, which is proportional to the level of the deterministic signal, the Probability of False Alarms $P_{fa}$ and on the Probability of Detection $P_d$ is reported in Fig. 5.

The Man-machine Synergy Algorithm also influences the decision process. The decision criterion is mainly based on the result of the thresholding process. However, before taking the final decision, additional parameters have to be added, such as detection sensitivity and payoff matrix. Detection sensitivity represents the confidence level that the decision process can attribute to the thresholding criterion. Sensitivity is constant in a fully automated process and variable from time to time and from task to task when human judgment is involved, The payoff matrix is a cost/benefit tool, which estimates the relative cost of making the two possible types of errors (false alarm and miss detection) and the relative benefit of making the possible two types of correct choices (correct detection and correct rejection). The elements of this matrix (Tab.1), which are predefined in a fully automated process, depend also on human judgment in the man-machine synergy algorithm.

| | **Yes** | **No** |
|---|---|---|
| **Signal Present** | Hit Rate (HR) | Miss Rate (MR) |
| **Signal Absent** | False Alarm Rate (FAR) | Correct Rejection Rate (CRR) |

Tab. 1: Payoff Matrix parameters.

## 5. CASE STUDY 1: STEADY STATE

Let us assume that the system is in a steady state (i.e. standard level of attention), with nfa= 10, corresponding to $P_{fa}=10^{-nfa}= 10^{-10}$. This state corresponds to a normalized threshold of 6.3 (Fig.6). If, at the same time, the S/N required to detect a threat is 15 dB, the resulting $P_d$ will be set up at 95% (Fig.7). In this case, the determination of the threshold will be taken mainly by the machine learning

process, as both the $P_d$ and the $P_{fa}$ are adequate to manage the occurrence of real alarms, in case of a discovered threat, and of false alarms, in case of absence of threats.
With regard to the payoff matrix in the decision process, the goal is to highlight both the hit rate and the correct rejection rate (Tab.2), while keeping both the miss rate and the false alarm rate at low levels. As a whole, the man-machine based process works in the same way as the fully automated process, as there is no substantial intervention by means of human judgment.

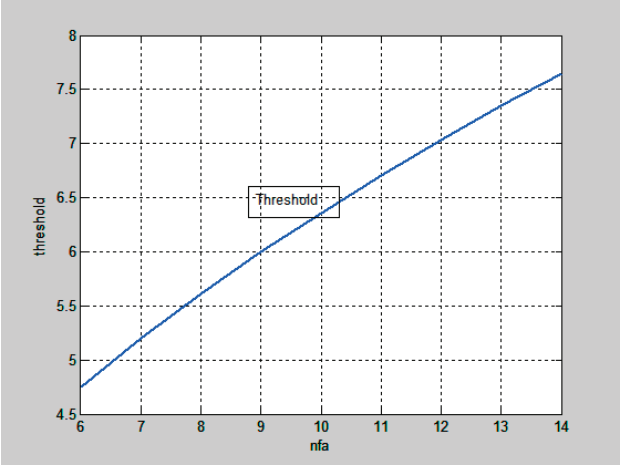


Fig. 6. Threshold calculation in the steady state.

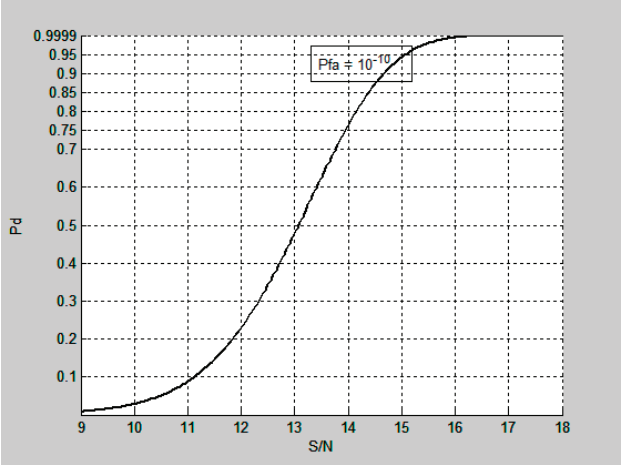


Fig. 7. $P_d$ calculation in the steady state.

| | Yes | No |
|---|---|---|
| **Signal Present** | Hit Rate HIGH | Miss Rate LOW |
| **Signal Absent** | False Alarm Rate LOW | Correct Rejection Rate HIGH |

Tab. 2: Payoff Matrix (steady state).

