2011 3rd International Conference on Cyber Conflict
C. Czosseck, E. Tyugu, T. Wingfield (Eds.)
Tallinn, Estonia, 2011 © CCD COE Publications

Artificial Intelligence in Cyber Defense

Enn Tyugu
R&D Branch
Cooperative Cyber Defense Center of Excellence (CCD COE)
and Estonian Academy of Sciences
Tallinn, Estonia
tyugu@ieee.org

Abstract- **The speed of processes and the amount of data to be used in defending the cyber space cannot be handled by humans without considerable automation. However, it is difficult to develop software with conventional fixed algorithms (hard-wired logic on decision making level) for effectively defending against the dynamically evolving attacks in networks. This situation can be handled by applying methods of artificial intelligence that provide flexibility and learning capability to software. This paper presents a brief survey of artificial intelligence applications in cyber defense (CD), and analyzes the prospects of enhancing the cyber defense capabilities by means of increasing the intelligence of the defense systems. After surveying the papers available about artificial intelligence applications in CD, we can conclude that useful applications already exist. They belong, first of all, to applications of artificial neural nets in perimeter defense and some other CD areas. From the other side – it has become obvious that many CD problems can be solved successfully only when methods of artificial intelligence are being used. For example, wide knowledge usage is necessary in decision making, and intelligent decision support is one of yet unsolved problems in CD.**

Keywords: applied artificial intelligence; intelligent cyber defense methods; neural nets in cyber defense; expert systems in cyber defense.

.

This paper expresses the author's ideas, and does not reflect an official position of CCD COE. The present work has been partially supported by the CCD COE and by the Centre of Excellence in Computer Science (EXCS)

I. INTRODUCTION

It is obvious that defense against intelligent cyber weapons can be achieved only by intelligent software, and events of the last two years have shown rapidly increasing intelligence of malware and cyber-weapons. Let us mention the Conficker worm for example. Some effects of Conficker on military and police networks in Europe have been cited in [1] as follows: "Intramar, the French Navy computer network, was infected with Conficker on 15 January 2009. The network was subsequently quarantined, forcing aircraft at several airbases to be grounded because their flight plans could not be downloaded. The United Kingdom Ministry of Defense reported that some of its major systems and desktops were infected. The virus has spread across administrative offices, NavyStar/N* desktops aboard various Royal Navy warships and Royal Navy submarines, and hospitals across the city of Sheffield reported infection of over 800 computers. On 2 February 2009, the Bundeswehr, the unified armed forces of the Federal Republic of Germany reported that about one hundred of their computers were infected. In January 2010, the Greater Manchester Police computer network was infected, leading to its disconnection for three days from the Police National Computer as a precautionary measure; during that time, officers had to ask other forces to run routine checks on vehicles and people."

Application of network centric warfare (NCW) makes cyber incidents especially dangerous, and changes in cyber defense are urgently required [2]. The new defense methods like dynamic setup of secured perimeters, comprehensive situation awareness, highly automated reaction on attacks in networks will require wide usage of artificial intelligence methods and knowledge-based tools.

Why has the role of intelligent software in cyber operations increased so rapidly? Looking closer at the cyber space, one can see the following answer. Artificial intelligence is needed, first of all, for rapid reaction to situations in Internet. One has to be able to handle large amount of information very fast in order to describe and analyze events that happen in cyber space and to make required decisions. The speed of processes and the amount of data to be used cannot be handled by humans without considerable automation. However, it is difficult to develop software with conventional fixed algorithms (hard-wired logic on decision making level) for effectively defending against the attacks in cyber space, because new threats appear constantly. Here is a place for artificial intelligence methods.

The second section of the present paper introduces artificial intelligence as a field of science and technology. In the third section we look at the existing artificial intelligence applications in cyber defense, grouped by the artificial intelligence techniques. The fourth section looks into the future and suggests new intelligent applications.

