



CCDCOE

NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Report on the Conference on the Law Applicable to the Use of Biometrics by Armed Forces in Tallinn, 23-24 October

Aleksi Kajander, Marten Zwanenburg, Natalia Myshina

NATO Cooperative Cyber Defence Centre of Excellence

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 military, government, academia, and industry, 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 gives 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 information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication.

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

1. Table of Contents

1.	Table of Contents.....	3
2.	Introduction	5
3.	Day 1, 23rd of October 2025	6
3.1	Opening Remarks	6
3.2	Keynote: Military Use of AI-Supported Biometrics: Some Legal Issues (Professor Marten Zwanenburg, University of Amsterdam, Netherlands Defence Academy).....	7
3.3	Panel 1: Regional Approaches to the Military Use of Biometrics.....	8
3.3.1	Data Protection in military counter terrorism operations in Nigeria: a review of legal responses (Dr. Uchenna Orji, African Center for Cyber Law and Cybercrime Prevention)	8
3.3.2	India’s Approach to the Use of Biometrics in Military Operations (Dr. Harsha Rajwanshi, Gujarat National Law University and Commander Mahavir Arya, Indian Navy; and Masoom Sanyal, Gujarat National Law University)	9
3.3.3	The Turkish Gendarmerie’s Use of Biometrics and the Support Provided to the Army in the use of Biometrics for Border Control, Identification of Illegal Immigrants and Foreign Fighters (Colonel Özgür Ecevit Taşci, Deputy Director, NATO Stability Policing Centre of Excellence) ...	10
3.3.4	Discussion.....	10
3.4	Keynote on the Operational Use of Biometrics in a NATO Context (Mr. Sam Henze, NATO HQ) testing testing testing.....	11
3.5	Biometrics and Border Control: Insights from eu-LISA (Dr. Javier Galbally, R&I team, eu-LISA)	12
3.6	Cooperation in the Use of Biometrics in the context of the Armed Forces (Mr. Willem Bochmann, Netherlands Ministry of Defense)	13
3.7	Panel 2: The Use of Biometrics and the Private Sector.....	14
3.7.1	Biometric Bodies in armed Conflict: Private Sector Influence and the Boundaries of IHL (Dr. Anna Greipl, Geneva Academy of International Humanitarian Law and Human Rights, and Dr. Jonathan Andrew, Pufendorf Institute)	14
3.7.2	Human Rights by Design and by Contract: Embedding Legal Safeguards into the Development and Procurement of Dual-Use Biometric Technologies (Mr. Rok Bizjak, Legal Advisor for the Slovenian Ministry of Defense and PhD Candidate)	15
3.7.3	Emotional Surveillance in Security Action: Dissecting the IHRL-IHL Biometric Compliance Conundrum (Dr. Paolo Levantino, Sant’Anna School of Advanced Studies, Pisa)	16
3.7.4	Discussion.....	17
4.	Day 2, 24 th of October 2025.....	18

4.1	Panel 3: Biometrics in Criminal Accountability Processes	18
4.1.1	Biometrics as Battlefield Evidence (Professor Joris van Wijk, Vrije Universiteit Amsterdam) 18	
4.1.2	The use of Biometrics during Investigations and Biometric Data as Evidence in (Domestic) War Crimes Trials (Dr. Karolina Aksamitowska, Tallinn University)	18
4.1.3	The Use of Biometrics during Investigations and Biometric Data as Evidence in (International) War Crime Trials (Dr. Rogier Bartels, International Criminal Court)	19
4.1.4	Discussion.....	20
4.2	Human Rights During an Armed Conflict: The Right to Privacy (Dr. Aleksi Kajander, NATO CCDCOE).....	21
4.3	Closing	21

2. Introduction

On 23-24 October 2025, the the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), together with the War Studies Research Centre (WSRC) of the Netherlands Defence Academy (NLDA) and the Amsterdam Center for International Law (ACIL) of the University of Amsterdam organised a conference on the law applicable to the use of biometrics by armed forces. This conference, held at CR14 in Tallinn, followed and built on the conferences that took place on the 25th of May 2023 in Amsterdam and 7-8 May 2024 in Tallinn on the same topic. 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.

