Searching for the Strong AI for Cybersecurity

Diana E. Vorobieva[1], Alexei S. Petrenko[1] and Sergei A. Petrenko[1,2]

[1] *Saint-Petersburg Electrotechnical University «lETI», ul. Professora Popova, 5, St Petersburg, 197022, Russia*
[2] *Innopolis University, Universitetskaya St, 1, Innopolis, Republic of Tatarstan, 420500, 420500, Russia*

Abstract

Currently, the creation of strong artificial intelligence (eng. Strong Artificial Intelligence (AI)) to ensure the required cybersecurity of digital platforms Industry 4.0 is one of the most interesting scientific and technical problems of our time. In the 1940s, when Norbert Wiener's book Cybernetics, or Control and Communication in the Animal and in the Machine, and other scientific papers on this topic were published, when the first computers of the von Neumann architecture appeared and began to be distributed. The mentioned problem was transferred from the field of science fiction to the field of real theoretical research and engineering developments. Since then, experts in the field of cyber security have been eagerly awaiting the emergence of fundamentally new technical information protection systems, the level of intelligence of which will be comparable to that of humans. That is, such engineering solutions, the distinctive ability of which will be the independent association and synthesis of new knowledge. Let's take a brief look at the history of the issue and dwell in more detail on the possible formulation of tasks for creating strong cybersecurity artificial intelligence.

Keywords

Industry 4.0, digital economy, cybersecurity, artificial intelligence, artificial neural network, genetic programming, cognitive computing, big data

1. Introduction

In the summer of 1956 at Dartmouth College, USA, a group of scientists guided by John McCarthy (1927-2011) marked the beginning of a new direction of science called Artificial intelligence [1-7, 11-27]. In the first scientific seminar on this topic, the possible formulations of the AI problems were considered, the solutions were outlined, including the requirements for the first formal (*logical*) systems and derived programming languages. *The first management issues*, *stability*, *noise immunity*, *adaptability* and *self-organization* of computing systems of the time were regarded and discussed (Figure 1).

BIT-2021: XI International Scientific and Technical Conference on Secure Information Technologies, April 6-7, 2021, Moscow, Russia
EMAIL: dinvor@mail.ru (A. 1); A.Petrenko1999@rambler.ru (A. 2); s.petrenko@rambler.ru (A. 3)
ORCID: 0000-0002-3181-5961 (A. 1); 0000-0002-9954-4643 (A. 2); 0000-0003-0644-1731 (A. 3)

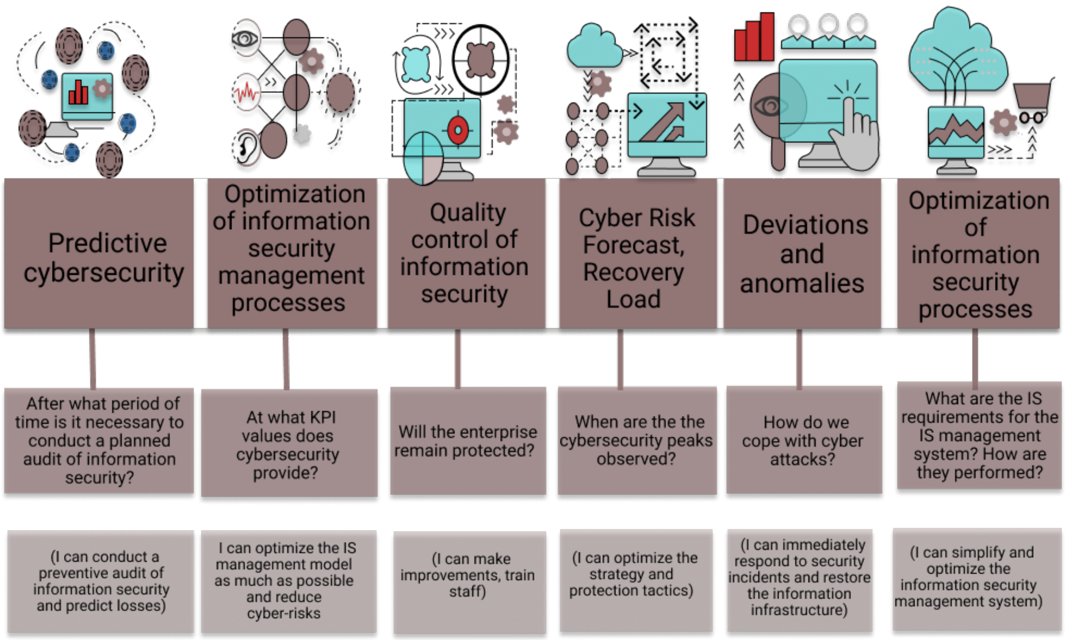

Figure 1: Possible AI issues in Cybersecurity

Lisp and Prolog programming languages

In 1960, at the Massachusetts Institute of Technology under the guidance of John McCarthy, the first functional Lisp programming language was created, based on the theoretical foundation of the lambda calculus by the famous mathematician Alonzo Church (1903–1995) [8-10, 22-24]. Afterwards, at the University of Edinburgh (Scotland), Robert Kowalski had developed the first logic programming language - Prolog, the practical implementation of which was implemented by Alain Colmari at the University of Marseille (France) in 1972. Then followed the period of the development of the first computer programs, including the Logical Theorist for the mathematical proof of the well-known Russell theorems, the General Problem Solver (*GPS*) for solving the formally defined problems, the *UNIMATE* robot in production. General Motors, *ELIZA* program that imitated the work of a psychotherapist, the Dendral system for studying the atomic structure of compounds of organic origin, various diagnostic programs, systems for generating the new scientific hypotheses and inventions, and much more. However, the results obtained in the form of the first models, methods and tools of AI could not be distributed to solve more complex problems. Mainly due to the problem of the so-called "combinatorial explosion", that manifests itself in an abrupt increase in the number of possible solutions that could not be resolved by the trivial brute force method. As a result, the cautious optimism was replaced by the first skepticism wave (or the first "*AI winter*") - funding for scientific research in the field of AI was sharply reduced, because of the certain mistrust in the results and the possibility of creating strong AI.