II. ABOUT ARTIFICIAL INTELLIGENCE

Artificial intelligence (AI) as a field of scientific research (also called machine intelligence in the beginning) is almost as old as electronic computers are. A possibility of building devices/software/systems more intelligent than human beings has been from the early days of AI "on the horizon". The problem is that the time horizon moves away when time passes. We have witnessed the solving of a number of intelligently hard problems by computers like playing good chess, for instance. During the early days of computing the chess playing was considered a benchmark showing a real intelligence. Even in seventies of the last century, when the computer chess was on the masters level, it seemed almost impossible to make a program that could beat the world champion. However, this happened sooner than expected. This had three reasons: increased computing power, development of a good search algorithm (that can be used in many applications beside chess, see the section on search below), and well organized knowledge bases that included all available chess knowledge (first of all, opening and end games). In essence, the chess problem could be solved because it was a specific intellectual problem belonging to so called *narrow AI*. A different case is translating from one language into another that requires *general AI*. In sixties of the last century, especially after N. Chomski's work in structural linguistics, it was expected that the natural language translation problem will be solved soon. It has not happened yet, although success is visible in some specific applications like, for instance, Google's AI linguistics. The reason is that this requires artificial general intelligence -- possessing of and ability to handle large amounts of knowledge in every field related to human activities.

It is generally accepted that AI can be considered in two ways: as a science aimed at trying to discover the essence of intelligence and developing generally intelligent machines, or as a science providing methods for solving complex problems that cannot be solved without applying some intelligence like, for instance, playing good chess or making right decisions based on large amounts of data. In the present paper we will take the second approach, advocate for applying specific AI methods to cyber defense problems, and will refer to the existing AI algorithms described in [3].

III. WHAT WE HAVE TODAY

After surveying the papers available about AI applications in CD, we are able to conclude that numerous useful applications already exist in this field. They belong, first of all, to applications of artificial neural nets in perimeter defense. On the other hand – it has become obvious that many more CD problems can be solved successfully only when AI methods are used. Wide knowledge usage is necessary in decision making, and the intelligent decision support is one of the yet unsolved problems in CD.

A large number of methods have been developed in the artificial intelligence field for solving hard problems that require intelligence from the human perspective. Some of these methods have reached a stage of maturity where precise algorithms exist that are based on these methods. Some methods have even become so widely known that they are not considered belonging to artificial intelligence any more, but have become a part of some application area, for instance, data mining algorithms that have emerged from the learning subfield of AI. It would be impossible to try to give more or less complete survey of all practically useful AI methods in a brief survey. Instead, we have grouped the methods and architectures in several categories: neural nets, expert systems, intelligent agents, search, machine learning, data mining and constraint solving. We outline these categories here, and we give references to the usage of respective methods in cyber defense. We are not going to discuss natural language understanding, robotics and computer vision which we consider specific applications of AI. Robots and computer vision have definitely impressive military applications, but we have not found anything specific to CD there.

A. Neural nets

Neural nets have a long history that begins with the invention of *perceptron* by Frank Rosenblatt in 1957 – an artificial neuron that has remained one of the most popular elements of neural nets [4]. Already a small number of perceptrons combined together can learn and solve interesting problems. But neural nets can consist of a large number of artificial neurons. Therefore neural nets provide a functionality of massively parallel learning and decision-making. Their most distinguished feature is the speed of operation. They are well suited for learning pattern recognition, for classification, for selection of responses to attacks [5] etc. They can be implemented either in hardware or in software.

Neural nets are well applicable in intrusion detection and intrusion prevention [6, 7, 8, 9, 10]. There have been proposals to use them in DoS detection [11], computer worm detection [12], spam detection [13], zombie detection [14], malware classification [15] and in forensic investigations [16].

A reason for the popularity of neural nets in cyber defense is their high speed, if implemented in hardware or used in graphic processors. There are new developments in the neural nets technology: third generation neural nets – spiking neural networks that mimic biological neurons more realistically, and provide more application opportunities. Good opportunities are provided by the usage of FPGA-s (field programmable gate arrays) that enable rapid development of neural nets and their adjustment to changing threats.

B. Expert systems

Expert systems are unquestionably the most widely used AI tools. An expert system is software for finding answers to questions in some application domain presented either by a user or by another software [17]. It can be directly used for

decision support, e.g. in medical diagnosis, in finances or in cyberspace. There is a great variety of expert systems from small technical diagnostic systems to very large and sophisticated hybrid systems for solving complex problems. Conceptually, an expert system includes a *knowledge base*, where expert knowledge about a specific application domain is stored. Besides the knowledge base, it includes an *inference engine* for deriving answers based on this knowledge and, possibly, additional knowledge about a situation. Empty knowledge base and inference engine are together called *expert system shel*l -- it must be filled with knowledge, before it can be used. Expert system shell must be supported by software for adding knowledge in the knowledge base, and it can be extended with programs for user interactions, and with other programs that may be used in hybrid expert systems. Developing an expert system means, first, selection/adaptation of an expert system shell and, second, acquiring expert knowledge and filling the knowledge base with the knowledge. The second step is by far more complicated and time consuming than the first.

