Edited volume

Artificial intelligence and international conflict in cyberspace

Call for chapters

AI technologies are expected to revolutionize operations, strategies, ethics, and norms of international cyber conflict. Thanks to their ability to process large volumes of data, technologies such as machine learning, natural language processing, quantum computing, neural networks, and deep learning, provide the military and intelligence with new operational solutions for predicting, actively countering, and conducting cyber operations. By doing so, AI-enhanced cyber capabilities further blur the already-contested boundaries between defense and offense in cyberspace, while also fundamentally challenging the cyber vs information security divide. For these reasons, the adoption of AI-enhanced cyber capabilities also represents an important strategic asset for states, with the ongoing global race towards the adoption of these technologies fully embedded in broader geopolitical conflicts and technonationalist narratives.

Besides providing operational and strategic opportunities, the adoption of AI technologies also exposes networks to a variety of security risks, primarily related to AI's reliance on (big) data: a broader 'attack surface' and vulnerability for the systems they purport to protect; the risk of potential bias in the data that might lead to miscalculations in cyber offense; and the illusion of security in cyber defense. As these technologies can be employed for intelligence, defensive, and offensive cyber operations - also by exploiting knowledge initially developed for applications in different contexts - international diplomats and regulators need to formulate analytical categories that can capture AI as both an asset and a threat to international cyber security.

This edited volume seeks to address these technical/operational, strategic/geopolitical, and ethical/normative/legal debates with the aim of providing a comprehensive analysis of the interplay between AI and international cyber conflict. We welcome empirical, theoretical, and conceptual submissions from different academic perspectives and disciplines that will contribute to our understanding of challenges and opportunities in

the context of cyber defense, offense, intelligence, and international diplomacy. Topics to be addressed within each thematic area include, but are not limited to:

1. **Technical and operational:** design and deployment; the issue of autonomy; data acquisition and knowledge production; threat modeling; domains of influence; the defense/offense dichotomy; proactive measures; applications in hybrid warfare; etc.

2. **Strategic and geopolitical:** national strategies; the issue of weaponization; international competition; strategic cooperation; strategic autonomy; the role of tech companies and defense industry; control of vs. cooperation with the private sector; deterrence; the problem of imitation and replication; persistent engagement; etc.

3. **Ethical, normative and legal:** responsible design; meaningful human control; transfer learning from civilian to military (and vice versa); normative developments in international fora (UN GGE and UN OEWG); autonomy vis-a-vis attribution and responsibility; legal subjecthood of smart systems; compliance with international legal obligations; etc.

Please submit an extended abstract of **800 words** (+/- 10%) to info@thehaguecybernorms.nl no later than **March 26th**. If you have any questions, you are welcome to contact Fabio Cristiano at f.cristiano@fgga.leidenuniv.nl.

Selected contributors will be invited to an authors' workshop and a thematic conference organized by The Hague Program for Cyber Norms and GEODE alongside the publication of the edited volume (open access). The workshop will be held in May and will provide contributors with the possibility to present their work and receive feedback from fellow contributors at the initial stage of the publication process. With this online workshop, we aim to facilitate in-depth conversations between authors and strengthen the overall coherence of the volume. The conference, open to the public, will be tentatively held in September with the aim of presenting the insights of the forthcoming book and contributions to a broader audience. We hope to be able to hold the conference in-person and welcome contributors to The Hague. If we are able to have an in-person event, we will cover travel and lodging for contributors.

Important dates:

- **26 March |** Deadline for abstract submission
- **9 April |** Notification of acceptance
- **11 May |** Deadline for chapter outline submission (2000 words)
- **18 May |** Authors' workshop (online)
- **25 June |** Deadline for chapter submission (7000-8000 words)
- **17 September |** Deadline for revised chapter submission
- **23 & 24 September |** Conference