ARTIFICIAL INTELLIGENCE IN ROMANIA AND IN THE EUROPEAN UNION

PhD. Student, Ramona MARGE, The Oradea University, România,
ramona.marge@yahoo.ro,
PhD., Ştefan IOVAN, West University of Timişoara, România,
stefan1.iovan2@gmail.com

Abstract: *Artificial Intelligence is not just science fiction; it is already part of our daily lives, from using a virtual personal assistant to planning our day to the songs our phones suggest. Artificial Intelligence aims at studying and designing intelligent agents, systems that perceive the environment and maximize the chances of their own success through behavior. In addition to making life easier, intelligent systems help us solve some of the world's greatest challenges: treating chronic diseases, fighting climate change and anticipating threats to cyber security. Artificial Intelligence is one of the most strategic technologies of the 21st century. Europe wants to be at the forefront of these developments - many major breakthroughs in the field of artificial intelligence have been carried out in European laboratories. Approximately one quarter of industrial robotics and robotics products for professional services is made by European businesses.*

Keywords: *artificial intelligence, robotics, cyber security, transformational technology, domain convergence*

1. INTRODUCTION

Artificial Intelligence is a technical term from Artificial Intelligence (AI), which designates a "*field of research*" in computer science. In current speech is a product resulting from this activity. The most accepted definition of artificial intelligence was given by John McCarthy in 1955: "a *computer that behaves in a way that could be considered intelligent if it were a man*".

Many people have tried to answer the question: what is artificial intelligence? The difficulty of finding a definition for this term is (mainly) two:

1. We do not really know what natural intelligence is in it self;

2. Those who try to formulate a definition are complex by the achievements of this field of computer science.

Researchers see themselves compelled to define what artificial intelligence should be, rather than what it actually is in the present. The origin of artificial intelligence as a branch of computer science is concealed in the years of the construction of the first electronic computers [1] that is when mankind first asked: how powerful can these new tools be capable of performing complicated calculations?

The central issues of research in AI are reason, knowledge, planning and learning, natural language processing (communication), perception, and manipulation of physical objects. In the broadest sense, Artificial Intelligence is any technology designed to mimic, in one way or another, the way a human works.

AI technology available today can not copy the human mind and turn it into a computer chip. Instead, the so-called "*human*" part refers to the experience the user perceives: it must be as close as possible to the interaction between two people.

In this sense, Artificial Intelligence systems work, for the most part, as a human works. It has to learn, to adapt to the surrounding conditions [1]. This is the same as it is for humans: by assimilation, processing, and keeping them for use in other similar situations.

2. THE EUROPEAN COMMISSION AND ARTIFICIAL INTELLIGENCE

The European Commission presented last year (2018) a series of measures designed to put artificial intelligence in the service of European citizens and boost Europe's competitiveness in this area. The Commission proposed a three-pronged approach aimed at increasing public and private investment, delivering the necessary training for socio-economic change and ensuring an appropriate ethical and legal framework [2].

The initiative responds to the call by European leaders to devise a European approach to artificial intelligence. Like the steam engine or electric current in the past, artificial intelligence transforms the world we live in. This involves new challenges that Europe needs to address jointly so that artificial intelligence can develop and benefit from it all. Several billions of Euros must be invested by the end of 2020.

The Commission fulfills its role: it gives researchers the incentive they need to develop the next generation of artificial intelligence technologies and applications, and businesses, the means they need to be able to adopt and integrate into their work.

Europe has researchers, laboratories and world-class start-ups in the field of artificial intelligence. Also in the European Union (EU) the robotics sector is heavily developed, and the transport, healthcare and manufacturing fields are world-class sectors that should adopt artificial intelligence to maintain its competitiveness.

However, given fierce international competition, coordinated action is needed to keep the EU at the forefront of developing artificial intelligence. Encouraging financial support and encouraging recourse to artificial intelligence in the public and private sectors of the EU (both in the public and private sectors) should increase investment in research and innovation in the field of artificial intelligence by several tens of billions of EUR by the end 2020.

