DESPITE CRITICISM, THE ADOPTION OF AI HAS REVOLUTIONSED INTELLIGENCE PRACTICES

NICOLÒ MIOTTO

ABSTRACT

Artificial Intelligence (AI) has been applied in different fields, ranging from healthcare to the defence industry. Although its application has brought about several advantages, ethical issues may have arisen from the use of the technology in policing and law enforcement. On one hand, supporters consider AI as key for the next technological revolution, on the other hand, skeptics view it as a dangerous tool that could endanger human rights' protection. As of now, intelligence agencies consider AI as an innovative tool to improve intelligence practices. Therefore, they are applying AI to reduce the impact of the cognitive constraints affecting the intelligence cycle and improve big data analysis. However, academics and policymakers believe that the adoption of AI is negatively affecting intelligence practices, leading to major legal and ethical issues. This article states that the adoption of AI has revolutionised intelligence practices. To support such a statement, both theoretical analysis and case studies will be provided, addressing the topics of cognitive constraints to the intelligence cycle and big data analysis.

KEYWORDS: Artificial intelligence; Intelligence collection; Big data; Ethics; Law enforcement; Project Maven

INTRODUCTION

Since Artificial Intelligence (AI) was founded as a major field of study in 1956 at the Dartmouth conference in the U.S. (Evangelista et al. 2020: 6), AI-based technologies have been at the centre of the debate among philosophers, academics and policymakers. Indeed, while AI offers evident advantages and innovative solutions to compelling problems, its application raises challenging dilemmas regarding ethics and human rights. Supporters demonstrate how the application of AI has been beneficial in sectors such as healthcare and economics, whereas opponents illustrate the systemic biases characterising the technology and its negative impact on civil liberties.

Intelligence agencies have been part of the debate as they have shown deep interest in the development of AI capabilities. Undeniably, intelligence officers may benefit from the adoption of AI technologies as they improve their capabilities to tackle issues such as terrorism and cyber threats (Ganor, 2019). However, scholars and policymakers have expressed their concern as they believe that vague legal and ethical boundaries and systemic errors of AI may bring about more disadvantages than advantages to intelligence agencies. Therefore, there is uncertainty whether AI has marked a revolution in intelligence practices or if it has, instead, negatively affected them.

Conversely, this essay aims to demonstrate that the development of Artificial Intelligence (AI) has marked a clear and unprecedented revolution in intelligence practices. Indeed, and although critics may argue the contrary, its application solves the cognitive problems characterising the intelligence cycle. Moreover, AI improves data collection and its processing, constituting a cutting-edge tool in Big Data analysis (Ibid.). In order to give empirical evidence of the statement proposed, this paper will provide examples of the use of AI in intelligence practices such as: 1) the U.S. Department of Defence, Project Maven; 2) and the Chinese Integrated Joint Operations Platform (IJOP). Given the complexity of the concept, this essay will first briefly explain what Artificial Intelligence (AI) is. After providing a coherent definition, specific sections will

further elucidate the statements and illustrate the two case studies. Another paragraph will address and challenge criticism regarding the use of AI in intelligence practices. The essay will then conclude by summarising the main ideas expressed.

KEY DEFINITION: ARTIFICIAL INTELLIGENCE (AI)

Artificial intelligence (AI) can be defined as

"The ability of a machine to perform cognitive tasks that we associate with the human mind. This includes possibilities for perception as well as the ability to argue, to learn independently and thus to find solutions to problems independently" (Kreutzer and Sirrenberg, 2020: 3).

Hence, what distinguishes AI from other technologies is its capacity of performing activities in a quick and independent manner while it also learns by doing and developing problem-solving options. Although the term 'machine learning' (ML)[1] may sound more appropriate in certain contexts, this essay will use only the concept of AI. Indeed, the definition proposed also implies independent learning, the main characteristic of ML. Where other terms related to AI are used, definitions and explanations can be found as footnotes.

AN AI-BASED INTELLIGENCE CYCLE

The adoption of AI has improved intelligence analysis' effectiveness, which may be undermined by complex cognitive problems. Among multiple factors, 'mental set'[2], 'fixation'[3] and 'recognition of relevant data'[4] play a key role in determining intelligence failures (Trent, Patterson and Woods, 2007: 83-88).Moreover, other cognitive issues such as 'confirmation bias'[5], 'layering'[6] and 'mirror-imaging'[7] negatively affect intelligence practices (Jackson, 2010: 6-7).

