

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Technologies in Peace and Conflict: Unraveling the Politics of Deployment

Jing Ge

Florida International University DOI: https://doi.org/10.55248/gengpi.5.0524.1273

ABSTRACT

The research explores the intricate intersection of artificial intelligence (AI), technology deployment, and global governance in the context of international security and conflict dynamics. Focusing on the evolving landscape shaped by emerging technologies like AI and GenAI, the discussion delves into the nuanced regulatory approaches adopted by the US and China. Key insights reveal the multifaceted impacts of AI, ranging from enhancing peacekeeping capabilities to posing significant threats through deepfakes and misinformation campaigns. The research emphasizes the necessity of robust AI regulations that transcend mere reactive measures, advocating for proactive, structural interventions to address systemic issues.

Also, in highlighting the divergent regulatory frameworks of the US and China, this research underscores the imperative for transparency, accountability, and ethical governance in AI development and deployment. The examination also underscores the importance of incorporating democratic principles into international governance mechanisms surrounding technology standards.

In the end, this research underscores the pivotal role of AI in reshaping global power dynamics, urging a concerted effort towards leveraging technology for positive peace and mitigating its potential for structural violence. By embracing inclusive, multi-stakeholder approaches, governments and tech stakeholders can forge a path towards responsible and sustainable technological advancements that prioritize human security and international stability.

Keywords: Artificial Intelligence (AI), technology deployment, international security, deepfakes, structural interventions.

The Russia-Ukraine war (2022) can be viewed as the most technologically advanced war in human history¹. The use of technologies such as Unmanned Aerial Vehicles (UAV) and Artificial Intelligence (AI) has shifted traditional warfare. More and more people believe that AI can potentially become a transformative technology for international security. The US government views AI as one of the key technologies that can have a great influence on national security strategy. Some US officials argue that AI may become the first advanced technology that can change the war's nature². Also, a series of questions have been triggered regarding how the trajectory of technological innovation can further transform global patterns, and what are technological deployment and competition among the major powers.

The risks and challenges posed by AI mainly stem from two aspects: AI itself and as a tool used for great power games. Therefore, AI regulation contains both the regulation of the inherent unpredictability and autonomy of AI itself, and the regulation of the political risks arising from the political competition between major powers using AI.

In 1942, in *Runaround*, Isaac Asimov proposed "The Three Laws of Robotics" to manage and regulate the ethical relationship between human beings and robots. Today, although the development of AI has not turned the scene of science fiction into reality, the safety concern brought by AI superintelligence has posed an increasing threat to human society in many aspects such as making emotional manipulation, spreading disinformation, and being used to target drone strikes.

¹ Ulrike Franke and Jenny Söderström, "Star tech enterprise: Emerging technologies in Russia's war on Ukraine", European Power, September 5, 2023: https://ecfr.eu/publication/star-tech-enterprise-emerging-technologies-in-russias-war-on-ukraine/#:~:text=For%20him%2C%20the%20war%20between,and%20the%20first%20AI%20war.

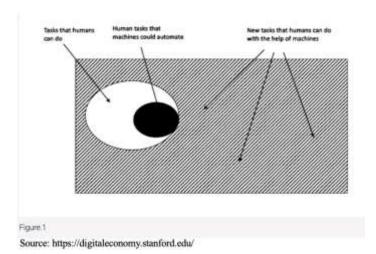
² Ben Garfinkel and Allan Dafoe. "ARTIFICIAL INTELLIGENCE, FORESIGHT, AND THE OFFENSE-DEFENSE BALANCE." December 9, 2019. Retrieved from https://warontherocks.com/2019/12/artificial-intelligence-foresight-and-the-offense-defense-balance/

³ Stone, Wesley L. "The history of robotics." In Robotics and automation handbook, pp. 8-19. CRC Press, 2018.

In the book titled *AI Unexplainable, Unpredictable, Uncontrollable*, Dr. Roman Yampolskiy argues that no existing scientific literature can prove that AI can be safely controlled⁴. According to Dr. Roman Yampolskiy, the AI control problem should have been solved before rather than after developing an AI. Although some mechanisms are proposed by experts for controlling AI, they cannot guarantee safety issues. Even so, efforts to minimize such risk still needed to be made as much as possible. In March 2023, AI experts such as Elon Musk, Steve Wozniak, and Yoshua Bengio signed an open statement to call for at least a six-month moratorium for any AI developments that are more powerful than OpenAI's GPT-4⁵. However, OpenAI CEO Sam Altman argues that OpenAI's iterative deployment technology can help institutions find potential safety risks by uncovering "relatively weak" and "deeply imperfect" issues⁶.

