# INTELLIGENCE AND AI

**Eros-Adrian ASĂNACHE***

**Abstract:**
*In today's reality, marked by technological transformations at an accelerated pace, Artificial Intelligence (AI) is emerging as a new player in intelligence operations, thus redefining the traditional paradigms of intelligence collection, analysis and exploitation. This paper aims to analyse the practical applications of AI, the challenges and benefits brought to Intelligence work. In the same context, it should be mentioned that the ethical and strategic risks generated by the integration of AI in the decision-making process will also be discussed, ranging from simple algorithmic errors and unintentional discrimination to the threat posed by deep fake information manipulation. Thus, a balanced approach is required between technological innovation and the benefits of AI, and the responsibility of the measures taken, by generating a modern intelligence system that meets both the security needs of states and their democratic values.*

**Keywords***: artificial intelligence; intelligence operations; national security; digital surveillance; deep fake.*

## Introduction

The accelerated technological developments of the 21st century have led to profound transformations in national security. In a global context where hybrid threats, transnational terrorism, cyber warfare and international conflicts are present, the way of looking at the conduct of intelligence operations needs to be rapidly adapted by national security agencies. Today's realities show that major world powers such as the US, China and EU states are adapting their intelligence structures to new digital realities.

* Graduate Student, "Mihai Viteazul" National Intelligence Academy, e-mail: erosadrianasanache@ gmail.com. Disclaimer: the material is a reflection of the authors' opinions and beliefs, and does not represent the opinions, policies or the views of the Romanian Intelligence Service or the National Intelligence Academy "Mihai Viteazul".

Artificial intelligence is gaining increasing importance in national security issues by offering extended capabilities to analyse, anticipate and respond to contemporary threats. AI is thus emerging as one of the most revolutionary tools in this respect, which can increase the efficiency of operations, while at the same time facing challenges related to their ethical and legal nature.

The aim of the paper is to highlight how AI has begun to transform the information activity by moving to a digitized system defined by automations, decision algorithms and predictive-predictive systems. The difficulties in this field are also represented by the delegation of decision to non-human systems, with the possibility of generating errors in strategic contexts and the impossibility to control the effects of such decisions. In this paper, analytical methods such as factorial and cost-benefit analysis will be addressed, based on information obtained from the online environment.

## Technologies with practical application in intelligence work

Technologies refer to the totality of techniques, methods, processes and tools used to create goods or services or to achieve objectives.

Since 2020, with the onset of the COVID-19 pandemic, there has been an explosion in the volume of online data. Big Data thus began to take on increasing importance, with algorithms beginning to learn, analyse and turn data into forecasts. The years 2021 and 2022 see a massive development of machine learning related processes. Starting in 2023, Big Data is helping to create intuitive platforms and complex analytics at the click of a button, also at the same time concerns about GDPR compliance are growing. In 2025, Big Data can be defined as a true partner, where it is no longer just a tool, but a partner.

**Machine Learning (ML)**: performs automated analysis of big data; moreover, ML can predict reactions and actions based on already learned patterns and generate relationships between actors and events. For example, ML algorithms are used in cyber-attack prevention systems to detect suspicious behaviours before they become real threats, such as the Darktrace platform, which uses ML for corporate network security (Sommer and Paxson, 2010).

**Natural Language Processing (NLP)**: is used to analyse and extract the essential meaning of written or spoken texts, for example in the detection of hostile actions against national security of subversion, extremism or terrorism. An example is the use of NLP in online message monitoring to identify radical speech and terrorist plots, such as the Jigsaw Perspective platform used to detect hate speech on the internet (Burnap and Williams, 2015).

**Computer Vision**: takes place by analysing satellite or drone imagery; it uses facial recognition technology and has practical application in monitoring and identifying suspicious persons in public spaces. For example, surveillance systems in major cities such as London use facial recognition to detect suspects in crowds (*Jain et al., 2016*).

**Anomaly Detection**: detection of atypical or risky behaviour; practical applicability for intelligence agencies as it easily detects unusual activity that could signal an imminent threat. An example is the use of anomaly detection in network traffic monitoring to identify cyber-attacks, as in the solutions offered by the company Splunk (Chandola et al., 2009).

