Cyber Wars under the Shadow of Artificial Intelligence: A Future Perspective

Utku Kose*‡, Sadi Fuat Cankaya*, Omer Deperlioglu**

*Dept. of Computer Engineering, Faculty of Engineering, Suleyman Demirel University, Suleyman Demirel University, Dept. of Computer Engineering, Faculty of Engineering, E9 Block, West Campus, 32260, Isparta, Turkey

**Dept. of Computer Technologies, Afyon Vocational School, Afyon Kocatepe University, Afyon Kocatepe University, Dept. of Computer Technologies, ANS Campus, Gazligol Street, 03200, Afyonkarahisar, Turkey

(utkukose@sdu.edu.tr , sadicankaya@sdu.edu.tr , deperlioglu@aku.edu.tr)

‡ Corresponding Author; Utku Kose, Suleyman Demirel University, Dept. of Computer Engineering, Faculty of Engineering, E9 Block, Z-23, West Campus, 32260, Isparta, Turkey, Tel: +90246 211 13 91, Fax: +90246 237 08 59, utkukose@sdu.edu.tr

This work was presented at the IDITAI Workshop 2017, which was held at Nisantasi University, Turkey on 28th December 2017.

Received: 18.05.2018 Accepted: 30.06.2018

Abstract- Artificial Intelligence has provided many benefits for achieving better life standards for people. But except from its advantages on improving life standards and solving real world problems effectively, there is currently a remarkable discussion on possible side-effects and even dangerous results caused by using Artificial Intelligence. In this context, it is also a serious research interest to think about cyber wars in which intelligent systems will probably have active role in the future. Moving from that, this paper presents a general discussion on how cyber wars of the future will be shaped by Artificial Intelligence based systems. By considering currently popular Artificial Intelligence oriented problems solutions and techniques, the paper tries to open readers' mind about the future with full of Artificial Intelligence and future perspectives in cyber wars.

Keywords- artificial intelligence; cyber wars; intelligent systems; intelligent agent; future of artificial intelligence

1. Introduction

As a result of more use of computer systems and influence of effective communication technologies like Internet, the world has transformed into a unique form of hybrid environment combining both real and virtual experiences, in order to make using, editing and sharing information fast and accurate. At the end, we are experiencing a real world dominated widely by the support of a digital world [1-4]. Even simple tasks done during a daily basis are easily done in the computer systems and even transferred to a very far place over just cables of communication systems. Here, although there are many different technological developments on the background, one of them gives us many discussions and predictions to be made on it. That technology is called as Artificial Intelligence and as also a scientific field, it has an important role on the way of humankind

and maybe even universe.

Artificial Intelligence has many innovative outputs in terms of applications – developments – improvements. In this context, it has a very wide application and problem solution scope as a result of technological achievements done so far [5-8]. Machine Learning, which is the most essential sub-field of Artificial Intelligence [9] has made it more possible to design autonomous systems and currently there is a remarkable interest in especially Machine Learning oriented technologies and also its new formation: Deep Learning, which was introduced to deal with great numbers of data, are attracting many people's attention [10]. On the other hand, while Artificial Intelligence is passing all innovative stages with large steps, there is also a serious discussion about its roles in the future. Because intelligent systems make our life greatly practical and they are strong enough to solve almost all real world problems somehow, role of such systems in different fields are widely discussed by considering their advantages, disadvantages and risks. In addition to discussions on how to achieve robust and beneficial Artificial Intelligence [11], there is also a remarkable effort to evaluate effects of intelligent systems in terms of ethics and safety [12-15]. In order to make everything as clear as possible and improve the associated literature in this manner, some future perspectives regarding different uses of Artificial Intelligence should be discussed.

In the context of the explanations provided so far, objective of this paper is to present a general discussion on how cyber wars of the future will be shaped by Artificial Intelligence based systems. It is clear that the future unfortunately open for cyber wars done in the digital world, as a result of more interaction occurred between the real and the digital world. Because of unstoppable needs of nations for more resources and data – information for having a strong place and rule the established hierarchical country-based orders. By considering currently popular Artificial Intelligence oriented problems solutions and techniques, the paper tries to open readers' mind about the future with full of Artificial Intelligence and future perspectives in cyber wars.

Moving from the subject of the paper, the remaining content is organized as follows: The next section is devoted to some predictions about how future of the world and cyber wars will possibly be. Following that section, the third section provides a general discussion what kind of applications will Artificial Intelligence based systems provide in such cyber wars of the future. Finally, the paper is ended by discussions about conclusions and some future work.

