Quest Journals
Journal of Research in Humanities and Social Science
Volume 14 ~ Issue 2 (February 2026) pp: 154-169
ISSN(Online):2321-9467
www.questjournals.org

Research Paper

The Secret Intelligence and the Artificial Intelligence

Viktor Galambos
(PhD student, University of Szeged (Hungary), Faculty of Law and Political Science)

ABSTRACT: *The appearance and explosive development of artificial intelligence (AI) can be seen in almost all areas of our lives, and the secret service sphere is no exception, where the AI opens up new perspectives both in information gathering and processing of the acquired information. Due to the development of the information society and technology, the information-gathering activity carried out in the online space is becoming more and more important, and the AI offers several tools that fundamentally change the methodology of the intelligence profession. The profiling of persons and/or organizations and the detection of their private and official networks become significantly more efficient with the AI-based solutions. Processing, organizing and connecting large amounts of information to explore various correlations, potential patterns, make predictions and draw conclusions is also unimaginable without AI applications. The special intelligence operations like disinformation and the whole toolbox of hybrid warfare are also transferred to the online space, adapting to the evolution of society's information consumption habits. Consequently, nowadays it is possible to deliver a (fake)message to a mass target or even to reach a well-defined target group. The AI provides significant assistance both in the compilation of the contents and in the implementation of the distribution strategy. Nevertheless, AI itself can help recognize the AI-manipulated contents and support the fight against the malicious disinformation efforts. Taking into consideration the above-mentioned opportunities for secret services utilizing AI capabilities, it is essential to focus on regulating the use of AI, with particular regard to the operational activities carried out in the online space. The acts on national security services authorize the services in every country to collect secret information and defines its conditions and tools, which is complemented by each service's own internal procedure and licensing regulations. At the same time, it is questionable whether the current legislation and internal regulations follow the explosive development of information technology. Last but not least, it is also important to keep in mind the limitations of the use of AI and the related operational and organizational challenges and security risks for secret services.*

KEYWORDS: *Artificial Intelligence, Secret Intelligence, National Security, Information Gathering, Disinformation, Profiling, Social Engineering, Datamanagement*

*Received 15 Feb., 2026; **R**evised 26 Feb., 2026; **A**ccepted 28 Feb., 2026 © The author(s) 2026.*
P**ublished with open access at **www.questjournals.org

I. INTRODUCTION

The emergence and explosive development of artificial intelligence (AI) is evident in almost every area of our lives, and the national security sphere is also no exception, where the application of AI opens up entirely new perspectives in both information gathering and the processing of acquired information. AI is not only changing the methodology of the "ancient profession", but also affecting organisational operations.

In my study, I aim to show the opportunities and challenges that the use of AI presents for an intelligence organisation. In this context, I examine how AI, and in a broader context, digitalisation and virtual space, are transforming intelligence activities through their impact on social processes and the opportunities arising from this. At the same time, I will also discuss the challenges that the specific characteristics of AI pose for intelligence organisations and the areas where it is necessary to rethink operating principles and organisational and regulatory frameworks.

II. THEORETICAL BACKGROUND OF AI

The term „artificial intelligence" was defined in 1955 by *John McCarthy*, a professor at Stanford University, as "the science and engineering of making intelligent machines". In this case, intelligence can be defined as the ability to learn in order to take appropriate steps to solve problems and achieve goals in a constantly changing environment. Consequently, a pre-programmed robot is flexible, accurate and consistent, but not

intelligent. According to the above definition, the essence of AI lies in the fact that it applies to machines that are capable of learning. [1]

According to IBM, a leading company in the development and application of artificial intelligence tools, "artificial intelligence is a technology that enables computers and machines to simulate human intelligence and problem-solving abilities. This enables AI to perform tasks that would otherwise require human intelligence or intervention." [2]

The basis of AI is therefore machine learning [3], and given that it does not operate in a deterministic manner, it is not completely transparent or predictable, even for the developers of the artificial intelligence tools. Deep learning is a subset of machine learning that automates most of the process, significantly reducing the need for human intervention. Deep learning algorithms are based on neural networks, which model the functioning of neurons in the human brain. Neural networks can be trained by inputting training data, thereby continuously improving their accuracy. Once fine-tuned, learning algorithms become powerful tools that allow us to systematize large and unstructured data sets quickly.

The literature classifies different types of AI according to functionality and capabilities, there is narrow/weak AI, general/strong AI and super AI, as well as reactive machines, limited memory, theory of mind (Theory of Mind) and self-aware AI (Self-awareness). [4]

Types of AI according to functionality:

- *Narrow or weak artificial intelligence* focuses on a specific task or area. It is designed to perform certain tasks and, although it is capable of learning from data, it cannot be used (or cannot be used reliably) in other areas.
- *General or strong artificial intelligence* represents a higher level, a type of AI where machines are designed to think, reason and behave like humans. They are capable of learning, reasoning and making decisions in a wide variety of contexts. Currently, no such system exists, but research is underway to develop one.
- *Super artificial intelligence* or artificial superintelligence would be capable of surpassing humans. The concept of super AI is still hypothetical.

Types of AI according to capability:

- *Reactive artificial intelligence* has limited capacity and no memory-based function, meaning it lacks the ability to learn from past experiences and respond to actions.
- *Artificial intelligence with limited memory* has the capabilities of reactive machines and is able to learn from past experiences and use this data in decision-making. Almost all current artificial intelligence systems, such as chatbots, self-driving cars and virtual assistants, fall into this category.
- *Theory of mind artificial intelligence* is the next advanced level of AI systems, which currently exists only as a hypothetical concept. This type of AI is capable of accurately understanding human emotions and behaviour.
- *Self-aware artificial intelligence* is the most advanced stage, which is also hypothetical at present. This will be possible when machines develop self-awareness and possess human consciousness. Self-aware AI machines will have the same needs, emotions and desires as humans.

III. THE APPLICATION OF AI

We can see that there are many hypothetical ideas about how artificial intelligence works, which also indicate the future of AI technology and its development directions. At the same time, AI – in its current "limited" form – is already part of our everyday lives, and we use it in almost every area of life (although we are often unaware of this).

Below, I will focus specifically on those areas of application that are relevant to the national security services, and within that, intelligence activities: the application of AI in an organisational environment, and the functioning of AI-supported systems and networks as potential sources of information.

3.1. AI as an information system

AI is primarily used in organisational environments for analysis, evaluation and decision support processes, so it is appropriate to view it as an information system [5] that can be described as a system of relationships between people, processes, data and technology. [6]

Below, I follow *Dr Csaba Csáki*'s approach, which examines the intertwining of AI development and application processes with existing organisational processes. He divides the work process related to AI implementation into three phases: development, solution implementation and daily use of AI.

- The development phase has three distinct areas: model development, data management, and (basic) model training.
- The solution implementation phase can also be divided into three areas: integrating the model into the (organisational) process, customising the model, and managing local data.

- The daily use of AI involves training the model during application, monitoring the model's performance and fine-tuning the model.

New roles are emerging both within and outside the organisation in connection with AI-supported work processes: data providers, data controllers, data scientists, tool developers, operators, context definers (legislators and professional organisations), users (and displaced employees), evaluators, experts, clients, "malicious actors" and those affected by the impacts.

The emergence of AI in work processes represents both an opportunity to increase efficiency and a challenge for organisational development, as well as the introduction of a new risk assessment mechanism for any organisation that wishes to use AI to support its own processes (especially if it is a security service dealing with highly sensitive data).

3.2. AI and decision-making processes

As a consequence of the above, it is worth briefly discussing the decision-making processes [7] that AI can support and the importance is essential to the national security services, either as users or as actors attempting to obtain information from an organisation that uses AI to support its processes.