There are many tools for developing expert systems. In general, a tool includes an expert system shell and has also a functionality for adding knowledge to the knowledge repository. Expert systems can have extra functionality for simulation [5], for making calculations etc. There are many different knowledge representation forms in expert systems, the most common is a rule-based representation. But the usefulness of an expert system depends mainly on the quality of knowledge in the expert system's knowledge base, and not so much on the internal form of the knowledge representation. This leads one to the *knowledge acquisition problem* that is crucial in developing real applications.

Example of a CD expert system is one for security planning [18]. This expert system facilitates considerably selection of security measures, and provides guidance for optimal usage of limited resources. There are early works on using expert systems in intrusion detection [19, 20].

C. Intelligent agents

Intelligent agents are software components that possess some features of intelligent behavior that makes them special: proactiveness, understanding of an agent communication language (ACL), reactivity (ability to make some decisions and to act). They may have a planning ability, mobility and reflection ability. In the software engineering community, there is a concept of software agents where they are considered to be objects that are at least proactive and have the ability to use the agent communication language. Comparing agents and objects, one can say that objects may be passive, and they do not have to understand any language (although they accept messages with well-defined syntax.)

Using intelligent agents in defense against DDoS has been described in [21] and [22], where simulation shows that cooperating agents can effectively defend against DDoS attacks. After solving some legal [23] and also commercial

problems, it should be possible in principle to develop a "cyber police" consisting of mobile intelligent agents. This will require implementation of infrastructure for supporting the cyber agents' mobility and communication, but must be unaccessible for adversaries. This will require cooperation with ISP-s. Multi-agent tools can provide more complete operational picture of the cyber space, for instance, a hybrid multi-agent and neural network-based intrusion detection method has been proposed in [24]. Agent-based distributed intrusion detection is described in [25].

D. Search

Search is a universal method of problem solving that can be applied in all cases when no other methods of problem solving are applicable. People apply search in their everyday life constantly, without paying attention to it. Very little must be known in order to apply some general search algorithm in the formal setting of the search problem: one has to be able to generate candidates of solutions, and a procedure (formally a predicate) must be available for deciding whether a proposed candidate satisfies the requirements for a solution. However, if additional knowledge can be exploited to guide the search, then the efficiency of search can be drastically improved. Search is present in some form almost in every intelligent program, and its efficiency is often critical to the performance of the whole program.

A great variety of search methods have been developed which take into account the specific knowledge about particular search problems. Although many search methods have been developed in AI, and they are widely used in many programs, it is seldom considered as the usage of AI. For example, in [26] and [27] dynamic programming is essentially used in solving optimal security problems, the search is hidden in the software and it is not not visible as an AI application. Search on and-or trees, αβ-search, minimax search and stochastic search are widely used in games software, and they are useful in decision-making for cyber defense. The αβ-search algorithm, originally developed for computer chess, is an implementation of a generally useful idea of "divide an conquer" in problem solving, and especially in decision making when two adversaries are choosing their best possible actions. It uses the estimates of minimally guaranteed win and maximally possible loss. This enables one often to ignore large amount of options and considerably to speed up the search.

E. Learning

Learning is improving a knowledge system by extending or rearranging its knowledge base or by improving the inference engine [28]. This is one of the most interesting problems of artificial intelligence that is under intensive investigation. Machine learning comprises computational methods for acquiring new knowledge, new skills and new ways to organize existing knowledge. Problems of learning vary greatly by their complexity from simple *parametric learning* which means learning values of some parameters, to complicated forms of *symbolic learning*, for

example, learning of concepts, grammars, functions, even learning of behavior [29].

AI provides methods for both -- *supervised learning* (learning with a teacher) as well as *unsupervised learning*. The latter is especially useful in the case of presence of large amount of data, and this is common in cyber defense where large logs can be collected. Data mining has originally grown out of unsupervised learning in AI. Unsupervised learning can be a functionality of neural nets, in particular, of self-organizing maps [30, 10, 16, 31].

A distinguished class of learning methods is constituted by parallel learning algorithms that are suitable for execution on parallel hardware. These learning methods are represented by genetic algorithms and neural nets. Genetic algorithms and fuzzy logic has been, for instance, used in threat detection systems described in [32].

