# Artificial Intelligence as a peacebuilding tool: what is missing?

A comparative legal analysis.

#### Sveva Ianese<sup>1</sup>

<sup>1</sup>Department of Economics and Management, University of Padova.

#### Abstract

This paper explores the role of Artificial Intelligence (AI) in conflict management and peacebuilding. This emergent research field is examined firstly through a bibliometric analysis of the current literature, based on a database of 158 documents collected by Scopus and published between 1985 and 2024. The analysis highlights the historical evolution of the research field while pinpointing some research gaps. Secondly, we offer a broad overview of the most recent Regulations on this topic (European AI Act, U.S. Executive Order, Chinese laws and political documents). A new perspective on the impact of AI in reducing conflicts emerges, although its driving role in promoting world peace has to be severely reinforced.

#### Keywords

artificial intelligence, peace, bibliometric analysis, literature review, regulation, AI Act, Executive Order, China.

## 1. Introduction

Artificial intelligence (AI) represents one of the most transformative technological innovations of our time [1]. Its ability to analyze massive amounts of information, learn from it and provide data-driven outputs offers potential benefits across many economic sectors [2]. One of the most promising, but also complex, areas in which AI has a significant impact is peacebuilding.

This concept differs from conflict management. While the latter involves diplomatic measures to keep intrastate or interstate disputes from escalating into armed conflicts [3], the former aims at reducing the risk of (re)lapsing into conflict by strengthening national capacities at all levels and at laying the foundation for sustainable peace and development [4]. Examples of AI applications in conflict management are detection of cyber attacks on critical infrastructures [5, 6], logistics, troops and equipment transportation [7], support for military decision-making processes [8] and the control over autonomous weapon systems [9, 10] [11, 12]. Examples of AI applications in peacebuilding are instead the delivery of humanitarian aids by drones [13], conflict prevention through sentiment analysis tools [14, 15], support for peacekeeping operations through NLP models to facilitate real-time dialogues [16] and negotiations [17].

Conflict theorization also embraces milder forms of tensions, such as ethnic, sexual or age discrimination, inequalities and other forms of social frictions that do not reach armed fights [18] (art. 1.2). Such situations may either turn into a conflict or not, due to their characteristics (prolongation in time, extension in space, degree of intensity) and/or the use of weapons  $^1$ [19]. For the purpose of this work we define *conflict* as any form of social or political tension, whether armed or unarmed, at the national or international level.

AI systems can exacerbate the detrimental effects of these phenomena by causing unfairness or breaching fundamental rights [20]. In order to consider Artificial Intelligence as an effective peace-

BEWARE (3rd Workshop on Bias, Ethical AI, Explainability and the Role of Logic and Logic Programming). Bolzano, Italy, 26-28 November 2024.

Sveva.ianese@studenti.unipd.it (S. Ianese)

D 0009-0002-6215-4139 (S. Ianese)

<sup>©</sup> ① © 2024 Copyright for this paper by its author. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

<sup>&</sup>lt;sup>T</sup>These situations do not determine an immediate peace breach, even when a fight occurs. In these cases, the criterion for establishing whether or not there is war is to be found in the intention of the parties (animus belligerenti) by considering both their declarations and material activities.

building tool, we analyze its impact on both conflict management and peace promotion and the way in which lawmakers around the world tried to deploy a set of rules for governing it. Many attempts have been made so far but, in this study, we limit our comparative analysis to the most recent AI regulations, specifically the European AI Act, the U.S. Executive Order and Chinese laws (both hard and soft ones).

The paper proceeds as follows: Section 2 illustrates the research questions. Section 3 presents the stages of the bibliometric analysis and its results. Section 4 provides a comparative analysis of the targeted regulations focusing on the role of AI in conflict reduction and peace promotion. Section 5 includes a discussion and some concluding remarks.

# 2. The problematization of AI as a peacebuilding tool

The role of artificial intelligence in promoting peace worldwide is one of the most interesting, yet under-implemented, perspectives of examining the ethics of AI nowadays. Our objective is to highlight how this technology could increase international prosperity and what is the role of current regulations in enabling it. We address the following research questions:

What is the state-of-the-art of empirical research on AI as an instrument of peace-making? Is it comprehensive or are there some gaps? Can we look at current legislations to derive suggestions on how to conceive of AI as a tool for improving peace worldwide?