The threats of AI stem from AI's strong learning ability to understand complicated code that human beings may hard to understand, and surpass humans in certain domains, such as AlphaGo and Atari video games. On a technical level, although AI control problems cannot be solved by reinforcement learning and utility functions methods, whether there is an emergency (shutdown) button that can be pressed when AI poses a threat, though AI may be able to learn how to avoid being turned off. In this regard, Google is developing a shutdown button for its AI products. The European countries are discussing whether this button should be mandatory or not. This needs a safety and interpretability-driven algorithm. In fact, the US-USSR arms control once had the same problem. As an important part of arms control, technical negotiations can build a strong control and command system. Therefore, we need to establish a "technical negotiation" system based on the algorithm to process uncontrolled AI. Moreover, we can think about what can humans do to maintain our control over the situations and preserve the existing tech peace.

Therefore, it is important to avoid falling into the "Turing Trap⁷," which refers to the dangers that the development of AI focuses on how to surpass human capabilities rather than complement humans. In Figure 1, we can see that approximately 80% of human tasks need the empowerment of technology. AI deployment should focus on improving the quality of service and living standards of the human being, rather than realizing a simple automation. Hence, AI should not be simply viewed as intruders who came to take something from us, but as enhancers of human capacities.



In this sense, humans can benefit from the development and value of AI systems. For instance, based on traditional drone technology, AI can analyze violence or potentially violent images (such as locations of lines of contact) combined with satellite imagery, thus, reducing or avoiding combatants' harm in peacekeeping operations. In addition, as an important element of the tech peace process, AI can provide solutions for building a just and inclusive environment. For instance, AI-collected data can be used to make peace negotiations and dialogues between different groups and communities to reduce hate speech and political violence. Also, through collecting historical data on mass violence and peace agreements, AI can draw models and trends in predicting conflict and peace dynamics⁸. As a connection tool, AI can build an Information and Communications Technology (ICT) platform for peacekeepers from different countries and regions to exchange more constructive ideas. According to the United States Institute of Peace (USIP) President

⁴ Yampolskiy, Roman V. AI: Unexplainable, Unpredictable, Uncontrollable. CRC Press, 2024.

⁵ OpenAI's GPT-4 is so powerful that experts want to slam the brakes on generative AI. March 29, 2023. Fast Company. Retrieved from <a href="https://www.fastcompany.com/90873194/chatgpt-4-power-scientists-warn-pause-development-generative-ai-letter#:~:text=%E2%80%9CThat%20point%20is%20now%2C%E2%80%9D,in%20and%20institute%20a%20moratorium.%E2%80%9D

⁶ Cat Zakrzewski, Cristiano Lima-Strong and Will Oremus. "CEO behind ChatGPT warns Congress AI could cause 'harm to the world'." May 16, 2023. The Washington Post. Retrieved from https://www.washingtonpost.com/technology/2023/05/16/sam-altman-open-ai-congress-hearing/

⁷ The Turing Trap: A conversation with Erik Brynjolfsson on the promise and peril of human-like AI. November 2, 2022. Retrieved from https://www.brookings.edu/events/the-turing-trap-a-conversation-with-erik-brynjolfsson-on-the-promise-and-peril-of-human-like-ai/#:~:text=They%20discussed%20the%20perils%20of,more%20comprehensively%20than%20traditional%20GDP

⁸ Heather Ashby. "A Role for AI in Peacebuilding." December 6, 2023. Retrieved from https://www.usip.org/publications/2023/12/role-ai-peacebuilding

Nancy Lindborg, "Dialogue is an important part of peacemaking, and the significance of dialogues is allowing people to solve divergence by using language before it changes into violence⁹." Therefore, the empowerment of technology could avoid or ease conflicts.

However, with the use of AI systems becoming more and more pervasive, technology can also be disempowered and become a political tool when it is deployed by governments to enhance its dominance in domestic and international governance. For instance, ChatGPT and Dall-E (the text-to-image generator) can create text, images, and sounds, which can cause safety risks such as private data leaks, identity theft, the proliferation of disinformation, cybersecurity, and government surveillance.

As two products of Generative AI (GenAI), Deepfakes and Large Language Models (LLMs) can be misused and pose major threats to social safety.

In 2017, the word "deepfake" was created by a user of Reddit, and was used in pornographic videos that used open-source face-swap. Deepfake is a synthetic technology where a person's image and sound can be swapped with another, thus, it can proliferate disinformation and threaten national security. Similarly, as a powerful language model, LLM can also be used with evil intentions.

