CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Report on the Conference on the Law Applicable to the Use of Biometrics by Armed Forces Tallinn, 7th – 8th of May 2024

Joep Aarts, Aleksi Kajander, Sebastian Cymutta, Marten Zwanenburg, Steven van de Put

NATO Cooperative Cyber Defence Centre of Excellence

Tallinn 2024

CCDCOE

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is a NATO-accredited knowledge hub offering a unique interdisciplinary approach to the most relevant issues in cyber defence. The heart of the CCDCOE is a diverse group of international experts from government, academia, industry and the military, currently representing 39 nations.

The CCDCOE maintains its position as an internationally recognised cyber defence hub, a premier source of subject-matter expertise and a fundamental resource in the strategic, legal, operational and technical aspects of cyber defence. The Centre offers thought leadership on the cutting edge of all aspects of cyber defence and provides a 360-degree view of the sector. The Centre encourages and supports the process of mainstreaming cybersecurity into NATO and national governance and capability, within its closely connected focus areas of technology, strategy, operations and law.

The *Tallinn Manual*, prepared at the invitation of the CCDCOE, is the most comprehensive guide for policy advisers and legal experts on how international law applies to cyber operations carried out between and against states and non-state actors. Since 2010, the Centre has organised Locked Shields, the biggest and most complex technical live-fire cyber defence challenge in the world. Each year, Locked Shields affords cybersecurity experts the opportunity to enhance their skills in defending national IT systems and critical infrastructure under real-time attacks. The focus is on realistic scenarios, cutting-edge technologies and simulating the entire complexity of a massive cyber incident, including strategic decision-making and legal and communication aspects.

The CCDCOE hosts the International Conference on Cyber Conflict (CyCon), a unique annual event in Tallinn, bringing together key experts and decision-makers from the global cyber defence community. The conference, which has taken place in Tallinn since 2009, attracts more than 600 participants each spring.

The CCDCOE is responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance. NATO-accredited centres of excellence are not part of the NATO Command Structure.

www.ccdcoe.org
publications@ccdcoe.org

Disclaimer

This publication is a product of the CCDCOE. It does not necessarily reflect the policy or the opinion of the Centre or NATO. The Centre may not be held responsible for any loss or harm arising from the use of the information contained in this publication and is not responsible for the content of any external sources, including websites, referenced in this publication.

Digital or hard copies of this publication may be produced for internal use within NATO and personal or educational use when for non-profit and non-commercial purposes, provided that copies bear a full citation.

Table of Contents

Report on the Conference on the Law Applicable to the Use of Biometrics by Armed Forces, Tallinn, 7th – 8th of May 2024

On the 7th and 8th of May 2024, the War Studies Research Centre (WSRC) of the Netherlands Defence Academy (NLDA) and the NATO CCDCOE organised a conference on the law applicable to the use of biometrics by armed forces. This conference, held at CR14 in Tallinn, followed the workshop that took place on the 25th of May 2023 in Amsterdam. The conference brought together around 50 practitioners and academic experts to discuss legal questions arising from the military use of biometrics. This document is intended to serve as a brief report of the conference.

1. Day 1, 7th of May 2024

1.1 NATO's Perspective on the Legal Questions on the Use of Biometrics in Military Operations

The conference was opened with a keynote speech by the Legal Adviser to the NATO Secretary-General, **John Swords (NATO)**. He started by reminding us of the many ways in which the use of biometrics can benefit NATO. It can be essential in, for example, screening local personnel and identifying known terrorists. However, it also comes with risks.

Therefore, NATO introduced a new biometrics policy in 2018. However, allies contemplating a NATO operation still need to consider their national laws on biometrics. Endorsing a NATO mandate does not prejudice their national position. This is also consistent with NATO policy.

It is crucial that biometric data is 'owned' by the nation that collects the data. This entails responsibility for the data. Collection, use, sharing and storing of data needs to be consistent with the national and international legal obligations of that state and NATO cannot be used as an excuse to circumvent this responsibility. However, there is an important role to play for NATO in resolving conflicting viewpoints on international law and untangling alternative approaches.

Nowhere is this more visible than when looking at data exchange, the legal framework for which is a key point for NATO. The exchange of data does not mean that the owner is no longer responsible, as national requirements will continue to apply to the data after sharing. The owner sets the conditions for further use and sharing; it is then also important to guarantee that other nations will offer the same measure of protection. Another issue to consider in this context will be the classification of potential data.