F. Constraint solving

Constraint solving or constraint satisfaction is a technique developed in AI for finding solutions for problems that are presented by giving a set of constraints on the solution, e.g. logical statements, tables, equations, inequalities etc. [3, 33]. A solution of a problem is a collection (a tuple) of values that satisfy all constraints. Actually, there are many different constraint solving techniques, depending on the nature of constraints (for example, constraints on finite sets, functional constraints, rational trees). On a very abstract level, almost any problem can be presented as a constraint satisfaction problem. In particular, many planning problems can be presented as constraint satisfaction problems. These problems are difficult to solve because of large amount of search needed in general. All constraint solving methods are aimed at restricting the search by taking into account specific information about the particular class of problems. Constraint solving can be used in situation analysis and decision support in combination with logic programming [34, 35].

IV. CHALLENGES IN INTELLIGENT CYBER DEFENSE

When planning the future research, development and application of AI methods in CD, one has to distinguish between the immediate goals and long-term perspectives. There are numerous AI methods immediately applicable in CD, and there are immediate CD problems that require more intelligent solutions than have been implemented at present. Until now we have discussed these existing immediate applications.

In the future, one can see promising perspectives of the application of completely new principles of knowledge handling in situation management and decision making. These principles include introduction of a *modular and hierarchical knowledge architecture* in the decision making software. This kind of architecture

has been proposed in [36]. A challenging application area is the knowledge management for net centric warfare [37]. Only automated knowledge management can guarantee rapid situation assessment that gives a decision superiority to leaders and decision makers on any C2 level. As an example, the paper [36] describes an idea of the hierarchical and modular knowledge architecture in the Joint Command and Control Information System of the Bundeswehr.

Expert systems are already being used in many applications, sometimes hidden inside an application, like in the security measures planning software [26]. However, expert systems can get wider application, if large knowledge bases will be developed. This will require considerable investment in knowledge acquisition, and development of large modular knowledge bases. Also further development of the expert system technology will be needed: modularity must be introduced in the expert system tools, and hierarchical knowledge bases must be used.

Considering a more distant future -- at least some decades ahead, perhaps we should not restrict us to the "narrow AI". Some people are convinced that the grand goal of the AI -- development of artificial general intelligence -- AGI can be reached in the middle of the present century. The first conference on AGI was held in 2008 at the University of Memphis. The Singularity Institute for Artificial Intelligence (SIAI), founded in 2000, warns researchers of a danger that exponentially faster development of intelligence in computers may occur. This development may lead to Singularity, described in [38] as follows: "The Singularity is the technological creation of smarter-than-human intelligence. There are several technologies that are often mentioned as heading in this direction. The most commonly mentioned is probably Artificial Intelligence, but there are others ... -- several different technologies which, if they reached a threshold level of sophistication, would enable the creation of smarter-than-human intelligence. ... A future that contains smarter-than-human minds is genuinely different in a way that goes beyond the usual visions of a future filled with bigger and better gadgets." A futurist Ray Kurtzwell has extrapolated the development to come up with Singularity in 2045 [39]. One need not to believe in the Singularity threat, but the rapid development of information technology will definitely enable one to build considerably better intelligence into software in coming years. (Consider the recent impressive performance of IBM-s Watson program [40].) Independently of whether the AGI is available or Singularity comes, it is crucial to have the ability to use better AI in cyber defense than the offenders have it.

V. CONCLUSIONS

In the present situation of rapidly growing intelligence of malware and sophistication of cyber attacks, it is unavoidable to develop intelligent cyber defense methods. The experience in DDoS mitigation has shown that even a defense against large-scale attacks can be successful with rather limited resources when intelligent methods are used.

An analysis of publications shows that the AI results most widely applicable in CD are provided by the research in artificial neural nets. Applications of neural nets will continue in CD. There is also an urgent need for application of intelligent cyber defense methods in several areas where neural nets are not the most suitable technology. These areas are decision support, situation awareness and knowledge management. Expert system technology is the most promising in this case.

It is not clear how rapid development of general artificial intelligence is ahead, but a threat exists that a new level of artificial intelligence may be used by the attackers, as soon as it becomes available. Obviously, the new developments in knowledge understanding, representation and handling [41, 42, 43] as well in machine learning will greatly enhance the cyber defense capability of systems that will use them.