Fifth generation computer

In the early 1980s, *Japanese* professionals started developing a so-called fifth-generation *computer* with advanced AI functions. By that time, Japan had achieved a significant success in the automotive and aviation industries, and intended to reach a new level of technological development. In the fact they were supposed to develop a new architecture of parallel computing systems (Figure 2) with a record-setting performance of 100 million -1 billion LIPS. At that time, the computer performance was about 100 thousand LIPS, where LIPS is a logical inference per second [22-31, 37-44].

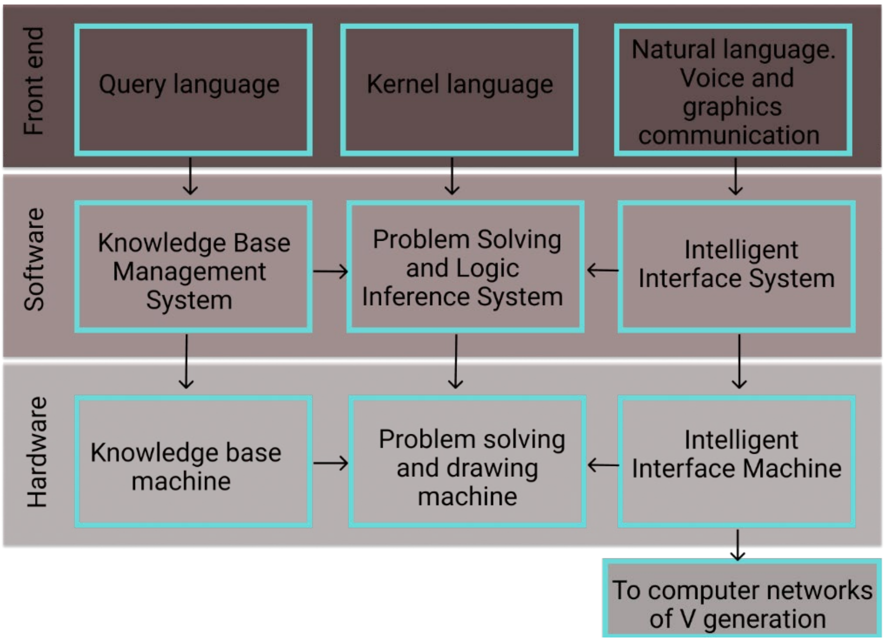

Figure 2: Fifth generation computer structure

The *features of the Fifth generation computer* are listed below**:**

- New computing system architecture (*not von Neumann*);
- New microcircuit production technology, which marks the transition from the silicon to gallium arsenide, increasing the speed of the main logic elements;
- New methods of information input-output - recognition and synthesis of speech and images;
- Rejection of traditional algorithmic programming languages (Fortran, Algol, etc.) in favor of functional Lisp and logical Prolog programming languages;
- Focus on the tasks of AI with automatic search for solutions based on logical inference.

The corresponding State program was launched in order to achieve the goals in Japan (*1982-1992*) [22-32, 45-50] with contributions from all of large private companies and costing *¥ 57 billion* (*about $ 500 million*). The example of Japan was followed by a number of technologically developed countries of the world, including the USA with a *similar Corporation for Microelectronics and Computer Technology (MCC) program*, the *UK Alvey program*, the *European ESPRIT program* and the *USSR program* for creating *MARS and Kronos* processor supercomputers (1985-1988).

Expert Systems

In the mid-1980s, the expert systems became widespread (see the excellent book by *Eduard Viktorovich Popov*), which were intended to replace the specialists in various subject areas. The classical expert system was a program based on the "if - that" (*the rules of the Post*), and allowed to recognize the situations and draw the simple logical conclusions. Hundreds of such expert systems were developed, including *Expert, Expert-PRO, GURU*, etc [22-24]. However, it turned out that the small expert systems were not beneficial enough, however the more powerful systems were too cumbersome and expensive to develop, operate and maintain. Also, the limitations of the computer the third and next generations, on the basis of the classical architecture of "von Neumann" for solving the tasks, were revealed. As a result, by the end of the 1980s, the second "winter of AI" had begin.

2. Artificial Neural Networks

In the 1990s, the relatively new models and methods of *neural networks and genetic programming* replaced the logical programming.

As a rule, an Artificial Neural Network (*ANN*) (Figure 3) is understood as a mathematical model, as well as its software and hardware implementation, based on the principles of organization and functioning of the biological neural networks - nerve cells of a living organism [**Ошибка! Закладка не определена.**6-32,37-44]. For example, the modifications of the first neural networks of *W. McCulloc* and *W. Pitts*, who have found an application in the pattern recognition problems, in control, prediction, imparting properties of adaptability and self-organization, and etc.