## Practical applications of AI in Intelligence

Nowadays, AI can be used in intelligence operations to achieve results faster and with greater efficiency. Technological developments mean a new approach in this area too. Models for the use of AI in the intelligence area are generally represented by the automation of OSINT analysis processes, the detection of behavioural patterns of actors involved, video surveillance through facial recognition and countering cyber threats.

**Automating OSINT analysis.** With the ability to mass process data from social networks, forums, news feeds and other online platforms, AI can accomplish (Wasserman, and Faust, 1994). Rapid identification of relevant actors: whether we are talking about suspects, organized groups or organizations, AI can understand their dynamics and predict their future actions based on the relationships between actors. Network analysis helps to prevent illegal activities by monitoring the evolution of networks and intervening quickly at identified key points.

a. Detect signs of radicalization: certain sudden behavioural changes can be easily observed by AI, which is useful for identifying the person or group that may become a threat Procedural algorithm can recognize changes in real time based on content analysis.

b. Automated decision making: after collecting and analysing data, AI can contribute to its value by forwarding recommendations and actions to be taken, thus prioritizing areas of interest for state actors and security agencies. Big Data platforms could develop the ability to filter alerts based on severity and likelihood.

**Combating cyber threats.** AI helps to detect cyber-attacks in real time by scanning network traffic and reporting anomalies: "Machine learning techniques offer significant promise for real-time anomaly-based intrusion detection by identifying deviations from normal network traffic behaviour." (Sommer and Paxson, 2010, p. 306) Machine learning algorithms have the ability to identify new types of cyber-attacks that traditional systems would not have detected. Unlike traditional intrusion detection systems (IDSs), which rely on fixed signatures of known attacks, machine learning (ML) algorithms have the ability to also identify new or unknown cyber-attacks.

AI is proving to be essential in this regard as it enables not only continuous network monitoring, but also automatic reaction to emerging threats, even previously unknown attacks (Buczak, and Guven, 2016). Thus, some examples are represented by:

a. Responding to attacks through autonomous defences: not only can AI detect attacks, but it also has the ability to autonomously respond to them; AI can block a suspicious IP, isolate a compromised area of the network, or temporarily disable sensitive processes to prevent serious consequences to the cyber architecture. A successful example is the Darktrace Antigena system, deployed in government and private sector organizations, which uses AI to understand the normal behaviour of IT infrastructure and intervene immediately when it detects deviations.

b. Predicting future attacks: access to databases containing past attacks, coupled with the ability to analyse long-term anomalous behaviours, AI can help intelligence agencies develop preventive strategies and predict the types of attacks that are likely to manifest in the coming period. One notable example is the use of AI at MIT Lincoln

Laboratory, where researchers developed a system that, based on network data collected in real time and a history of attacks, could predict with high accuracy spear-phishing attempts or lateral moves into infrastructure up to 48 hours before the actual impact.

**Facial recognition and video surveillance.** The use of facial recognition and video-surveillance, with the involvement of AI, is an essential solution in monitoring and identifying individuals in real time (Jain, Ross and Nandakumar, 2011, p. 98).

a. Large-scale surveillance: large cities have a multitude of surveillance cameras, and AI has the advantage of simultaneously analysing thousands of security cameras to identify individuals or groups of interest, independent of manual human analysis; this allows quick and efficient operational decisions to be made on the targets of security agencies. For example, in Chongqing (China) or London (UK), video surveillance networks in Chongqing (China) or London (UK) use facial recognition systems integrated with AI to locate wanted persons in real time without the need for continuous manual monitoring.

b. Improved accuracy: AI has the ability to adapt to changes in the environment and recognize people from a distance or in low-light, moving or static conditions, proving to be more effective than traditional systems. For example, the Clearview AI system, used by some US police forces, has demonstrated a high recognition rate even on distorted or low-quality images

c. Detection of suspicious activities: certain behaviours, actions or movements made by people in the environment can be easily identified by AI which, based on algorithms, sends signals to a human operator who can then take operational action against them. The Behavioural Recognition System developed by BriefCam and deployed in airports in Israel and the USA provides real-time alerts to human operators, who can intervene promptly to prevent incidents or attacks.