### 3. Literature analysis

As academic debate on AI and peace is still emergent, it is useful to develop a structured and explicative review of the topic. We aim to clarify the evolution of research on AI as a peacebuilding tool over time and the intellectual structure of this rising field of study.

The examination is conducted through a bibliometric analysis of 158 documents indexed in the Scopus database, which is one of the most important instruments for collecting systematic information on global scientific literature [21, 22, 23]. It is especially useful for mapping an emergent field of research, as it is not limited to ISI (International Scientific Indexing) journals. As Borgman and Furner (2002) [24] explain, bibliometrics offers a powerful set of techniques and measures for studying the structure of scholarly communication [25].

The sample contains 66 articles and 92 conference papers at any publication stage, in order to include also the most recent works on this topic. Only English documents are considered and we do not set a specific time span. The final cluster includes 128 sources and a time window of approximately 40 years. At this point, bibliometric data are analyzed using the *bibliometrix* software, a flexible tool for conducting comprehensive mapping analysis [26].

Table 1 displays the principal information regarding the bibliographic data frame.

Referring to the time window, most of the works on AI and peace had been published from 2016 onwards. The highest levels of scientific production have been registered in 2018, 2021 and 2023 respectively (Fig. 1). Those peaks coincide with a phase of increased war conflicts and social tensions worldwide (e.g. Syria in 2018, India in 2021, Ukraine in 2023) [27]. Moreover, many of these events were characterized by the adoption of AI in military settings [28, 29, 30].

The geography of the scientific production reflects international dynamics too. The most prolific countries are not only those driving global technological progress but also those where AI has been applied in conflictual contexts (both armed and unarmed), such as China and the U.S. [29] (Fig. 2).

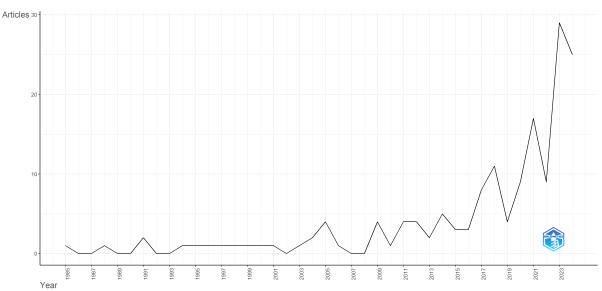
Scholars' attention on the relationship between AI and armed conflicts seems to be largely drawn by international dynamics consequently.

Moving to the conceptual structure of the targeted knowledge, various thematic clusters emerge through a co-occurrence analysis (Fig. 3).

# Table 1Main sample information

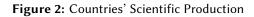
Description	Results
Main information about data	
Timespan	1985:2024
Sources (Journals, Books, etc)	128
Documents	158
Average citations per document	8,62
References	4838
Indexed keywords	1327
Document types	
Article	66
Conference paper	92
Authors	
Authors	469
Authors of single-authored documents	35
Authors of multi-authored documents	434

#### Figure 1: Evolution of the scientific production



- A first (purple) cluster relates to the military applications of AI, with associated keywords like *disaster* and *military application*.
- A second (orange) cluster explores the topic of human-machine interaction and its implications for human life, as it relates to words like *machine learning* and *human*.
- A third (green) cluster highlights the relation between AI specifically machine learning and international relations, due to its matching with keywords like *forecasting* and *international relations*.
- Finally, the fourth (red) cluster links the use of AI to purposes unrelated to armed conflicts. This area includes technological applications for improving the quality of citizens' life, as suggested by *social aspects, e-learning* and *education* keywords.

A keywords analysis concludes our bibliometric scrutiny. Figure 4 is developed using the *word-clouds.com* software starting from the keywords listed by the authors in the sampled papers. Alongside terms associated with armed conflicts (e.g. war, weapons, conflict), the cloud provides other terms related to unarmed tensions (e.g. surveillance, dispute resolution) and individual prosperity (education, learning, SDGs). *Peace* word emerges explicitly in the cloud.