To conceptually describe the decision-making process, *John Boyd* created a model that applies equally to the decision-making processes of individuals and organisations. Boyd identified the four steps of the process as a repeating cycle of Observe–Orient–Decide–Act, known as the OODA loop. [8]

The application of AI can have a significant impact on all four phases of the cycle, with the aim of increasing the speed and accuracy of the decision-making process, i.e. shortening the OODA loop and making it more efficient:

- *Observation:* the first step in the cycle, which aims to provide the most comprehensive and accurate picture of the situation.
- *Orientation:* the second phase, which involves placing the data and information obtained during observation into context and interpreting it. Thanks to the use of AI, the amount of data that can be processed increases significantly, and AI is free from any emotional or psychological influence when interpreting and drawing conclusions. At the same time, when drawing conclusions, there is a possibility of distortion in the case of AI due to possible errors made by programmers or the processed data not being sufficiently comprehensive or representative, and it must be taken into account that cultural and social constraints do not apply in the case of AI.
- *Decision:* the third step, which involves selecting the option that is most likely to yield the best result from among the alternatives. In this respect, the opportunities and risks associated with the use of AI are the same as those described in the orientation phase.
- *Action:* the fourth element of the cycle is the implementation of decisions, which is carried out by AI tools under human control or independently, but even in the latter case, human control and/or the incorporation of technological constraints are essential.

AI can also play a role in decision-making in the areas of modelling and risk analysis. AI's large and flexible data processing capabilities can help decision-makers respond more quickly and with fewer cognitive errors to dynamically changing situations. Furthermore, because AI is capable of developing alternatives for all possible combinations of variables, it can even formulate unexpected recommendations for action.

At the same time, it is important to precisely define the "scope" of AI in decision-making processes, i.e. to clearly and precisely delineate the cases in which AI can make decisions independently (if this is possible at all), the cases in which AI is "only" responsible for preparing decisions, and when decision-making is a human task and responsibility (noting that if an organisation grants AI decision-making authority in certain areas, responsibility must still be traceable to the position/organisational element that granted such authority to the AI – *this will be discussed later)*.

3.3. AI and networks

Network research [9] is of particular importance (also) from the perspective of intelligence organisations, as understanding the structure and dynamics of networks is fundamental to all phases of information gathering. The emergence of AI has also generated revolutionary changes in the field of networks.

The network approach [10] is extremely well suited to analysing our increasingly complex world in the wake of socio-economic and technological developments and simplifying complex systems, thereby enabling us to map patterns that would otherwise remain hidden from us.

By examining an organisation's communication network, it is possible to identify the communication channels within the organisation and the actors involved in the process. This makes the flow of information within the organisation visible.

The connections between actors can be examined as a network at any level of organisational research, whether they are human-human (interpersonal), human-machine or machine-machine connections. The network approach is also suitable for depicting how the actors in the network influence each other, and beyond direct connections, it also shows the interaction between actors even if they are several steps away from each other.

The application of AI in network research enables the management and systematisation of the vast and sometimes unstructured amounts of data that are essential for the study of networks, and facilitates the visual representation of networks, which is a great help in identifying patterns and supporting decision-making processes. An important element of network research is the study of knowledge networks, which involves a system of connections between network actors whose primary purpose is to share the knowledge possessed by the actors and, through this, to create new knowledge. [11] It is important to note that actors can include not only humans, but also certain robots, software robots, or other technological devices.

In relation to machines appearing as actors in networks, it is necessary to mention smart devices connected to networks (the Internet of Things, IoT) [12], which, while making our lives incredibly easier, pose significant challenges in many areas, particularly in the field of security and data protection. IoT devices can be particularly vulnerable to external attacks, thereby increasing the exposure of the network (including information flowing within the networks and information related to network participants). Another security and data protection concern is that IoT devices often collect user data and transmit it without minimal data security protection or attention to ethical principles, and in many cases the conditions under which the collected data is stored and used are unknown.

The use of AI is, of course, also important in the development and networking of IoT devices. Through the devices we use to perform our everyday routine tasks, almost all of us are part of basic human-machine networks – home automation, building automation, driving assistance and navigation, home and mobile entertainment solutions, or even social communication support (e.g. foreign language translation) – and the areas of application are constantly growing, with these devices continuously collecting information about us and all the networks we are part of and which these devices also have access to.

With the advancement of technology, machines have become not only participants in individual networks, but also organisers of them, through algorithms that operate social media platforms or platforms that enable organisational work sharing and knowledge transfer. AI is also present in this area. In addition to regulating the flow of information and the formation of contacts between participants as the "organiser" of networks, it also appears as an actor in its own right, even as a virtual substitute for human participants. With the gradual shift of social networks to virtual space, this trend seems to be continuing, and AI is actively contributing to the expansion of virtual reality and the increase in the speed of information generation, making it increasingly difficult for participants to verify the authenticity of content spreading across networks.

3.4. AI and virtual space [13]

Various social media platforms provide a space for the transfer of social relationships to virtual space. It is worth examining how AI is related to individuals' activities in online space and on social media platforms, and what opportunities this opens up for the actors of the national security sector.

Users leave numerous "digital footprints" in the online space. These data traces can be created actively or passively. In the former case, we consciously share information about ourselves (although we are often unaware of how much additional personal information we are disclosing and what happens to it afterwards), such as filling out an online questionnaire, performing a series of actions on any registration-based website, or even accepting a website's cookies.

A passive digital footprint is created when individual web pages collect information about the user without their knowledge. This may include how often certain users visit a given website, where they come from, and what their IP address is. This also includes social media sites and advertisers who collect users' likes, shares and comments. [14]

Through the involvement of data brokers [15] and online targeting [16] specialists, data sources that are otherwise separate and isolated on different servers become interoperable, creating a mass of data about each individual that could be used to create a 360-degree profile of a person. Of course, this activity raises a number of data protection concerns, and following the introduction of the GDPR [17], several EU Member States have launched investigations into data collection companies.

The AI tools used to process vast amounts of data can serve as a much more effective tool for profiling than before, which essentially contributes to the marketing activities of business players with invaluable information in product development and the development of personalised sales and advertising strategies[1]. At the same time, profiles compiled on individuals are also used by political actors in their political marketing activities,

[1] When it comes to free social media platforms, it can be said that, as in all areas of life, nothing is free. In this case, we pay not with money, but with our data. Companies operating free social media platforms strive to collect as much data about us as possible in order to fine-tune the marketing activities of advertisers who provide them with revenue.

which operate on the same principles as commercial marketing, in order to formulate political messages and deliver them effectively to existing or potential voters. And, of course, organised crime groups and secret services are no exception, with modern intelligence activities focusing on the acquisition and processing of digital footprints or even complete profiles[2].

The exposure of social media users is not limited to the acquisition and use of their personal data, but also includes unauthorised access to the content they share and the spread of fake news. It is extremely common on social media to share content uploaded by others, which means that it can spread extremely quickly and, after a while, its original author becomes unidentifiable. Furthermore, the registration required to access certain platforms is relatively easy to circumvent.

A further problem is that there is no guarantee of the authenticity of the information shared. This is compounded by the trust factor inherent in social media, whereby we tend to accept content posted by users belonging to a group with similar interests as credible. All of these factors combine to create a fertile breeding ground for disinformation, whether it be innocent, well-intentioned misinformation shared out of ignorance, or deliberately constructed, malicious influence operations backed by organisations with business, political or even intelligence backgrounds.

AI can be a powerful tool in generating such misleading content and, when combined with profiling, in its targeted dissemination.

