Journal of Politics and Ethics in New Technologies and AI

Vol 3, No 1 (2024)

Journal of Politics and Ethics in New Technologies and AI

The Use of Artificial Intelligence (AI) in National Security: Defining International Standards and Guidelines

Christina Meleouni, Iris Panagiota Efthymiou

doi: 10.12681/jpentai.37847

Journal of Politics and Ethics in New Technologies and AI
Volume 3, Issue 1 (2024)
e-ISSN: 2944-9243

https://doi.org/10.12681/jpentai.37847

RESEARCH ARTICLE

The Use of Artificial Intelligence (AI) in National Security: Defining International Standards and Guidelines

Christina Meleouni
PhD Candidate, Panteion University of Social and Political Scientists, Greece; Political Scientist – International Relations Specialist.

Iris Panagiota Efthymiou
Adjunct Lecturer, University of Greenwich, UK; Researcher, Laboratory of Health Economics and Management, University of Piraeus, Greece.

Abstract
The increasing use of AI in national security emphasizes the need to regulate its ethical and responsible use through international rules and regulations. This article examines the importance of AI to national security, with a particular focus on how it impacts cybersecurity, intelligence gathering, and defense strategies. Even though AI has been contributing in the reinforcement of national security, it still raises moral issues and potential security risks, while the need to create international laws and standards is becoming more and more evident. Moreover, this article assesses the use of AI in national security, highlighting the benefits, drawbacks and need for oversight. In addition to examining governance issues, the importance of integrating safety standards with moral and ethical concerns is emphasized, with a particular focus on international cooperation and the evaluation of current institutions.

Keywords: Artificial Intelligence (AI), National Security, International Norms, Partnerships, International Collaboration, International Standards

Introduction

During the last decade, countries are increasingly aware of what Artificial Intelligence (AI) provides in connection with national security. Nevertheless, eradication of barriers that obstruct the major usage of AI in this field requires recognizing and forming such standards and guidelines that protect and manage societal impacts. Currently, AI studies are still closely tied to research on big data, data mining, and machine learning. AI as it applies to (national) security has not been popularized as yet. In this proposed study, concepts of a standard and guideline as well as ethical AI principles are investigated in the context of national security in defense.

Individual countries might use the same state-of-the-art technology or have similar approaches, but as AI technologies are tightly connected with national strategies, applications/algorithms differ not only

from a technical point of view. Countries, where differences are solidified through cultural or other aspects, would tend to have a different approach to the ethical use of AI. So, how do we determine if disparate methodologies on the ethical use of AI should conform to agreed standards?

AI is now an integral part of national security and is changing military strategy. However, the extensive use of AI in national security raises ethical and security concerns and emphasizes the need for global standards and norms. The lack of a single comprehensive legal framework leads to supervisory deficits, transparency problems and ethical dilemmas. This rapid development of AI has necessitated a globally coordinated approach. The risks are serious and have the potential to drastically change people's perception of security and the global environment (United Nations, 2023). Against this background, this article aims to contribute to the ongoing debate by providing a detailed overview of the issues and opportunities related to the development of international guidelines for the ethical use of AI in national security.

Use of Artificial Intelligence (AI) as an Instrument of National Security

During the digital revolution, AI is increasingly being used as a powerful tool to address national security concerns (Meleouni & Efthymiou, 2023). According to the United States Environmental Protection Agency (EPA), national security is *"the security and defense of a nation state, including its citizens, economy, and institutions, which is regarded as a duty of government. Originally conceived as protection against military attack, national security is now widely understood to include non-military dimensions, such as security from terrorism, minimization of crime, economic security, energy security, environmental security, food security, and cyber-security. Similarly, national security risks involve international threats, such as cyber criminals and violent non-state extremists; as well as the domestic threats posed by hazardous material releases and natural disasters. Governments rely on a range of measures, including political, economic, military power, and diplomacy, to safeguard the security of a nation-state. They may also act to build the conditions of security regionally and internationally by reducing transnational causes of insecurity, such as climate change, economic inequality, political exclusion, and nuclear proliferation"* (EPA, 2024).