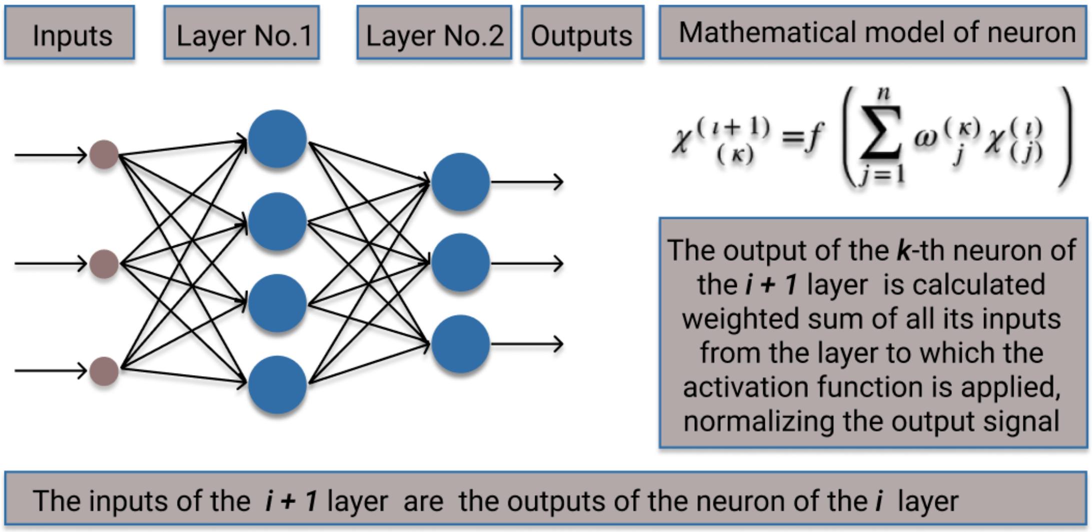

Figure 3: Neural network model

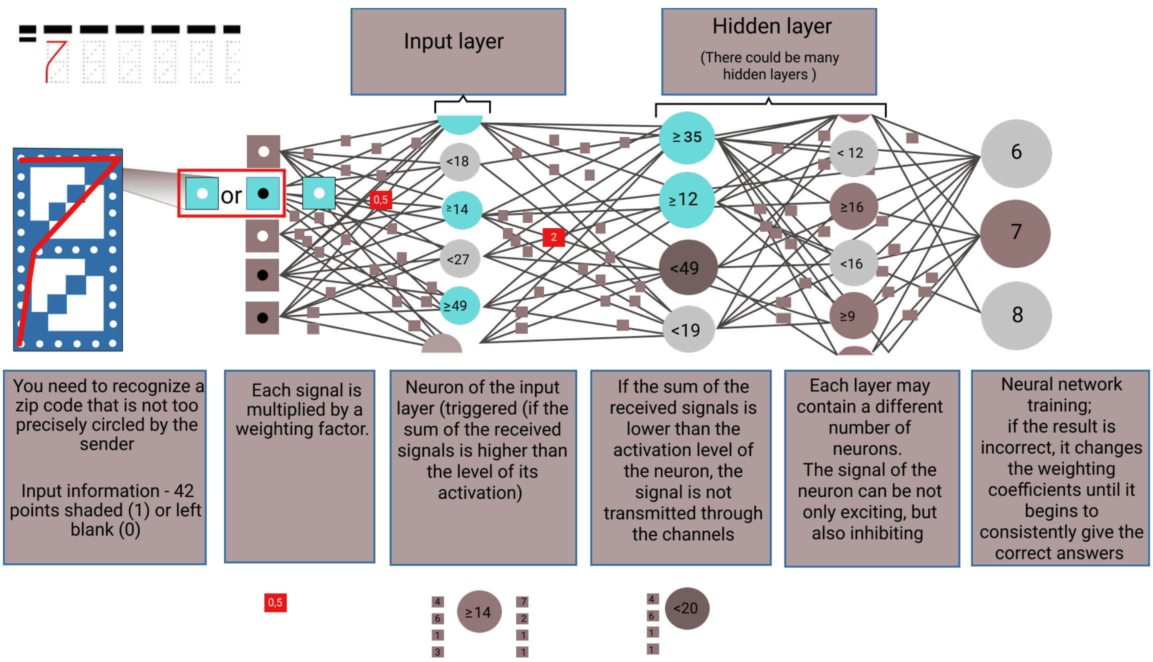

Figure 4: Sample of handwriting recognition

From an engineering point of view, an ANN is a system of the relatively simple processors (artificial neurons) that receive and send signals to each other. At the same time, the neural networks are not programmed in the usual sense of the word, but are learnt. Here the opportunity to be learnt is one of the main advantages of neural networks over traditional algorithmic systems. Technically, learning is to find the coefficients of connections between neurons. In the process of learning, the neural network is able to detect the complex dependencies between the input and the output data, as well as perform a generalization. This means that in case of successful learning, the network will be able to return the correct result, based on data that was missing in the learning sample, as well as in the partially distorted data (incomplete and/or "noisy") (Figure 4).

Let us note that the basic models of the neural networks have been known since the late 1950s, but they became widespread after the development of the *backpropagation*, which allowed training the multi-layer neural networks. Such multilayer networks in which there was at least one intermediate ("hidden") layer of neurons between the input and output layers can be trained how to perform a much larger number of functions, compared to their simpler predecessors. In combination with the computer technology achievements and the supercomputers' construction, this allowed the construction of the first neural networks, which quite successfully solved, among other things, the cybersecurity problems. (Figure 5 and Figure 6) [22-44, 49-50].