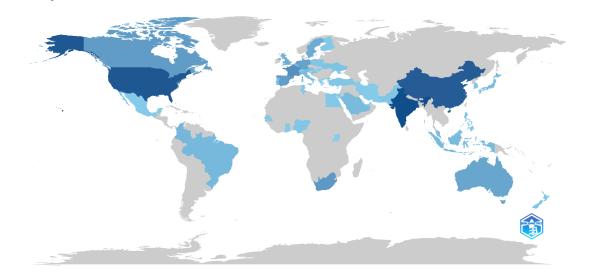
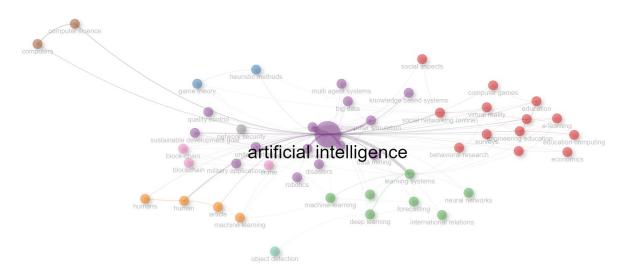


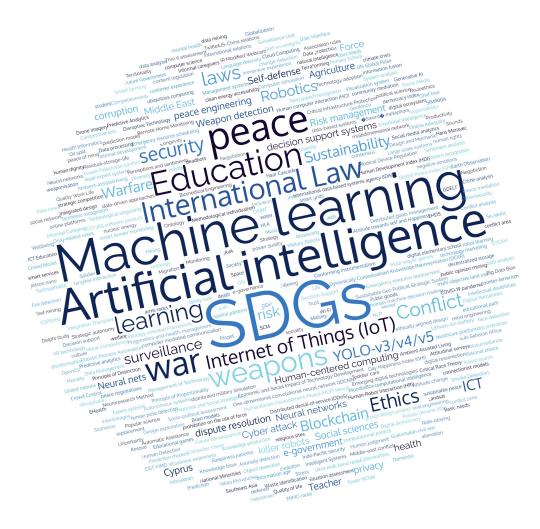
Figure 3: Co-occurrence network



# 4. AI and peacebuilding. A comparative legal perspective.

An in-depth analysis of current regulations serves us to verify how lawmakers are addressing the potential of AI in conflictual environments. In recent years, many legal initiatives have tried to untangle the topic of artificial intelligence but in this work we focus on the most developed projects, meaning the European Regulation on Artificial Intelligence, the U.S. Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence and a set of provisions adopted by the People's Republic of China (PRC). These acts differ significantly from each other in their approach and main purposes but, despite all the differences, they constitute the most mature attempts to rule the development and commercialization of AI systems globally. The following sections offer a brief analysis of each regulation to highlight whether, and eventually how, the role of AI as a peacebuilding instrument is assessed by lawmakers.

#### Figure 4: Keywords word cloud



#### 4.1. The European Regulation on Artificial Intelligence

The European Regulation on Artificial Intelligence (or "Artificial Intelligence Act") resulted from the effort of the European Union to join the technological race [31]. It offers a regulatory framework for the development, the placing on the market, the putting into service and the use of AI systems by adopting a horizontal approach that aims to cover their applications across all economic sectors (Recital 1). The Regulation is strongly inspired by European foundational values and promotes anthropocentric artificial intelligence [32, 33].

These provisions are built on the assumption that AI systems may cause different risks and impact on fundamental rights in various ways [34, 35]. Therefore, depending on the expected level of risk (unacceptable, high, limited or minimal), the lawmaker established a set of rules that developers, producers and distributors must comply with. For example, the use of unacceptable risk systems (e.g. biometric categorization systems based on sensitive characteristics, emotion recognition systems used in the workplace and social scoring systems) is banned. High risk systems, such as those whose adoption could undermine safety or fundamental rights, are permitted although their use is subject to strict obligations [36].

Transparency duties are set for general-purpose AI systems and for those solutions that imply an

interaction with users (e.g. chatbots) since they pose specific, even lower, risks (e.g. disinformation).

Looking at the relationship between artificial intelligence and conflicts, the Regulation expressly excludes from its application AI systems used solely for military purposes. Those are not subject to the rules set out in the AI Act [31] (Recital 24).

