ARTIFICIAL INTELLIGENCE AND SECURITY. SECURITY 4.0

Prof. Radulov, N., PhD
Department National and International Security, New Bulgarian University, Sofia, Bulgaria

nradulov@nbu.bg

Abstract: The Artificial Intelligence (AI) has giant possibilities to optimize the fight against crime and strengthen national security. In the conditions of unimaginable accumulation of information and the need for rapid decision-making, only the use of AI can lead to success. Intelligence, counterintelligence, forensic science, counteracting organized crime, rapid processing of available information, drafting of varied decisions, creating plans and multivariate scenarios, performing various analyzes is a time-consuming process. Only its use can significantly shorten this time and thus dramatically increase the possibilities for detection, prevention and curbing crimes.

Keywords: Artificial Intelligence; Intelligence; counterintelligence; security; forensic science; investigation; crime.

1. Introduction

Artificial Intelligence (AI) can turn into reality the scenarios of today's fantastic movies: intellectual operating systems and digital assistants. It may even be possible for robots to perform basic police functions. In practice today, if the police have high-quality computer systems with the scope of an AI, much of their routine office work can be done by them, resulting in new reservations being made to increase police presence in urban areas. One of the main resources today - the human - in police activity is increasingly burdened with administrative and cabinet activities, which leads to fewer police officers on the street. AI is now in a position to ensure the monitoring of video-data flows and data collected from a large number of sensors and can warn security services of suspicious activity. It is not far the complete integration of nowadays CCTV networks, their synthesis with modern image search programs, the parallel inspection of all available databases of people with contact with compromised persons, their ranking according to predefined indicators developed by experts. Today the police is already using robots to conduct search and rescue operations[1], to dispose explosive devices in terrorist activity[2] and even to destroy armed criminals[3].

2. Integration of AI into our familiar world

Today, Orbital Insight is practicing machine self-training for low resolution photos from Landsat (US) and Sentinel (in the EU) satellites. It leads to easier identification of military sites, terrorist camps, solving problems of domestic and international security, counteracting organized crime, for example, monitoring and tracking channels for human trafficking and smuggling of goods.

Practice shows that the largest amount of funds are invested in programs in the national security sphere of the individual countries – since September 11, 2001, over $ 500 billion were given for NSA's electronic intelligence systems, and most high-tech products originated from military projects - for example, ARPA-Internet.[4] This creates an additional and serious threat to predominantly militarization of AI by individual countries and individuals with the necessary assets. It is quite possible that some organized crime circles allocate funds and gain access to AI and specialized military and spy-oriented robots[5].

[1] https://www.intechopen.com/books/search-and-rescue-robotics-from-theory-to-practice/introduction-to-the-use-of-robotic-tools-for-search-and-rescue

[2] https://www.hsdl.org/?abstract&did=484061

[3] https://www.uclalawreview.org/policing-police-robots/

[4] Investments in the robot industry in 2019, according to experts, will exceed $ 135 billion, almost twice as high as in 2015 (n. a.)

[5] It can now be estimated that transnational crime accounts for 15-20% of the world gross product as purely criminal turnover and not less than 25% as legal turnover controlled by criminal groups. Generally speaking, criminal groups control not less than a third, but rather about 50% of the global turnover of all kinds of goods and services, assets and finances. – Goodman, Marc. Future Crimes. Inside the Digital Underground and the Battle for Our Connected World, Penguin Random House, 2016.

3. AI self-learning (Deep Learning)

We must proceed from the fact that adequate quality system can solve every task assigned to it, so it is necessary to formulate such a task that the solution found by the machine is unquestionable in the interest of man. The basic idea is that the purpose of the machine must be concluded in a maximum outreach of beneficial for people targets, but it does not have to know in advance what they are. In addition to being useful for the people, the solution must be guaranteed in its security and safety. New technologies, such as quantum computing, may change the AI's approach to getting information about different issues, and allow it to learn by receiving feedback, and perhaps even imitate human cognitive contact functions with the world. If this happens, AI will bring economic benefits, working without inherent human errors due to uniformity and cumulative fatigue. Giant information systems with security-related information stored in them can serve as a basis for comparing, improving and intensifying the deep learning process in a specific area such as national, international and civil security. There are many routine procedures in security processes that AI can handle with ease, but it is important to have a proactive and creative action with preemptive nature. Such action, based on a series of AI-proposed management solutions due to electronic forecasting, observed and corrected by talented managers and analysts, will lead to a major breakthrough in countering modern security threats in its broad and narrow sense. Early identification of threats, accurate forecasts in a different timeframe, provided sufficiently and timely, backed up with detailed multi-factor scenarios of management decisions, can dramatically optimize the fight against crime worldwide.