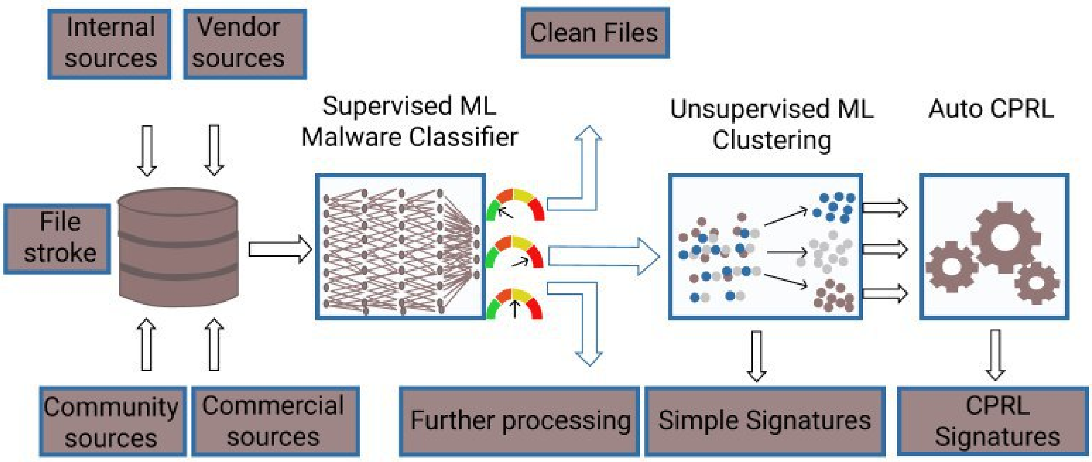

Figure 5: Malicious code recognition example

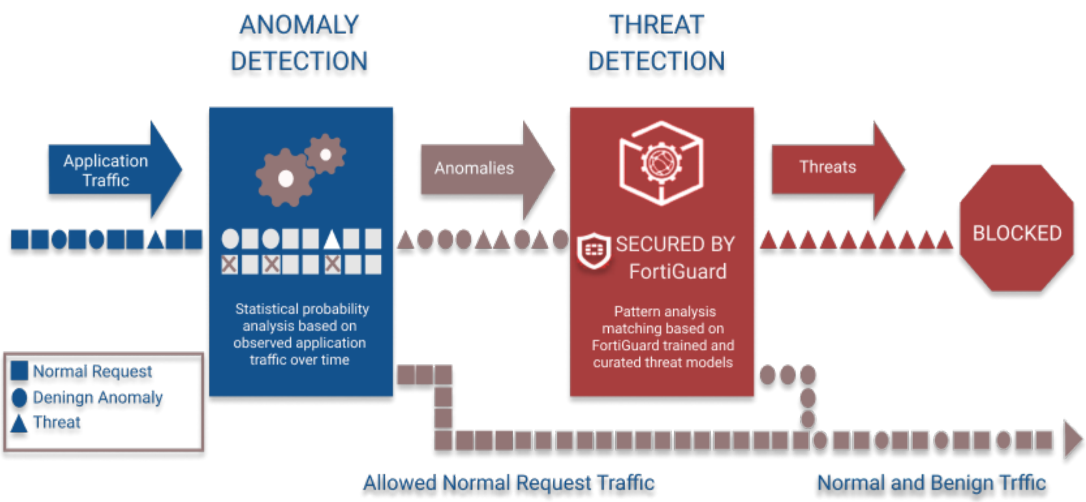

Figure 6: An example of the detection of infrastructure anomalies

Genetic programming

Genetic programming is a type of *evolutionary computing* method. Here, some initial populations (data structures and/or data processing programs) are considered as initial data. As a result of the random mutation and reproduction ("crossing"), the new populations appear. At the same time, a certain selection criterion (fitness function) allows selecting the best solutions. As Nick Bostrom had correctly noted, "In practice, however, getting evolutionary methods to work well requires skill and ingenuity, particularly in devising a good representational format. Without an efficient way to encode the candidate solutions (a genetic language that matches latent structure in the target domain), evolutionary search tends to meander endlessly in a vast search space or get stuck at a local optimum.” At the same time, the evolutionary computations require the significant computational resources.

Software tools.

In practice, in order to apply the models and AI methods in cybersecurity (Figure 7), the special software tools may be needed. These include the open source libraries, ready-made applications, such as the *Gigster platform*, as well as *Microsoft Azure Machine Learning* cloud services, *Amazon Machine Learning,* and others. A number of companies such as *Google, Apple, Facebook, Amazon,* and Microsoft have opened the third-party developers an access to their *AI*-bots to integrate the voice commands into applications. Also, there are a number of functional platforms, such as *Datanomiq*, a data science startup based on *SAP* solutions and services, as well as a number of open source *AI* application libraries, including the *Microsoft Cognitive Toolkit*. (Figure 8).