In 2024, 78 countries are going to have election¹⁰, such as the US presidential election, South Africa's national elections, and India's general election. Therefore, the misuse of GenAI, especially deepfakes, can pose potential risks for these elections. Alla Polishchuk in her article titled "AI Poses Risks to Both Authoritarian and Democratic Politics" discussed how AI-driven elections or propaganda affect politics, especially in an authoritarian context. For instance, in the Russia-Ukraine war, Russian hackers uploaded a deepfake video of Ukrainian President Volodymyr Zelensky to a popular Ukrainian website. In the video, President Zelensky urged the Ukrainian army to surrender¹¹.

GenAI is also misused by the Chinese government to infiltrate and influence Taiwan's domestic affairs and elections. However, most of China's strategy tends to be ineffective. According to Kenton Thibaut, Taiwan has established many civil society groups, such as DoubleThink Lab, which aims to combat foreign meddling. Taiwan's government also takes measures to address safety issues such as rooting out the proliferation of disinformation from China's agents or proxies¹². They also developed new AI applications to recognize misleading content posted on social media platforms, and reduce foreign cyberattacks on Taiwan's information space. Taiwan's government has also made efforts to block disinformation. In 2023, it established a special group, consisting of the Digital Affairs Ministry, the Ministry of Education, the Central Election Commission, and the Ministry of Justice, to monitor information manipulation regarding the election on social media platforms.

Given that both the unpredictability of AI itself and its use as a tool for realizing political purposes can pose threats to social and national security, governments and international organizations prioritize AI regulation agenda.

In the following paragraphs, I will mainly discuss how the US and China construct their AI governance, respectively.

The US and China regulatory systems are similar to their national standardization systems. The US adopts decentralized regulation approaches. The US has approximately 50 independent regulatory bodies¹³. Also, different states and institutions can make their own rules. Ultimately, the best of the US's AI-controlled regulation will stand out. Unlike the US decentralized structure, the Chinese government reserves the right of final decisions on AI laws and regulations. Also, AI algorithms need to be reviewed by the Chinese government and must adhere to the Chinese core ideology of socialism.

China's AI Regulations

In December 2022, the Cyberspace Administration of China (CAC) issued the first deepfakes regulation in the world— "Provisions on the Administration of Deep Synthesis of Internet-based Information Services.¹⁴" The regulation states that rumor refutation mechanisms need to be established; the deepfake tools are prohibited from being used for any activities that are banned by national laws and administrative regulations, and a signature or watermark must be added to deepfake work, otherwise, creators will face \$14,500 fine, and both civil and criminal prosecution. In addition to regulating deepfakes, China also put limits on emerging media technologies. According to Giulia Interesse, the Chinese government also takes measures to control generated text,

⁹ Adam Gallagher. "How 'Peace Tech' is Changing Global Conflict." May 10, 2018. Retrieved from https://reliefweb.int/report/world/how-peace-tech-changing-global-conflict

¹⁰ E. Strickland, "Content credentials will fight deepfakes in the 2024 elections," IEEE Spectrum, 2023. [Online]. Available: https://spectrum.ieee.org/deepfakes-election

¹¹ Alla Polishchuk. "AI Poses Risks to Both Authoritarian and Democratic Politics." January 26, 2024. Wilson Center. Retrieved from https://www.wilsoncenter.org/blog-post/ai-poses-risks-both-authoritarian-and-democratic-politics

¹² Prakash Nanda. "Taiwan Uses Artificial Intelligence To Puncture China's Info War; Beijing's Plan Of 'Threat Unification' Thwarted." January 14, 2024. The Eurasian Times. Retrieved from https://www.eurasiantimes.com/taiwan-uses-artificial-intelligence-to-puncture-chinas/

¹³ Bill Whyman. "AI Regulation is Coming- What is the Likely Outcome?" October 10, 2023. Retrieved from https://www.csis.org/blogs/strategic-technologies-blog/ai-regulation-coming-what-likely-outcome

¹⁴ Ananya Bhattacharya. "China goes a step further in regulating deepfakes." January 9, 2023. Retrieved from https://qz.com/china-new-rules-deepfakes-consent-disclosure-1849964709

image augmentation, and virtual scenery¹⁵. Also, in August 2023, China enacted GenAI Measures, which aim to inhibit chatbots from generating content that is related to the subversion of Chinese national power¹⁶. Therefore, China's AI regulations seem to become a new tool of political control and coercion

In addition to becoming a new political control tool, China's deepfake regulations have three main limitations. First, they do not mention specific parameters on how to address particular issues. Second, the application of China's deepfake regulation is still patchy. Third, China's regulations are not applicable abroad since deepfake can still be used for spreading disinformation against the US. According to a study, Pro-CCP Spamouflage has been using Deepfakes to promote China's positive image in global politics. Since late 2022, Spamouflage has been creating many fake social media accounts to praise China while criticizing speeches and protests that are unfavorable to the Chinese government. Also, deepfakes are used for political propaganda in Chinese news broadcasts. For instance, deepfake videos use two Caucasian-looking news anchors to criticize the US's failure to control gun violence, to highlight China's social safety; and how the US needs China's cooperation for the global economy¹⁷.