**Drones and advanced robotics.** Drones and robots represent another stage in the evolution of modern intelligence, with practical application in missions where human action would be impossible and risky, jeopardizing the entire operational success of a mission. Thus, of interest in this area would be:

a. Reconnaissance missions in inaccessible areas: UAVs with AI capabilities have the ability to penetrate conflict zones, radioactive environments or other hazardous areas, increasing the security of operations and reducing risks. For example, the **RQ-11 Raven** and **Black Hornet Nano** drones, used by the US military and NATO, have been deployed in combat zones such as Syria and Afghanistan to provide real-time tactical reconnaissance without exposing soldiers to danger.

b. Autonomous decision making: drones with AI capabilities can move and make decisions without human intervention, such as avoiding obstacles, adjusting the trajectory based on weather conditions or identifying a more efficient alternative route while allowing surveillance of the target. For example, **Skyborg** drones, developed by the U.S. Air Force, can operate semi-autonomously in reconnaissance and air support missions, using AI to make tactical decisions without constant human control.

c. Long-term monitoring and data collection: autonomous drones can carry out long-term monitoring missions, reducing reliance on human resources and maximizing efficiency, including in hard-to-access or dangerous areas. An example is the use of **Sentinel** drones by EU border agencies for continuous monitoring of external borders, including at night and in difficult weather conditions. This reduces costs and the reliance on permanent human patrols.

## Challenges and risks

*Ethical issues.* In my opinion, the use of AI in intelligence entails major ethical risks. First, automating decisions could potentially lead to algorithm-based discrimination. Biased models may be brought into the data analysis, meaning that the judgment may not be correct. I believe that individual rights and freedoms may be affected by the lack of transparency in decision-making, so security agencies have an obligation to strike a balance between technological efficiency and the fundamental principles to be respected in the rule of law.

*Technological vulnerabilities.* In terms of deep fake and other forms of artificially generated content, there is a risk in allowing false information to be disseminated quickly and efficiently, but dangerously at the same time. These tools can be used in influence or disinformation

operations, putting a huge strain on information security. European intelligence services have warned that groups backed by hostile states are using AI-generated content to influence public opinion during election campaigns or social protests. Thus, my opinion is that it is becoming an imperative requirement for security agencies to develop robust cyber detection and defence capabilities, while maintaining control over the integrity of AI systems.

*Over-dependence on technology.* The embedding of AI capabilities in more and more intelligence operations (e.g. in automated information selection and sorting, analysis of behavioural patterns or generation of operational alerts) may create the conditions for a dependency on this technology.

In this context, I can note that there is a reduction in the processing, critical analysis and rapid reaction capacity of members of security agencies. I also consider that the adaptability of the human factor, often regarded in the intelligence area as its most important quality, is thus visibly vitiated by not training it in decision-making and adopting a predetermined one generated by AI.

In the same context, when the algorithms have not had proper training or the data has been inconsistent, the decisions that the AI generates may be inappropriate or noticeably erroneous. This phenomenon is commonly seen in AI systems that suffer from "data bias" or "biased training data," leading to skewed results. For example, in 2018, a criminal recidivism risk prediction system used in the US, called COMPAS, was criticized for overestimating the risk of recidivism in people of colour based on biased historical data, leading to controversial judicial decisions. The fact that AI systems could decide on their own the operational decisions to be taken could lead to huge strategic losses, which is why it is essential to keep the operational decision in the hands of the security agencies, with human factors driving it, human expertise proving to be essential in the analysis and decision process.

## Conclusions

The integration of advanced technologies is a modern-day imperative for state security agencies to achieve. At the same time, the practical applications of AI in the field of intelligence operations, which

demonstrate its significant potential: from identifying cyber threats and monitoring online behaviour, to crisis management and critical infrastructure protection, are worth watching closely. These come with a range of risks and vulnerabilities, with ethical, legal and social challenges raising important questions about the application of automated operational decisions. The key to the sustainability of AI in national security is a balanced approach, where technological innovation and respect for fundamental human rights are intertwined. In conclusion, AI is not just a set of technological methods and means, but a strategic component that needs to be carefully integrated into the national security architecture and intelligence operations of the future.