Currently, these developments are definitely an emphasis point. The use of emerging technologies may add to the existing legal requirements and is also visible in a greater push towards legislating these practices. Likewise, we can see that the advance of further technologies may lead to an ability to unleash powerful new capacities.

Mr. Swords concluded by stating that there are ample doctrinal and domestic frameworks which can be expected to address most legal issues. NATO policy can serve to address the gaps between these legal frameworks. This policy can facilitate the important role biometrics can play during NATO operations, serving as a powerful tool for NATO member states to fulfil their legal obligations and protect the territory from further attack.

1.2 Panel Discussion: Facial Recognition and AI in Military Operations

Following the keynote speech, the first of two panel discussions took place. This panel, chaired by Prof **Marten Zwanenburg (NLDA)**, focused on facial recognition technology (FRT) and artificial intelligence (AI) in military operations.

Decision-support systems, FRT and Predictive Algorithms under the Law of Targeting

The first presentation was by **Emelie Andersin (Leiden University)**, whose presentation was titled *Decision-Support Systems, Facial Recognition Technology and Predictive Algorithms under the Law of Targeting*. As a case study, she used the 'Gospel' system reportedly used by the Israeli Defence Forces to highlight legal challenges that arise when using FRT and AI in the targeting process. She highlighted several challenges with using FRT and AI, including ensuring adherence to the principle of distinction, as FRT can identify but not determine the status of targets, risking false positives. She also highlighted the advantages of using FRT and AI, demonstrating that AI's ability to predict movements and patterns enhances intelligence and collateral damage estimations. However, its opaque nature poses issues for military commanders, who may lack the technical expertise to fully understand this technology. As a further condition, the principle of precaution requires commanders to critically assess AI-driven recommendations. Automation bias, where over-reliance on AI occurs, for instance under stress, highlights the need for thorough validation and cautious application of AI and FRT in targeting decisions.

In the discussion, further issues were raised. These included the role of prior strikes as an indication for further assessments by the system and the topic of responsibility under international law whenever commanders rely on the system to facilitate strikes. The distinction between autonomous weapon systems on the one hand and AI-supported decision support systems on the other hand was highlighted.

1.3 Facial Recognition-Based Targeting under International Law

The second presentation, by **Magdalena Pacholska (Asser Institute)**, was titled *Facial Recognition-Based Targeting under International Law.* She introduced the basic workings of FRT, which steps it requires and its reliability. Although no documented cases of FRT being used explicitly for targeting exist, its integration into the targeting processes is anticipated. FRT's passive data collection capability makes it suitable for identification in combat scenarios, especially in non-international armed conflicts where adversaries often weaponise anonymity.

She then further developed the legal framework regarding the use of such technologies. First, it is important to note that International Humanitarian Law (IHL) remains neutral to technology, and can thus be applied to any (new) technology. In theory, FRT can enhance compliance with the principle of distinction by providing additional layers of information. However, challenges include the potential for mistaken identity and the necessity of maintaining human oversight due to current technological limitations. The use of FRT must ensure that it does not shift targeting towards punitive rather than preventive actions. FRT is not prohibited by IHL, but its employment must be carefully managed, requiring human oversight until technology surpasses human performance under combat conditions.

After the presentation, the discussion focused on the (parallel) application of human rights law and IHL. This concerned, among other things, the scope of the exception to the applicability of human rights during an 'active phase of hostilities' as developed in the case law of the European Court of Human Rights (ECtHR). This provides an obvious challenge in applying human rights obligations in this context.

1.4 Biometric Data in Targeting Operations and the European Convention on Human Rights (ECHR)

The final presentation in the panel was titled *Biometric Data in Targeting Operations and the ECHR* and was given by **Elisabeth Hoffberger-Pippan (Peace Research Institute Frankfurt)** and **Kushtrim Istrefi (Utrecht University)**. They used several hypothetical scenarios to explain the territorial and extraterritorial application of the ECHR, which follows from Article 1 of the ECHR and is based on the concept of 'jurisdiction'.