All the factors mentioned previously pose problems related to data collection, processing, analysis and decision-making, activities that AI can efficiently perform without being affected by cognitive biases.

Indeed, artificial intelligence provides information systems such as Decision Support Systems (DSSs)[8] with both 'diagnosis' and 'look-ahead reasoning' (Pomerol, 1997: 10-21). Such activities can be conducted by human officers, but AI applies human-like reasoning with more efficiency amid constantly changing analysis strategies. For instance, AI-based Fuzzy Logic Systems produce outputs operating on the premise that decision making in humans involves all intermediate possibilities between the values YES and NO (Zadeh, 1988: 83-85). Because fuzzy logic is programmed to include even contradictory results, this technology challenges confirmation biases and improves intelligence officers' assessments. Moreover, because AI tools learn by doing, they adopt new behaviours and strategies while tackling the issue of mental set.

1 Considered a subset of artificial intelligence, machine learning can be defined as the study of algorithms that improve independently.

2 Mental set implies the tendency to solve problems privileging successful strategies used in the past. This may prevent the analyst from creating new and better effective strategies.

3 Fixation, also defined as 'cognitive dissonance' in psychology, occurs when analysts struggle with replanning after finding disconfirming evidence.

4 Recognition of relevant data becomes challenging when diverse and complex information is found. Analysts may find it difficult to select what data are relevant and what are not.

5 Confirmation biases reflect analysts' inclination to consider only facts and figures that confirm their assumptions.

6 Layering occurs when intelligence estimates rely upon previous assessments without integrating inconsistencies of the same assessments.

7 Mirror-imaging occurs when analysts assume that the subjects studied behave and think the way analysts do.

8DSSs are information systems which support decision-making processes. They are applied in different fields, ranging from business to healthcare.

9 Intelligent agents (IAs) are programs which operate autonomously based on the inputs they receive. Examples of IAs are Amazon's Alexa and Apple's Siri.

Furthermore, AI supports intelligence officers in delivering accurate and well-informed intelligence products. For instance, Intelligent Decision Support Systems, based on intelligent agents (IAs)[9], play a fundamental role in crisis action procedures (e.g., war, terrorism, and nuclear disasters) (Bui and Lee, 1999). As for this, academics have already demonstrated the benefits of IAs in the intelligence cycle (Edmiston, Gregg, and Wirth, 1998). Indeed, once the user – e.g., the intelligence officer – has requested IAs for information, not only do intelligent agents collect and analyse information rapidly by updating data, but a Central Coordinating Agent (CCA) also assesses whether redundancies or unnecessary information are present in the IAs' reports. Moreover, the intelligence product of the CCA does not present preconceived ideas that may instead characterise human analysts' reports. Indeed, cognitive problems such as mirror-imaging and layering are absent as IAs do not assume characteristics regarding the subjects studied. It instead integrates analyses that may contradict previous assessments.

ALGORITHMIC INTELLIGENCE: THE PROJECT MAVEN CASE

A prominent case of the use of AI to solve cognitive problems is the Algorithmic Warfare Cross Functional Team – also called Project Maven – established by the U.S. Department of Defence in 2017 (Work, 2017: 1-2). Since its deployment in the Middle Eastern theatre of operations, Project Maven has demonstrated to be an efficient tool to tackle cognitive limits. Indeed, it provides intelligence officers with a cutting-edge object recognition algorithm, based on AI. Its natural language user interface offers an intuitive coding of data to intelligence officers, who can then easily access large amounts of information (Markin, 2018: 29-31). Project Maven results are fundamental in solving the problem of recognition of relevant data. As the algorithm is incorporated into unmanned aerial vehicles (UAVs), complex full-motion videos can be quickly analysed and intelligence officers can better identify military targets. Moreover, all the collected data is processed and it offers the best comparative analysis of the external environment. Therefore, the algorithms improve strategic situational awareness (SA) whose accuracy depends on "the ability to observe the operating environment" (On the Radar n.d.). Modern theatres of operations are becoming extremely complex, requiring intelligence officers to continuously conduct monitoring. As for this, Project Maven positively affects surveillance activities increasing SA and ameliorating intelligence officers' understanding of the combat zones.