Finally, social media platforms pose a risk to unsuspecting users and their personal information, increasing their vulnerability by making it easier than ever to connect with users who share similar worldviews. This leads to the creation of identity bubbles [18], which can manifest themselves in the following ways from the individual's point of view: identification with a given social network (social identification); a tendency to interact with like-minded people (homophily); primary reliance on information from like-minded people appearing on social media (information bias). The dynamics and internal operating principles of the open or closed virtual communities that develop in this way differ, but they share the common feature that the shared values that give the community its cohesive power create a relationship of trust between members, through which they open up to each other and are willing to share information about themselves. For members who "infiltrate" the community for the purpose of gathering information and/or exerting influence, this is a real gold mine.

The information collected in this way further enriches the data set that can be processed quickly and efficiently with the help of AI. Furthermore, the analysis and processing of individuals' activities in virtual communities can contribute not only to the profiling of individuals, but also to the processing of the community as a network. If a given user is a member of several virtual communities (which is tipical), these networks are interconnected and create a new network, the structure, functioning and information flow of which can also be easily analysed, and the use of AI tools can reveal numerous patterns and correlations. information flow and participants can also be easily examined.

IV. METHODOLOGICAL BACKGROUND OF THE INTELLIGENCE ACTIVITY

In order to understand how AI contributes to intelligence activities, I have briefly reviewed the functioning of AI and its areas of application in segments relevant to intelligence. However, in order to understand the connections and clarify what is relevant from an intelligence perspective, it is necessary to introduce at least the basics of its methodology.

First, we need to clarify what we mean by intelligence. The national security system (often referred to colloquially as the secret services) can basically be divided into two areas of expertise: counterintelligence and intelligence.

In a collection of studies entitled "The General Theory of National Security" published by the National University of Public Service, *László Ádám* defines the purpose and tasks of counterintelligence as follows: "To detect and prevent the activities of hostile secret services, uncover their logistical background and learn about their methods; to anticipate the areas and current or long-term tasks that may be of interest to the organisations in question, and which may thus become their targets (...) to protect the proper functioning of democratic institutions against undesirable external and internal influences that could disrupt them". [19]

In the same collection of studies, *Dr. János Béres*[3] defines intelligence as follows: "Intelligence is a complex system of activities carried out by the intelligence service, which contributes to the protection of national values and interests and the enforcement of national interests through open and covert information gathering abroad and the execution of secret and covert intelligence operations. The state organises, directs and controls intelligence through secret service legislation granting special rights." [20]

[2] Later on, we will see that the methods used by organised criminals and secret services often show surprising similarities.

[3] Lieutenant General Dr. János Béres was Director General of the Hungarian Military National Security Service until 2023.

In this study, I focus specifically on intelligence, given that it provides a more vivid illustration of the multifaceted applications of AI[4]. To this end, it is worth pausing for a moment to define the concept of intelligence, because it leads us to deduce the methodology of the activity.

International literature has attempted to define intelligence in many forms and approaches. In this regard, *Dr. Michael Warner*, a former member of the CIA's History Staff, is noteworthy for collecting and analysing various definitions and then creating his own based on them. [21]

As a starting point, he defined the main attributes of intelligence:

- It is carried out by government employees for government purposes under the direction of civilian and/or military leaders of the state.
- It focuses on foreigners – usually other states, often foreign citizens, and foreign organisations and groups.
- The activity involves the acquisition, processing and transfer of information.
- It involves influencing foreign entities through (covert) means that cannot be attributed to the government in question – since if this activity were open and declared, it would be diplomacy.

Based on the above, Warner's definition is: *"Intelligence is a secret, state activity aimed at understanding or influencing foreign entities."*

In light of the above, intelligence activities can be divided into three main groups: information gathering, information processing, and influence. In the following, I will examine the methods and areas of application of AI in this breakdown.

4.1. Information gathering

The purpose of information gathering is to obtain information that can be used in intelligence work, i.e. to meet the specific information needs (so-called intelligence requirements) of national security intelligence organisations (state/government). At the same time, this information can often only be obtained through complex, multi-phase operations, in which the individual phases (or even individual operations) build on each other, and in order to move from one phase or operation to the next, new and new information is needed. Accordingly, operational information provides the knowledge necessary to move forward, while proceeding step by step, one eventually arrives at information that can be used in intelligence work.

In the information gathering phase of the intelligence cycle[5], intelligence requirements are transformed into operational information requirements, i.e. it is necessary to plan what operational steps will lead to the acquisition of the information specified in the intelligence requirement and what (operational) information is needed to plan each operational step.

The first and most important (operational) question is where and from whom the information that needs to be obtained can be found. Given that intelligence works with a foreign focus, i.e. practically the whole world is its "hunting ground", answering such a question is often not so simple. It is therefore necessary to identify the entities that have the information we are looking for (or at least through which we can find out in which direction it is worth continuing our search). The identified entity may be a specific person or group of persons, or possibly an organisation. This is followed by the so-called processing work, which aims to identify the person(s) who has/have access to the information sought, in the case of an organisation or group. This is called object processing, where all relevant (operational) information related to the target object[6] must be obtained (structure, roles, internal dynamics, information flow, information storage, information protection, external relations, etc.). Once this has been done, not only will the circle of persons involved be known, but also, presumably, information about communication hubs and formal and informal communication channels, which can be used to identify targets.

If the processed groups or organisations form a network with both human and machine actors (which is highly likely), both individuals (those with access to information) and machines (IT systems, machine actors in communication networks) can be identified during target designation.

The purpose of designating machines as operational targets may be to obtain information that directly responds to intelligence requirements, or it may contribute to the acquisition of further operational information (e.g. to reveal the human and/or machine vulnerabilities of a given organisation or network).

In the case of individuals as operational targets, so-called personal processing takes place, in which information related to the individual is collected in order to answer three basic questions: intelligence value, recruitability, suitability:

---

[4] Many of the intelligence methods presented can also be found in information gathering activities, which form the basis of counterintelligence work, just as the objectives and tasks of counterintelligence and intelligence cannot be completely separated. Accordingly, in some countries, the same state organisation is responsible for both counterintelligence and intelligence, at the same time, there are methods that are indisputably only found in the intelligence toolkit.

[5] The classic elements of the intelligence cycle: receiving information and intelligence requirements (1), information gathering (2), processing the information obtained (3), analysis and evaluation (4), briefing (5)

[6] The target object may be not only a formal organisation, but also an informal community.

- The *intelligence value* is determined by whether the target has access to the information that intelligence needs – information that can be used to answer intelligence questions or information that contributes to the effectiveness of the operation. This is the first step, which is only followed by further steps if the intelligence value is confirmed.
- When assessing *recruitability*, intelligence gathers information on whether the individual can be persuaded in some way to voluntarily provide the information that intelligence needs. In this case, the target person is aware of handing over information, which may be sensitive (or even classified), in exchange for some form of financial compensation, or free of charge, purely out of principle, or under some form of coercion (pressure). This is the second stage of processing.
- When assessing *suitability*, intelligence services seek to determine whether the target's physical and mental condition is suitable for participation in a covert information gathering operation, i.e. whether they will change their mind, break down or betray someone.

At the end of the above information gathering process, the operation can continue with the approach of the target. In this case, intelligence services will contact the person, which requires gathering further information about when and under what circumstances this should take place, and whether it should be done openly or covertly (i.e. whether the intelligence officer should reveal their true background or use some form of cover to disguise themselves[7]).

At the same time, it may also happen that the preliminary information gathering leads to the conclusion that the target person, although he or she has intelligence capabilities, cannot be won over, cannot be persuaded in any way to pass on information of his or her own accord, or is not suitable for such a task. In this case, the direction of information gathering related to that person changes, and the focus shifts to finding ways to obtain the information in their possession without their knowledge. In the course of this, data is collected on where and how the target person handles and stores the information sought, with whom and through what communication channels they share it, and what communication tools and IT systems they use.