While biometrics aid in identifying targets, they do not themselves actually engage in targeting, thus involving issues related to the right to private life and the prohibition of discrimination, rather than, for example, the prohibition of torture or the arbitrary deprivation of life. In the context of armed conflict, chaotic conditions can negate jurisdiction in the sense of Article 1 ECHR. Extraterritorially, jurisdiction typically requires effective control over territory or individuals. However, biometrics, by enabling precise identification, could potentially lead to a state exercising 'functional' control, impacting jurisdiction. The speakers discussed the recent case law of the ECtHR on the scope of application of the ECHR, which revolves around the concepts of 'chaos' and 'proximity'. They concluded that what ultimately matters in determining whether a state exercises jurisdiction are precision, clarity and/or functional control. They argued that the use of biometrics will increase the chances of establishing jurisdiction as it increases precision, clarity and functional control over individual targets.

In the discussion following the presentation, an analogy was made between biometrics and other means of identification. Whereas the ECtHR has not directly addressed the topic in cases concerning biometrics, an analogy can be made with many other cases dealing with the topic of identification. It was noted that if 'chaos' can lead to the ECHR not applying, this might provide a perverse stimulus for states to create as much chaos as possible in order to avoid human rights obligations.

1.5 Past, Present and Future of Battlefield Evidence

Rikke Rietveld (Cranfield University) opened the second part of the first conference day by presenting her research on battlefield evidence. Her presentation was titled *Past, Present and Future of Battlefield Evidence.* She aims to develop a battlefield forensics framework through historical analysis and assessment of current practices. Motivated by resource constraints, technological advancements and legal issues, the study identifies key stakeholders, legal frameworks and operational challenges. Case studies in Ukraine and Iraq highlight coordination difficulties and legal challenges. NATO's technical exploitation capabilities encompass various domains, emphasising the need for collaboration. Her findings have revealed limited understanding, inadequate doctrine and challenges in intelligence sharing. She underscored the importance of international collaboration due to resource constraints. However, at present most activities in the context of battlefield evidence remain nationally based.

1.6 NATO Biometrics Programme

Rietveld's presentation was followed by **Sam Henze (NATO)**, whose presentation was titled *The Use of Biometrics in Military Exercises – Perspectives and Solutions*. He asserted that the effective use of biometrics in military operations necessitates a clear legal framework and understanding of capabilities. Biometrics, which involves automated recognition based on behavioural and biological traits, presents specific considerations and risks. Biometric data encompasses various samples that are crucial for linking events with individuals.

Identification and verification processes differ, with scalability allowing diverse operational uses across different stages of military operations, from offensive to enabling operations. Political guidance is essential, with command structures planning operations based on commanders' priority information requirements.

The NATO biometrics programme aims to establish shared processes, capability development and privacy-enhancing technologies. However, challenges include a focus on threat actors rather than supporting military personnel and integrating biometrics with other intelligence sources. Bridging the gap between technological potential and reality is crucial, alongside transitioning from counterterrorism to deterrence and defence strategies. Counter-intelligence considerations underscore the need for comprehensive policy and doctrine development.

During the discussion, the question was raised whether we should ignore the fact that biometric technology is already being used, even if the military is behind in this development.

1.7 The Use of Biometrics in Military Exercises – Perspectives and Solutions

The next presentation was given by **Dominique Vanhaelemeesch (Belgian Ministry of Defence)** and **Willem Bochmann (Netherlands Ministry of Defence)**, titled *The Use of Biometrics in Military Exercises – Perspectives and Solutions.*

The presenters noted that military data protection encompasses the processing of personal data within a broad military context, including both military and civilian staff. Rooted in the right to privacy, data protection is a fundamental right, distinct from but closely related to privacy rights. Implementing the General Data Protection Regulation (GDPR) is essential, requiring formal legislation in the Netherlands and Belgium to provide a lawful basis for the processing of personal data.

The GDPR serves as a standardised legal instrument, leaving minimal room for customisation, aimed at ensuring uniformity across EU member states. However, challenges arise in interpreting and implementing data protection laws within defence and national security contexts. Collaborations between NATO and the EU aim to bridge legislative gaps and ensure equality in legislation, which is crucial for addressing legal uncertainties.

Practical examples, such as the use of biometrics, highlight the need for legal frameworks to guide data processing activities. Establishing a data protection working group within NATO seeks to find common ground among member states, emphasising the importance of proportional and lawful data processing practices. While the EU provides guidance, NATO serves as the primary platform for addressing data protection challenges within a military context, ensuring the protection of individuals' identities and rights.