## 6. CASE STUDY 2: EMERGENCY STATE

When the system is in the emergency state, nfa is sensibly lower than usual, i.e. the probability of false alarms is higher (nfa= 6, corresponding to $P_{fa}=10^{-6}$, see Fig.8), in order to achieve a better performance in terms of probability of detection. This state corresponds to a normalized threshold of 4.7 (see initial threshold in Fig.8). If the S/N required to detect a threat is, for example, 12 dB, the resulting $P_d$ will be only 80% (Fig.9). Due to the risk connected to such low probability in the emergency state, human intervention is necessary. The man-machine synergy algorithm is capable to provide the above intervention, which changes the value of the threshold from 4.7 to 3.7 (see final threshold in Fig. 8). As a consequence of this modification, the value of nfa will change into 4, corresponding to $P_{fa}=10^{-4}$, while $P_d$ will increase to a level over 95% , which is adequate for the considered state.
With regard to the payoff matrix in the decision process (Tab.3), human intervention is beneficial to increase the hit rate and keep the miss rate as low as possible, at the expense of some increase of the false alarm rate, while improving the correct rejection rate.

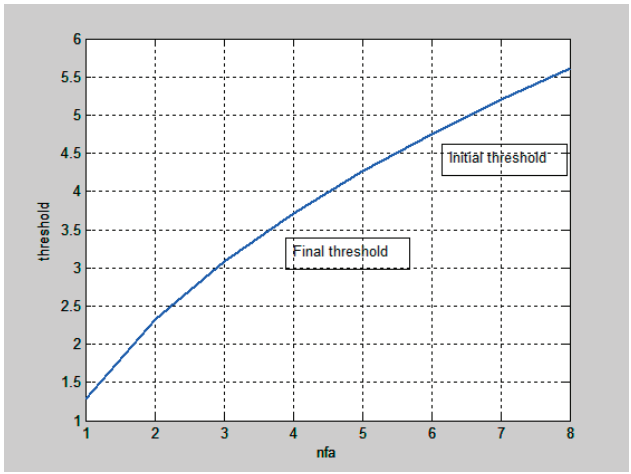


Fig. 8. Threshold change in the emergency state.

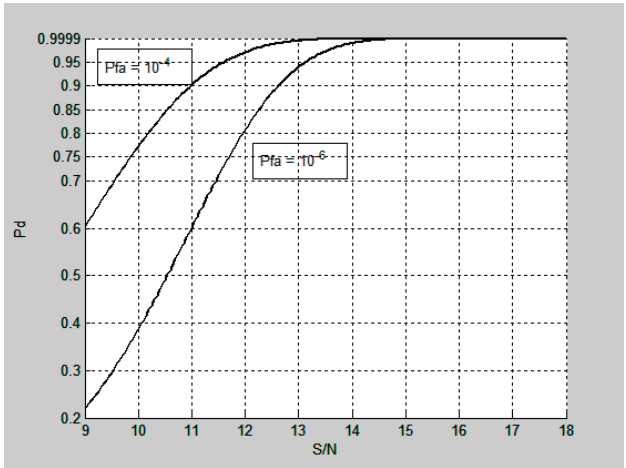


Fig. 9. $P_d$ calculation in the emergency state.

| | Yes | No |
|---|---|---|
| **Signal Present** | Hit Rate HIGH | Miss Rate MEDIUM to LOW |
| **Signal Absent** | False Alarm Rate LOW to MEDIUM | Correct Rejection Rate LOW to MEDIUM |

Tab. 3: Payoff Matrix (emergency state).

## 7. CASE STUDY 3: FALSE ALARM REDUCTION

When the system is in the "false alarm reduction" state, the probability of false alarms is at medium level (nfa= 8, corresponding to $P_{fa}=10^{-8}$, see Fig.10), in order to prevent the system from false alarms. This state corresponds to a normalized threshold of 5.6 (see initial threshold in Fig.10). If, the S/N required to detect a threat is, for example, 15 dB, the resulting $P_d$ will be higher than 98% (Fig.11). As the main problem in this state is not threat detection but false alarm reduction, the man-machine synergy algorithm can increase the threshold level to 7, in order to decrease $P_{fa}$ to $10^{-12}$ (see Fig.11). After this change, $P_d$ will go down to a level around 80% , which can be acceptable in this state, as the risk connected to the occurrence of an attack has been considered very low, while the main goal is to reduce false alarms.