AI technologies have been rapidly advancing, surpassing human capabilities in solving complex problems and carrying out tasks that were once exclusive to human intelligence. Also, AI has developed a powerful tool for enhancing knowledge, driving economic growth, and enhancing the quality of life. Machines can now perceive, analyze, and respond more quickly and accurately than humans, giving them a competitive edge across various industries, whether civilian or military (Federarion of American Scientists, 2021).

In particular, AI in the military sector allows security experts to analyse large amounts of data in real or near real time, through sensors, satellites, social media, surveillance systems, aircraft and weapon systems (Tamir, 2024), where timely and thorough access to information is vital for the military and security services, as the implementation of self-managed systems improves performance and reduces risks (Deloitte, n.d.). Furthermore, the use of AI in the military has resulted in the creation of autonomous weapons systems. These include drones and semiautonomous and autonomous vehicles that can operate independently or with very little human input. Their capabilities, such as target tracking and reconnaissance, mark a major advancement in defense technology (Utilities One, 2023). This support is crucial for strategy formulation, planning military actions and successfully adapting to dynamic and complex events, thereby strengthening the country's security system (Army War College, 2020). On the other hand, one major advantage is the enhancement of decision-making processes, resulting in quicker and more informed choices. More specifically, AI plays a crucial role in aiding security agencies to make decisions based on data analysis (Aldoseri et al., 2023), since having strong skills in spotting possible dangers and creating effective strategies to counter them is essential for enhancing national security defense (Lee, 2023).

Finally, AI continues to be a key element in identifying cyber security threats. By monitoring network data and detecting suspicious activity or trends, AI contributes to the development of proactive security systems necessary to combat growing cyber threats. This proactive strategy is important to protect sensitive information and critical infrastructure from malicious individuals in the digital realm (Data Science Dojo, 2023).

National Security and AI: Challenges and Responses

Integrating AI into national security comes with many challenges, including technology implementation and ethical considerations. The use of AI in surveillance techniques presents a number of complexities, such as privacy concerns in data capture and the use of facial recognition technology (Yu & Carroll, 2021). These technologies are used to collect and analyse large amounts of personal data without the explicit consent of the data subjects (Mehta, n.d.). This use of AI raises concerns and questions the protection of privacy, individual rights and human rights in general (European Commission, 2021). To address these issues and ensure the appropriate use of AI technologies, a strong legal framework needs to be established (Ben-Israel et al., 2020).

The likelihood of human rights violations increases when systems capable of making autonomous decisions are created and utilized in the context of national security (Rodrigues, 2020). The lack of

transparency and the risk of discrimination are serious concerns, that require the creation of a clear legal framework to protect human rights and avoid prejudice. To reduce these risks and protect the fundamental values of human rights, ethical application must be ensured (Group of Governmental Experts, 2023).

The rapid progress in the development of AI is not usually accompanied by the creation of appropriate legislation and policy, since new technologies often go beyond the legal and ethical framework required to oversee their use. This leads to regulatory delays that prevent the development of timely and effective oversight (Utilities One, 2023). Additionally, the ambiguous aspect of AI development pose challenges in assessing decision-making processes (Felzmann et al., 2020). This lack of transparency impedes the enforcement of essential standards for accountability (e.g. for those involved in safeguarding national security), which is necessary for the ethical and responsible deployment of AI across different sectors. Algorithmic biases are also a problem. More specifically, biases could arise from AI systems that inadvertently pass on biases identified in the training data. This problem arises in the context of decision-making, as unreliable systems can unintentionally reinforce or magnify existing socio-economic imbalances (Borgesius, 2018).