The presentation and the discussion that followed highlighted that legislation is an absolute necessity for using biometric data. NATO members are committed to the protection of the identity of people, but this raises the question of whether it is proportional to use all their biometric data in, for instance, identifying casualties. These types of questions all require answers in legislation.

1.8 The Use of Synthetic Data in Biometrics Exercises

After a short break, a presentation was given by **Willem Bochmann (Netherlands Ministry of Defence)**, titled *The Use of Synthetic Data in Biometrics Exercises.* He discussed this subject based on an example from his practice.

The Netherlands faces a legal gap in operational readiness concerning the use of biometric data. Legislation has been adopted that makes the GDPR applicable, *mutatis mutandis*, to military operations and provides for the possibility to derogate from it, in certain circumstances. The absence of specific legal provisions for operational readiness raises questions about the lawfulness of processing biometric data in that context. Article 9 of the GDPR prohibits processing biometric data without a legal basis, presenting challenges for training exercises involving biometric databases. In a case where a large fingerprint database was offered for an exercise, legal issues prompted the decision not to use it. To address this issue, several solutions were considered:

- Seeking explicit consent, but concerns arose over legality and practicality.
- No longer exercising in this field, risking operational readiness.
- Collaboration with other government actors for training purposes, such as the national police.

Utilising synthetic data offers realistic alternatives to real personal data, such as synthetic fingerprint generators. Synthetic data, while not real, provides a close approximation to real data and offers various training possibilities.

The presentation highlighted a few of the practical issues that militaries face when using biometric data for exercises. It is important that an adequate legal framework is used and the experts are consulted beforehand to enable them to react proactively.

1.9 Integrating Legal Challenges of Biometric Data Usage into Cyber Exercises and Data Extraction Operations for the Training of AI-Powered Weapons Systems

The final presentation of the first conference day was given by **Sebastian Cymutta**. He condensed two presentations into one. The presentations were titled *Integrating Legal Challenges of Biometric Data Usage into Cyber Exercises* and *Data Extraction Operations for the Training of AI-Powered Weapons Systems*. Based on the scenario that was used in a NATO cyber exercise, some best practices were discussed: for example, the situation when commanders had been critical of the incorporation of the legal scenario in the cyber exercise, due to new, controversial and unresolved issues being included. As Cymutta pointed out, those are the most relevant problems to address, and their inclusion in exercises may end up providing ideas on how to solve them. During his presentation, Cymutta shared his extensive experience with exercises through best practices that enabled him to address reservations by demonstrating how legal scenarios enhance the overall exercise and are a valuable addition.

2. Day 2, 8th of May 2024

2.1 Panel Discussion: Biometrics and (In-)Security in Military Operations

Steven van de Put (NLDA), chair of the second panel, opened the second day of the conference and introduced the panel members. This panel focused on biometrics and (in-) security in military operations).

The first presentation was by **Lily Hamourtziadou (Birmingham City University)** and **Welmoet Wels (University of Groningen)**, whose presentation was titled *Analysing Data of the Dead: Casualty Recording, Identification and the Human Security Approach to Biometrics of Human Remains in Armed Conflict.* They discussed the connection between human security and biometrics from a humanitarian perspective. Several treaty obligations refer to the protection of the deceased. Relying on this, they introduced the concept of 'necrometrics' of the deceased, as opposed to the biometrics of the living; necrometrics also help to contextualise the deceased by identification. Hamourtziadou and Wels used the Iraqi body count project as an example of necrometrics: the idea of the project was to contextualise the individuals who were killed during the war and thoroughly tell their stories. This can uncover patterns of harm and lend weight to advocacy against the use of certain weapons or tactics. They concluded that necrometrics can show the complexity and dynamics of war. Contextualisation of casualties helps to understand direct and indirect loss of life. The use of necrometrics is a powerful mechanism to comply with IHL and to strengthen human security.

In the discussion that followed, the practicalities of these obligations were emphasised. States are formally the duty bearer under international law, but operational circumstances might dictate who executes this task. Currently, there is no legal standard for collecting data. Further discussion then focused on the deceased as persons under IHL. It was noted that, currently, the literature leans towards treating them as objects, but that this is also context-dependent. Some experts have also noted that they might form a separate category.

