Clauberg R.
Doctor in Natural Sciences, Associate Professor, Department of International Management, Economics and Information Security, Higher School of Social Sciences, NSLU.
r.clauberg@hispeed.ch

THE INFLUENCE OF ARTIFICIAL INTELLIGENCE ON INTERNATIONAL SECURITY IN GEOPOLITICAL CONFRONTATIONS IN THE 21ST CENTURY

Ключевые слова: искусственный интеллект, дроны, роботы, фейковые новости, военные стратегии.
Keywords: artificial intelligence, drones, robots, fake news, military strategies.

Introduction

Presently the influence of artificial intelligence (AI) on all kinds of processes is a hotly discussed aspect. This article will concentrate on the area of international security in geopolitical confrontations. In 2023 Henry Kissinger and Graham Allison published an article titled "The Path to AI Arms Control" [6] in which they described their view on artificial intelligence with the USA and China as the presently only AI superpowers. They compared the situation of AI with that of nuclear bombs used in Hiroshima and Nagasaki and urged the leaders of both countries to start negotiations to stop the uncontrolled spreading of AI. If such a renowned politician as Henry Kissinger together with Graham Allison — adviser to every USA secretary of defense for presidents Reagan to Obama — comes to such a conclusion, it is necessary to analyze the situation from a fundamental point of view and identify the explicit risks of this technology in situations of geopolitical confrontations in our time as well as the future. Kissinger's and Allison's comparison of AI with a nuclear bomb points to a view which envisions artificial intelligence as a very specific and very expensive system with an enormous destruction potential. To verify, refuse or substantially modify this conclusion we must analyze the characteristics of AI with a special focus on its potential impact on future geopolitical confrontations. This includes open wars as well as more hidden operations to change the present status of specific nations or the entire world.

At this point, we should very briefly explain the basics of artificial intelligence. AI is based on the application of algorithms. An algorithm is a sequence of instructions to perform a specific operation or application. Algorithms may be written entirely in software or may be physically implemented in application-specific neural networks trained for the application. The neural network solutions are the more complex and flexible solutions, but they always need their physically existing neural network which may be implemented into a drone or other type of robot. On the other hand, the software implementation of an algorithm can be implemented into a computer virus or complex computer worm [4] and then transferred into a specific computer system. The computer virus or worm implementation allows very sophisticated attacks on cyber-physical systems [1] which the virus or worm will modify to change the function of the cyber-physical system.

In the following we will first consider autonomous drones and robots, then attacks on infrastructure and industrial production, followed by AI for tactical and strategic decisions, and AI generation of fake news.

Drones and robots

In the last two years small, inexpensive drones in large numbers, overwhelmed expensive border protection systems in Israel, even the famous Iron Dome came close to its limits. They also damaged cargo ships in the Gulf of Aden, thereby stopping corresponding commercial traffic. These drones were not products of the named AI superpowers (USA and China), some were self-build others probably came from Iran. Also, Israel's military uses AI controlled drones and reports that especially the introduction of AI systems which create a coordinated swarm of drones is much more efficient than the corresponding number of drones acting uncoordinated [3]. In 2020 I had already published an article which analyzed the chances and threats of cyber-physical systems and artificial intelligence [1], and stated that all hardware and software components, as well as all necessary knowledge to build AI-controlled drones were openly available at very

low cost. Therefore, we can say that Kissinger and Allison were right about the importance of AI, but they made one important error — AI is applicable in all or nearly all areas, it is not like an expensive nuclear weapon which only superpowers can afford. AI enables building cheap, but efficient unmanned autonomous operating vehicles already with publicly available information and components. AI is a tool, applicable in many different areas. Most tools can be changed into a weapon without a large effort. Many people already use AI tools from different sources for their job or for personal hobbies. Yes, there are applications which may need very large expensive data-centers to train their AI, but in the battlefield, we only need the trained units which fit into the drones and robots. AI may be as important as nuclear bombs but is very different from a nuclear bomb.

Nevertheless, the military activities of the last two years show the need to include drones and robots into military strategies. In addition, drone-based surveillance enables control of much larger areas than with standard solutions. And drones usually don't rely on GPS but use other means like visual objects to identify their position and to find their path to an aim. Also, drones may be operating in sizes where they are very difficult to detect. Already in 2019 autonomic nano-drones (size of a few square-centimeters) with fully operating navigation systems were reported [12] and the European Tornado fighter in the 1980s used visual objects together with path calculations based on starting position, velocity, and directions of the flight to improve the determination of its position. Due to these capabilities swarms of small drones may be able to survey very large areas to detect hidden military units. Mark A. Milley (Chairman of the USA Joint Chiefs of Staff from 2019 to 2023) and Eric Schmidt (Ex-Chair of Google) [10] therefore conclude that the occurrence of small and cheap unmanned vehicles (in air, on earth or under water) requires not only a change of the military procurement system from very expensive systems with a ten year procurement cycle to one enabling also much smaller procurement times for cheap, fast changing systems, but in addition requires substantial changes in military strategy and education due to the enhanced surveyance possibilities of the new tools.

