Call for papers

Conference on the law applicable to the use of biometrics by armed forces

Tallinn, 23 – 24 October 2025

Introduction

The NATO Cyber Cooperative Cyber Defence Centre of Excellence, the War Studies Research Centre of the Netherlands Defence Academy and the Amsterdam Centre for International Law (ACIL) are organizing an international conference on the law applicable to the use of biometrics by armed forces, contractors working with armed forces, and ICT companies involved in military acquisition and procurement. The aim of the conference is to provide a platform for debate between academics, practitioners and policy-makers to discuss the legal aspects of the military use of this technology. The conference will build on the fruitful discussions held during two previous conferences devoted to this topic held in Amsterdam (May 2023) and Tallinn (May 2024).

The conference will take place on 23 – 24 October in Tallinn, Estonia. The format is currently planned to be in-person.

We invite those interested to submit a proposal to present a paper at the conference.

Submission deadline: **28 March 2025**

Background

'Biometrics' is the automated recognition of individuals based on their biological and behavioural characteristics. It uses such characteristics to recognize persons. Facial recognition is one example of this type of technology, but there are many other characteristics that can also be used, such as hand topography, voice, gait, and DNA. These characteristics are unique, which makes them very suitable for identifying persons with a high degree of certainty.

The technology was initially developed for use in civilian government and commercial applications. Such use is now widespread: examples include biometric recognition to log in to electronic devices, border control, physical access to restricted areas, and online banking. Biometric technology is however also increasingly employed by armed forces. Some of these applications concern the use of biometrics internal to the armed forces, such as limiting access to facilities or particular systems. External applications include their use in military operations to identify personnel and potential security threats.

The military use of biometrics has raised questions concerning the applicable law(s). Which legal regime(s) apply in the first place? How do the rules in those regimes regulate the use of a technology that is not expressly provided for in those rules? Are new interpretations of existing rules of international law necessary to provide guidance? Does the military use of this technology require completely new rules? What about the interplay between rules from different legal regimes that apply concurrently? And, finally, how can a State best deal with this technology under its domestic law?

The two previous conferences devoted to the law applicable to the use of biometrics have begun to scratch the surface of these issues, however, many questions remain. This conference aims to build upon those discussions.

The workshop organizers invite proposals to present papers dealing with questions concerning the law applicable to the use of biometrics by armed forces, including, but not limited to the following the themes:

• Lessons to be learned from the (regulation of) the use of biometrics in other sectors for the use of this technology in the military sector

Biometrics is used in a wide range of sectors, including in the security sector by other actors than armed forces. Examples could be the use of biometrics in humanitarian assistance operations, for example for registering refugees and preventing assistance fraud. Another example is the use of biometrics in policing and law enforcement, including stability policing. Lessons learned from these uses, the application and implementation of existing legal frameworks and regulatory approaches in these sectors may prove useful for the use of this technology in the military sector.

• (Comparative) domestic (or regional) legal regulations on the use of biometrics by armed forces

A number of States have put in place specific regulation concerning the use of biometrics by the armed forces. An example is the Netherlands. Very little research has so far been done on how individual States (or regional organisations) have regulated the use of this technology by their armed forces. More research in this area would allow for a comparative approach. This could provide valuable insights on the advantages and disadvantages of particular approaches.

• The legal framework for the sharing of biometric information in multinational operations, between operations and outside of operations

The sharing of biometric data between different States exponentially increases the utility of biometrics. This is particularly the case in multinational operations in which States work together closely. The sharing of such data raises particular issues, such as the possibility for misuse of such information and the principle of purpose limitation in data protection law. Similarly, the use of biometrics by the armed forces outside of the context of military operations or an armed conflict comes with specific challenges. So far, little research has been done on the (im)possibilities of biometrics usage by the armed forces outside the operational context.

• Legal aspects of specific uses of biometrics by armed forces

There is relatively little publicly available information on specific use cases of biometrics by armed forces and how issues concerning the applicable law were addressed in those cases. Further studies on specific cases could help identify relevant questions as well as practical solutions to those questions.

• Domestic and international accountability and the use of biometric data

How can accountability for the use of biometrics in violation of applicable law be ensured, and which role can biometrics play in ensuring accountability for other violations of the law? Questions can arise concerning accountability for the use of biometrics in breach of applicable law. How can such accountability be ensured, and does criminal law have a role to play in this regard? How would questions of (criminal) accountability play out in a multinational environment? Do international organizations have a responsibility of their own in this regard? Can developers of biometric systems be held to account? Biometrics can also play a role in holding actors accountable for violations of applicable law(s). The use of this technology in the context of battlefield evidence is an example. What is the legal framework that applies to such use of biometric data, for example when biometric data is used as evidence by domestic or international courts and tribunals?

• Legal questions pertaining to the development and procurement of military and dual-use technologies that employ biometric data

Biometric systems that are employed by the armed forces are often developed and built by the private sector. Legal questions arise concerning the application of procurement procedures and the role of the private sector in ensuring that biometric systems can and will be used in accordance with the law. Research shows that the design of technology can play an important role in how it will be used in practice.

Submissions:

Researchers and practitioners interested in addressing the issues above are invited to respond to this call for papers with a 1-2 page proposal for an article and presentation, along with a brief CV. Proposals should be submitted to prof. dr. Marten Zwanenburg (m.c.zwanenburg@uva.nl) no later than **28 March 2025**.

Publication:

The organisers of the workshop are interested in exploring publication opportunities for selected papers. Papers based on the first conference on this topic were published in a symposium in the Military Law and the Law of War Review.