2. Future Predictions Based On Artificial Intelligence

As a result of rapid improvements in Artificial Intelligence, many problem solutions that we could just see in science fiction movies or series in the past are now just real things. Although the exact intelligent machines like the ones similar to humans and acting in science-fiction movies have not been developed well enough yet, such developments and many more seems possible in a theoretical manner. Nowadays, there is a serious separation among researchers that some of them think about rise of risky 'super-intelligent' machines in the future and some other ones think still that such bad ideas will be always remain as science-fiction [16]. But at least it is now possible to derive – imagine some ideas on how an optimum future will be thanks to support of Artificial Intelligence.

2.1. Autonomous Future

As one of the most important functions of Artificial Intelligence, there future will be probably based on mostly existence of autonomous systems – machines. Even today computer systems are very useful to eliminate many human oriented disadvantages and have more accurate, effective and fast solutions for real world problems, potential of Artificial Intelligence supported systems will indisputably great to cause many developments and improvements in the future. At this point, we can indicate that almost all tasks done by humans or both humans and computer systems will be done by autonomous intelligent systems. Because the nature of human always need for a better, practical daily life and because all these needs are met with innovative technologies, which take needs more steps far again and again, a very predictable view about that can be more active role of an autonomous future.

2.2. More and More Dominant Digital World

As it was mentioned already at early paragraphs of this paper, there is the fact that the digital world has a remarkable dominance over the real world. Although currently it is a common interaction of both real and digital world, which is affecting the humankind, the future with Artificial Intelligence will bring a greatly improved dominancy of the digital world. People will of course experience a real world around them (in the most positive thinking) but flow of life and even the nature will be shaped by numerical things running on the background of the 'ruler' digital world. Because the digital world will be probably owned by Artificial Intelligence and giving a 'digital personality' in a philosophical manner to it.

2.3. Existence of the Super-intelligent Machines – Systems

Still we cannot predict well enough whether it will be good or not for the humankind, existence of the super-intelligent machines – systems will be a real, common thing in the future with Artificial Intelligence. Even today there are many different types of intelligent machines – systems, which are better than in solving problems according to the most intelligent person in the world, it is not too science-fiction to think about existence of the concept of superintelligence, which is for

explaining the intelligence surpassing the human brain in the context of general intelligence [17] and its outputs as machines or intelligent software systems running on the background [18, 19].

2.4. Realization of Technological Singularity

Among research works regarding the future of Artificial Intelligence, there is a serious hypothesis, which briefly expresses that the Artificial Intelligence will result to transformation of civilizations and the human nature into new formations radically, as a result of its greatly improved influence in the world of the future [20-22]. Again we do not know if it will be good or not for us, realization of this hypothesis can be possible in a theoretical manner by looking at the latest stage Artificial Intelligence has reached today.

2.5. Changed Rules of Tasks – Works – Events

As a result of many changed – transformed things because Artificial Intelligence and many other factors, the 'doing something' will be of course changed in the future. As a result of instant use of intelligent systems, many tasks and works done by humans have new rules, which will maybe useful and important for only Artificial Intelligence based systems. The future will also probably bring new types of jobs, tasks done by intelligent systems – machines. That change will also cause new jobs to be done by humans and many different jobs that are done widely by humans currently and will be taken over by intelligent systems – machines in the future, as discussed in the literature [23]. All these changes will be associated with other ideas on the future as mentioned so far. Additionally, the events of the future will be instantly under the shadow of Artificial Intelligence. For example, political decisions, medical treatments, even dealing with natural disasters will be probably taken to different levels thanks to intelligence machines – systems. In the context of subject scope of this paper, we can also think about cyber wars, which are currently based on critical roles of humans as in the role of hackers controlling computer systems, will probably occur differently in the future because of Artificial Intelligence.

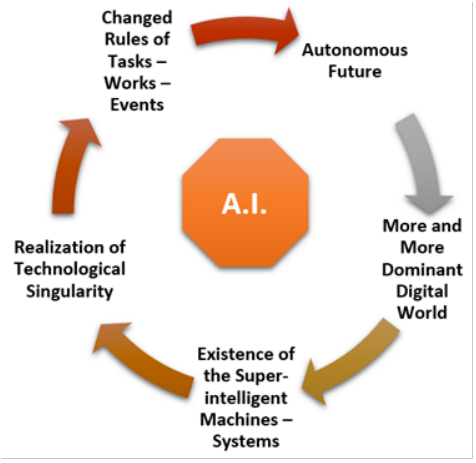

Figure 1. Some of future predictions based on Artificial Intelligence

3. Results and Discussion

The term of cyber war is used for defining the attacks – works done within the digital world of computer systems to get control of other digital systems or perform other harmful tasks like stealing data, causing fatal errors – hardware and software oriented problems and many more [24-26]. In this context, it is a widely researched subject because of increasing importance of storing valuable data in computers and computer oriented systems. Because of its importance, even nations have started to special education processes for having trained staff to deal with the problems caused by cyber-attacks. In time, the term of cyber war has gained popularity as a result of discussions about that the future of nations will be directed by also cyber wars performed in the digital world [27-29]. Of course, this term will gain new meanings as a result of technological developments and currently, a remarkable discussion can be made by taking the Artificial Intelligence into consideration. The following paragraphs have been written down by the authors by imaging possible scenarios of cyber wars that will be done by intelligent systems of the future.