With regard to the payoff matrix in the decision process (Tab.4), human intervention is beneficial to reduce the false alarm rate at the expense of decreasing the hit rate. As a consequence of this change, there will be some increase of the correct detection rate, together with a possible increase of the miss rate.

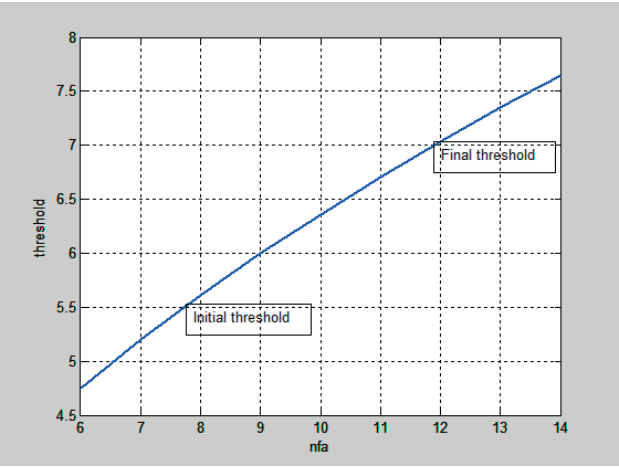


Fig. 10. Threshold change in the "false alarm reduction" state.

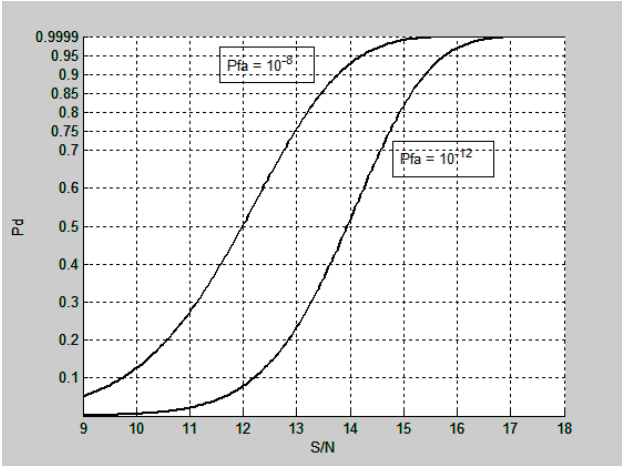


Fig. 11. $P_d$ calculation in the "false alarm reduction" state.

| | Yes | No |
|---|---|---|
| **Signal Present** | Hit Rate HIGH to MEDIUM | Miss Rate LOW to MEDIUM |
| **Signal Absent** | False Alarm Rate MEDIUM to LOW | Correct Rejection Rate MEDIUM to HIGH |

Tab. 4: Payoff Matrix (false alarm reduction state).

## 8. CONCLUSIONS

This paper describes a novel integrated man-machine approach for Homeland Protection, based on the synergy between automated machine learning and human judgment. This approach relies on the general concepts of detection theory processes and decision processes and on the balanced synergy between all the above processes. The man-machine synergy algorithms merge the Gaussian signal detection theory on the one hand and the decision theory on the other. Taking into account the Gaussian signal detection theory, the sensory process is assumed to have a continuous output based on random Gaussian noise combined with a deterministic signal. The decision process is based on detection sensitivity and payoff matrix. Detection sensitivity represents the confidence level that the decision process can attribute to the thresholding criterion. The payoff matrix is a cost/benefit tool, which estimates the relative cost of making the two possible types of errors (false alarm and miss detection) and the relative benefit of making the possible two types of correct choices (correct detection and correct rejection). From the examination of some case studies, we demonstrate that the proposed approach, applied to an architecture including sensory elements, artificial intelligence and human agent/ intelligence elements, is particularly suited to enhance the security level in Homeland Protection tasks.

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

[6] Peebles, Jr., P. Z., Probability, Random Variables, and Random Signal Principles, McGraw-Hill, New York, 1987.

[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.

[29] Hall, D. & McMullen, S.A.H. (2004) Mathematical techniques in multisensor data fusion. Artech House.

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

[31] Ramsvik, H. AIS as a tool for Safety of Navigation and Security - Improvement or not?

[32] Svensson, P. Technical survey and forecast for information fusion. In: RTO IST. Symposium on Military Data and Information Fusion. 20-22 October, 2003.

[33] Wald L., 1999, Some Terms of Reference in Data Fusion, IEEE Transactions on Geoscience and Remote Sensing Vol.37 No.3 May 1999.