In order to support these efforts, the Commission is increasing its investments in the Horizon 2020 research and innovation program for the period 2018-2020. It is expected that these investments will mobilize another several billion Euros representing funding in existing public-private partnerships, for example in the area of big data and robotics.

They will support the development of artificial intelligence in key sectors, from transport to health, will allow the networking and strengthening of research centers across Europe across the whole of Europe, and will encourage testing and experimentation [3].

The Commission will also support the development of an "*Artificial Intelligence Platform on Demand*" which will provide access for all users to relevant resources in the field of artificial intelligence in the EU. In addition, the European Investment Fund will be used to provide additional support to businesses and start-ups, allowing them to invest in artificial intelligence.

It is intended that, through the European Fund for Strategic Investments, investments of more than half a billion euro will be mobilized by 2020 in different key sectors.

The Commission will also continue its efforts to create an environment conducive to investment. As data is the raw material for most artificial intelligence technologies, the Commission is proposing a legislative act aimed at making more data available for re-use, as well as measures to facilitate the exchange of data. This includes data from public utilities and environmental data, as well as research data and health data.

2.1. Socio-economic changes generated by artificial intelligence

After entering into the era of artificial intelligence, many jobs will be created, while others will disappear, and most will undergo transformations. The Commission therefore encourages Member States to modernize their education and training systems and to support labor market transitions based on the European Social Rights Pillar.

The Commission will support business and education partnerships designed to attract and retain more artificial intelligence professionals in Europe, set up specialized training programs with financial support from the European Social Fund, support digital competences and skills in the fields of science, technology, engineering and mathematics, entrepreneurship and creativity.

Proposals included in the next EU Multiannual Financial Framework (2021-2027) will also include increasing support for training activities aimed at acquiring advanced digital skills including specific knowledge in the field of artificial intelligence.

It is necessary to ensure an adequate ethical and legal framework. Like any transformational technology, artificial intelligence can raise new ethical and legal issues related to accountability or potentially biased decision-making processes. Technological progress should not mean a change in values.

At the end of 2018, the Commission presented ethical guidelines on the development of artificial intelligence. These have been developed on the basis of the EU Charter of Fundamental Rights, taking into account principles such as data protection and transparency, and taking into account the work of the European Group on Ethics in Science and New Technologies. To help shape these guidelines, the Commission will bring together all relevant stakeholders in a European Alliance for Artificial Intelligence.

Also, by mid-2019, the Commission will publish, in the light of technological developments, a guide on the interpretation of the liability directive for defective products so as to ensure greater legal clarity for consumers and producers in the case of defective products.

2.2. Next steps

The Commission will start working with the Member States to draft a coordinated plan on artificial intelligence. The main objective is to maximize the impact of investments at EU and national level, to encourage cooperation across the EU, to exchange best practices and to define by mutual agreement the way forward to ensure the EU's global competitiveness in this sector.

The Commission will also continue to invest in initiatives that are essential for artificial intelligence, including the development of more efficient electronic components and systems (such as chips specially developed for artificial intelligence operations) in high-performance computing world-wide such as and in the emblematic projects related to quantum technologies and human brain mapping.

3. ARTIFICIAL INTELLIGENCE PROTECTION

Studies show that such large-scale industrial infrastructures are struggling with morally outdated systems, which are hard to replace by their considerable size, and impossible to secure with traditional endpoint security methods.

Companies operating in such domains typically rely on Universal Serial Bus (USB) devices to upgrade IT systems a method that increases the potential for malware and targeted attacks. From recent history, the most common example of a critical infrastructure attack was the Stuxnet worm, which used malware to dismantle an essential part of the country's nuclear program.

In addition, besides the risk of cyber attacks that could cause physical damage or threaten the safety of individuals, it is known that many industrial control systems used on critical infrastructures run outdated operating systems, making them vulnerable to threats.

Even if it was not necessarily measured in lost money, potential damage from companies in areas like the ones mentioned above may be colossal. In energy, for example, the damage generated by a successful computer attack can be quantified, inter alia, in terms of interruptions of power grids for entire geographic areas, which makes such infrastructures often considered national interest.