Tampering is another possibility, because AI systems are vulnerable to hostile attacks where malicious people, states and/or non-state actors can deliberately provide false data to fool the system or disrupt its work. These attacks have the potential to undermine AI-based systems and severely threaten their reliability in safeguarding national security (Comiter, 2019). In addition, cyberattacks and cybercrime also pose a threat to national security, e.g. attacks on critical infrastructure such as energy and power grids, hacking a state's communication and information systems. AI-based cyberattacks are expected to become increasingly advanced, intensifying cyber warfare and creating problems in monitoring and responsing to security threats (Fernandez, 2024). Developing and strengthening cybersecurity measures can protect critical infrastructure and systems from this kind of attacks. In addition, educating citizens and staff about the risks of cybersecurity and AI attacks can help prevent this type of incidents and overcome these challenges (NSTXL, 2024). Furthermore, the use of AI in lethal autonomous weapons raises both moral and legal issues. The development and deployment of these weapons in military settings brings up significant ethical concerns regarding accountability, legality, and potential unforeseen outcomes. It is imperative for all states to promptly adhere to existing laws and regulations to address questions of responsibility and potential misuse of AI-based technology in weapons systems (Meleouni, 2021).

In order to effectively combat the risks AI presents to national security, it is crucial to establish a unified and cohesive approach. This requires creating a thorough ethical code that outlines guidelines for the research, creation, and implementation of AI technology. It is essential to consider key factors like fairness, responsibility, openness, and the protection of human rights throughout this process (High-Level Expert Group on Artificial Intelligence, 2019). Moreover, fostering collaboration between policy makers, technologists, ethicists and stakeholders is vital. This collaboration will enable the creation of flexible regulatory structures that can respond to the rapidly changing technological environment. It is also important to introduce continuous monitoring and adaptation processes to ensure that international rules keep pace with AI developments and address new ethical challenges (Díaz-Rodríguez et al., 2023).

Thus, there should be a strong focus on the ethical and human rights-compliant application of AI in national security issues, both in research and in application. The integration of AI technology should ensure a careful balance between security and human rights norms based on ethical considerations (Sanclemente, 2023).

Current Strategies and Guidelines for AI

It is evident that the need for international cooperation is becoming increasingly important in the rapidly growing field of AI. A coordinated, global plan is needed to overcome the difficulties posed by the global spread of this technology. Threats to national security have become globalised and interdependent. Due to the complexity of the threats, no nation can adequately address these challenges alone. The lack of cooperation risks increasing divergence, conflict and difficulties in addressing global security issues (Meltzer & Kerry, 2021).

The introduction of international regulations prevents inequalities in technology or ethical standards and guarantees fair competition between nations. This can reduce the frequency with which certain states gain advantages or act in ways that jeopardize the stability and security of the world (Kavanagh, 2019). States can encourage innovation in AI technology by stimulating collaboration, while ensuring ethical development and application. The combination of knowledge and expertise can lead to more reliable and ethical AI systems (Kavanagh, 2019). Attempts have been made to establish various governmental and non-governmental organizations to monitor and use AI. This chapter summarizes the most important organizations whose goal is to establish uniform and generally accepted rules for the proper use of AI.

The Organization for Economic Cooperation and Development (OECD) in particular is one of the organizations researching the use of AI. Studies published by the organization have examined the advantages and disadvantages of AI and developing technologies, in general, including their impact on human rights and justice (OECD, 2022), while underlining the challenges and the development of generally accepted standards for the proper use of AI (OECD, 2019). Recently, OECD member countries adopted a revised version of the organization's definition of AI, which further clarifies the definition of the AI system, in order to support its continued relevance and technical soundness (OECD, 2024). In addition, the Partnership for Artificial Intelligence (PAI), which is made up of industry executives, researchers and non-governmental organizations (NGOs), is essentially a forum for collaboration and information sharing. It aims to reflect a broader range of international perspectives while developing policies and guidelines for AI (Partnership On AI, n.d.; ICAI, 2023). The Global Partnership on Artificial Intelligence (GPAI) is an important platform that aims to promote cooperation at various levels of AI. The focus is on the ethical aspect of AI, data management, the nature of work in the future, creativity and work ethics, in order to create best practises and standards of behaviour (The Global Partnership on Artificial Intelligence, 2021). Furthermore, the UN Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS) has taken the initiative to initiate discussions and meetings to discuss the ethical and legal issues surrounding autonomous weapons systems (UN, 2023; Group of Governmental Experts, 2023). For its part, the EU is trying to develop a common framework for all Member States, that defines the concept of AI technology and emphasizes its ethical and appropriate use. (European Commission, n.d.).