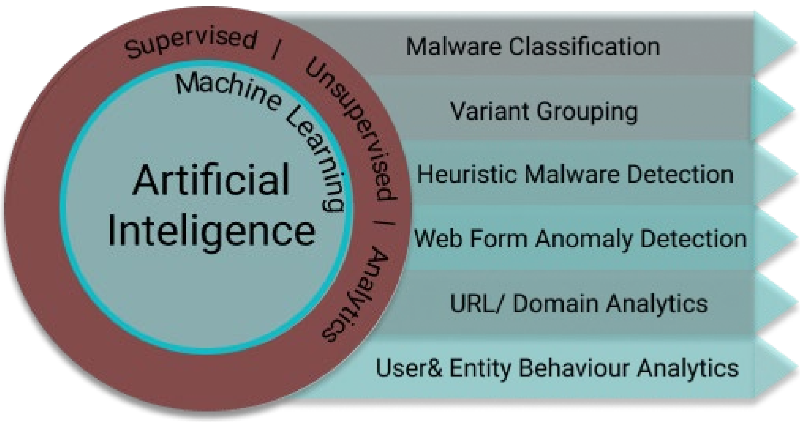

Figure 7: Cybersecurity AI Applications

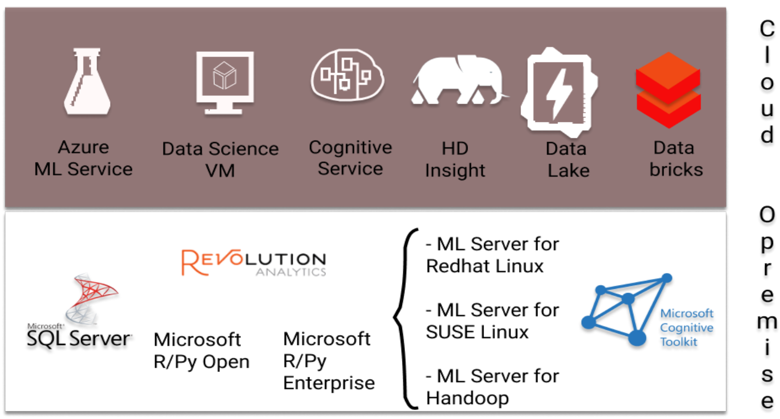

Figure 8: Possible machine learning tools

Also, in order to build a multilayer deep neural network, you can apply the capabilities of the *DGX-1* supercomputer from *NVIDIA*, which allows more than 12 times increase the performance of learning tasks, compared to the classical architecture of the "*von Neumann*" computer. At the same time, the library of the *DGX-1* programs[3] will significantly simplify the process of developing the Deep Learning applications. Let us note that the library includes the *NVIDIA Deep Learning GPU Training System* (*DIGITS*)[4], a full-featured interactive system for creating the *Deep neural networks* (*DNN*), and a *GPU-*

[3] https://developer.nvidia.com/deep-learning#source=pr
[4] https://developer.nvidia.com/digits#source=pr

accelerated library of primitives for creating *DNN* - the *NVIDIA CUDA Deep Neural Network* (*cuDNN*). In addition, the system contains a number of optimized frameworks for deep learning - *Caffe, Theano* and *Torch. DGX-1*, etc.

3. NBIC-Technology

In the 2000s, in the developed countries (USA, EU countries, China, Russia and others) a new technological structure of society was formed on the basis of so-called convergent *NBIC* technologies. For example, in the United States, a program of the *National Science Foundation* and the *Department of Commerce* under the *NBIC - Nanotechnology, Biotechnology, Information technology and Cognitive science* is being implemented. In the European Union, the following programs are being implemented: *GRAIN* (*Genetics, Robotics, Artificial Intelligence and Nanotechnology*) and *BANG* (*Bits, Atoms, Neurons, Genes*). China has launched a similar *China Brain* program. The national technology initiative *Neuronet* had started development in Russia (*CoBrain or Web 4.0 program*). Under this program, a number of leading national research and production companies, research institutes and universities, including *OJSC Radar system Technology Information (RTI)*, Research and Development Center of Kurchatov Institute, Research Institute of Neurocybernetics named after A. Kogan, Military Space Academy named after AF Mozhaisky, Moscow Institute of Physics and Technology, St. Petersburg Electrotechnical University "*LETI*", National Research University of Information Technologies, Mechanics and Optics, started the pilot production of hybrid and artificial biosimilar materials, technical systems of bionic type and technological platforms based on them. In the future, it is planned to create the complex anthropomorphic technical systems and "nature-like" technologies, combining the components of animate and inanimate nature.

The term *cognitive* comes from the Latin word *cognitio* (*cognition*). The improvement of mathematical models of thinking processes contributed to the development of a cognitive approach in the technical field. The first "*artificial cognitive systems*" appeared, representing "*intelligent*" software and hardware systems based on the traditional architecture of the Hungarian-American mathematician and physicist John von Neumann.

The prerequisites of the modern cognitive approach were the fundamental results [22-24]:

- Mathematical logic (from Aristotle to A. N. Kolmogorov);
- Mathematical computability theory (from Alan Turing to A. I. Maltsev);
- Computer science of John von Neumann's architecture;
- Theories of generative grammars of A. N. Chomsky;
- Theory of computational neurophysics of David Marr.

The core of the modern cognitive approach is the methods of cognition, perception and information accumulation, as well as methods of thinking or using this information for the "judicious" solution of the problems. It is believed that artificial cognitive systems are able to "repeat" the complex behavioral functions of the nervous system and even the work of the human mind.

Modern studies of the cognitive systems are conducted on the basis of the neurophysiological principles of the nervous system construction and the cognitive methods of human cognitive and mental activity. For example, in the work of L. A. Stankevich "Artificial cognitive systems" the use of artificial cognitive systems with hybrid architectures in robotics is justified. At the same time, a cognitive system is defined as a system that is capable of learning about its environment and adapting/changing it, due to the accumulated knowledge and acquired skills in the operation process. Two main types of artificial cognitive systems are clearly distinguished: the cognitive and emergent ones.

The actual cognitive systems include:

- Traditional character systems (*Allen Newell and Herbert Simon*);
- Systems, based on the theory of cognition, which applies training and the acquisition of symbolic knowledge (*J. Anderson*);
- Systems, based on the theory of practical reason and high-level psychological concepts of persuasion, plans and intention (*Michael Bratman*).