3.1. Wars Not Too Controllable by Humans

It is not too false to mention that advanced Artificial Intelligence of the future will bring less control to humans. Because of that we can draw a scenario of cyber wars done among intelligent agents, which are not too controllable by humans. Today, it is possible to develop an intelligent system and give directives to it for performing desired tasks. But in the future, the fact of 'intelligent systems developed by intelligent systems', which will probably be not too possible to control how intelligent systems will act during cyber wars. So, destinies of such wars will probably be not definable by humans. At this point, we can also just think about possibilities on how humans can develop ancestor intelligent systems having pre-knowledge provided by humans and having at least some mechanisms to control the future developments. This question is somehow input for research works regarding Artificial Intelligence Safety [30, 31].

3.2. Hierarchical Agents

The future developments of Artificial Intelligence will probably include advanced agents, which have more awareness-level according to the ones today and such agents will have ability to develop new agents, and even form a general hierarchical organization among them to deal with cyber wars better. In detail, it is possible to think about agents, which are in the role of soldiers – attackers in cyber wars, and also some other agents, which are commanders or just workers on the background to track the war and maybe design war strategies. All these roles are of course related to advanced, intelligent agents, which are able to think and behave in too small periods of time by also being aware of their roles, state of all other agents, which are also allies and many other things that we cannot control as humans but advanced Artificial Intelligence can perform

many tasks over them, as including analyzing, evaluating, predicting and controlling.

3.3. Defensive and Offensive Systems

As similar to the white hat hackers today, there will be defensive Artificial Intelligence based systems in the future cyber wars. In a digital, war environment of intelligent systems – agents, role of such systems will be only protecting the data or other intelligent systems. These terms of 'defensive' and 'offensive' systems maybe just top hierarchical statues of the future agents and the roles mentioned under the previous sub-section can be included under these two hierarchical terms. If we discuss more about defensive and offensive systems, it is possible to mention that all these systems will be connected to whole smart devices and any other things regarding the digital world of the future. Because of many different environmental factors to be considered and also strong enough technological capabilities to deal with all of them in the future, there will probably be need to run Machine Learning oriented systems on the background of cyber war environment by locating fast and advanced enough agents to be located on the war arena by having no learning abilities or low-level learning abilities to perform their tasks well enough and protecting the 'learning' structure of the Artificial Intelligence from any attacks done by other intelligent systems.

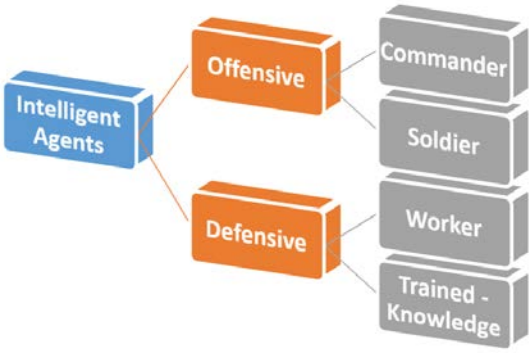

Figure 2. Hierarchical agents within future of cyber wars.

3.4. Advanced Deep Learning and Internet of Things

It is clear that the future is full of surprising developments including also newer types of Artificial Intelligence oriented techniques and some other supportive technologies but we still can imagine something by moving from current developments. In this sense, because of increasing number of data and unpredictable amount regarding the future, we can think about advanced form of Deep Learning, which is a popular Artificial Intelligence technique dealing with Big Data today [32-34]. At this point, because it will be always important for Artificial Intelligence to perform effective learning mechanism even environmental factors are increased, the Deep Learning will evolve different kinds of 'Machine Learning oriented techniques' and the term of 'advanced' is currently enough to indicate that enough. Additionally, the future will be also the arena of Internet of Things, which is a network of intelligent machines communicating each other [35, 36] and advanced future with full of Artificial Intelligence will require advanced form of also that technology.