Besides drones there is the possibility to use small robots as the first line to enter dangerous territories. This could substantially decrease the number of human soldiers becoming victims to hidden mines or other similar traps. In principle one can even imagine a complete change with autonomous robot systems as the major force in future wars and humans only far behind the front lines. The goal then would be to destroy the enemy's robot force and the infrastructure necessary to survive and thereby enforce a capitulation.

AI for attacks on infrastructure and industrial production

In Industry 4.0 or Smart factory projects there are computer-controlled infrastructure systems as well as industrial production systems connected to the public internet. Already in 2020, I warned that the coupling of information technology with operational technology exposes previously protected operational technology to the known attacks of information technology. Operational technology in such systems is now exposed to cyber-attacks by highly sophisticated computer worms [1, 4]. Computer worms are a specific form of artificial intelligence realized by algorithms in software instructions instead of those physically implemented as artificial neural networks. The Stuxnet worm [2, 4] demonstrated its capability to destroy industrial production systems by first analyzing the physical as well as software parts of the system, and only after verification that this was one of the systems it should destroy, it started to modify the systems parameters necessary to destroy it. Therefore, it seems clear that corresponding artificial-intelligence-based attacks on infrastructure should be able to destroy important water and energy controlling systems as well as disturbing all kinds of transport systems. Experience from past wars shows that a substantial disturbance of water, energy, and transport systems critically weakens the defensive capacities of an enemy.

AI for tactical and strategic decisions

Until recently, the use of AI in the USA military was limited to the analysis of satellite or airborne photographs, and other data sources in project Maven (Algorithmic Warfare Cross Functional Team). In 2020 Maven for the first time was coupled to an M142 Himars—or High Mobility Artillery Rocket System and demonstrated the automatic destruction of a tank identified by AI from an airborne photograph [8]. There are advocates of a fast transition of the AI system

from laboratory to real combat who fear that the USA will fall behind China in AI. But this reference also reports that these advocates are countered by sceptics who believe that the USA military's networks and data are not yet good enough for this.

The USA is not the only country who applies AI to military activities. Already in 2023 Israel was reported to embed AI systems in military operations for selecting targets for air strikes with aircrafts as well as drones [3, 11]. In all these cases one driving argument is that advanced AI algorithms may surpass human capabilities and therefore can decide the winner. The problem with such AI systems is of course that up to now we don't have a solution to proof the correctness of systems built on artificial neural networks (ANN). There is no software code which can be checked for correctness. There only is a highly complex neural network whose connections between neurons are based on its underlying architecture as well as on the data used to train the ANN. There are many issues observed with such ANNs caused by the choice of data used to train the ANNs. In military activities such an error may kill a huge number of innocent people and evolve a minor local war into the next world war.

Besides these AI-based combat systems, there are war-game-based analyses of political and military strategic decisions. Kissinger, Schmidt, and Mundie [7] consider the use of artificial intelligence for decision making and discuss that AI on the one hand introduces a new possibility for objectivity in strategic decision making, but that on the other hand experiences with AI based war-games point to a stronger tendency for escalation and the use of excessive force than in such games where decisions are made by humans. These authors also believe that there is a tenuous and shifting equilibrium in present power distribution and fear that a severe asymmetric adoption of AI could create a very dangerous world. Others may see a different situation with an imbalance between the developed and the still developing nations as the reason for many issues. But in both views, it looks likely that there will be a race to adopt AI for military purposes.

AI generation of fake news

Besides the direct war strategies, there is the possibility to use AI to create extremely realistic looking false information [5, 9] to influence political decisions or elections and potentially even start wars this way. Known examples are discriminating fake photographs, audio reports, or videos of politicians or other important public figures. But knowing about this kind of fake news and the difficulty to realize the fake, we can easily imagine very real looking false news about terror attacks or movements of military units. While the creation of false information is reported part of warfare since at least 2500 years ("The art of war" attributed to Sun Tzu), the most advanced creation of these kind of fake pictures, audio messages, and videos started with the appearance of Generative Adversarial Networks in which one artificial neural network is used to test the fit of a presented object against a large number of known real objects and a second artificial neural network creates and adapts new objects-to-test until the testing neural network accepts the new creations as true objects. Published successful results cover pictures of art as well as created fake videos of famous politicians. But, as mentioned above, fake pictures or videos of troop movements may be even more decisive in the situation of a war. The search to improve the methods to identify fakes is of course in a race with the search to improve the quality of fakes so that they are indistinguishable from real pictures or videos.