It is therefore clear that the process of obtaining information is preceded by an extremely extensive and meticulous operational information gathering process, during which intelligence agencies collect information about organisations, the human and machine networks that comprise them, and the human and machine actors within those networks. This generates a huge amount of data, which must be continuously processed and evaluated in order to lay the groundwork for and prepare the next operational step.

4.2. Information processing

The next stage in the national security intelligence process is analysis and evaluation, the aim of which is to provide reliable, timely, analysed and evaluated information to users (decision-makers or those who formulate intelligence requirements) in order to prepare their decisions. [22] In the course of this, analysts supplement and compare the information obtained through operational means with information from other sources, which they extract from various databases, precedents[8] and open sources, i.e. sources accessible to anyone.

Analysts must synthesise vast amounts of raw and partially processed information and data, keeping in mind the news demand at all times and, if necessary, formulating further clarifying questions to the operational area that provided the information. Closely related to analysis is evaluation, which not only synthesises the available information, but also draws conclusions based on it, highlights connections and, where appropriate, makes recommendations.

Finally, it is extremely important that the intelligence service presents the information it has obtained and processed to decision-makers in a digestible and transparent manner. This final phase of responding to intelligence requests, the presentation, is at least as difficult as the other stages, as summarising a huge amount of data in a concise and understandable way is no small challenge, which can be aided by the use of various visual elements and infographics. At the same time, it is important to bear in mind that a state intelligence organisation, depending on its size and capacity, may be working on several hundred pieces of information material at the same time, all of which must meet the strictest content and format requirements, which also represents a significant coordination and work organisation task.

4.3. Influence operations

A very special operational activity of intelligence, influence, which can be classified as a tool of hybrid warfare, somewhat "sticks out" from the classic intelligence cycle outlined above.

Hybrid threats are one of the most significant security challenges of our time. According to the European Union's 2016 joint communication [23], hybrid threats are considered to be a mix of coercive and subversive

[7] „False flag” operation

[8] Previously generated and stored information.

activities, as well as traditional and non-traditional methods (e.g. military, diplomatic, economic, technological) that can be used in a coordinated manner by state or non-state actors to achieve certain goals while remaining below the level of officially declared warfare. The emphasis is generally on exploiting the vulnerabilities of the target and creating an ambiguous situation with the aim of influencing political decision-making, manipulating public opinion, exerting political pressure, undermining confidence in government and democratic systems.

In this study, I start from a case where the influencing party is a state actor, i.e. a country decides to use hybrid tools. The influence activity is the result of a political decision, with the intervention being ordered by the highest level of government leadership, but its implementation is often carried out by the national security organisations, and given that the influence is directed against foreign targets, it is usually the responsibility of the intelligence services.

The implementation of influence operations is preceded by the intensive and large-scale information gathering and analysis and evaluation activities described above, although the purpose of which is not to inform decision-makers, but to plan and prepare the operation (active measure).

V. THE USE OF AI IN INTELLIGENCE WORK

In the previous chapters, I presented the areas of application of AI that are relevant to this study, as well as the methods of intelligence operations, and at some points I pointed out where the two are connected. Below, I will continue to explain these connections, focusing specifically on the intersection between AI-supported applications and intelligence activities.

In intelligence work, AI can be applied in two ways: on the one hand, AI-supported tools, systems or networks can be the target of individual information-gathering operations; on the other hand, intelligence itself can use AI capabilities to operate and develop its own tools and systems and to support its work processes.

5.1. Information gathering

In the context of information gathering, AI is used in two main areas: technical information gathering and online information gathering.

Technical information gathering tools can also be used against individuals, machines and communication channels connecting network participants. Typical areas of application:

- *Surveillance* (e.g. cameras, microphones, other image and sound recording devices), which, thanks to the possibilities offered by AI, have reached such a level of sophistication in terms of both miniaturisation and automation that they remain virtually undetectable during operation and can be controlled remotely, thus minimising the risk of detection.
- *Spyware* and *malware* attack the affected devices and, while remaining hidden from users, continuously leak information stored or processed on the attacked device. They are also capable of infecting other devices connected to the network and, ultimately, the entire network. AI provides significant support in both the development of this malware and the discovery of security vulnerabilities necessary for its delivery.
- Closely related to spyware (even considered as part of it) are *tools that specifically exploit the vulnerabilities of "smart devices"* to gain access to data and information collected by so-called "smart applications".
- *Decrypting encryption keys*. Any organisation that handles sensitive data (whether it is a government or a business) pays special attention to data security, and given that data transmission is the most vulnerable point, it uses encrypted channels to protect it, in line with the level of development of the organisation in question. These may be commercially available solutions or proprietary, custom-developed tools that encrypt or scramble the data to be transmitted. The extremely complex encryption algorithm is provided by a so-called encryption key. [24] AI is a great help in deciphering these algorithms, i.e. breaking the encryption.

When it comes to obtaining information online, it is worth mentioning that, in addition to the "surface" or "visible web", there is also the so-called "deep web" and "dark web". [25] The surface or visible web refers to the World Wide Web as it is commonly used, which can be "discovered" using simple search engines (e.g. Google). The deep web is a deeper layer where the content cannot be accessed using simple search engines. However, this does not mean that the information there is illegal. Typically, this includes various password-protected or registration-required web interfaces and online databases that cannot be accessed by everyday search robots. Finally, the dark web is a hidden segment of the deep web that can only be accessed with special browsers and anonymity tools. Appearing on the dark web is not illegal in itself, but the legality of using the necessary tools and software is questionable, while most content shared on the dark web is explicitly illegal (it was created specifically for sharing such content). National security services are keen to gather information on all three platforms.

Social media platforms are a key area for online information gathering, offering the following possibilities:

- *Identifying individuals* (face, voice and motion recognition or other methods of biometric identification [26]). Part of a person's digital footprint is the images or audio recordings of them that end up on the internet, whether they know it or not. AI can help to identify the person from these or fragments of them and link them to other databases.
- *Profiling individuals* (personality traits, values, interests, orientation, preferences, hobbies, relationships, geolocation, etc.). One of the most important parts of personal data processing is gathering as much information as possible about the target person. Significantly more meaningful information about an individual can be gathered from various databases based on their social media activity, statements and interactions. AI provides enormous support in synthesising the information sets collected in this way, supplemented with data obtained from physical space.
- *Behaviour analysis and prediction*. With the help of AI, models can be created based on information collected about a given person in online and physical space, which can be used to predict that person's reactions with a high degree of certainty, which is key to planning and preparing further operational steps.
- *Building a network of connections*. Social media platforms and networks that can be discovered in online space are also excellent for mapping a person's circle of connections, including professional, family and friends. In terms of depth and breadth, this can far exceed the information that can be obtained from physical space (e.g. through physical observation of the person), although the latter can be an extremely useful supplement, especially in cases where the individual deliberately wishes to hide a relationship and therefore consciously strives to ensure that it cannot be linked to them in the online space. AI is capable of synthesising all the relationships associated with a given person and creating the network(s) of which that person is a member. When this is represented, connections may be revealed that were not apparent during observation in either physical or online space, and may even give a whole new direction to operational planning.
- *Group profiling*. Of course, the tools and methods used to process individuals can be extended not only to individuals but also to groups and networks. The internal cohesion, dynamics, communication and sentiment analysis of online communities, especially closed groups, communication, and mood analysis can provide insights that, when analysed using AI, can contribute to drawing conclusions about the group's organisation, structure, members, and relationships with other groups, identifying the group's vulnerabilities, and even predicting the group's behaviour. This can greatly contribute to covert infiltration to the group.