## References:

1. Buczak, A. L., and Guven, E. (2016). "A survey of data mining and machine learning methods for cyber security intrusion detection." *IEEE Communications Surveys & Tutorials*, 18(2), pp. 1153-1176.

2. Burnap, P., and Williams, M. L. (2015). "Cyber hate speech on Twitter: An application of machine classification and statistical modelling for policy and decision making." *Policy & Internet*, 7(2), pp. 223-242.

3. Chandola, V., Banerjee, A., and Kumar, V. (2009). "Anomaly detection: A survey." *ACM Computing Surveys (CSUR*), 41(3), p. 15.

4. Jain, A. K., Ross, A., and Nandakumar, K. (2011). *Introduction to biometrics*. Springer.

5. Jain, A., Ross, A., and Nandakumar, K. (2016). *Handbook of biometrics*. Springer.

6. Sommer, R., and Paxson, V. (2010). "Outside the closed world: On using machine learning for network intrusion detection." *2010 IEEE Symposium on Security and Privacy*, pp. 305-316.

7. Wasserman, S., and Faust, K. (1994). *Social Network Analysis: Methods and Applications*. Cambridge University Press.

8. Russell, S., and Norvig, P. (2020). *Artificial Intelligence: A Modern Approach* (4th Ed.). Pearson.

9. Goodfellow, I., Bengio, Y., and Courville, A. (2016). *Deep Learning*. MIT Press.

10. McKinsey Global Institute. (2018). *Notes from the AI frontier: Applications and value of deep learning*. McKinsey & Company.

11. Floridi, L., and Cowls, J. (2019). "A unified framework of five principles for AI in society." *Harvard Data Science Review*.

12. Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., and Floridi, L. (2016). "The ethics of algorithms: Mapping the debate." *Big Data & Society*, 3(2).

13. Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press.

14. Zeng, Y., Lu, E., and Huangfu, C. (2019). "Linking artificial intelligence principles." *Association for Computing Machinery*.

15. Choi, E., & Choi, S. (2019). "Advances in AI applications in cybersecurity." *IEEE Access*, 7, pp. 95343-95362.

16. Brundage, M., Avin, S., Clark, J., et al. (2020). *Toward trustworthy AI development: Mechanisms for supporting verifiable claims*.

17. Brown, T. B., Mann, B., Ryder, N., et al. (2020). "Language models are few-shot learners." *Advances in Neural Information Processing Systems*.

18. OpenAI. (2023). *GPT-4 Technical Report*. OpenAI.

19. Varshney, K. R. (2016). "Engineering safety in machine learning." in *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*.

20. Office of the Director of National Intelligence (ODNI). (2021). *Artificial Intelligence and National Security*. U.S. Government Report.

21. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (2022). *Artificial Intelligence and Cyber Defence*.

22. US Department of Defence. (2019). *Summary of the 2018 Department of Defence Artificial Intelligence Strategy*.

23. European Commission. (2021). *Proposal for a Regulation laying down harmonized rules on artificial intelligence (Artificial Intelligence Act)*.

24. Mozur, P. (2019). "Inside China's dystopian dreams: AI, shame and lots of cameras." *The New York Times*.

25. Liu, H., & Fan, W. (2020). "AI-enabled security technologies for the Internet of Things." *IEEE Internet of Things Journal*.

26. Nguyen, T. T., and Nguyen, Q. H. (2021). "Detecting deep fakes using neural networks: A survey." *IEEE Transactions on Information Forensics and Security*.

27. West, D. M. (2018). *The future of work: Robots, AI, and automation*. Brookings Institution Press.

28. Crootof, R. (2016). "The killer robots are here: Legal and policy implications." *Cardozo Law Review*, 38(5).

29. Bryson, J. J. (2018). "Patience is not a virtue: The design of intelligent systems and systems of ethics." *Ethics and Information Technology*, 20(1), 15-26.