However there are "mixed" solutions that can be developed for both military and non-military purposes, such as drones or biometric recognition systems. Additionally, if an AI system is developed or placed on the market exclusively for warfare but is subsequently used for other purposes (e.g. for civilian or humanitarian aims), such a system still falls within the scope of the AI Act (Recital 24). In these hypotheses the Regulation plays a key role in promoting the adoption of AI systems aligned with human rights and EU democratic values by establishing a set of strict obligations for their usage. These limitations may reduce the risk of technological abuses in not-solely-military contexts and the occurrence of armed conflicts by encouraging a human-focused AI development [37, 38].

A first example of these guarantees concerns the use of AI for migration management, asylum and border control, access to essential public services and employment management, which have always been critical sectors for the emergence of social and political tensions. Since those are classified as high-risk systems (art. 6; Annex III), the Regulation imposes a bunch of additional guarantees for their development and use - like the preliminary drafting of a fundamental rights impact assessment, logs recording, human oversight against algorithmic drift and transparency and accuracy obligations. These constraints aim to avoid AI-driven discrimination against weak or underrepresented citizens [39] and promote equal access to essential services or jobs. Compliance with these obligations could dramatically reduce socio-political conflicts caused by technological unfairness.

The second example concerns deepfakes, for which the AI Act establishes transparency and labeling obligations (art. 50) [40, 41, 42]. In fact, AI-generated contents relate to serious political tensions [43, 44, 45] so a reliable use of these technologies may promote a clearer propaganda and a subsequent reduction in political frictions.

In conclusion, the European Regulation lays relevant foundations for a human-centered usage of intelligent systems in unarmed conflicts while not addressing warfare issues. It seeks to unsettle social and political frictions by encouraging the development of AI in accordance with democratic values.

#### 4.2. Artificial intelligence - the U.S. framework

The United States is leading the AI race in many economic sectors but, unlike Europe, they lack a homogeneous legislative framework at Federal level while Member States assumed stricter or more tolerant regulatory positions on this topic [46]. The most significant initiative at Federal level is represented by the White House Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence [47, 48]. It presents eight guiding principles and priorities to be followed in the governance, development and use of AI systems.

The application of such technology in military and intelligence sectors is explicitly addressed in the document. It asks for a national memorandum to explore the role of AI as a key component of the U.S. intelligence and defense strategy, analyzing its impact on citizens' (and exceptionally foreigners') rights (Sec. 4.8). Regarding security and cybersecurity threats, the Executive Order identifies a set of actions to be adopted in order to (i) mitigate the risk that AI is used improperly for developing biological weapons or other chemical perils (Sec. 4.4); (ii) encourage the use of AI for discovering and fixing national IT vulnerabilities (Sec. 4.3); (iii) protect critical infrastructures (Sec. 4.2).

The document also covers the topic of deepfakes. It calls for guidelines and tools for authenticating, detecting, labeling and auditing AI-generated or manipulated contents (Sec. 4.5). Its objective is to facilitate the detection of those contents in order to increase communications transparency. These predictions aim to reduce political frictions by weakening misinformation [49, 50].

Furthermore, the Executive Order highlights the importance of non-discriminatory use of AI in contexts that could generate social and political tensions, such as workplace (Sec. 6), healthcare and justice (Sec. 7-8), data protection (Sec. 9). It sets out a roadmap for achieving these objectives in the coming year while diminishing the risk of algorithmic abuse and biased decisions.

To conclude, the Executive Order covers both warfare and nonmilitary matters. It recognizes the key role of AI in restraining armed and unarmed conflict, algorithmic discrimination and disinformation. Unlike the European Regulation, the document emphasizes the centrality of AI in the U.S. military and intelligence sectors for promoting defence and protecting its citizens from armed attacks (Sec. 4.8).

#### 4.3. The Chinese rules for artificial intelligence

From 2021 onwards, the People's Republic of China has issued a bunch of sectoral regulations and political documents dedicated to AI. These provisions set out new requirements for algorithms development and application, disclosure obligations and technical performance standards [51, 52]. The Chinese approach is "vertical" as it focuses on the main characteristics or applications of AI systems for designing its discipline. However, these provisions have common features that allow for some generalizations [53].