REFERENCES

[1] http://en.wikipedia.org/wiki/Conficker

[2] R. A. Poell, P. C. Szklrz. R3 – Getting the Right Information to the Right People, Right in Time. Exploiting the NATO NEC. In: M.- Amanovicz. Comcepts and Implementations for Innovative Military Communications and Information Technologies. Military University of Technology Publisher, Warsaw, 2010, 23 – 31.

[3] E. Tyugu. Algorithms and Architectures of Artificial Intelligence. IOS Press. 2007.

[4] F. Rosenblatt. The Perceptron -- a perceiving and recognizing automaton. Report 85-460-1, Cornell Aeronautical Laboratory, 1957.

[5] G. Klein, A. Ojamaa, P. Grigorenko, M. Jahnke, E. Tyugu. Enhancing Response Selection in Impact Estimation Approaches. Military Communications and Information Systems Conference (MCC), Wroclaw, Poland, 2010.

[6] J. Bai, Y. Wu, G. Wang, S. X. Yang, and W. Qiu, "A novel intrusion detection model based on multi-layer self-organizing maps and principal component analysis," in Advances in Neural Networks - ISNN 2006, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, May 2006, pp. 255–260.

[7] F. Barika, K. Hadjar, and N. El-Kadhi, "Artificial neural network for mobile IDS solution," in Security and Management, 2009, pp. 271–277.

[8] D. A. Bitter, T. Elizondo, Watson. Application of Artificial Neural Networks and Related Techniques to Intrusion Detection. WCCI 2010 IEEE World Congress on Computational Intelligence. July, 18-23, 2010 - CCIB, Barcelona, Spain, 2010, pp. 949 – 954.

[9] R.-I. Chang, L.-B. Lai, W. D. Su, J. C. Wang, and J.-S. Kouh, "Intrusion detection by backpropagation neural networks with sample-query and attribute-query," International Journal of Computational Intelligence Research, vol. 3, no. 1, 2007, pp. 6–10.

[10] L. DeLooze, Attack Characterization and Intrusion Detection using an Ensemble of Self-Organizing Maps, Proceedings of the IEEE Workshop on Information Assurance United States Military Academy, West Point, NY, 2006.

[11] B. Iftikhar, A. S. Alghamdi, "Application of artificial neural network in detection of dos attacks," in SIN '09: Proceedings of the 2nd international conference on Security of information and networks. New York, NY, USA: ACM, 2009, pp. 229–234.

[12] D. Stopel, Z. Boger, R. Moskovitch, Y. Shahar, and Y. Elovici, "Application of artificial neural networks techniques to computer worm detection," in International Joint Conference on Neural Networks (IJCNN), 2006, pp. 2362–2369.

[13] C.-H. Wu, "Behavior-based spam detection using a hybrid method of rule-based techniques and neural networks," Expert Systems with Applications, vol. 36, no. 3, Part 1, 2009, pp. 4321–4330.

[14] P. Salvador et al. Framework for Zombie Detection Using Neural Networks. In: Fourth International Conference on Internet Monitoring and Protection ICIMP-09, 2009.

[15] M. Shankarapani, K. Kancherla, S. Ramammoorthy, R. Movva, and S. Mukkamala. Kernel Machines for Malware Classification and Similarity Analysis. WCCI 2010 IEEE World Congress on Computational Intelligence. Barcelona, Spain, 2010, pp. 2504 – 2509.

[16] B. Fei, J. Eloff, MS Olivier, H. Venter. The use of self-organizing maps of anomalous behavior detection in a digital investigation. Forensic Science International, v. 162, 2006,pp. 33-37.

[17] http://en.wikipedia.org/wiki/Expert_system. Expert System. Wikipedia.

[18] J. Kivimaa, A. Ojamaa, E. Tyugu. Graded Security Expert System. Lecture Notes in Computer Science, v. 5508. Springer, 2009, 279-286.

[19] D. Anderson, T. Frivold, A. Valdes. Next-generation intrusion detection expert system (NIDES). Technical Report SRI-CSL-95-07, SRI International, Computer Science Lab (1995).

[20] TF. Lunt, R. Jagannathan. A Prototype Real-Time Intrusion-Detection Expert System. Proc. IEEE Symposium on Security and Privacy, 1988, p. 59.

[21] I. Kotenko, A. Ulanov. Multi-Agent Framework fo Simulation of Adaptive Cooperative Defense Against Internet Attacks. In: International Workshop on Autonomous Intelligent Systems: Agents and Data Mining. LNCS, Springer, v. 4476.