The Wassenaar Arrangement, in which 42 countries are involved, is also worth mentioning. More specifically, the Wassenaar Arrangement was established to contribute to regional and international security and stability by promoting transparency and greater accountability in the transfer of conventional arms, goods and technology, particularly those relevant to national security, in order to prevent terrorists from acquiring these types of weapons (The Wassenaar Arrangement, n.d.). However, the existence of competing national interests has so far prevented the creation of common, accepted international rules. These inherent limitations draw attention to the continuing difficulties of creating a comprehensive and generally recognised control of AI.

Conclusions

The use of AI in national security has undoubtedly improved cybersecurity, surveillance, and defense strategies. However, AI brings both benefits and risks, as its rapid advancement raises ethical concerns, especially when it comes to human rights. Establishing international guidelines and standards for the

use of AI in national security is crucial, as transparency, accountability and human rights should be the main concerns of these measures, implemented through global cooperation by all stakeholders.

International collaboration on data sharing and the development of global standards for the application of AI in national security with a broad range of stakeholders, including governments, businesses, academic institutions and the public sector (Meltzer & Kerry, 2021) could serve as a model for AI innovation, adoption and use (AI HLEG, 2019). Moreover, educating policymakers, security experts and citizens in general about the ethics of AI, security risks and compliance will help users make informed decisions (Leslie, 2019; AI HLEG, 2019) which will be based on generally accepted rules, while the continuous evaluation and monitoring of new technologies can keep pace with new AI developments and ethical rules (OECD, 2022; Stahl et al., 2023).

In conclusion, collaboration, teamwork and adherence to ethical principles are essential to creating effective AI rules and national security standards. Applying these concepts can open the door to a safer, more reliable and more respectable use of AI in national security.

References

AI HLEG. (2019, April 8). *Ethis Guidelines For Trustworthy AI*. Retrieved January 2014, from European Parliament: https://www.europarl.europa.eu/cmsdata/196377/AI%20HLEG_Ethics%20Guidelines%20for%20Trustworthy%20AI.pdf

Aldoseri, A., Al-Khalifa, K. N., & Hamouda, A. M. (2023). Re-thinking data strategy and integration for artificial intelligence: concepts, opportunities, and challenges. *Applied Sciences, 13*(12), 7082. https://doi.org/10.3390/app13127082

Army War College. (2020, January). *Army Force Management Model*. Retrieved January 2024, from Army War College: https://ssl.armywarcollege.edu/dclm/pubs/HTAR.pdf

Ben-Israel, I., Cerdio, J., Ema, A., Friedman, L., Ienca, M., Mantelero, A., . . . Vayena, E. (2020, December). *Towards Regulation of AI Systems. Global perspectives on the development of a legal framework on Artificial Intelligence systems based on the Council of Europe's standards on human rights, democracy and the rule of law*. Retrieved December 2023, from Council of Europe: https://rm.coe.int/prems-107320-gbr-2018-compli-cahai-couv-texte-a4-bat-web/1680a0c17a

Borgesius, F. (2018). *Discrimination, artificial intelligence, and algorithmic*. Retrieved from Council of Europe: https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73

Comiter, M. (2019, August). *Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It*. Retrieved January 2024, from Belfer Center for Science and International Affairs, Harvard Kennedy School: https://www.belfercenter.org/publication/AttackingAI

Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., de Prado, M. L., Herrera-Viedma, E., & Herrera, F. (2023). Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion, 99*, 101896. https://doi.org/10.1016/j.inffus.2023.101896

Data Science Dojo. (2023, August 2). *AI in Cybersecurity: Revolutionizing threat detection and defense*. Retrieved January 2024, from Data Science Dojo: https://datasciencedojo.com/blog/ai-in-cybersecurity/#

Deloitte. (n.d.). *The Age of With™ - The AI advantage in defence and security*. Retrieved January 2024, from Deloitte: https://www2.deloitte.com/content/dam/Deloitte/fi/Documents/public-sector/ca-en-final-aoda-deloitte-ai-defence-security-pov-v2%20(2).pdf