What do security vendors do to protect such infrastructures from the cyber attacks of the present and, above all of the future? One of the most interesting proposals is the use of artificial intelligence. For example, one of the most famous names in the world of information protection has recently announced that it will launch, in early 2019, a neural network protection solution for critical infrastructure.

According to what the company has revealed so far, the new solution, which comes as an integrated threat scanning platform, will use artificial intelligence to prevent known and unknown attacks on Internet of Things (IoT) devices already in use largely by large industrial firms [6] - and operational infrastructures by detecting and providing protection against malware installed on USB devices.

Why such a concern over USB devices? Several audit studies of large operational infrastructures have shown that up to 50% of USB devices used in such infrastructures are infected with malware. USB devices are offered at various events, are shared by employees and are re-used many times, thus generating the risk of malicious or accidental infection.

The clear advantage of some neural platform solutions proposed by security firms is to simplify the scanning process of devices connected to very large networks. Such a scanning process is critical to global security of hygiene because the operational environments of large industrial firms are often found in isolated areas or in field operations far away from the IT teams of the organization [3, 6].

Once installed, such a neural platform will ensure automatic scanning of the entire network without the need for human presence and will take measures to block the access point or access points detected as potentially harmful until the inserted device is replaced.

Furthermore, at least in the case of the AI-based solution the platform will also detect any attempts to launch machine learning adversity in the attacked network and, through its own machine learning machine, initiate self-learning procedures to provide protection against threats unknown.

Dangers such as the above are as current as possible and will intensify in the future. At the International Security Exhibition held in London in 2018, the participating experts warned about these issues, saying that mankind is becoming increasingly interconnected and that millions of USB devices are connected to the internet in an insecure manner every day, so they are all the chances that some of them will get into networks of critical infrastructure, and thus generate major harmful effects for large areas of the population and even for whole societies.

4. ARTIFICIAL INTELLIGENCE, GROWTH MOTOR

Medium-sized companies globally are much more optimistic about the conditions and opportunities of the business environment than in 2017 according to study findings [4]. Growth prospects improved in 2018 for all major economies, with the International Monetary Fund (IMF) forecasting a 3.9% increase in Gross Domestic Product (GDP) in 2018. In this positive context, business leaders are optimistic about revenue growth.

The annual survey [4] run by 2,766 executives from medium-sized companies in 21 countries and nine key sectors, shows that global confidence in business development has strengthened over the past year. 60% of companies target increases between 6 and 10%, compared with 34% reporting similar year-on-year growth ambitions.

Another 27% target increases of over 10%, a small decrease compared to 2017, when 30% of companies were in this category of significant growth. In addition, none of the 2018 respondents expect a slowdown in growth, compared with 5% in 2017.

Middle-sized leaders plan higher incomes they create more full-time jobs and implement innovative technologies to meet their ambitious growth targets [5]. However, they remain concerned about cash flow deficits, more restrictive loans or lower global demand, which could pose major long-term risks.

4.1. The Race for the Adoption of Artificial Intelligence

Smart automation and machine learning technology have become essential to the growth ambitions of medium-sized companies. Attitudes towards new technologies evolved rapidly compared to 2017.

If in 2017, 74% of global mid-level executives say they will never adopt process automation through RPA (Robotic Process Automation), only 12 months later, 73% of respondents say they are already adopting or planning to adopt artificial intelligence over the next two years.

According to the study [4], companies recognize the need to become more agile. However, by their desire to adopt new technologies and incorporate AI into their business, company leaders are in danger of underestimating the magnitude of cyber threats. In fact, only 7% of them plan to invest in technologies to reduce the risk of cyber attacks in the coming year, and 6% believe that cyber threats are a challenge for growth.