BIG DATA ANALYSIS AND AI

The world of Big Data[10] poses new challenges to the intelligence community because of its four dimensions: 'variety, volume, velocity and veracity' (Atwood, 2015: 25). Interest in Big Data mining arises from the fact that it offers opportunities in improving the provision of information and risk management. As a consequence, major intelligence agencies have shown their interest in developing AI-based tools that enhance collection and analysis of Big Data. For instance, the Central Intelligence Agency (CIA) was one of the first intelligence agencies to fund AI projects such as 'In-Q-Tel' to improve Big Data analytics capabilities (In-Q-Tel - Central Intelligence Agency, 2017).

The use of AI benefits data mining, whose goal is "to extract knowledge from the available data by capturing this knowledge in a human-understandable structure" (Newton, 2013: 66). Specifically, algorithms can complete different tasks more efficiently and quickly if compared to traditional intelligence practices. Indeed, five different families of algorithms[11] perform diverse and complex operations such as the detection and identification of unconventional data points and the clustering of information

(Van Puyvelde, Coulthart and Hossain, 2017). Investigation of patterns and identification of irregularities provide intelligence analysts with predictive capabilities. By applying AI to Big Data analysis, intelligence agencies have developed the policy strategy defined as predictive policing (PP) which,

"aims to forecast where and when the next crime or series of crimes will take place by identifying trends and relationships that may not be readily apparent to us among the collected data" (Hung and Yen, 2020: 1)

AI-BASED INFORMATION PROCESSING:THE INTEGRATED JOINT OPERATIONS PLATFORM (IJOP) CASE

The Chinese Integrated Joint Operations Platform (IJOP) is the most prominent case of AI-based Big Data analysis. The IJOP is a large network of surveillance practices applied by the Chinese Communist Party in the Xinjiang region (Gorssman et al., 2020: 16-18). It conducts predictive policing operations to control the local population and, specifically, cells linked to the Uyghur secessionist movement. In order to develop effective predictive capabilities, the Chinese government has integrated AI algorithms into the IJOP to analyse data collected by both human intelligence and machine sensors (Layton, 2020: 880).

This cutting-edge tool is pivotal in strengthening the security strategies of the Chinese government. It supports intelligence officers in counterterrorism operations based on the analysis of diverse and disaggregated data. Specifically, not only are factors such as possible timing and location of the attacks addressed, but also vulnerability to radicalisation and suspects' interactions on social media are analysed (McKendrick, 2019: 9-10). The processing of data has improved as artificial intelligence interrelates information in more efficient ways. Moreover, other AI-based systems are integrated with the IJOP.

For instance, iris and voice recognition technologies have been applied in the Xinjiang region since 2016 (Leibold, 2020: 51). The collected biometric data are then processed via the IJOP which identifies risks and potential threats while outlining predictive policing actions. Clearly, this high-tech system strengthens intelligence officers' data collection and analysis capabilities, and provides the Chinese government with efficient and highly precise intelligence reports.

CRITIQUES: ETHICS AND SYSTEMIC ERRORS

Diverse professionals in the fields of law, political sciences and engineering argue that an extensive adoption of AI in intelligence practices does not mark a revolution, but, oppositely, results will be detrimental due to ethical issues and systemic biases that render predictive policing (PP) ineffective (Osoba and William, 2017). For instance, academics have noted that while it is true that video surveillance and biometric techniques based on AI are effective in tackling terrorism, such technologies pose a serious threat to the fundamental right to privacy if used on ordinary citizens (Cataleta, 2020: 45). Moreover, AI technologies may be negatively affected by systemic errors such as 'misbehaving algorithms' (Osoba and William, 2017: 7-8). Such biases may lead to misinterpretation of information and, therefore, even to inequitable predictive policing behaviour (Ibid.:13). Analysts have also stated that the use of AI may be ineffective because of the intrinsic characteristics of terrorism such as irregularity and lack of a common terrorist's profile (Verhelst et al., 2020: 3). Finally, former policymakers, such as Henry Kissinger[12], have taken a strong stand against the use of AI which is stated to deprive

10 Big Data is a term that describes structured and unstructured data that inundate a business on a day-to-day basis.

11 According to data scientist Brandon Rohrer, the five families of algorithms are: 1) binary/multiclassification algorithms; 2) anomaly detection algorithms; 3) regression algorithms; 4) unsupervised learning algorithms; 5) reinforcement machine leaning algorithms. Five Questions Data Science Answers title (e2eml.school)

leaders "[...] of time to think or reflect on the context, contracting the space available for them to develop vision" (Kissinger, 2018).