EPA. (2024, March 19). *National Security Defined* . Retrieved April 2024, from United States Environmental Protection Agency EPA: https://www.epa.gov/national-security/national-security-defined

European Commission. (2021, April 21). *Proposal for a Regulation of the European Parliament and of the Council. Laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts.* Retrieved January 2024, from European Commission: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206

European Commission. (n.d.). *A European approach to artificial intelligence*. Retrieved January 2024, from European Commission: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

Federarion of American Scientists. (2021, March 22). *The National Security Commission on Artificial Intelligence's (NSCAI)*. Retrieved January 2024, from Federarion of American Scientists: https://irp.fas.org/offdocs/ai-commission.pdf

Felzmann, H., Fosch-Villaronga, E., Lutz, C., & Tamò-Larrieux, A. (2020). Towards transparency by design for artificial intelligence. *Science and engineering ethics, 26*(6), 3333-3361. https://doi.org/10.1007/s11948-020-00276-4

Fernandez, E. (2024, January 3). *AI Is Driving a Silent Cybersecurity Arms Race*. Retrieved January 2024, from Government Technology: https://www.govtech.com/artificial-intelligence/ai-is-driving-a-silent-cybersecurity-arms-race

Group of Governmental Experts. (2023, March 10). *Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects*. Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons System, CCW/GGE.1/2023/CRP.1. Retrieved January 2024, from: https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2023)/CCW_GGE1_2023_CRP.1_0.pdf

High-Level Expert Group on Artificial Intelligence. (2019, April 8). *Ethics Guidelines for Trustworthy AI*. Retrieved January 2024, from European Parliament: https://www.europarl.europa.eu/cmsdata/196377/AI%20HLEG_Ethics%20Guidelines%20for%20Trustworthy%20AI.pdf

ICAI. (2023, February 2). *ICAI joins Partnership on AI*. Retrieved January 2024, from ICAI: https://icai.ai/icai-joins-partnership-on-ai/

Kavanagh, C. (2019, August 28). *New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?* Retrieved December 2023, from Carnegie Endowment For International Peace: https://carnegieendowment.org/2019/08/28/new-tech-new-threats-and-new-governance-challenges-opportunity-to-craft-smarter-responses-pub-79736

Lee, T. (2023, November 13). *Where AI Can Improve National Security*. Retrieved January 2024, from Government Technology Insider: https://governmenttechnologyinsider.com/where-ai-can-improve-national-security/

Leslie, D. (2019). *Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector*. Retrieved January 2024, from The Alan Turing Institute: https://www.turing.ac.uk/sites/default/files/2019-06/understanding_artificial_intelligence_ethics_and_safety.pdf

Mehta, A. (n.d.). *The Threat of Facial Recognition Technology*. Retrieved January 2024, from United Nations: https://sdgs.un.org/sites/default/files/2023-05/A6%20-%20Mehta%20-%20The%20Threat%20of%20Facial%20Recognition%20Softwares.pdf

Meleouni, C. (2021). *The military use of Artificial Intelligence* . Retrieved December 2023, from Πανδημος: http://pandemos.panteion.gr/index.php?op=record&lang=el&pid=iid:21219

Meleouni, C., & Efthymiou, I. (2023). Artificial Intelligence (AI) and its Impact in International Relations. *Journal of Politics and Ethics in New Technologies and AI, 2*(1), e35803. https://doi.org/10.12681/jpentai.35803

Meltzer, J., & Kerry, C. (2021, February 17). *Strengthening international cooperation on artificial intelligence*. Retrieved December 2023, from Brookings: https://www.brookings.edu/articles/strengthening-international-cooperation-on-artificial-intelligence/

NSTXL. (2024, January 24). *How Artificial Intelligence is Changing the Future of Military Defense Strategies*. Retrieved January 2024, from NSTXL: https://nstxl.org/how-artificial-intelligence-is-changing-the-future-of-military-defense-strategies/

OECD. (2019, May 22). *Forty-two countries adopt new OECD Principles on Artificial Intelligence*. Retrieved January 2024, from OECD: https://www.oecd.org/science/forty-two-countries-adopt-new-oecd-principles-on-artificial-intelligence.htm

OECD. (2022, November 15). *Harnessing the power of AI and emerging technologies: Background paper for the CDEP*, OECD Publishing. Retrieved January 2024, from Digital Economy Papers, No. 340: https://doi.org/10.1787/f94df8ec-en.