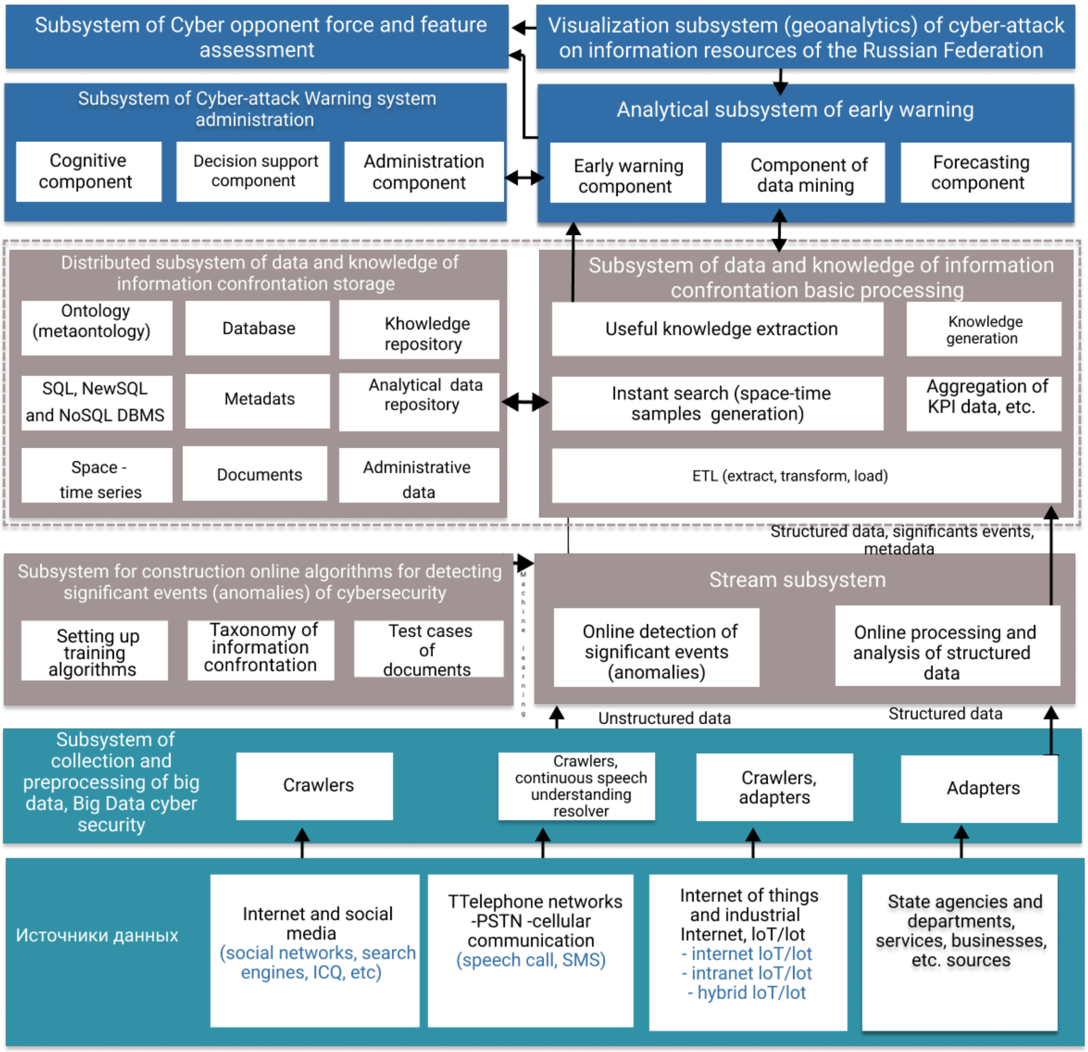

Figure 9: An example of a cognitive cyber attack detection system

Here the former are capable of generating some character structures or expressions. In this case, a symbol is a physical pattern that represents a certain component of an expression (or a character structure). The second ones are based on a system of products and a generalized model of human thinking and knowledge, containing memory, knowledge, decision making, and learning. In this case, the learning contains declarative and procedural steps, depending on the student knowledge. Others implement a decision-making process similar to the traditional practical conclusion.

The emergent systems consist of:

- Connectionist systems;
- Dynamic systems;
- Inactive systems.

The former implements the parallel processing of the distributed activation patterns, applying the statistical properties, rather than logical rules. The latter study the various self-organizing motor systems and human perception systems, examining the relevant metastable behavioral patterns. For others, the definition of a cognitive entity, that is, a purposeful behavior of the system, occurs when they interact with the environment.

Thus, the general methodology for the development of hybrid cognitive technical systems was proposed and substantiated:

- Formalized cognitive concepts and methods for creating the effective self-learning and self-modifying systems;

- Methods for the synthesis of the original cognitive components (modules and networks of modules) capable of accumulating knowledge through training and self-learning. At the same time, the components are built on the basis of a combination of neurological, immunological and triangulation adaptive elements that are most effective for multidimensional functional approximation, as well as corresponding behavioral networks;
- Methods for implementing the cognitive components and systems, based on specially developed software. The software implementation of cognitive components is based on the original models of information processing and training, and cognitive systems are based on multi-agent technology. This cognitive multi-agent allows creating the distributed cognitive systems with a high level of behavior complexity.

4. Conclusion

It is significant that the cognitive systems (Figure 9), unlike other well-known solutions (*CERT/SCIRT, MSSP/MDR, SOC 2.0, IDS/IPS, etc*.), have the ability to independently learn and behave in the real conditions of destructive hardware and software of intruders, affecting the protected critical information infrastructure. This will effectively solve the following tasks:

- Recognize patterns (patterns and clusters) that determine the preparation and the beginning of computer aggression;
- Training and development of the typical scenarios of warning, detection and counteraction in cyberspace;
- Generation, accumulation and processing of the new knowledge about the quantitative laws of opposition in cyberspace;
- Representations of the “deep” semantics of confrontation in cyberspace;
- Preparation and implementation of the adequate decisions, in response to cyber - attack.

5. Acknowledgements

The publication was carried out with the financial support of Russian Foundation for Basic Research (RFBR) in the framework of the scientific project No. 20-04-60080.