Some of the information available in the online space, particularly on social media platforms, can be obtained automatically using various tools, also supported by AI. *Viktor Erdész*' collection [27] provides an excellent illustration of this, with AI-based information gathering systems from specialised companies that are also available on the civilian commercial market:

- The Airbus platform is capable of automatically collecting, extracting and analysing large amounts of unstructured information from the surface web, the deep web and the dark web using cloud-based technology. Its functions include entity extraction[9] (person, place, organisation, event, equipment), sentiment analysis[10], automatic translation, speech-to-text conversion, searching in video and audio files, character recognition in images and videos, and speaker identification.
- British Aerospace's cloud-based system, IntelligenceReveal, is capable of monitoring information posted on Twitter, Facebook, Google+ and YouTube comments, as well as articles uploaded to RSS feeds. Its capabilities are demonstrated by the fact that the basic configuration can handle 100,000 Twitter messages per hour. The system can track 50 million events in its default configuration and 500 million events in its maximum configuration. [28]
- The Cobwebs Technologies module is capable of automatically extracting information from the deep and dark web, social networks and mobile phone applications. An additional advantage of CobWebs is that it can also hack user profiles if necessary. [29]
- ATIS systems' Klarios software is used to analyse, narrow down, organise and search for information obtained from telecommunications providers and intercepted communications in a user-friendly, transparent interface. Klarios is designed to process nationwide telecommunications information and, accordingly, handles many billions of pieces of metadata. It is suitable for voice recognition, the extraction and display of geographical (geographic information system) data, and the construction and import of such

[9] The algorithms underlying the technology automatically recognise metadata, individuals, organisations, etc. (entities) contained in the documents fed into the system.

[10] This is one of the advanced applications of machine learning capabilities. The technique can be used to infer whether the person or group sharing the content has a positive or negative opinion about an event or phenomenon.

databases. It is capable of integrated management of various telecommunications modes (PSTN, ISDN, GSM, UMTS, LTE, LTE-Adv., VoLTE, VoIP, NGN and IP). It can be connected to national video surveillance, passport and subscriber databases, as well as software for social media detection. [30]

- Using its web-based (virtual) global system called Rayzone ECHO, it is able to extract smartphone metadata (location, time, call list, etc.) in large quantities anywhere in the world and analyse it using advanced algorithms. The system is also capable of monitoring all internet users with smartphones in a given country. [31]
- BlackSky offers a wide range of geospatial intelligence services. The company currently processes data from 25 satellites, more than 40,000 news sources, 100 million mobile devices, 70,000 ships and aircraft, eight social media providers, 5,000 environmental sensors and thousands of IoT devices to produce products whose main purpose is to increase customers' situational awareness. In the future, it plans to launch 60 of its own satellites. [32]

The companies presented above offer separate service packages to government agencies and private companies. The latter are typically "dumbed down", meaning that certain intelligence modules are not available, and their prices are extremely high. In addition to all this, it is important to note that although these professional large companies are privately owned, they are always in contact, openly or less openly, with their own governments' national security organisations and, although they consistently deny this, they presumably also share information about their customers' needs.

However, automated information gathering is not always sufficient to obtain "deep" information[11]. In such cases, HUMINT[12] techniques, which have been used in physical space for centuries, must be applied in the online space. This involves infiltrating the target's environment or even establishing direct contact with the target in order to gather information about and from them. In the case of the "simple HUMINT method", this task is performed by professional intelligence personnel, i.e. the case officer himself, while in the case of the "complex HUMINT method", it is performed by a cooperating person (agent) selected and trained for this purpose, also known as an operational contact. [33]

For the purposes of my study, I do not distinguish between the two methods, as in both cases, when applied in the online space, the same thing is required: a virtual entity (fake profile) must be created that can perform this function. We regard the fake profile or avatar as the virtual operational connection (virtual agent) of intelligence, which, unlike flesh-and-blood connections, can be shaped and prepared as perfectly as possible and always performs the tasks assigned to it with precision. while also taking into account that the avatar is often managed by a member of the operational staff. At the same time, it can also be regarded as a "cover", i.e. a set of measures serving to conceal the real identity and intelligence background of the case officer.

AI provides a great deal of support in the creation and use of fake profiles:

- *Image manipulation*. For the sake of authenticity, it is advisable to associate a photograph with the profile, which obviously cannot be a picture of the case officer themselves. At the same time, social media platforms are using increasingly complex control mechanisms to filter out fake images, precisely in order to weed out fake profiles. To circumvent this, it is essential to use AI, which can be used to produce not only static photographs but also manipulated audio and video recordings, further enhancing the authenticity of the fake profile.
- *Profile building*. In connection with personal data processing, I have already mentioned how much information a person's digital footprint can contribute to the creation of their profile. In this case, the reverse of this process must be imagined, i.e. all profile elements that partly support the authenticity of the fake profile and are partly suitable for achieving the operational objectives related to the target person (infiltration, establishing contact) must be created and placed. AI-based tools are capable of developing complete profiles based on specified criteria (including biographical elements or personal introductory texts).[13]
- *Activity*. Continuous activity (comments, content sharing) is key to maintaining the authenticity of a social media presence and profile. Some of this must be done manually, especially considering that online activities must serve the operational purpose of getting closer to the target person through the fake profile. At the same time, AI can be used to automate part of the activity, which publishes specific regular posts, shares content, and also eliminates language barriers (which is particularly important in foreign-oriented intelligence work).

[11] Direct information about the target person that is closely related to the target person's activities to be investigated.

[12] Human Intelligence: information gathering using human resources.

[13] The creation of a false profile and digital footprint is not only important in the case of operations carried out in the online space. It can also provide useful support for HUMINT activities carried out in physical space, when the cover used by a live operations officer or contact needs to be legitimised by creating a virtual extension of it, as nowadays it is considered unusual if someone has no digital footprint at all.

- *Social engineering.* [34] I have already mentioned that the primary and most important purpose of a fake profile is to get close to the target person or infiltrate a particular group in order to obtain information. According to the cybersecurity company ESET, "social engineering" or psychological manipulation "...refers to when an authorised person transfers data to an unauthorised user or provides them with access to the system due to the other person's deceptive behaviour. Psychological manipulation is a type of attack in which the cybercriminal does not exploit technological vulnerabilities, but rather uses human susceptibility as their main weapon." [35] In this case, it is not a cybercriminal behind the fake profile, but an officer or an agent of an intelligence organisation, but the method is the same, and AI helps to develop it.
- *Anonymity*. An important element in the creation and use of fake profiles is the use of tools and software that make it difficult to identify the true identity of users. This is not only a question of "content", i.e. the attributes of the fake profile, but also a technical one, as it is necessary to conceal all (meta)data that refers to the IT or communication network used to create or operate the fake profile, or to configure it in such a way that it fits the character of the fake profile (e.g. in the case of a Chinese fake profile, use of a Chinese IP address, Chinese keyboard, Chinese image or text editor, timestamp, etc.). To this end, the user employs AI-supported tools that are capable of creating this appearance and concealing the real background.