Security issues are also the issues of the safety and vulnerability of AI. Although the specialized AI offers vast opportunities to society, it can also be deceived, penetrated, or misled. Breaking the security systems is doubly devastating because it affects not only themselves but also the quality of their product – national, public and civil security. We need to be sure that the decisions taken by the machine are not the result of external interference and can not be changed by cyber attacks.

4. Features and capabilities of AI

In order to be aware of the security-related AI capabilities, we need to consider the following features.

The AI changes over time. Today, artificial intelligence is commonly referred to as machine learning opportunity - programming approaches using different algorithms and methods such as linear regression, decision trees, Bayesian networks[6], evolutionary algorithms, and artificial neural networks. Our understanding of what is AI varies with the passing of each milestone in this field. Adaptability, flexibility, predictability and

[6] Bayesian networks, also known as "belief networks" or "causal networks", are graphical models for representing multidimensional probability distributions. – http://www.cs.cmu.edu/afs/cs.cmu.edu/project/learn-43/lib/photoz/.g/web/glossary/bayesnet.html

proactivity in terms of minimum time resources, the speed of decision-making and scenarios realizing them should be the priorities of the AI used in the security sphere.

AIs, robots and people work better when it comes together, there is a factual synergy. In practice it has already shown that people who carry out complex actions or play games are more effective and win when interacting with high-tech applications than when analogous activity is done only by people or just by computers. Increased creativity of man helps to train the AI so that it strives to create original solutions using its capabilities quickly process huge data sets, classifying and arranging a giant number of operations, operative decisions and scenarios that allow special services to implement them successfully. In the field of security, it is clear that this, who apply high technology, uses more, better-processed and verified information, has a wider range of standard management to which he can rely. He receives more detailed scenarios for strategic and operational solutions, and his control capabilities are enhanced. This presupposes a natural basis for creative thinking and management therefore intelligence service gets a great resource for anticipating impact and success.

There are AI systems that help leverage data obtained from open sources, but their use for machine training needs to be arranged and protected accordingly. Data generated by specific forces and means, as well as by processing and monitoring of publicly available sources, are equally actively used in the security field. Allen Dulles claimed that intelligence works with over 90% acquired from open sources data [7]. Therefore, the AI in the security can use all the possibilities for collecting, sorting and managing the data existing in the information space, which optimizes the performance of a quality, timely and effective activity in providing national and civil security.

Even the best intelligent systems can make mistakes and deviations. In the field of security, the data obtained should be further verified in order to eliminate the possibility of both incompetence and subsequent crisis and possible deliberate misinformation resulting from an enemy's operation.

The security impact of AI will depend on the approach and how it is used. The practical application for solving real problems will be decisive. Increasing the capabilities and influence of intelligent systems and robots will increase the importance of creative decisions taken by executives in the sector about location and time of use. This will require a radical change in the security manager's profile regarding his management culture – the set of knowledge, habits and skills, as well as a change in the subjects he will study and practice – cyber-management, cyber-planning, cyber-forecasting, cyber-scenarios, etc.

5. Artificial Intelligence and Counteracting Crime

Collecting information

Collecting data on crime situation is a way to derive the necessary knowledge from large data sets. In other words, this is an approach to discover hidden relationships between organizations and individuals committing crimes by using artificial intelligence methods. The wide range of data mining applications has become a significant area of research nowadays, as part of these applications are related to detection, prevention and curbing crimes. We must not forget the postulate that information and its analysis lie at the heart of the successful fight against crime, as well as the management of this counteraction.

Criminology

Criminology is one of the most important areas of application of intelligent data analysis. It is a process whose purpose is to identify the criminal characteristics. In fact, crime analysis involves investigating and detecting crimes and linking them to criminals. The large numbers of crime data and the complexity of links between them have turned criminology into a suitable area for the application of artificial intelligence analysis methods. Identifying the signs of crime is the first step for further investigation. Using this approach, crime information can be automatically collected and entered into law enforcement databases [8].

AI, training, deep learning and fighting crime

Machine Learning - computer algorithms that allow AI to learn to work with a large amount of data are widely used by technology giants such as Google, Apple and Netflix. The same technology that allows programs to recommend films or to set the order in the Google search results list is now successfully used to combat crimes of varying severity.