6. References

[1] Barabanov A., Markov A., Tsirlov V. Procedure for Substantiated Development of Measures to Design Secure Software for Automated Process Control Systems. In Proceedings of the 12th International Siberian Conference on Control and Communications (Moscow, Russia, May 12-14, 2016). SIBCON 2016. IEEE, 7491660, 1-4. DOI: 10.1109/SIBCON.2016.7491660.
[2] Barabanov A., Markov A., Tsirlov V. On Systematics of the Information Security of Software Supply Chains. Advances in Intelligent Systems and Computing. 2020. V. 1294. P. 115-129. DOI: 10.1007/978-3-030-63322-6_9.
[3] M. Ben Neria, N.-S. Yacovzada, and I. Ben-Gal, ‘‘A Risk-Scoring Feedback Model for Webpages and Web Users Based on Browsing Behavior,’’ ACM Trans. Intell. Syst. Technol., vol. 8, no. 4, pp. 1–21, 2017.
[4] A. Kleinmann and A. Wool, ‘‘Automatic Construction of Statechart-Based Anomaly Detection Models for MultiThreaded Industrial Control Systems,’’ vol. 8, no. 4, pp. 1–21, 2016.
[5] G. Wang, X. Zhang, S. Tang, C. Wilson, H. Zheng, and B. Y. Zhao, ‘‘Clickstream User Behavior Models,’’ ACM Trans. Web, vol. 11, no. 4, pp. 1–37, 2017.
[6] D. Codetta-Raiteri and L. Portinale, ‘‘Decision Networks for Security Risk Assessment of Critical Infrastructures,’’ ACM Trans. Internet Technol., vol. 18, no. 3, pp. 1–22, 2018.
[7] F. Angiulli, L. Argento, and A. Furfaro, ‘‘Exploiting Content Spatial Distribution to Improve Detection of Intrusions,’’ ACM Trans. Internet Technol., vol. 18, no. 2, pp. 1–21, 2018.
[8] C. X. Lu et al., ‘‘Snoopy: Sniffing Your Smartwatch Passwords via Deep Sequence Learning,’’ Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. Artic., vol. 1, no. 152, 2017.

[9] A. Squicciarini, C. Caragea, and R. Balakavi, ''Toward Automated Online Photo Privacy,'' ACM Trans. Web, vol. 11, no. 1, pp. 1–29, 2017.
[10] N. Sabar, X. Yi, and A. Shong, ''A Bi-objective Hyper-Heuristic Support Vector Machines for Big Data Cyber-Security NASSER,'' IEEE Access, vol. 56, no. 5, pp. 280–287, 2018.
[11] C. Yin, Y. Zhu, J. Fei, and X. He, ''A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks,'' vol. 5, 2017.
[12] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, ''A Deep Learning Approach to Network Intrusion Detection,'' IEEE Trans. Emerg. Top. Comput. Intell., vol. 2, no. 1, pp. 41–50, 2018.
[13] H. Peng, Z. Sun, X. Zhao, S. Tan, and Z. Sun, ''A Detection Method for Anomaly Flow in Software Defined Network,'' IEEE Access, vol. 6, pp. 27809–27817, 2018.
[14] C. Wang, Z. Zhao, L. Gong, L. Zhu, Z. Liu, and X. Cheng, ''A Distributed Anomaly Detection System for In-Vehicle Network Using HTM,'' IEEE Access, vol. 6, pp. 9091–9098, 2018.
[15] Y. Han, T. Alpcan, J. Chan, C. Leckie, and B. I. P. Rubinstein, ''A Game Theoretical Approach to Defend Against Co-Resident Attacks in Cloud Computing?: 146606 VOLUME 8, 2020
[16] I. Wiafe et al.: Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature Preventing Co-Residence Using Semi-Supervised Learning,'' IEEE Trans. Inf. Forensics Secur., vol. 11, no. 3, pp. 556–570, 2016.
[17] L. Dritsoula, P. Loiseau, and J. Musacchio, ''A Game-Theoretic Analysis of Adversarial Classification,'' vol. 12, no. 12, pp. 3094–3109, 2017.
[18] N. S. Safa, ''A Logit Boost-Based Algorithm for Detecting Known and Unknown Web Attacks,'' IEEE Access, vol. 5, pp. 26190–26200, 2017.
[19] V. T. Alaparthy and S. D. Morgera, ''A Multi-Level Intrusion Detection System for Wireless Sensor Networks Based on Immune Theory,'' IEEE Access, vol. 6, pp. 47364–47373, 2018.
[20] M. H. Ali, B. Abbas, D. Al, A. Ismail, and M. F. Zolkipli, ''A New Intrusion Detection System Based on Fast Learning Network and Particle Swarm Optimization,'' IEEE Access, vol. 6, pp. 20255–20261, 2018.
[21] P. Feng, J. Ma, C. Sun, and Y. Ma, ''A Novel Dynamic Android Malware Detection System With Ensemble Learning,'' IEEE Access, vol. 6, pp. 30996–31011, 2018.
[22] Sergei Petrenko, Developing a Cybersecurity Immune System for Industry 4.0, 2020 River Publishers, River Publishers Series in Security and Digital Forensics. ISBN: 9788770221887, e-ISBN: 9788770221870, 386 p.
[23] Sergei Petrenko. Cyber Resilience, ISBN: 978-87-7022-11-60 (Hardback) and 877-022-11-62 (Ebook). 2019 River Publishers, River Publishers Series in Security and Digital Forensics, 1st ed. 2019, 492 p.
[24] Petrenko S. Cyber resilient platform for internet of things (IIoT/IoT)ed systems: survey of architecture patterns. Voprosy kiberbezopasnosti [Cybersecurity issues]. 2021. N 2 (42). P. 81-91. DOI: 10.21681/2311-3456-2021-2-81-91.
[25] Korneev N.V. Intelligent complex security management system FEC for the Industry 5.0. IOP Conference Series: Materials Science and Engineering. Ser. Advanced Problems of Electrotechnology, 2020. P. 012016. DOI:10.1088/1757-899X/950/1/012016.
[26] Markov A.S., Timofeev Y.A. Industry 4.0 Cybersecurity Standards by the Example of Germany and Russia. In CEUR Workshop Proceedings, 2021 (Information Systems and Technologies in Modeling and Control, ISTMC'2021).
[27] Zegzhda D.P., Vasilev Y.S., Poltavtseva M.A., Kefeli I.F., Borovkov A.I. Advanced production technologies security in the era of digital transformation. Voprosy kiberbezopasnosti [Cybersecurity issues], 2018, N 2(26). P. 2-15. DOI: 10.21681/2311-3456-2018-2-2-15. (In Russ.)
[28] D. Hu, L. Wang, W. Jiang, and S. Zheng, ''A Novel Image Steganography Method via Deep Convolutional Generative Adversarial Networks,'' IEEE Access, vol. 6, pp. 38303–38314, 2018.
[29] Y. Gao, Y. U. Liu, Y. Jin, J. Chen, and H. Wu, ''A Novel Semi-Supervised Learning Approach for Network Intrusion Detection on Cloud-Based Robotic System,'' IEEE Access, vol. 6, pp. 50927–50938, 2018.
[30] Y. Ma, L. Wu, X. Gu, J. He, and Z. Yang, ''A Secure Face-Verification Scheme Based on Homomorphic Encryption and Deep Neural Networks,'' vol. 5, no. 1, 2017.
[31] L. Fernandez Maimo, A. L. Perales Gomez, F. J. Garcia Clemente, M. Gil Perez, and G. Martinez