2.2 The Military Fantasy of Biometrics: Neglecting the Risks of Normalising Bodies During Armed Conflicts

The second presentation, by **Anna Greipl (Geneva Academy)**, was titled *The Military Fantasy of Biometrics: Neglecting the Risks of Normalising Bodies During Armed Conflicts*. She focused on persons with disabilities, being the world's largest minority group though often overlooked when discussing the effects of military operations. Biometrics, while effective for identifying individuals quickly and accurately, present challenges for disabled persons due to the assumption of normality in behaviour and physical presentation; this assumption often leads to misidentification or exclusion of disabled individuals. Moreover, biometric systems may flag disabled individuals as threats due to atypical behaviours that fall outside the norm recognised by these systems. The UN Convention on the Rights of Persons with Disabilities emphasises the diversity and agency of disabled persons. This highlights the need to recognise and accommodate the broad spectrum of disabilities in both the development and operational phases of biometrics. In the development phase, it is crucial to ensure hardware accessibility and to build algorithms that are inclusive of disability data. During the operational phase, comprehensive military training and the inclusion of disability-specific policies, systematic inclusion and dedicated budgets for adaptations are necessary.

In the ensuing discussion, it was commented that most of the problems posed in the presentation relate to persons who want to be identified, but are not because of their disabilities; however, in military operations, there is often a need to find people who do not want to be identified. The presentation aimed to shift away from threat detection (discussed on the first conference day) and focus on biometrics for the protection of the civilian population. A socialisation process has to take place. We have to see the diversity within our population. On the military side, the personnel using the systems must have a grasp of the data/assumptions underlying the system. It was submitted that we have to engage with the complexity and not consider it as something magical.

2.3 Military in Security Operations and Biometrics under the European Union AI Act

The final presentation in the panel was titled *Military in Security Operations and Biometrics under the European Union AI Act* and was given by **Rigmor Argren (Örebro University)**. She explained that the EU AI Act promotes AI adoption while addressing its risks, categorising them into unacceptable, high, limited, and minimal. It excludes AI used exclusively for military, defence or national security purposes. In military security operations, AI and biometrics play crucial roles but present challenges. The Act imposes strict regulations on high-risk AI, including biometric identification used in law enforcement. Military operations may support law enforcement, requiring states to strike a balance between International Human Rights Law and IHL. Argren noted that the use of remote biometric identification, without the knowledge of the persons involved, raises privacy concerns. The EU AI Act aims to ensure technological advancement while protecting human rights, potentially setting global standards akin to the GDPR. Comprehensive strategies are needed to manage AI deployment across both civilian and military contexts.

The AI Act is the first attempt to regulate AI for the private sector. It does not apply to AI systems exclusively used for military, defence or national security purposes. During the discussion, the question was raised about how ‘military’ should be defined in this context. For instance, many military security operations are carried out by gendarmerie forces who are both military and law enforcement. Then there is the issue of many systems not being developed by the military, but by the private sector. Should states be involved in making AI exclusively for military purposes? Further in the discussion, the legal similarity with the GDPR was also raised.

2.4 Handbook on Data Protection in Armed Conflict – Stakeholder Consultation (Aleksi Kajander)

The final presentation of the conference was given by **Aleksi Kajander (CCDCOE)**. He shared the information that the NATO CCD COE is working on a Handbook on Data Protection in Armed Conflict. The CCDCOE already publishes a book, *The Rights to Privacy and Data Protection in Times of Armed Conflict*, but the Handbook will ‘translate’ this more theoretical work into a practical handbook. It aims to provide a guide for practitioners with a traffic light principle (red, orange, green) to designate geographical areas in which the right to data protection is more or less restricted depending on the intensity/military relevance of the armed conflict in that area. The main part of this presentation was on gathering input for improving the Handbook.

This feedback was put forward in the discussion. It was suggested that the traffic light system might provide an interesting framework for all human rights obligations, and it thus would not need to be restricted to data protection. Some further considerations for the authors were also raised, including how to deal with operations that are not territorially bound (cyber) or extraterritorial operations.

2.5 Closing

Prof. **Marten Zwanenburg** and **Sebastian Cymutta** made their closing remarks and used the opportunity to gather input for a possible follow-up conference.