

## **Artificial Intelligence across Security Domains: How to Secure AI?**

On 1 April 2026, the Asser Institute will host a 1-day conference to explore how AI shapes the global security ecosystem, critically examining the role of international law. It will bring together a number of experts across various security domains to capture different perspectives and foster collaboration on the opportunities and challenges for the regulation and governance of AI.

This event will involve expert panel sessions and a keynote presentation. A keynote presentation will be given by a leading expert in the field, addressing contemporary AI developments in the security domain and the need for meaningful engagement with relevant stakeholders throughout the lifecycle of AI systems. Five panel sessions will be held on key themes surrounding the topic of AI developments in the security domain, including:

- (1) AI-enabled targeting operations
- (2) AI in cyber operations and cyber warfare
- (3) AI in law enforcement and criminal justice
- (4) The role of the private sector
- (5) Governance and regulation of AI in the security domain

### **(1) AI-enabled targeting operations**

This panel will discuss AI applications for intelligence and targeting across the security domain, including military, law enforcement, and counter-terrorism operations. It will explore how various international law regimes governing these areas are impacted by the integration of AI-enabled systems, incorporating cross-cutting issues such as data management, surveillance, and targeting platforms.

- **Dr Daragh Murray**, Reader in international law Queen Mary University
  - Tentative title: “AI-supported decision making in the security domain: human rights implications”
- **[ICRC speaker]**
  - Tentative title: “The production of military targets using AI”
- **Dr Tasniem Anwar**, Assistant Professor at the Vrije Universiteit Amsterdam
  - Tentative title: “Algorithmically defining terrorists: the use of AI in counter-terrorism operations”

### **(2) AI in cyber operations and cyber warfare**

This panel will examine AI in the cyber domain, including AI-enabled cyber applications, and what lessons can be learnt from the emergence of cyber technologies for legal compliance and responsibility under international law.

- **Nick Wobma**, Deputy Law Branch Head at the NATO CCDCOE
  - Tentative title: “International law and the interplay of AI and cyber”
- **Dr Peter Pijpers**, Col./Associate Professor at the University of Amsterdam

- Tentative title: “Legal accountability for malicious cyber operations”
- **Mathew Cross**, Counsel at the Office of the Prosecutor, International Criminal Court
  - Tentative title: “ICC OTP policy and criminal responsibility for cyber international crimes”

### (3) AI in law enforcement and criminal justice

This panel will explore the law enforcement and criminal justice implications of AI in the security domain. It will consider how law enforcement agencies and (international) courts and tribunals will grapple both with their own use of AI and how to address AI-enabled crimes.

- **Lodovica Raparelli**, Head of research and projects at the Oxford Institute of Technology and Justice
  - Tentative title: “Developing AI agents for criminal justice applications”
- **Judge Iulia Motoc**, Judge at the International Criminal Court
  - Tentative title: “Artificial intelligence in international criminal justice: the perspective of the ICC”
- **Prof Bart Custers**, Professor of Law and Data Science at Leiden University
  - Tentative title: “Predictive policing, risk assessment, and artificial intelligence in law enforcement”

### (4) The role of the private sector

This panel will address how the private sector engages with international law and international law actors in the development, use, and regulation of AI in the security domain. Recent developments indicate the rapidly expanding role for private sector actors, with examples including Microsoft’s engagement with the ICC policy on cyber or NATO’s recent acquisition of Palantir’s Maven platform, suggesting a wider trend of industry intervention in international security.

- **Dr Ilia Siatitsa**, Programme Director and Senior Legal Officer at Privacy International
  - Tentative title: “Engaging industry in the militarisation of AI”
- **Dr Marijn Hoijtink**, Associate Professor of International Relations at the University of Antwerp
  - Tentative title: “The platform as a software architecture and business strategy for defense”
- Tentative title: “Developing AI for the security domain: an industry perspective”

### (5) Governance and regulation of AI in the security domain

This panel explores how AI is governed and regulated across the security domain. Speakers examine legal frameworks, accountability mechanisms, ethical constraints, and international coordination, addressing the needs for measures to address risks, offer transparency and oversight, and provide accountability and redress in rapidly evolving technological security environments.

- **Dawn Lui**, Programme Manager, Research and Training at the Geneva Centre for Security Sector Governance
  - Tentative title: “Governance of AI in the security sector”
- Tentative title: “Civilian applications and implications for international peace and security”
- Tentative title: “How AI is reshaping global security and the legal order”

## **Tentative Programme**

09:00–09:30 Arrival & Coffee

09:30–09:50 Opening

09:50–10:50 Panel Session 1: AI-enabled targeting operations

10:50–11:05 Coffee Break

11:05–12:05 Panel Session 2: AI in cyber operations and cyber warfare

12:05–12:20 Coffee Break

12:20–13:20 Panel Session 3: AI in law enforcement and criminal justice

13:20–14:20 Lunch

14:20–15:20 Panel Session 4: The role of the private sector

15:20–15:35 Coffee Break

15:35–16:35 Panel Session 5: Governance and regulation of AI in the security domain

16:35–16:50 Coffee Break

16:50–17:40 Keynote Presentation: Professor Lorna McGregor

17:40–18:00 Closing