[32] Perez, ‘‘A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks,’’ IEEE Access, vol. 6, pp. 7700–7712, 2018.
[33] Z. Tang, X. Ding, Y. Zhong, L. Yang, and K. Li, ‘‘A self-adaptive bell-lapadula model based on model training with historical access logs,’’ IEEE Trans. Inf. Forensics Secur., vol. 13, no. 8, pp. 2047–2061, 2018.
[34] M. A. Javed, E. Ben Hamida, A. Al-fuqaha, and B. Bhargava, ‘‘Adaptive Security for Intelligent Transport System Applications,’’ IEEE Intell. Transp. Syst. Mag., vol. 10, no. April, pp. 110–120, 2018.
[35] K. Khanna, B. K. Panigrahi, and A. Joshi, ‘‘AI-based approach to identify compromised meters in data integrity attacks on smart grid,’’ 2018.
[36] N. Nissim, A. Cohen, and Y. Elovici, ‘‘ALDOCX: Detection of Unknown Malicious Microsoft Office Documents Using Designated Active Learning Methods Based on New Structural Feature Extraction Methodology,’’ IEEE Trans. Inf. Forensics Secur., vol. 12, no. 3, pp. 631–646, 2017.
[37] H. Sedjelmaci and S. M. Senouci, ‘‘An Accurate Security Game for Low-Resource IoT Devices,’’ vol. 66, no. 10, pp. 9381–9393, 2017.
[38] Y. Du, J. Wang, and Q. Li, ‘‘An android malware detection approach using community structures of weighted function call graphs,’’ IEEE Access, vol. 5, pp. 17478–17486, 2017.
[39] L. Li, Y. Yu, S. Bai, Y. Hou, and X. Chen, ‘‘An Effective Two-Step Intrusion Detection Approach Based on Binary Classification and k -NN,’’ IEEE Access, vol. 6, pp. 12060–12073, 2018.
[40] A. Sahi, D. Lai, Y. A. N. Li, and M. Diykh, ‘‘An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment,’’ IEEE Access, vol. 5, pp. 6036–6048, 2017.
[41] A. L. I. S. Sadiq, B. Alkazemi, S. Mirjalili, N. Ahmed, S. Khan, and I. Ali, ‘‘An Efficient IDS Using Hybrid Magnetic Swarm Optimization in WANETs,’’ IEEE Access, vol. 6, pp. 29041–29053, 2018.
[42] K. Huang, Q. Zhang, C. Zhou, N. Xiong, S. Member, and Y. Qin, ‘‘An Efficient Intrusion Detection Approach for Visual Sensor Networks Based on Traffic Pattern Learning,’’ vol. 47, no. 10, pp. 2704–2713, 2017.
[43] S. Li, F. Bi, W. Chen, X. Miao, J. Liu, and C. Tang, ‘‘An improved information security risk assessments method for cyber-physical-social computing and networking,’’ IEEE Access, vol. 6, pp. 10311–10319, 2018.
[44] P. Tao, Z. H. E. Sun, and Z. Sun, ‘‘An Improved Intrusion Detection Algorithm Based on GA and SVM,’’ IEEE Access, vol. 6, pp. 13624–13631, 2018.
[45] Z. Liu, T. Qin, X. Guan, H. Jiang, and C. Wang, ‘‘An integrated method for anomaly detection from massive system logs,’’ IEEE Access, vol. 6, pp. 30602–30611, 2018.
[46] H. Liu, Y. Wang, J. Liu, J. Yang, Y. Chen, and H. V. Poor, ‘‘Authenticating Users Through Fine-Grained Channel Information,’’ IEEE Trans. Mob. Comput., vol. 17, no. 2, pp. 251–264, 2018.
[47] M. S. Parwez, D. B. Rawat, and M. Garuba, ‘‘Big data analytics for user-activity analysis and user-anomaly detection in mobile wireless network,’’ IEEE Trans. Ind. Informatics, vol. 13, no. 4, pp. 2058–2065, 2017.
[48] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon, and D. Gan, ‘‘Cloud-Based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning,’’ IEEE Access, vol. 6, pp. 3491–3508, 2018.
[49] L. Xiao, S. Member, Y. Li, X. Huang, X. Du, and S. Member, ‘‘Cloud-Based Malware Detection Game for Mobile Devices with Offloading,’’ vol. 16, no. 10, pp. 2742–2750, 2017.
[50] M. N. Napiah, M. Y. I. Bin Idris, R. Ramli, and I. Ahmedy, ‘‘Compression Header Analyzer Intrusion Detection System (CHA - IDS) for 6LoWPAN Communication Protocol,’’ IEEE Access, vol. 6, pp. 16623–16638, 2018.