Detecting crimes

Because AI is able to analyze a huge amount of data, it can be used to both investigate and prevent crime. An example of this is the advertising of sex services on the Internet. Sex workers are thought to be relatively anonymous and advertise their services almost under the nose of law enforcement authority. But every message on the web leaves a digital trace. Cyber experts can use algorithms for digital tracking data on the internet to train AI to see if women volunteer or coerced advertise their services, focusing on seemingly insignificant details. By processing the input data, algorithms are programmed to analyze such details as a boom of small theft arrests in the area where sex services are advertised. AI may detect an increase in thefts of the least important things, such as toothpaste or soap. The idea of this methodology is that if someone is a victim of human trafficking and is brought from another region, he may be deprived of access to basic subjects for a normal life. Furthermore, AI training is applicable to data related to hotel rooms paid in cash in areas where sexual services are provided and advertised during major events such as concerts or sporting events. This algorithm applies to other details related to trafficking in human beings. For example, analyzing the above-mentioned messages, law enforcement officers use the training opportunities of AI to establish links between ads and their authors, paying attention to such nuances as similar styles of writing and settings used in more than one ad , on websites in missing persons' databases. A learning algorithm is also used to track payment transactions to provide intimate services to identify the links of those paying for advertising with larger organizations involved in trafficking. Machine learning technology for AI can be applied not only to the detection of crimes related to human trafficking and forced prostitution but also for practically any other types of crime.

Forced labor

By training and self-learning AI, law enforcement can determine whether some business works together with companies using forced labor. In the area of supply chain logistics, the use of forced labor is not unusual. AI can help investigate allegations of labor violations or complaints against companies using forced labor. Analysis of data through AI may reveal links that would otherwise be difficult to identify.

Cybercrime

AI can help companies prevent cyber-crime that can cause financial damage and harm their reputation. It can be trained to recognize keywords or topics related to harmful content, thus stopping the potential cyber attack.

Burglary

Law enforcement can use training to detect crimes such as burglary. For example, data on a large volume of theft (date and time when offenses were committed, crime objects and methods, tools to commit) may show similarities with other comparable crimes that have not been resolved. After gathering information

[7] The Craft of Intelligence, 1963, Lyons Press; Reprint edition, May 1, 2016

[8] https://www.forbes.com/sites/bernardmarr/2017/09/19/how-robots-iot-and-artificial-intelligence-are-transforming-the-police/#58325e805d61

about the crime (investigation of the crime scene, interviewing witnesses, investigating crime objects, etc.), they can be used to train AIs to analyze this data, find links with others crimes. AI can easily detect it when formalizing a large enough volume of crime data, or identify suspects and identify gaps in the investigation, and at the same time relieve police officers of unnecessary work to be able to focus on other important aspects of the investigation.

DNA analysis

Modern forensic expertise of DNA is critical to the investigation of crimes, but the interpretation of the DNA code can be quite complicated. Specialized AI training techniques can be used to simplify the interpretation of DNA, especially when it comes to DNA samples of several individuals. There is a huge amount of data that is not currently read solely because our limited capabilities, but the computer algorithms of AI can easily do this [9].

Face recognition [10]

A common method of combating crime using AI is the Face Detection Technology. It is often used at airports to include mapping of human images into law enforcement database files, which allows to identity the perpetrator.

Prevention of crimes of a terrorist nature

Scanning social networks to find people who can be radicalized is another activity that AI can effectively perform after appropriate training. Nowadays, some law enforcement agencies are already using social networking monitoring and analysis to prevent attempts to recruit new members of terrorist organizations such as ISIS and others like them[11]. One such monitoring tool is called iAWACS or the AWACS internet system. This name is similar to the abbreviation used by the US military to describe its intelligence stations. The purpose of iAWACS is to prevent negative events by monitoring the activity on the Internet, identifying and locating potential criminal scenarios.

6. Conclusion

The abovementioned abilities of artificial intelligence in the security sphere impress with the breadth of application and the possible positive effect. Without expanding the scope of the solutions discussed, which can be implemented with the help of the AI, we can certainly argue that it and Security 4.0 will completely change the possibilities for enhancing the quality and intensity of the product “civil and national security” and this change is close and forthcoming.

Bibliography

1. Dulles, A., The Craft of Intelligence, 1963, Lyons Press; Reprint edition, May 1, 2016

2. Goodman, Marc. Future Crimes. Inside the Digital Underground and the Battle for Our Connected World, Penguin Random House, 2016

3. www.cs.cmu.edu/afs/cs.cmu.edu/project/learn-43/lib/photoz/.g/web/glossary/bayesnet.html

4. www.forbes.com/sites/bernardmarr/2017/09/19/how-robots-iot-and-artificial-intelligence-are-transforming-the-police/#58325e805d61

5. www.hsdl.org/?abstract&did=484061

6. www.intechopen.com/books/search-and-rescue-robotics-from-theory-to-practice/introduction-to-the-use-of-robotic-tools-for-search-and-rescue

7. www.roboticsbusinessreview.com/ai/ai-advances-facial-recognition-robots/

8. www.smartdatacollective.com/future-social-media-depend-artificial-intelligence/

9. www.uclalawreview.org/policing-police-robots/

10. https://watermark.silverchair.com/labmed39

[9] https://watermark.silverchair.com/labmed39
[10] https://www.roboticsbusinessreview.com/ai/ai-advances-facial-recognition-robots/
[11] https://www.smartdatacollective.com/future-social-media-depend-artificial-intelligence/