By doing a connection among the mentioned techniques – technologies and cyber wars, we can predict that the future of cyber wars will be very critical for 'learning' intelligent systems and because both the enemy and ally will be digital, intelligent system, fast and accurate learner systems taking place on the background will be having more advanced algorithmic structures. It is possible to express that the destiny of cyber wars will depend on critical decisions made by well-trained intelligent systems, which will also interact with intelligent machines and use them as ally in the cyber war or just try to hack them to obtain important data, take advantages and also win the war eventually in this manner.

3.5. Encryption – Decryption Wars on the Background

The future of cyber wars will also be full of encryption – decryption performances done by intelligent machines at the level to which any human cannot reach. Because the whole cyber war environment will include Artificial Intelligence based systems, interaction among ally systems will be based on encrypted digital languages developed by them. Here, it will be not the data of a nation or person encrypted to be protected by intelligent systems but also themselves not to be hacked by other intelligent systems or just having clear communication with other ally agents without being affected by other instant data flow occurred during cyber wars.

Figure 3. Some ideas – scenarios regarding future of cyber wars with Artificial Intelligence

3.6. Advanced Social Systems to Hack Systems and Humans

Even a typical cyber war occurs in the digital world, it may have some connections with the human factor because the possibility of false actions done by humans often be used by hackers to reach desired objectives. In the future, cyber wars will probably include also advanced agents, which have some 'social' abilities and knowledge to hack other intelligent agents – systems or humans. Although some encryption – decryption wars (mentioned under the previous sub-section) can take place in case of interaction between social agent and a soldier agent, that situation will be not safe enough for humans if they encounter with a social agent trying to tricking him / her. On the other hand, there is also a research interest in brain-computer interfaces as a technology regarding the future and at this point, hacking of such systems is another discussed problem in the context of data safety [37]. Considering that, one of the roles of social agents will probably be hacking such systems and so, there will be also protective intelligent agents – systems to defend such systems in the future.

It is of course not clear if humans will take enough role on protecting data or we will just give all responsibilities to Artificial Intelligence but the authors think that human can be key actors even in the advanced future, because they are the exact sources of all these technological developments and improvements. But when we focus on an autonomous, intelligent system as a product Artificial Intelligence, there is still something to discuss and analyze for any possible dangerous – harmful intelligent system, which is not always humans' technological friend.

4. Conclusions and Future Work

This paper has focused on possible scenarios on future of cyber wars done with the existence of Artificial Intelligence and also express some ideas regarding that. Out of the expressed ideas – scenarios here, there are many different probabilities to think about but current state of Artificial Intelligence and technological developments enable us to derive some ideas and scenarios of cyber wars as provided in the paper. Cyber wars are key factors of the future any the future will focus more on cyber wars instead of physical wars. But there is not any sign that cyber wars will be less harmful and destructive for the humankind. Because the whole world is highly connected to the digital world and the 'data', we can think that destructive effects of cyber wars in the future may be more than we can imagine.

In addition to the research provided here, the authors will also follow some future works planned. In this context, theoretical background will be always followed and the literature will be supported with similar research works. Also, there will be some research efforts to develop and simulate some cyber wars oriented applications done with current Artificial Intelligence based techniques – systems.

References

[1] A. Martin, "Digital literacy and the 'digital society'". Digital literacies: Concepts, policies and practices, 30, 2008, 151-176.

[2] Y. K. Dwivedi, M. R. Wade, and S. L. Schneberger, Information Systems Theory: Explaining and Predicting Our Digital Society (Vol. 1). 2011, Springer Science & Business Media.

[3] K. Mossberger, C. J. Tolbert, and R. S. McNeal, "Digital Citizenship: The Internet, Society, and Participation. 2007, MIT Press.

[4] B. M. Compaine, (Ed.). The Digital Divide: Facing a Crisis or Creating a Myth?. 2001, MIT Press.

[5] L. Iliadis, I. Maglogiannis, H. Papadopoulos, S. Sioutas, and C. Makris, Artificial Intelligence Applications and Innovations. 2016, Springer International Pu.

[6] A. I. Strong, "Applications of Artificial intelligence & associated technologies". Science [ETEBMS-2016], 2016, 5(6).

[7] N. J. Nilsson, Principles of Artificial Intelligence. 2014, Morgan Kaufmann.

[8] P. R. Cohen, and E. A. Feigenbaum, (Eds.). The Handbook of Artificial Intelligence (Vol. 3). 2014, Butterworth-Heinemann.

[9] R. S. Michalski, J. G. Carbonell, and T. M. Mitchell, (Eds.). Machine learning: An artificial intelligence approach. 2013, Springer Science & Business Media.