Regarding the role of AI in the military context, since 2019 China has been promoting the "intelligentization" of armed conflict based on the integration of artificial intelligence, quantum computing, big data and other cutting-edge technologies with human tactics [54, 55, 56]. A substantive legislation on AI in warfare is still lacking but non-mandatory provisions have been adopted in order to provide international guidelines on this topic. We refer to the Position Paper of the People's Republic of China on the regulation of military applications of artificial intelligence [57]. The document stresses the importance of preventing the escalation of conflicts and instability at global level while urging governments on the responsible development and application of AI. It calls for strengthening mutual efforts to regulate warfare applications of such technology but admit internal policies allowing the development of weapon systems for countries' defense.

China recently adopted another political document about AI ethics. The Position Paper on Strengthening Ethical Governance of Artificial Intelligence explains the Chinese commitment in advocating a human-centered approach to AI and the principle of *AI for good* [58]. It calls on governments to prioritize ethics and improve accountability mechanisms for protecting the rights of all civic groups. Additionally, the document invites foreign countries to (i) prohibit the use of AI technologies in contrast with laws, regulations, policies and international standards; (ii) identify potential ethical risks implicit in AI.

On the other hand, China disentangled the role of AI systems in unarmed conflicts by adopting a specific regulation on "deep synthesis". The Regulation on Deep Integration Management of Internet Information Services [59] applies to AI-based technology that enables content synthesis provided within the Republic. It aims to both strengthen the management of those systems by promoting their reasonable and effective use in accordance with the law and preserve a good ecology in cyberspace. In order to address specific issues related to deep fakes, the Regulation bans the dissemination of fake news (art. 6) and the alteration of people's biometric characteristics without their consent (art. 14). It forces service providers to authenticate their users before providing them any data or information (art. 9), as this technology can be used to produce, copy and disseminate illegal or false information or assume other people's identities. Finally, it poses a set of technical obligations on content creators (e.g. security assessment when these contents "might involve national security") (art. 15) and forces watermarking for AI-generated contents (art. 17). Consequently the Regulation sets a "red line" of deep synthesis services in order to protect communication transparency and reduce frauds.

To sum up: Chinese provisions point out the central role of AI in governing armed conflict. They allow the use of AI for defense purposes but reject military applications of intelligent systems for obtaining hegemony in warfare. With respect to unarmed conflicts, a sectoral Regulation aspires to reduce the circulation of misleading or sensitive content, which may lead to socio-political tensions (art. 4).

# 5. Discussion and final remarks

The relationship between AI and conflicts (in particular armed ones) appears well established in the literature. Our analysis reveals a rising attention of the scientific community on the relationships between AI, conflict management and human wellbeing in the last years (Fig. 1). In particular, the co-occurrence analysis pinpoints a deep focus on the role of artificial intelligence either in performing conflicts or in improving the quality of people's life (Fig. 3). *Peace* keyword appears as bold in our wordcloud, which means that its linkage with AI systems has been largely explored by scholars (Fig. 4).

But while our analysis detects a deep relationship between AI and human prosperity, the concept of peacebuilding seems to be flattened on its individual dimension. In other words, the literature privileges framing "peace" as individual well-being rather than as a collective good. This assumption is supported by the fact that terms like *education*, *health*, *caregiver* and *SDGs* are associated with AI in our analysis (Fig. 3, 4). In conclusion, a hint on the actual role of artificial intelligence in advancing world peace seems to be lacking in the literature.

This gap offers a significant starting point for investigating how lawmakers tried to disentangle the concrete involvement of AI technologies in promoting peace globally. A comparative analysis of targeted regulations clarifies the main differences among the three legal ecosystems. Unlike the Artificial Intelligence Act, the U.S. Executive Order and the Chinese provisions explicitly handle the use of intelligent systems for military purposes, establishing a set of guiding principles for conflict management at the national and international level. AI is considered a risky weapon so both disciplines admit its use only for national defense while recalling the importance of ethics in this sector [47, 57].

The three legislations also take into account the role of AI in reducing unarmed conflicts. Despite ideological differences, they condemn the irresponsible use of these systems in generating social inequalities and disinformation. They all stress the central role of AI in promoting crystal communications and non-discrimination among individuals, considering it a key factor for political and social stability. However, only the Artificial Intelligence Act includes binding countermeasures for minimizing broad additional sources of social tensions, like migration flows and border control, delivery of essential public services and workplace. For each field, it provides targeted duties in order to reduce the risk of socio-political frictions (art.6 seq.).