Although critics raise fundamental points that the intelligence community should address, these arguments are, in fact, misleading. Indeed, first and foremost ethical problems can be solved by incorporating ethics into AI technologies. For example, AI developers have already formulated the concept of 'Responsible Artificial Intelligence', which incorporates important principles like fairness and privacy to detect discriminatory behaviours (Barredo et al., 2020: 103-104). Moreover, both coders and intelligence officers observe due diligence on AI technologies, conducting oversight to correct, if necessary, systemic biases and errors (Lucas Jr, 2013: 12-13). On the top of that, AI designers have already demonstrated the efficiency of AI in predictive policing (PP). As a matter of fact, models based on deep neural network (DNN)[13] target terrorists with a 95% accuracy, predicting locations and type (e.g., stabbing, and suicide bombing) of terrorist attacks (Uddin et al., 2020: 8).

CONCLUSION

In conclusion, it is clear that the adoption of AI has marked a revolution in intelligence practices. AI represents indeed an effective solution to cognitive problems and improves Big Data mining capabilities. As for this, the cases mentioned above are prominent examples of the beneficial effects of AI in intelligence practices. Project Maven demonstrates how AI can support intelligence officers in dealing with cognitive constraints, while the Integrated Joint Operations Platform (IJOP) illustrates how artificial intelligence improves Big Data analysis.

Although critics believe that AI negatively affects intelligence practices because of ethical issues and systemic dysfunctions which undermine predictive policing (PP), their arguments are, in fact, fallacious.It has been demonstrated that ethical and legal principles such as 'fairness' and 'privacy' can be integrated into AI-based tools and systemic errors can be solved by exercising oversight. Moreover, predictive capabilities have already been tested and empirical evidence of their effectiveness has been verified.

Even if artificial intelligence will continue to be at the centre of debate for years to come, it is indubitable that AI has marked a formidable and unprecedented revolution in intelligence practices. Intelligence officers can now employ a groundbreaking technology which enhances intelligence practices by mitigating cognitive constraints and improving data collection and analysis.

BIBLIOGRAPHY

- "On the Radar." n.d. On the Radar. (2020) *Center for Strategic and International Studies.* [Online][Accessed December 9, 2020. Available at https://ontheradar.csis.org/]
- Atwood, Chandler P. (2015). "Activity-Based Intelligence: Revolutionizing Military Intelligence Analysis". *Joint Forces Quarterly* 77 (2): 24-33.
- Barredo Arrieta, Alejandro, Rodríguez, N.D., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., Garcia, S., et al. (2020). "Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI." *Information Fusion* 58: 82–115. DOI: 10.1016/j.inffus.2019.12.012.
- Bui, Tung, and Jintae Lee. (1999). "An Agent-Based Framework for Building Decision Support Systems." *Decision Support Systems* 25 (3): 225–37. DOI: https://doi.org/10.1016/s0167-9236(99)00008-1.
- Cataleta, Maria Stefania, and Cataleta, Anna. (2020). "Artificial Intelligence and Human Rights, an Unequal Struggle." *CIFILE Journal of International Law* 1 (2): 40-63. DOI: 10.30489/cifj.2020.223561.1015.
- Central Intelligence Agency (CIA). "In-Q-Tel: A New Partnership Between the CIA and the Private Sector." [Online][Last modified September 6, 2017. Available at https://www.cia.gov/library/publications/intelligence-history/in-q-tel#copy.]
- Edmiston, Marcia R., Gregg, Darrel R., Jr., Wirth, David G. (1998). "Decision Support for Reconnaissance Using Intelligent Software Agents." Master's Thesis, (Naval Postgraduate School, Monterey, California).

12 Henry Kissinger served as United States Secretary of State and National Security Advisor under the presidencies of Rihcard Nixon and Gerald Ford.