Conclusion

In total, the sections about drones and robots, potential attacks on infrastructure, the use of AI for tactical and strategic decisions, and the potential for generating fake news show the broad range of applications for AI in modern geopolitical confrontations. Realizing all these dangers which can stem from artificial intelligence systems, the natural reaction of politicians will be of course a cry for extreme control of artificial intelligence products, but as mentioned before, AI is already an important factor in many technologies, components for AI systems are freely available, and the necessary knowledge for creating arbitrary AI tools from available components is also available. The usability of AI components for civilian as well as military applications makes an efficient control nearly impossible. The pandora box has been opened and can't be closed anymore. Also, AI tools offer huge positive results for humanity. So, the only way forward seems to be to adapt military and public security systems as well as politics to the new reality.

References

1. *Clauberg R.* Cyber-physical systems and artificial intelligence: chances and threats to modern economies // Мировые цивилизации. — 2020. — № 3–4(5). — С. 1–9.
2. *Farwell J. P., Rohozinski R.* Stuxnet and the Future of Cyber War // Survival. — 2011. — No 1(53). — P. 23–40.
3. *Gross J. A.* In apparent world first, IDF deployed drone swarms in Gaza fighting // The Times of Israel. — https://www.timesofisrael.com/in-apparent-world-first-idf-deployed-drone-swarms-in-gaza-fighting/
4. *Karnouskos S.* Stuxnet worm impact on industrial cyber-physical system security. — 2011. — P. 4490–4494. — https://www.researchgate.net/publication/228456054_Stuxnet_Worm_Impact_on_Industrial_Cyber-Physical_System_Security
5. *Kaur A.* [et al.]. Deepfake video detection: challenges and opportunities // Artificial Intelligence Review. — 2024. — Vol. 57, N 159.
6. *Kissinger H. A., Allison G.* The Path to AI Arms Control // Foreign Affairs. — https://www.foreignaffairs.com/united-states/henry-kissinger-path-artificial-intelligence-arms-control
7. *Kissinger H. A., Schmidt E., Mundie C.* War and Peace in the Age of Artificial Intelligence // Foreign Affairs. — https://www.foreignaffairs.com/united-states/war-and-peace-age-artificial-intelligence
8. *Manson K.* AI Warfare Is Already Here // Bloomberg.com. — https://www.bloomberg.com/features/2024-ai-warfare-project-maven/
9. *Maras M.-H., Alexandrou A.* Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos // The International Journal of Evidence & Proof. — 2019. — No 3(23). — P. 255–262.
10. *Milley M. A., Schmidt E.* America Isn't Ready for the Wars of the Future // Foreign Affairs. — 2024. — No 5(103). — P. 26–37.
11. *Newman M.* Israel Quietly Embeds AI Systems in Deadly Military Operations // Bloomberg.com. — https://www.bloomberg.com/news/articles/2023-07-16/israel-using-ai-systems-to-plan-deadly-military-operations
12. *Palossi D.* [et al.]. A 64-mW DNN-Based Visual Navigation Engine for Autonomous Nano-Drones // IEEE Internet of Things Journal. — 2019. — No 5(6). — P. 8357–8371.

Ковалев С.Г.
д.э.н, профессор, профессор Санкт-Петербургского государственного экономического университета

ЦИФРОВИЗАЦИЯ МИРОПОРЯДКА: ГЛОБАЛЬНАЯ ТЕНДЕНЦИЯ И СТРАТЕГИЯ РФ

Ключевые слова: цифровизация миропорядка, БРИКС, экономика созидания РФ.
Keywords: digitalization of the world order, BRICS, economics of creation of the Russian Federation.

Выделим в данной проблеме три момента: 1) становление новейшего миропорядка как цифрового; 2) БРИКС и цифровые деньги в глобальной цифровой нейросети; 3) экономика созидания для РФ как стратегия не попадания в ловушку цифрового неоимпериализма.

1. Становление новейшего миропорядка как цифрового

Новейший миропорядок — это смысловое и реальное планетарное явление. Миропорядок многомерен, он находится в новой фазе своего становления, Ялтинско-Потсдамское политическое и экономическое устройство мира сменяется новым. Однозначно определить его сущностную квинтэссенцию и формы сложно, но есть отдельные черты: а) новая многосторонняя