Therefore, the question we need to think about is whether China's rules and regulations of AI are equally applicable to every participator including its state apparatus, or the Chinese government is the exception for obeying them.

Moreover, China's AI regulation is fragmented¹⁸. Instead of releasing AI legislation as a whole, the Chinese government prefers to set AI rules as individual pieces. For instance, there are AI regulations only specified for deepfakes, and one only for GenAI. Although China's fragmented AI regulation may rapidly respond to evolving technologies, it also causes complexities and potential conflicts that impede the responsible use of AI.

The US's AI Regulations

The US government views AI as a key priority.

Currently, the US remains adopting the sectoral and self-regulatory AI approach. Although federal efforts on AI have not met expectations yet, it presents a positive landscape. For instance, the White House enacted an executive order about voluntary commitments on AI development between the US government and the leading private sectors. In July 2023, the Biden administration and seven leading AI companies— Amazon, Anthropic, Google, Inflection, Meta, Microsoft, and OpenAI signed voluntary commitments to make the development of AI technology more safe, secure, and transparent¹⁹. Different from the EU's safety and rights priority, the US government keeps consistency with its private sectors on prioritizing innovation. In addition to enacting the executive order, other efforts are made by the US, such as AI legislative frameworks developed by the US Senate, AI Risk Management Framework 1.0 proposed by the National Institute of Standards and Technology (NIST), as well as the joint interagency statement on AI announced by officials from agencies: Department of Justice (DOJ), Equal Employment Opportunity Commission (EEOC), and Consumer Financial Protection Bureau (CFPB). Also, AI legislative rules and regulations on both federal and state levels focus more on the responsible use of AI and data protection²⁰. New laws on AI transparency, deepfakes, and platform accountability are proposed by the US Congress, though the specific details are still unclear.

Can the existing AI rules and regulations proposed by the US and the Chinese government fundamentally reduce the threats and conflicts caused by the technological competition between the two nations? The hypothesis I presented is that it is very unlikely to be realized unless AI regulation mechanisms capable of addressing structural issues can be established.

¹⁵ Diego Laje. "China's Deep Fake Law Is Fake." June 1, 2023. Retrieved from https://www.afcea.org/signal-media/cyber-edge/chinas-deep-fake-law-fake

¹⁶ "Interim Measures for the Management of Generative Artificial Intelligence Services," Cyberspace Administration of China, July 13, 2023, http://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm.

¹⁷ China Uses Deepfake Anchors to Spread Political Propaganda. Metanews. February 13, 2023. Retrieved from https://metanews.com/china-uses-deepfake-anchors-to-spread-political-propaganda/

¹⁸ Tate Ryan-Mosleyarchive, Melissa Heikkiläarchive, and Zeyi Yangarchive. "What's next for AI regulation in 2024?" January 5, 2024. Retrieved from https://www.technologyreview.com/2024/01/05/1086203/whats-next-ai-regulation-2024/

¹⁹ FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI. July 21, 2023. Retrieved from https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/#:~:text=As%20part%20of%20this%20commitment,help%20move%20toward%20safe%2C%20secure%2C

²⁰ Artificial Intelligence Review and Outlook – 2024. February 8, 2024. Retrieved from https://www.gibsondunn.com/artificial-intelligence-review-and-outlook-2024/

Positive or Negative Peace?

Based on peace and conflict research, peace theorist Johan Galtung coined the term "positive peace," and distinguished between positive and negative peace²¹. Positive peace can be viewed as the absence of structural violence. Structural violence refers to the inequality of society and any aspects of social institutions that prevent people from meeting their basic needs, achieving their potential, and enjoying their rights. Unlike direct violence, structural violence operates through social, economic, and political engagements. However, negative peace can be defined in two ways. First, it refers to the peace in the shadow of terror. More specifically, this type of negative peace is brought by terror, inequality, threats, and suspicion. In other words, it is a tense peace. Second, according to Galtung, negative peace is the absence of direct violence. For instance, even though both parties have temporarily ceased hostilities through some agreements, the underlying tension between them still remains high. In such a scenario, the resulting peace can be viewed as a negative peace.