[10] M. Chui, Artificial Intelligence the Next Digital Frontier?. McKinsey and Company Global Institute, 2017, 47.

[11] S. Russell, D. Dewey, and M. Tegmark, M. "Research priorities for robust and beneficial artificial intelligence". Ai Magazine, 36(4), 2015, 105-114.

[12] P. Lin, K. Abney, and R. Jenkins, R. (Eds.). Robot Ethics 2.0: From Autonomous Cars to Artificial Intelligence. 2017, Oxford University Press.

[13] J. Davies, "Program good ethics into artificial intelligence". Nature, 2016, 538(7625).

[14] R. V. Yampolskiy, and M. S. Spellchecker, Artificial Intelligence Safety and Cybersecurity: a Timeline of AI Failures. arXiv preprint arXiv:1610.07997, 2016.

[15] M. R. Waser, Discovering the Foundations of a Universal System of Ethics as a Road to Safe Artificial Intelligence. In AAAI Fall Symposium: Biologically Inspired Cognitive Architectures,

2008 (pp. 195-200).

[16] V. C. Müller, and N. Bostrom, N. Future progress in artificial intelligence: A survey of expert opinion. In Fundamental issues of artificial intelligence (pp. 553-570). 2016, Springer International Publishing.

[17] N. Bostrom, Superintelligence: Paths, dangers, strategies. 2014, OUP Oxford.

[18] S. Schneider, (Ed.). Science Fiction and Philosophy: From Time Travel to Superintelligence. 2016, John Wiley & Sons.

[19] F. Heylighen, Return to Eden? Promises and perils on the road to a global superintelligence. The End of the Beginning: Life, Society and Economy on the Brink of the Singularity. 2014, Retrieved December 1, 2017, from http://pespmc1.vub.ac.be/Papers/BrinkofSingularity.pdf.

[20] M. Shanahan, The Technological Singularity. 2015, MIT Press.

[21] B. Goertzel, "Human-level artificial general intelligence and the possibility of a technological singularity: A reaction to Ray Kurzweil's The Singularity Is Near, and McDermott's critique of Kurzweil". Artificial Intelligence, 171(18), 2007, 1161-1173.

[22] R. Kurzweil, The Singularity is Near: When Humans Transcend Biology. 2005, Penguin.

[23] S. Bernezzani, 10 Jobs Artificial Intelligence Will Replace (and 10 That Are Safe). 2017, HubSpot.com. Retrieved December 1, 2017, from https://blog.hubspot.com/marketing/jobs-artificial-intelligence-will-replace

[24] R. A. Clarke, and R. K. Knake, Cyber War. 2014, Tantor Media, Incorporated.

[25] A. A. Galushkin, "Theoretical and legal aspects of cyber warfare". Mediterranean Journal of Social Sciences, 7(1), 2016, 570.

[26] J. Chen, and A. Dinerman, On Cyber Dominance in Modern Warfare. In European Conference on Cyber Warfare and Security, 2016, (p. 52). Academic Conferences International Limited.

[27] J. Arquilla, and D. Ronfeldt, "Cyberwar is coming!". Comparative Strategy, 12(2), 1993, 141-165.

[28] J. Stone, "Cyber war will take place!". Journal of Strategic Studies, 36(1), 2013, 101-108.

[29] J. Carr, Inside Cyber Warfare: Mapping the Cyber Underworld, 2011, O'Reilly Media, Inc..

[30] R. V. Yampolskiy, and M. S. Spellchecker, Artificial Intelligence Safety and Cybersecurity: a Timeline of AI Failures, 2016, arXiv preprint arXiv:1610.07997.

[31] R. Yampolskiy, and J. Fox, "Safety engineering for artificial general intelligence". Topoi, 32(2), 2013, 217-226.

[32] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning". Nature, 521(7553), 2015, 436-444.

[33] X. W. Chen, and X. Lin, "Big data deep learning: Challenges and perspectives". IEEE Access, 2, 2014, 514-525.

[34] M. A. Alsheikh, D. Niyato, S. Lin, H. P. Tan, and Z. Han, "Mobile big data analytics using deep learning and apache spark". IEEE Network, 30(3), 2016, 22-29.

[35] J. Ritz, and Z. Knaack, "Internet of things". Technology & Engineering Teacher, 76(6), 2017, 28-33.

[36] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey". Computer Networks, 54(15), 2010, 2787-2805.

[37] S. Martin, AI warning to humanity: Brain-computer interfaces could be HACKED by robots, experts say, 2017, Express.co.uk – Web Site. Retrieved December 2, 2017, from https://www.express.co.uk/news/science/882933/artificial-intelligence-US-defense-department-elon-musk-neural-implants