[22] I. Kotenko, A. Konovalov, A.Shorov. Agent-Based modeling and Simulation of Botnets and Botnet Defence. In: C. Czosseck, K. Podins (eds.). Proc. Conference on Cyber Conflict. CCD COE Publications, Tallinn, Estonia, 2010.

[23] B. Stahl, D. Elizondo, M. Carroll-Mayer, Y. Zheng, K. Wakunuma. Ethical and Legal Issues of the Use of Computational Intelligence Techniques in Computer Security and Computer Forensics. In: WCCI 2010 IEEE World Congress on Computational Intelligence, Barcelona, Spain. 2010, pp. 1822 – 1829.

[24] E. Herrero, M. Corchado, A. Pellicer, A. Abraham, "Hybrid multi agent-neural network intrusion detection with mobile visualization," Innovations in Hybrid Intelligent Systems, vol. 44, 2007, pp. 320–328.

[25] V. Chatzigiannakis, G. Androulidakis, B. Maglaris. A Distributed Intrusion Detection Prototype Using Security Agents. HP OpenView University Association, 2004.

[26] J. Kivimaa, A. Ojamaa, E. Tyugu. Pareto-Optimal Situation Analysis for Selection of Security Measures. Proc. MilCom, 2008.

[27] J. Kivimaa, A. Ojamaa, E. Tyugu. Managing Evolving Security Situations. MILCOM 2009: Unclassified Proceedings, Boston, MA. Piscataway, NJ: IEEE, 2009, pp. 1 - 7.

[28] P. Norvig, S. Russell. Artificial Intelligence: Modern Approach. Prentice Hall, 2000.

[29] AK. Ghosh, C. Michael, M. Schatz. A Real-Time Intrusion Detection System Based on Learning Program Behavior. Proceedings of the Third International Workshop on Recent Advances in Intrusion Detection, 2000, pp.93-109.

[30] J. Bai, Y. Wu, G. Wang, S. X. Yang, and W. Qiu, A novel intrusion detection model based on multi-layer self-organizing maps and principal component analysis, in Advances in Neural Networks. Lecture Notes in Computer Science. Springer, 2006, pp. 255–260.

[31] V. K. Pachghare, P. Kulkarni, D. M. Nikam. Intrusion Detection System using Self Organizing Maps. Proc. International Conference on Intelligent Agent & Multimedia-Agent Systems, IAMA 2009.

[32] R. Hosseini, J. Dehmeshki, S. Barman, M. Mazinani, S. Qanadli . A Genetic Type-2 Fuzzy Logic System for Pattern Recognition in Computer Aided Detection Systems.

IEEE World Congress on Computational Intelligence. Barcelona, Spain, 2010, pp. 215 – 221.

[33] B. Mayoh, E. Tyugu, J. Penjam. Constraint Programming. NATO ASI Series, v. 131, Springer Verlag. 1994.

[34] I. Bratko. PROLOG Programming for Artificial Intelligence. Addison-Wesley, 2001 (third edition).

[35] Xinming Ou. A logic-programming approach to network security analysis. PhD Thesis, Princeton University, 2005.

[36] U. Kaster, B. Kuhiber. Information and Knowledge Management in C2 Systems – The Gap Between Theory and Practice is not all that big. In: M.- Amanovicz. Comcepts and Implementations for Innovative Military Communications and Information Technologies. Military University of Technology Publisher, Warsaw, 2010, pp. 98 – 107.

[37] J. Kaster. Combined Knowledge Management and Workflow Management in C2 Systems – a user centered approach. Fraunhofer Institute for Communication, Information Processing and Ergonomics. Report ID # 197, 2009.

[38] http://singinst.org/overview/whatisthesingularity/

[39] R. Kurtzwell. The Singularity is Near. Viking Adult. 2005.

[40] http://www.ted.com/webcast/archive/event/ibmwatson

[41] M. Chmielewski. Ontology Applications for Achieving Situation Awareness in Military Decision Support Systems. LNAI/LNCS, Proc, ICCCI 2009, Wroclaw, 2009.

[42] P. Lorents, E. Tyugu Lattices of knowledge systems. Proc. International Conference on Artificial Intelligence Proc. WORLDCOMP'09: IC-AI´2009, Las Vegas, CSREA Press, July 2009.

[43] U. Schade, M. R. Hieb. A Battle Management Language for Orders, Requests and Reports. In: 2007 Spring Simulatin Ineroperability Workshop. Norfolk, USA, 2006