In my view, although most AI regulatory approaches enacted by the US and China are designed to reduce conflicts, they can only achieve negative peace. Instead of being developed as a tool to reduce structural violence, in some circumstances, AI tools such as deepfake, are developed as a new form of digital abuse, and increase structural violence.

Therefore, I argue that effective AI regulatory methods require the attribute of "structural intervention." The concept of "structural interventions" is proposed by Farmer et al²². It refers to efforts aimed at addressing underlying systemic or structural issues within a society, economy, and political system. These interventions focus on changing the fundamental factors (such as advancing policy reforms and enhancing self-research and development capability) that cause the problems rather than simply treating their symptoms. Therefore, to achieve positive peace, the US needs to continue to take a leading role in technological regulation efforts by creating non-political structural intervention AI regulation methods against and reducing China's digital abuse in the following two approaches. First, implement regulations that require both domestic and foreign companies to provide algorithmic transparency and accountability, as well as how they make decisions, which can help identify and reduce the spread of disinformation or harmful content propagation. Also, establish mechanisms for auditing AI systems to ensure compliance with ethical standards. Second, launch research and development initiatives that focus on easing digital abuse. Establish multi-stakeholder task forces or advisory boards to develop strategies, share best practices, and coordinate responses to emerging digital threats. Moreover, whether the regulatory systems are bottom-up or top-down, if societies are to advance, both systems should be using the merits of their systems to reduce structural negativity, respectively.

In the end, although positive peace of technology may hard to be achieve at this stage, there are three things we can do to prevent technology-driven conflicts as much as possible.

First, technology companies and governments should be responsible for developing and deploying technologies for peace.

Second, governments and relevant departments need to make regulations to lower potential digital risks such as private data leaks, identity theft, proliferation of disinformation, cybersecurity, and government surveillance.

Third, it is important to responsibly use peace tech collectively, by enhancing cooperation among different stakeholders, such as intergovernmental organizations, the international community, and technology companies. Involving multi-stakeholders promotes safe and sustainable technological solutions for peace.

Also, the existing literature did not consider how democratic theory can be employed within the governance of tech standards and in informing how IGOs relate to them. Therefore, I recommend more applied research that mobilizes democratic theory to inform discussions on how tech policy can be a tool for making technical standards both more widespread and more democratic in the governance and effect of technopolitics. One of the critiques of IGOs is about their transparency and accountability. While they may have internal mechanisms for these, their operations and decision-making processes can sometimes appear opaque to the public. This lack of transparency can raise concerns from a democratic perspective. Also, many IGOs now recognize the importance of civil society in their operations and decision-making processes. Therefore, including NGOs and other civil society groups can enhance the democratic nature of IGOs by ensuring that a broader set of voices and interests is considered.

Relative to traditional political interventions, non-political structural interventions attend to the interests of civic engagement that realize effective AI regulatory measures by altering the structural context in which new technologies emerged.

Therefore, I recommend more applied research that mobilizes democratic theory to inform discussions on how tech policy can be a tool for making technical standards both more widespread and more democratic in the governance and effect of techno-politics. Technically, one of the critiques of the existing AI regulations is about their transparency and accountability. Although regulatory institutes may have internal mechanisms for these, their operations and decision-making processes can sometimes appear opaque to the public. This lack of transparency can raise concerns from a democratic perspective. Also, different governments now recognize the importance of civil society in their operations and decision-making processes. Therefore, including civil society groups can enhance the democratic nature of governments by ensuring that a broader set of voices and interests is considered.

²¹ Galtung, Johan. "Violence, peace, and peace research." Journal of peace research 6, no. 3 (1969): 167-191.

²² Farmer, Paul E.; Nizeye Bruce; Stulac Sara; Keshavjee Salmaan (October 24, 2006). "Structural Violence and Clinical Medicine". PLOS Medicine. 3 (10): 1686–1691. doi:10.1371/journal.pmed.0030449.

First, mobilizes civil engagement to require both domestic and foreign companies to provide algorithmic transparency and accountability, as well as how they make decisions, which can help identify and reduce the spread of disinformation or harmful content propagation. Also, establish civic mechanisms for auditing AI systems to ensure compliance with ethical standards. Second, launch research and development initiatives that focus on easing digital abuse. Establish multi-stakeholder task forces or advisory boards to develop strategies, share best practices, and coordinate responses to emerging digital threats. Moreover, whether it is the US's bottom-up regulatory regime or China's top-down regulatory system, if societies are to advance, both systems should be using the merits of their systems to reduce structural negativity, respectively.