5.2. Information processing

The processing, systematisation and linking of large amounts of information, the discovery of various connections and possible patterns, and the drawing of predictions and conclusions are unimaginable today without the use of AI. In the analysis and evaluation phase of information processing, I do not distinguish between information intended for operational and governmental purposes, given that AI performs the same functions in both cases:

- *Big data processing.* [36] With the help of AI-supported fusion systems, even large amounts of data from a wide variety of sources, with different structures and formats, can be easily reviewed, previously undetected correlations can be identified, and opportunities for cooperation between intelligence organisation units (whether within the operational or analytical-evaluative areas, or between them) are created. In addition to all this, an important consideration is the time factor, i.e. the amount of time required to process the available information is reduced to a fraction through the use of AI.
- *Database management*. AI-based solutions suitable for handling large amounts of data not only enable their processing and analysis, but can also be continuously expanded and updated as data warehouses with newly acquired information, linked to other databases, and queried based on a wide variety of parameters. These solutions also have workflow support functions in that they serve the work of multiple organisational units, while also being able to handle the "need-to-know" rule of organisations dealing with sensitive information by allowing different access and authorisation levels to be set up.
- *Data analysis and recognition*. Recognition and selection of specific types and formats of data from large amounts of data. This includes AI-based solutions that are capable of speech and caption recognition, creating transcripts based on audio and video recordings, filtering out potentially manipulated audiovisual content, quickly and accurately extracting large amounts of text, and recognising patterns and trends that may appear in the available information. All this, of course, in any foreign language.
- *Prediction and recommendation*. By using AI to process large amounts of information, it is possible to draw conclusions and make predictions, which greatly assist the decision-making process. AI can even be involved in developing various recommendations based on these conclusions and predictions.
- *Validation and source search*. The fast and almost unlimited information processing capacity supported by AI plays an important role in verifying the information generated during intelligence work. This function can be used to compare specific information (e.g. from an agent) with information available from open sources or information generated earlier. This allows not only the authenticity of the information to be verified, but also the reliability of the agent from whom the information originated.

The final phase of the intelligence cycle is the compilation of briefing material for decision-makers based on the processed information, in which the use of AI can also be of great help:

- *Visualisation.* This has already been mentioned several times, but at this point it is worth reiterating the ability of AI-based systems to display large and opaque data sets in a way that is quick and easy for decision-makers to interpret.
- *Preparation of information materials (reports)*. In addition to the use of templates that automatically include formal and content requirements, the rapid availability and exportability of information, as well as task management and collaboration capabilities, greatly facilitate and accelerate report writing.
- *Workflow support*. AI also effectively supports the distribution of reports, for example, by compiling and maintaining various recipient lists and linking them to the recipients of each report type. This enables the

quick and accurate sorting of various information materials. If we add another element to the information phase of the intelligence cycle, namely feedback (on the information material sent out), this can even be interpreted as a new intelligence requirement, i.e. the start of a new intelligence cycle. In this way, based on the distribution pattern of the information materials, the forwarding of questions and feedback received within the organisation (even to several cooperating organisational units), and possibly the assignment of related tasks (in the case of several cooperating organisational units, even broken down into subtasks) can also be managed by an AI-based tool.

5.3. Influence operations

As a part of the intelligence methodology, I already mentioned the complexity and diversity of this very specific operational segment. For the purposes of this study, I would like to illustrate the possibilities of AI application through a very effective and "popular" method of influence, namely disinformation operations.

Disinformation operations are in fact communication activities, so I consider *Roman Jacobson's* communication model to be applicable to their analysis. According to Jacobson, there are six conditions for communication: communicator, receiver, message, context, contact and code. Just like modern marketing communication theories, disinformation operations are also based on this model, and when planning and executing an operation, these conditions must be understood and ensured, for which AI can provide support in a number of ways:

- *Context, contact, code*. The effectiveness of disinformation operations is greatly enhanced by the nature of social media, which allows for the rapid and often uncontrolled sharing of information. Virtual space, and within it social media platforms, are an ideal medium for disinformation operations. With the help of AI, virtual groups that provide contact can be fully processed, making both the context and the code system used perfectly understandable and reproducible.
- *Communicator.* The basis of disinformation operations, like any other clandestine activity, is that they cannot be linked in any way to their actual perpetrator, in this case the intelligence service. In order to conceal this, an entity (fake profile) must be created that can fulfil the role of communicator. Whether the disinformation operation takes place in physical or online space (or a combination of both), for the sake of credibility, this entity must have a virtual extension that can be shaped according to the purpose of the operation. AI can help in creating and operating this, as already described.
- *Recipient.* The target of the disinformation operation may be a specific person, but typically it is a target group. The success of the operation depends to a large extent on concepts known from the marketing profession, such as segmentation, targeting and positioning [37], i.e. on the selection of the target group and knowledge of its members and their information consumption habits. The operational processing activities required for this and the possibilities for applying AI are the same as those described in relation to information gathering.
- *Message.* The essence of disinformation operations is the content, the message, which typically consists of a mixture of real facts and false statements that may be suitable for misleading the audience. AI can provide several useful supports for compiling disinformation content. On the one hand, it can help by summarising and synthesising the data generated during the processing of the nature of the contact, the context and the code system of the audience (target group), the nature of the contact, the context and the aggregation and synthesis of the data set generated during the processing of the code system, it can help to determine the formal and content parameters of the message so that it reaches the audience as quickly and accurately as possible in the given medium and then spreads to the rest of the target group. On the other hand, AI can be used in the technical compilation of disinformation content, the manipulation of images, video and audio materials, and the creation of deepfakes. [38]

VI. CHALLENGES AND RISKS

So far, I have tried to show the wide range of applications that AI offers in intelligence work, and while it seems clear that intelligence work without AI is practically unimaginable today, we must also address the challenges and risks that come with using AI. These arise, on the one hand, from the nature of AI and, on the other, from the specific characteristics of intelligence work (and secret services in general). In the former case, the main risks are the learning ability that underpins AI and the unpredictability of AI's "thinking" processes. In the latter case, a key consideration is ensuring the covert nature of the activity.

6.1. Deconspiracy

The risk of de-conspiracy, i.e. exposure, arises in the use of AI in that, due to its self-learning algorithm, AI saves related activities, so even a simple search or an AI-supported operation can carry a risk of de-conspiracy. It is not always possible to know who has access to the 'fed' information and for what purpose, and during the systematic use of non-proprietary AI tools or systems by intelligence services, even the application operator may

become aware of the connections investigated by the intelligence service or the entities in which it has a particular interest for any reason.

6.2. Misleading results

Due to the opacity of non-proprietary AI systems, it is impossible to know what databases they learn from or how representative the input data is, raising questions about how misleading the results may be. AI systems do not operate in isolation, but are embedded in a social environment, and the results of their decisions are also realised in this environment, which means that so-called "biased" AI responses may occur as a result of possible discriminatory patterns in the given social environment. At the same time, even in the case of AI applications developed in-house, there is a risk that the input data may not be sufficiently representative, which may also distort the conclusions (e.g. in law enforcement practice, only criminals and/or individuals who follow deviant norms are included). Therefore, analyst control and process regulation are essential, and the method of integrating AI into internal decision support processes must be precisely defined.

6.3. Information flow is redirected to physical space

An objective limitation on the use of AI in information gathering may arise if the individuals or groups under surveillance minimise their own exposure risk and the vulnerability of their communication channels by reverting to methods of communication used before the information and technology revolution.[14] Of course, AI-supported tools can still be used to process the information obtained, but the possibilities for gathering information from the online space are reduced or completely eliminated in such cases. At the same time, it should be noted that if someone has no digital footprint at all, this is very unusual nowadays, and it can be assumed that they have consciously chosen this method of "hiding", which may lead to further conclusions.

6.4. Security-conscious users

As a corollary to the previous idea, there is a much more widespread form of behaviour in which users do not "disappear" from the virtual space, but simply try to be as cautious as possible and minimise the amount of information that can be obtained about them.

Based on the examples listed above, we can say that there is no security-conscious behaviour that would make it impossible to gather information about a given person, but it can certainly make the work of intelligence organisations significantly more difficult.

6.5. Organisational and HR challenges

A common challenge for organisations using AI technology is to develop new methodologies for optimising human-machine collaboration and implementing them into existing work processes. Intelligence organisations are, of course, no exception. Accordingly, new practices must be adopted in both technology application and human resource management. The new working environment is based on building trust in the software used for data processing, acquiring the skills necessary for user-level application use, and, most importantly, developing a new approach and operating protocol that seamlessly integrates the processing and use of large amounts of data. All this must be done in the various functional organisational units, in line with their own tasks, and then coordinated across the organisation as a whole. Last but not least, expert groups dealing with data management, IT systems and data security must be set up and/or developed, as well as roles and processes dealing with data authentication and human control of AI systems.