Although these provisions represent a fundamental step in promoting AI ethics worldwide, none of them seems to perceive such technology as an effective peacebuilding tool. Its adoption is governed by the same provisions that are setting the rules for AI development in traditional or not-only-military contexts. None of the targeted regulations includes an additional set of rules specifically dedicated to the development and use of AI for peacebuilding purposes. This equivalency may slow down the adoption of intelligent systems in this sector, as developers and deployers are subject to a very strict set of obligations. This circumstance may interfere with the technology-driven advancement of peacebuilding techniques and make the objective of sustainable world prosperity more difficult to achieve.

This conclusion provides a useful point of departure for designing the trajectory of future works aimed at reinforcing the role of artificial intelligence in the peacebuilding sector. We invite lawmakers, governments and international activists to put this topic at the center of their efforts and initiatives and to develop a dedicated set of rules, through mandatory or political documents, that might facilitate the development of cutting-edge solutions for promoting and preserving world peace.

This study has some limitations that should be acknowledged. We include the choice of the initial search keywords, which inevitably affect the results of our work. Also, the comparative legal analysis targets three very different countries that adopt politically-driven approaches regarding the use of intelligent systems. The results are largely affected by the socio-political background of these countries and this aspect might weaken our conclusions. Additionally, our study could be complemented by further research on other regulations and international laws and documents dedicated to examine the role of AI in promoting global peace.

This work initiates an international discussion on the future trajectories of AI as a peacebuilding tool, both as a theoretical concept and a diplomatic and political issue. Through preventing conflict and supporting peace operations, AI can become a powerful ally in creating a nonviolent and human-

centered world.

# References

- [1] O. Ozmen Garibay, B. Winslow, S. Andolina, M. Antona, A. Bodenschatz, C. Coursaris, G. Falco, S. M. Fiore, I. Garibay, K. Grieman, et al., Six human-centered artificial intelligence grand challenges, International Journal of Human–Computer Interaction 39 (2023) 391–437.
- [2] R. Calo, Artificial intelligence policy: a primer and roadmap, UCDL Rev. 51 (2017) 399.
- [3] F. Tanner, Conflict prevention and conflict resolution: limits of multilateralism, International review of the Red Cross 82 (2000) 541–559.
- [4] International Peace Institute (IPI), Peacebuilding. Task Forces on Strengthening Multilateral Security Capacity, Technical Report 10, International Peace Institute (IPI), New York, 2009. URL: https://www.ipinst.org/wp-content/uploads/publications/peacebuilding\_1.pdf.
- [5] B. Guembe, A. Azeta, S. Misra, V. C. Osamor, L. Fernandez-Sanz, V. Pospelova, The emerging threat of ai-driven cyber attacks: A review, Applied Artificial Intelligence 36 (2022) 2037254.
- [6] M. Rege, R. B. K. Mbah, Machine learning for cyber defense and attack, Data Analytics 2018 (2018) 83.
- [7] B. A. de Castro, P. G. C. Pochmann, E. B. Neves, Artificial intelligence applications in military logistics operations, in: Multidisciplinary International Conference of Research Applied to Defense and Security, Springer, 2023, pp. 89–100.
- [8] A. Basuchoudhary, Ai and warfare: A rational choice approach, Eastern Economic Journal (2024) 1–13.
- [9] ICRC, Artificial intelligence and machine learning in armed conflict: A human-centred approach, ICRC Geneva, 2019.
- [10] M. M. Yamin, M. Ullah, H. Ullah, B. Katt, Weaponized ai for cyber attacks, Journal of Information Security and Applications 57 (2021) 102722.
- [11] A. B. Rashid, A. K. Kausik, A. Al Hassan Sunny, M. H. Bappy, Artificial intelligence in the military: An overview of the capabilities, applications, and challenges, International Journal of Intelligent Systems 2023 (2023) 8676366.
- [12] G. U. Osimen, O. M. Fulani, F. Chidozie, D. O. Dada, The weaponisation of artificial intelligence in modern warfare: Implications for global peace and security., Research Journal in Advanced Humanities 5 (2024) 24–36. URL: https://royalliteglobal.com/advanced-humanities/article/view/ 1654/771. doi:10.58256/g2p9tf63.
- [13] A. Rejeb, K. Rejeb, S. Simske, H. Treiblmaier, Humanitarian drones: A review and research agenda, Internet of Things 16 (2021) 100434.
- [14] E. Albrecht, Predictive Technologies in Conflict Prevention: Practical and Policy Considerations for the Multilateral System, 2023. URL: https://unu.edu/sites/default/files/2023-09/predictive\_ technologies\_conflict\_prevention\_.pdf.
- [15] U. Sasikumar, A. Zaman, A.-R. Mawlood-Yunis, P. Chatterjee, Sentiment analysis of twitter posts on global conflicts, arXiv preprint arXiv:2312.03715 (2023).
- [16] D. Masood Alavi, M. Wählisch, C. Irwin, A. Konya, Using artificial intelligence for peacebuilding, Journal of Peacebuilding & Development 17 (2022) 239–243.
- [17] D. J. Olsher, New artificial intelligence tools for deep conflict resolution and humanitarian response, Procedia Engineering 107 (2015) 282–292.
- [18] U. Nations, Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, 1977. URL: https://www.ohchr.org/ sites/default/files/protocol2.pdf.
- [19] S. Vité, Typology of armed conflicts in international humanitarian law: legal concepts and actual situations, International review of the red cross 91 (2009) 69–94.
- [20] M. Brundage, S. Avin, J. Clark, H. Toner, P. Eckersley, B. Garfinkel, A. Dafoe, P. Scharre, T. Zeitzoff,