OECD. (2024, March 5). *Explanatory memorandum on the updated OECD definition of an AI system*. Retrieved April 2024, from OECD iLibrary: https://www.oecd-ilibrary.org/science-and-technology/explanatory-memorandum-on-the-updated-oecd-definition-of-an-ai-system_623da898-en

Partnership On AI. (n.d.). *Partnership On AI*. Retrieved from Partnership On AI: https://partnershiponai.org/

Rodrigues, R. (2020). Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. *Journal of Responsible Technology, 4*, 100005. https://doi.org/10.1016/j.jrt.2020.100005

Sanclemente, G. (2023, July). *Digital Tools: Safeguarding National Security, Cybersecurity, and AI Bias*. Retrieved January 2024, from CEBRI: https://cebri.org/revista/en/artigo/112/digital-tools-safeguarding-national-security-cybersecurity-and-ai-bias

Stahl, B. C., Antoniou, J., Bhalla, N., Brooks, L., Jansen, P., Lindqvist, B., ... & Wright, D. (2023). A systematic review of artificial intelligence impact assessments. *Artificial Intelligence Review, 56*(11), 12799-12831. https://doi.org/10.1007/s10462-023-10420-8

Tamir, E. (2024, January 2). *Transforming Aerospace and Defense: The AI Revolution*. Retrieved January 2024, from Defense Update: https://defense-update.com/20240102_2023-leaders-in-military-ai.html

The Global Partnership on Artificial Intelligence. (2021, November). *About GPAI*. Retrieved January 2024, from The Global Partnership on Artificial Intelligence: https://gpai.ai/about/gpai-faq.pdf

The Wassenaar Arrangement. (n.d.). *The Wassenaar Arrangement*. Retrieved January 2024, from The Wassenaar Arrangement: https://www.wassenaar.org/about-us/#about-us

UN. (2023). *Convention on Certain Conventional Weapons* . Retrieved January 2024, from United Nations. Office for Disarmament Affairs: https://meetings.unoda.org/ccw-/convention-on-certain-conventional-weapons-group-of-governmental-experts-on-lethal-autonomous-weapons-systems-2023

United Nations. (2023, July 18). *International Community Must Urgently Confront New Reality of Generative, Artificial Intelligence, Speakers Stress as Security Council Debates Risks, Rewards*. Retrieved January 2024, from United Nations. Meetings Coverage and Press Releases: https://press.un.org/en/2023/sc15359.doc.htm

Utilities One. (2023, November 19). *Engineering and the Ethics of Regulating Emerging Technologies*. Retrieved January 2024, from Utilities One: https://utilitiesone.com/engineering-and-the-ethics-of-regulating-emerging-technologies

Utilities One. (2023, November 26). *Innovations in Military Reconnaissance and Intelligence Systems*. Retrieved January 2024, from Utilities One: https://utilitiesone.com/innovations-in-military-reconnaissance-and-intelligence-systems

West, D. M., & Allen, J. R. (2018, April 24). *How artificial intelligence is transforming the world*. Retrieved 2024, from Brookings: https://www.brookings.edu/articles/how-artificial-intelligence-is-transforming-the-world/

Young, C. (2022, April 19). *How Artificial Intelligence Is Transforming National Security*. Retrieved January 2024, from U.S. Government Accountability Office: https://www.gao.gov/blog/how-artificial-intelligence-transforming-national-security

Yu, S., & Carroll, F. (2021). Implications of AI in National Security: Understanding the Security Issues and Ethical Challenges. In Montasari, R. J. (Ed.). *Artificial Intelligence in Cyber Security: Impact and Implications. Advanced Sciences and Technologies for Security Applications.* Springer, Cham.