VII. REGULATORY ISSUES

It is particularly important to mention regulation, especially given that this study deals with the application of AI in an area that could lead to the restriction or violation of fundamental personal rights, thereby raises a number of regulatory and ethical issues.

The concerns raised in relation to AI stem precisely from the functions and operational characteristics that are exploited by intelligence services. At the same time, it should be added that this is not only the privilege of national security services; private companies operate in very similar ways in their marketing activities. Therefore, regulation covering all segments (not just intelligence organisations) and requiring a general approach has become necessary to ensure the enforcement of personal rights, the inviolability of privacy and the protection of data.

7.1. European Union regulation

On 13 March 2024, the European Parliament adopted the EU regulation on AI (Artificial Intelligence Act – AIA). [39] This was the world's first comprehensive legislation specifically addressing the development

[14] An example of this is the tragic event in 7. Oct. 2023., the preparation of the Hamas attack against Israeli civilians, which could not be detected by Israel's hi-tech countermeasures precisely because of this.

and use of AI, with the aim of, among other things, promoting the safe operation of AI and protecting the fundamental rights of individuals. The regulation introduces risk-based regulation for artificial intelligence systems, which also prohibits the use of certain types of AI systems and introduces strict rules for high-risk AI solutions.

The adopted regulation is based on the European Commission's proposal [40], which defines four risk levels for AI systems:

- All AI systems that clearly endanger people's safety, livelihood and rights are considered *to pose an unacceptable risk* and are therefore banned.
- AI systems classified *as high risk* may also restrict people's rights, so their use is subject to strict conditions.
- *Limited risk* refers to the lack of transparency of AI systems, and therefore specific transparency obligations are introduced in terms of both operation and data processing.
- Applications *with minimal or no risk*. The vast majority of AI systems currently used in the EU fall into this category.

In addition to the above, the European AI Office [41], established within the European Commission in February 2024, will oversee compliance with and enforcement of the regulation by Member States. Its aim is to create an environment where AI technologies respect human dignity, rights and trust. The Office strives to ensure that Europe plays a leading role in the ethical and sustainable development of AI technologies.

While the EU's efforts to develop regulations deserve recognition and support in every respect, it is important to note that national intelligence agencies still have the possibility to restrict or violate fundamental personal rights in the course of their information-gathering activities, within the framework of their own national regulations.

Therefore, the regulatory environment needs to be developed from this perspective as well. I consider it appropriate to review the legislation governing the operation of national security organisations, with particular regard to the rules on secret information gathering, and to address the main area of AI application, namely information gathering in the online space and the conditions for processing the data thus generated.

In parallel with the above, the same elements must also be included in the internal regulations of national security services, particularly in the following areas:

- Internal regulation of *information gathering activities* and operational procedures. The use of AI in information gathering and related operational activities in the online space must comply with the requirements of legality, documentation, proportionality and purpose limitation, and the authorisation processes and levels must be precisely defined.[15]
- The conditions for the use of AI *in information processing* must also be regulated, with particular regard to the control of the phases of the analysis and evaluation process performed by AI.
- *Data management, IT and information security* rules also need to be reconsidered, given that with the 'deployment' of AI, the amount of information received by the organisation is expected to increase many times over, but the conditions for its storage, management, retrieval and use must be ensured in such a way that it remains traceable and the organisation's internal data management and information security principles are not compromised, while preserving the benefits of efficient processing of large amounts of data. An important part of this is making policy decisions on the procurement/development of AI-based applications and defining the 'scope' of AI.

7.2. The question of responsibility

In connection with the use of artificial intelligence in an organisational environment, I have already mentioned the role that AI can play in decision-making processes and the importance of precisely defining the "scope of action" and decision-making competence that can be assigned to AI. The intelligence sector is in itself considered a "dangerous operation" in terms of both the purpose of its activities and its operational characteristics, so the use of AI in this area makes the question of who bears responsibility for the "activity " of AI in work processes related to both information gathering and information processing particularly sensitive.

In this regard, in the absence of specific regulations tailored to intelligence organisations, I consider the European Parliament's resolution on the civil liability regime for artificial intelligence to be a good starting point. [42]

According to point 6 of the resolution, there is no need for a complete overhaul of well-functioning liability systems, but the complexity, connectivity, opacity, vulnerability, updatability, autonomous learning capabilities and potential autonomy of AI systems, and the large number of actors involved pose a significant challenge to the effectiveness of EU and national liability frameworks, and that certain coordinated changes are needed in liability regimes to avoid situations where persons who suffer harm or damage to their property are left

[15] The creation and use of a false profile, for example, may simultaneously affect the rules on the use of operational cover and the employment of operational contacts.

without compensation. Point 7 notes that, although any physical or virtual activity, device or process controlled by AI systems may, in technical terms, be the direct or indirect cause of harm or damage, it is almost always created by someone who builds, deploys or intervenes in those systems. The opacity, connectivity and autonomy of AI systems make it very difficult or even impossible in practice to trace certain harmful actions of AI systems back to specific human interventions or design decisions. However, in line with widely accepted concepts of responsibility, this pitfall can be avoided by holding accountable the various individuals involved in the entire value chain who create, maintain or control the risks associated with the AI system.

7.3. Self-regulatory mechanisms

Last but not least, it should be noted that initiatives by companies operating social media platforms promise to be more effective than regulation in combating the malicious use of AI technology. Meta, which operates the world's most popular platforms, Facebook and Instagram, announced on 5 April 2024 [43] that it will begin labelling AI-generated content from May 2024, i.e. it will mark sounds, images and videos created with the help of AI on its social media sites. Other IT giants, such as Microsoft, Google and OpenAI, have made similar commitments, which will certainly pose new challenges for intelligence organisations wishing to use AI.

VIII. CONCLUSION

In summary, it is no exaggeration to say that AI, digitalisation and the explosive growth of virtual space are causing tectonic shifts in the world of intelligence.

In the field of intelligence gathering, we are on the threshold of a paradigm shift that will place the previous operational approach on an entirely new footing. The "traditional" methodological approach to HUMINT and OSINT[16] activities has been fundamentally applied in physical space, while their extension to online space and their combined application not only means a transformation of operational methodology, but also a rethinking of external and internal procedural and authorisation rules.

The same is true for analytical, evaluative and informational work, where previously unimaginable perspectives are opening up in data processing. All these changes must go hand in hand with a rethinking of organisational functioning, the division of tasks and cooperation within the organisation, and work processes. At the same time, however, timeless principles such as legality, proportionality, purpose limitation and documentation in information gathering, as well as compliance with data management and need-to-know rules in each phase of the work, must not be compromised.

Among the functions supporting the core activity (information gathering and processing), human resource management faces serious challenges, not only in the transformation of operational processes, but also in the development of a human resource replenishment strategy adapted to new challenges and in the management of the emergence of new roles. Organisational units responsible for IT systems and security also have a huge responsibility to develop, procure and integrate AI-supported systems and to ensure the reliable and secure operation of related data management systems.

In the context of intelligence activities, it is particularly important to note that the use of AI becomes truly effective on a multinational scale, for example through the truly diverse and large data sets of global big data. Given that information gathering in the online space – in particular the use of AI-supported, high-capacity, automated systems – is geographically difficult to define, the use of AI for intelligence purposes in a multinational environment must also be taken into account when reviewing national regulations. Furthermore, the information obtained in this way may be suitable for sharing within the framework of international cooperation, either to achieve the common goals of allied countries or to pursue universal objectives such as the fight against terrorism or organised crime.