B. Filar, et al., The malicious use of artificial intelligence: Forecasting, prevention, and mitigation, arXiv preprint arXiv:1802.07228 (2018).

- [21] P. Mongeon, A. Paul-Hus, The journal coverage of web of science and scopus: a comparative analysis, Scientometrics 106 (2016) 213–228.
- [22] S. A. S. AlRyalat, L. W. Malkawi, S. M. Momani, Comparing bibliometric analysis using pubmed, scopus, and web of science databases, JoVE (Journal of Visualized Experiments) (2019) e58494.
- [23] J. Li, J. F. Burnham, T. Lemley, R. M. Britton, Citation analysis: Comparison of web of science<sup>®</sup>, scopus<sup>™</sup>, scifinder<sup>®</sup>, and google scholar, Journal of electronic resources in medical libraries 7 (2010) 196–217.
- [24] C. L. Borgman, J. Furner, Scholarly communication and bibliometrics, Annual review of information science and technology 36 (2002) 1–53.
- [25] B. Cronin, H. B. Atkins, The web of knowledge: A festschrift in honor of Eugene Garfield, Information Today, 2000.
- [26] M. Aria, C. Cuccurullo, bibliometrix: An r-tool for comprehensive science mapping analysis, Journal of informetrics 11 (2017) 959–975.
- [27] G. C. D. Lab, Number of armed conflicts, World, ???? URL: https://ourworldindata.org/grapher/ number-of-armed-conflicts.
- [28] S. Penati, L. Pistarini Teixeira Nunes, On the Use of Artificial Intelligence in the framework of the Syrian War, Technical Report, Budapest Centre for Mass Atrocities Prevention, Budapest, 2021. URL: https://www.genocideprevention.eu/files/On\_the\_Use\_of\_Artificial\_Intelligence\_in\_the\_ framework\_of\_the\_Syrian\_War.pdf.
- [29] T. Khurshid, The impact of artificial intelligence militarization on south asian deterrence dynamics, BTTN Journal 2 (2023) 134–150.
- [30] R. Lindelauf, H. Meerveld, M. Postma, Leveraging decision support in the russo-ukrainian war, Atlantisch Perspectief 47 (2023) 36–41.
- [31] European Union, Regulation 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828, 2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L\_202401689.
- [32] F. Vainionpää, K. Väyrynen, A. Lanamaki, A. Bhandari, A review of challenges and critiques of the european artificial intelligence act (aia) (2023).
- [33] M. Comunale, A. Manera, The economic impacts and the regulation of ai: A review of the academic literature and policy actions (2024).
- [34] C. Novelli, F. Casolari, A. Rotolo, M. Taddeo, L. Floridi, Ai risk assessment: A scenario-based, proportional methodology for the ai act, Digital Society 3 (2024) 13.
- [35] D. Casaburo, I. Marsh, Ensuring fundamental rights compliance and trustworthiness of law enforcement ai systems: the aligner fundamental rights impact assessment, AI and Ethics (2024) 1–14.
- [36] M. Jacobs, J. Simon, Assigning obligations in ai regulation: A discussion of two frameworks proposed by the european commission, Digital Society 1 (2022) 6.
- [37] J. J. Bryson, A. Theodorou, How society can maintain human-centric artificial intelligence, Human-centered digitalization and services (2019) 305–323.
- [38] M. Estévez Almenzar, D. Fernández Llorca, E. Gómez, F. Martinez Plumed, Glossary of humancentric artificial intelligence, Sevilla: Joint Research Centre (Seville Site) (2022).
- [39] B. Xavier, Biases within ai: challenging the illusion of neutrality, AI & SOCIETY (2024) 1–2.
- [40] M. Łabuz, Deep fakes and the artificial intelligence act—an important signal or a missed opportunity?, Policy & Internet (2024).
- [41] F. Romero Moreno, Generative ai and deepfakes: a human rights approach to tackling harmful content, International Review of Law, Computers & Technology (2024) 1–30.
- [42] M. Westerlund, The emergence of deepfake technology: A review, Technology innovation management review 9 (2019).