4.2. Domain convergence is accelerating

Domain convergence has become another important factor to boost growth; with nearly a quarter of world leaders (23%) considering that it have the second most significant impact on business after demographic changes (33%). For US business leaders, convergence is the main force that will fuel their growth ambitions (31%). [7]

In a demonstration of confidence in the sustainability of growth 39% of companies intend to increase the number of full-time specialists in the next year. This is a significant increase from 13% in 2017.

In addition, only 1% of respondents intend to reduce the number of employees, decreasing from 9% in 2017. The attraction of talents with the necessary skills is at the forefront of the list of factors that accelerate the growth [6, 7], before the efficiency of the processes and new technologies.

4. CONCLUSIONS

As we have become accustomed to in recent years, the Romanian economy is developing on a model similar to the world economy having the struggle to attract talent and digitization as the main disruptive forces of this growth.

Now, more than ever, we see how technology and diversity of talents influence each other and together they sometimes dramatically trigger the emergence of new sectors and accelerated growth [8, 9]. One of the areas that appears to be of great interest to IT firms and where new technologies are to be deployed in the near future is critical infrastructure in large industrial [8, 9] industries such as oil & gas, energy or transport. Why would specific IT security solutions for such infrastructures be needed?

5. REFERENCES

[1] Marge, R. şi Iovan, Şt. (2018) *Învăţarea şi inovarea baza creşterii performanţelor individuale*, Conferinţa Ştiinţifică cu Participare Internaţională "Simbioza Educator-Manager în Contextul Paradigmelor Educaţionale Inovative", Oradea, 5 – 6 oct., (în curs de publicare);

[2] Iovan, Şt**.** şi Iovan, A.-A. (2016) *Avantajul cunoaşterii şi abordarea proactivă*, Cluj-Napoca: Editura Eikon, România, "Educaţia din perspectiva valorilor**"**, (Coordonatori:, Octavian Moşin, Ioan Scheau, Dorin Opriş), Tom IX: SUMMA THEOLOGIAE, ISBN: 978-973-757-730-6, pag. 197 – 202;

[3] Ivănuş, Cr. şi Iovan, Şt. (2015) *Internet – The Foundation for the Future Societies Permanently Connected*, Bucureşti: Proc. of 16th European Conference (E_COMM_LINE 2015), Romania, ISSN: 2392-7240, ISSN-L: 2066-6829;

[4] Ernst & Young, *EY Growth Barometer*, www.ey.com/growthbarometer, (accesat în dec. 2018);

[5] Iovan, Şt. (2013) *The Importance and the Definition of e-Skills for Europe*, Iasi: Editura PIM, Proceedings of the International Conference: "Transforming the educational relationship: intergenerational and family learning for the lifelong learning society", Romania, ISBN: 978-606-13-1558-1, pag. 258 – 269;

[6] Ivănuş, Cr. şi Iovan, Şt. (2013) *"Internet of Things" – A new Technological Evolution*, Targu Jiu: "Academica Brancusi" Publisher, Annals of the "Constantin Brancusi" University, Engineering Series, Issue 4/2013, (CONFERENG 2013), ISSN: 1842 – 4856, pag. 165 - 170;

[7] Iovan, Şt. (2017) *Problema Competenţelor Digitale în România şi în Europa*, Cluj-Napoca: Editura Eikon, România, Educaţia din perspectiva valorilor (Editori: Dorin Opriş, Ioan Scheau, Octavian Moşin), Tom XII: SUMMA PAEDAGOGICA, ISBN: 978-606-711-686-1, pag. 207 – 212;

[8] Iovan, Şt. şi Marge, R. (2017) *Some Legal Aspects on Cybercrime*, Targu Jiu: "Academica Brancusi" Publisher, Annals of the "Constantin Brancusi" University, Engineering Series, Issue 3/2017, (CONFERENG 2017), ISSN: 1842–4856, pag. 181–186;

[9] Ivănuş, Cr. şi Iovan, Şt. (2017) *Cybercrime in the European Union*, Targu Jiu: "Academica Brancusi" Publisher, Annals of the "Constantin Brancusi" University, Engineering Series, Issue 3/2017, (CONFERENG 2017), ISSN: 1842–4856, pag. 187–192;