The emergence of AI therefore places a heavy burden not only on national security services, but also on the state/governmental organisations that control and supervise them. The political responsibility that comes with the information gathering and processing opportunities opened up by AI includes reviewing and supervising regulatory frameworks, knowledge sharing within international cooperation forums, and the "recycling" of the experience accumulated by national security services in order to protect the institutions and citizens of their own countries and increase their security awareness.

REFERENCES

[1]. CHRISTOPHER MANNING: *Artificial Intelligence Definitions.* Stanford University Human-Centered Artificial Intelligence, 2020. https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf; downloaded: 08.03.2024.
[2]. IBM company website. https://www.ibm.com/topics/artificial-intelligence; downloaded: 08.03.2024.
[3]. IBM company website. https://www.ibm.com/blog/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks/; downloaded: 08.03.2024.
[4]. Eaton Business School website. https://ebsedu.org/blog/7-types-of-artificial-intelligence; downloaded: 28 March 2024.

[16] Open Source Intelligence: open source information gathering.

[5]. CSABA CSÁKI: *Systematic examination of the risks arising from the spread of artificial intelligence.* In: Dr Zoltán Kovács (ed.): Examination of the effects of artificial intelligence and other disruptive technologies 2023. Military National Security Service. Budapest, 2023. pp. 27-51.

[6]. https://repository.dinus.ac.id/docs/ajar/Kenneth_C._Laudon,Jane_P_._Laudon_--_Management_Information_System_12th_Edition_.pdf; downloaded: 09.03.2024.

[7]. TAMÁS CSIKI VARGA: *The effects of artificial intelligence on security theories.* In: Dr. Zoltán Kovács (ed.): Examining the effects of artificial intelligence and other disruptive technologies 2023. Military National Security Service. Budapest, 2023. pp. 423-439.

[8]. MICHAEL T. PLEHN: *Control Warfare: Inside the OODA Loop.* Air University Maxwell School of Advanced Airpower Studies, Maxwell Air Force Base, Alabama, U.S., 2000.

[9]. MARCINIAK RÓBERT – BAKSA MÁTÉ: *Human and Machine Networks: The Impact of Digital Technologies and Artificial Intelligence on Cooperation between Actors.* In: Dr. Zoltán Kovács (ed.): Examining the Impact of Artificial Intelligence and Other Disruptive Technologies 2023. Military National Security Service. Budapest, 2023. pp. 265-300.

[10]. MÁTÉ BAKSA – GYÖRGY DRÓTOS: *Network theory of organisations: steps towards a new paradigm.* Magyar Tudomány, vol. 182, no. 1. Akadémiai Kiadó, 2021. pp. 69–80.

[11]. BAKSA, MÁTÉ – BÁDER, NIKOLETT: *The conditions of knowledge request and knowledge sharing – an analysis of an organisational knowledge network.* Management Science / Budapest Management Review Vol. LI, No. 1. Corvinus University of Budapest, Faculty of Business Administration, 2020. pp. 32-45.

[12]. KAREN ROSE – SCOTT ELDRIDGE – LYMAN CHAPIN: *The Internet of Things: An Overview.* The Internet Society (ISOC), 2015.

[13]. ISTVÁN ÜVEGES: *The social and political consequences of the use of artificial intelligence in social media.* In: Dr Zoltán Kovács (ed.): Examining the effects of artificial intelligence and other disruptive technologies 2023. Military National Security Service. Budapest, 2023. pp. 301-327.

[14]. Kaspersky company website. https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint; downloaded: 13 March 2024.

[15]. MATTHEW CRAIN: *The limits of transparency: Data brokers and commodification.* New Media & Society, 20/1, 2018. pp. 88–104. https://www.studocu.com/en-us/document/university-of-northern-iowa/direito-processual-penal/thelimits-of-transparency-data-brokers-and-commodification/27311719; downloaded: 28 March 2024.

[16]. RUSSEL BRUNSON: *Mastering Online Marketing.* Marketing Amazing Ltd., 2017.

[17]. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[18]. FABIANA ZOLLO ET AL: *Debunking in a world of tribes.* PLoS ONE, 24 July 2017, https://doi.org/10.1371/journal.pone.0181821; downloaded on 10 March 2024.

[19]. LÁSZLÓ ÁDÁM: *The task system of counterintelligence.* In: Imre Dobák (ed.): General Theory of National Security. National University of Public Service, Institute of National Security. Budapest, 2014. pp. 129–144.

[20]. DR. JÁNOS BÉRES: *The task system of intelligence*. In: Imre Dobák (ed.): General Theory of National Security. National University of Public Service, Institute of National Security. Budapest, 2014. pp. 117–128.

[21]. MICHAEL WARNER: *Understanding Our Craft Wanted: A Definition of "Intelligence".* https://www.cia.gov/resources/csi/static/Wanted-Definition-of-Intel.pdf; downloaded on 13 March 2024.

[22]. CSABA VIDA: *The basics of intelligence analysis and evaluation.* Felderítő Szemle, vol. XII, no. 3, December 2013. pp. 90–99.

[23]. JOIN(2016) 18 final - JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, A common framework for countering hybrid threats, Brussels, 6 April 2016.

[24]. JÁNOS GONDA: *Some issues of encryption.* Budapest, 2010. https://www.inf.elte.hu/dstore/document/286/A_rejtjelezes_nehany_kerdese.pdf; downloaded on 21 March 2024.

[25]. Kaspersky company website. https://www.kaspersky.com/resource-center/threats/deep-web; downloaded: 21 March 2024.

[26]. https://digipedia.hu/cikk/mi-az-a-biometrikus-azonositas-es-miert-jo-ha-hasznalod; downloaded on 21 March 2024.

[27]. ERDÉSZ VIKTOR: *What opportunities does the spread of new technologies offer for detection?* In: Dr. Kovács Zoltán (ed.): Examining the effects of artificial intelligence and other disruptive technologies 2023. Military National Security Service. Budapest, 2023. pp. 440-465.

[28]. BAE Systems website. https://www.baesystems.com/en/cybersecurity/home; downloaded on 28 March 2024.

[29]. Cobwebs company website. https://cobwebs.com; downloaded: 28 March 2024

[30]. Atis company website. https://www.atis-systems.com/en/interception-management-system/; downloaded: 28 March 2024

[31]. Rayzone company website. https://rayzone.com/echo-global-virtual-sigint-system/; downloaded on 28 March 2024.

[32]. Blacksky company website. https://www.blacksky.com/products/; downloaded on 28 March 2024.

[33]. REGÉNYI KUND ET AL: *Sources of information gathering.* National University of Public Service. Budapest, 2019. pp. 13-15.

[34]. ESET website. Social Engineering - what is it and how does it work? ESET; downloaded: 22 March 2024.

[35]. ESET company website. https://www.eset.com/hu/it-biztonsagi-temak-cegeknek/social-engineering/; downloaded on 22 March 2024.

[36]. Microsoft company website. https://azure.microsoft.com/hu-hu/resources/cloud-computing-dictionary/what-is-big-data-analytics; downloaded: 21 March 2024.

[37]. PROF JOHAN STRYDOM: *Introduction to marketing (third edition).* JUTA Academic, 2007

[38]. TechTarget company website. What is deepfake AI? A definition from TechTarget; downloaded on 22 March 2024.

[39]. P9_TA(2024)0138 Artificial Intelligence Act European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD).

[40]. COM/2021/206 final Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON ESTABLISHING HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS.

[41]. European Commission website. https://digital-strategy.ec.europa.eu/en/policies/ai-office; downloaded on 22 March 2024.

[42]. P9_TA(2020)0276. Civil liability regime for artificial intelligence. European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL))

[43]. Meta company website. https://about.fb.com/news/2024/04/metas-approach-to-labeling-ai-generated-content-and-manipulated-media/; downloaded on 9 April 2024.