- [43] C. Whyte, Deepfake news: Ai-enabled disinformation as a multi-level public policy challenge, Journal of cyber policy 5 (2020) 199–217.
- [44] C. Vaccari, A. Chadwick, Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news, Social media+ society 6 (2020) 2056305120903408.
- [45] M. Groh, A. Sankaranarayanan, N. Singh, D. Y. Kim, A. Lippman, R. Picard, Human detection of political speech deepfakes across transcripts, audio, and video, Nature Communications 15 (2024) 7629.
- [46] N. Maslej, L. Fattorini, E. Brynjolfsson, J. Etchemendy, K. Ligett, T. Lyons, J. Manyika, H. Ngo, J. C. Niebles, V. Parli, et al., The ai index 2023 annual report, AI Index Steering Committee, Institute for Human-Centered AI, Stanford University, Stanford, CA (2023).
- [47] J. R. Biden, Executive order on the safe, secure, and trustworthy development and use of artificial intelligence (2023).
- [48] M. Wörsdörfer, Biden's executive order on ai and the eu's ai act: A comparative computer-ethical analysis, Philosophy & Technology 37 (2024) 74.
- [49] B. Chesney, D. Citron, Deep fakes: A looming challenge for privacy, democracy, and national security, Calif. L. Rev. 107 (2019) 1753.
- [50] M. Pawelec, Deepfakes and democracy (theory): How synthetic audio-visual media for disinformation and hate speech threaten core democratic functions, Digital society 1 (2022) 19.
- [51] H. Roberts, J. Cowls, J. Morley, M. Taddeo, V. Wang, L. Floridi, The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation, Springer, 2021.
- [52] A. H. Zhang, The promise and perils of china's regulation of artificial intelligence, Available at SSRN (2024).
- [53] I. A. Filipova, Legal regulation of artificial intelligence: Experience of china, Journal of Digital Technologies and Law 2 (2024) 46–73.
- [54] S. C. I. Office, China's National Defense in the New Era, 2019. URL: https://www.gov.cn/zhengce/ 2019-07/24/content\_5414325.htm.
- [55] P. Paszak, The security strategy of the people's republic of china in light of the 2019 defence white paper, The Bellona Quarterly 700 (2020) 49–64.
- [56] J. Wuthnow, M. T. Fravel, China's military strategy for a 'new era': Some change, more continuity, and tantalizing hints, Journal of Strategic Studies 46 (2023) 1149–1184.
- [57] P. R. of China, Position Paper of the People's Republic of China on Regulating Military Applications of Artificial Intelligence (AI), 2021. URL: http://geneva.china-mission.gov.cn/eng/dbdt/202112/ t20211213\_10467517.htm.
- [58] P. R. of China, Position Paper of the People's Republic of China on Strengthening Ethical Governance of Artificial Intelligence (AI), 2022. URL: https://www.fmprc.gov.cn/eng/zy/wjzc/202405/ t20240531\_11367525.html.
- [59] C. A. of China, Regulation on the Management of Deep Synthesis of Internet Information Services, 2022. URL: https://www.cac.gov.cn/2022-12/11/c\_1672221949354811.htm.