13 Deep neural networks are computing systems that aim to replicate human neural circuits.

- Evangelista, João Rafael Gonçalves, Renato José Sassi, Márcio Romero, and Domingos Napolitano (2020). "Systematic Literature Review to Investigate the Application of Open Source Intelligence (OSINT) with Artificial Intelligence." Journal of Applied Security Research, May, 1–25. DOI: https://doi.org/10.1080/19361610.2020.1761737.
- Ganor, B. (2019). Artificial or Human: A New Era of Counterterrorism Intelligence? Studies in Conflict & Terrorism, pp.1–20.
- Grossman, Derek, Curriden, C., Ma, L., Polley, L., Williams, J.D. and Cooper III, C. A. (2020). "Chinese Views of Big Data Analytics." (Santa Monica, CA: RAND Corporation), [Online][Available at https://www.rand.org/pubs/research_reports/RRA176-1.html]
- Hung, T. W., and Yen, C. P. (2020). "On the person-based predictive policing of AI." Ethics and Information Technology. DOI: https://doi.org/10.1007/s10676-020-09539-x.
- Jackson, Peter. (2010). "On Uncertainty and the Limits of Intelligence." In The Oxford Handbook of National Security Intelligence, ed. Loch K. Johnson, 452–71. Oxford University Press. DOI: 10.1093/oxfordhb/9780195375886.003.0028.
- Kissinger, H.A. (2018). How the Enlightenment Ends The Atlantic. [Online][Available at: https://www.theatlantic.com/magazine/archive/2018/06/henry-kissinger-ai-could-mean-the-end-of-human-history/559124/]
- Kreutzer, Ralf T., and Sirrenberg, Marie. (2020). "What Is Artificial Intelligence and How to Exploit It?" In Understanding Artificial Intelligence, 225-233. Springer International Publishing. DOI: https://doi-org.ezproxy.lib.gla.ac.uk/10.1007/978-3-030-25271-7.
- Layton, Peter. (2020). "Artificial intelligence, big data and autonomous systems along the belt and road: towards private security companies with Chinese characteristics?". Small Wars & Insurgencies 31 (4): 874-897. DOI: 10.1080/09592318.2020.1743483.
- Leibold, James. (2019). "Surveillance in China's Xinjiang Region: Ethnic Sorting, Coercion, and Inducement." Journal of Contemporary China 29(121): 1–15. DOI: https://doi.org/10.1080/10670564.2019.1621529
- Lucas Jr., George R (2013). "Engineering, ethics and industry: the moral challenges of lethal autonomy." In Killing by Remote Control: The Ethics of an Unmanned Military, ed. Bradley Jay Strawser, 211-228. (New York: Oxford University Press). DOI: 10.1093/acprof:oso/9780199926121.001.0001.
- Marlin, Elizabeth M. (2018). "Using Artificial Intelligence to Minimize Information Overload and Cognitive Biases in Military Intelligence". Master's Thesis. (School of Advanced Military Studies, Kansas).
- McKendrick, Kathleen. (2019). "Artificial Intelligence Prediction and Counterterrorism." London, Chatham House, [Online][Available at https://www.chathamhouse.org/2019/08/artificial-intelligence-prediction-and-counterterrorism]
- Newton, Lee. (2013). "Artificial Intelligence and Data Mining." In Counterterrorism and Cybersecurity, 63-80. (New York: Springer-Verlag). DOI: 10.1007/978-1-4614-7205-6_5.
- Osoba, Osonde A., and William Welser IV. (2017). "An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence." (Santa Monica, CA: RAND Corporation), [Online][Available at https://www.rand.org/pubs/research_reports/RR1744.html]
- Pomerol, Jean-Charles (1997). "Artificial intelligence and human decision-making." European Journal of Operation Research, 99 (3): 3-25. DOI: 10.1016/S0377-2217(96)00378-5.
- Trent, Stoney A., Patterson, Emily S., and Woods, David D (2007). "Challenges for Cognition in Intelligence Analysis." Journal of Cognitive Engineering and Decision Making 1 (1): 75-97. DOI: 10.1177/155534340700100104.
- Uddin, M. Irfan, Zada, N., Aziz, F., Saeed, Y., Zeb, A., Shah, S. A. A., Al-Khasawneh, M. A., and Mahmoud, M. (2020). "Prediction of Future Terrorist Activities Using Deep Neural Networks." Complexity. DOI: https://doi.org/10.1155/2020/1373087.
- Van Puyvelde, Damien, Coulthart, Stephen, and Hossain, M. Shahriar. (2017). "Beyond the buzzword: big data and national security decision-making". International Affairs 93 (6): 1397-1416. DOI: 10.1093/ia/iix184.
- Verhelst, H.M., Stannat, A.W., and Mecacci, G. (2020). "Machine Learning Against Terrorism: How Big Data Collection and Analysis Influences the Privacy-Security Dilemma." Science and Engineering Ethics. DOI: https://doi.org/10.1007/s11948-020-00254-w.
- Work, Robert O., Deputy Secretary of Defense, (April 26, 2017). Department of Defense, Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven), 1010 Defense Pentagon Washington, DC 20301-1010.
- Zadeh, L.A. (1988). "Fuzzy Logic." Computer 21 (4): 83–93. DOI: https://doi.org/10.1109/2.53.