3. Day 1, 23rd of October 2025

3.1 Opening Remarks

The conference was opened by Mr. Christoph Kühn, the deputy director of the CCDCOE. He emphasised the importance of fostering discussions on the intersection of technology, security, and law. He noted the growing reliance on identity verification and authentication technologies in both civilian and military applications, which inevitably results in a convergence between cybersecurity and biometrics.

Mr. Kühn highlighted the importance of the secure and responsible use of biometric data by armed forces through not only technological solutions, but a clear legal and ethical framework that provides effective oversight. Furthermore, he emphasized the role of the CCDCOE as a platform for multidisciplinary cooperation committed to the bridging of technical and legal expertise. Conferences represent an important step in bringing academics and practitioners from the armed forces together and strengthening co-operation to address the challenges posed by emerging technologies.

Before concluding his opening words, the Deputy Director thanked the organizing committee, the War Studies Research Centre of the Netherlands Defence Academy and the Amsterdam Center for International Law, and Professor Marten Zwanenburg in particular for his continued contributions in continuing the series of biometrics conferences.

Professor Zwanenburg opened his remarks with a welcome to the participants in the third iteration of the Conference on the Use of Biometrics by Armed Forces, a series of conferences that began in Amsterdam in 2023 and moved to Tallinn in 2024. In addition, he expressed his gratitude to the NATO CCDCOE for hosting and supporting the event, which continues to grow an international community of experts on the topic.

Looking back, he recalled to the audience the idea behind the conferences, which originated from informal professional exchanges between researchers and military legal advisors on the increasing role of biometric technologies in an operational role. The conference provides a focused lens that allows the broader legal and ethical issues linked to the use of data and biometrics to be examined and discussed.

Moreover, Professor Zwanenburg highlighted the three key aims for the 2025 edition of the conference:

1. Highlighting some under-researched aspects of the topic, such as the role of the private sector, accountability processes, and non-European regional perspectives.
2. Further pursuing the discussions on the legal implications of biometrics in the context of military operations, especially in regard to data protection, international human rights law (IHRL) including the right to privacy, and International Humanitarian Law (IHL).
3. Fostering collaboration and co-operation among the interdisciplinary community of interest of practitioners, researchers, and technical experts that has formed over the successive iterations of the conference.

Professor Zwanenburg emphasized that the use biometrics may contribute to improving military effectiveness and situational awareness. However, its use also raises concerns in regard to compliance

with international law. To this end, he encouraged all participants to critically reflect on how existing legal frameworks, especially IHL and IHRL, must evolve to remain effective and meaningful amongst emerging technologies.

Moreover, the importance of the conference as a platform for knowledge exchange and cooperation, such as the sharing of national best practices, lessons learned, and policy approaches, was highlighted by Professor Zwanenburg. In this vein, he encouraged the active participation of the attendees in the discussions and to engage beyond disciplinary and institutional boundaries. Finally, Professor Zwanenburg announced that selected papers from the conference would be developed for publication in the *Military Law and the Law of War Review*.

3.2 Keynote: Military Use of AI-Supported Biometrics: Some Legal Issues (Professor Marten Zwanenburg, University of Amsterdam, Netherlands Defence Academy)

Professor Zwanenburg started his keynote presentation by pointing out that traditional biometric systems suffer from certain weaknesses, some relating to the biometric system itself and some to environmental factors. The introduction of AI to biometric systems can help address these limitations: AI can make biometric systems faster, more accurate, robust and reliable. One significant contribution is that AI enables 'multimodal biometrics', i.e. biometric systems that make use of more than one biometric characteristic.

He pointed out however that the introduction of AI also introduces new risks and vulnerabilities. Some of these have to do with risks of AI itself (such as inaccuracies flowing from poor data quality that the system is trained on) and some with the fact that the use of AI also opens up new vulnerabilities of biometric systems in the form of adversarial interference.

Professor Zwanenburg then turned to the legal framework that governs the military use of AI-supported biometrics. He noted that there are no international law instruments that specifically regulate the military use of biometrics, let alone AI-supported biometrics. The applicable legal framework primarily consists of the general rules from three regimes: IHL, IHRL and data protection law.

Professor Zwanenburg noted that the use of AI-supported biometrics raises various issues under these three legal regimes, at various stages of the 'biometrics process', from the planning stage to the sharing of biometric data with others. He went on to highlight some of these issues in the context of the planning for the use of biometric systems (including their development), the storage of biometric data and the matching of biometric data. With regard to the latter, by way of example, he noted that one issue is the accuracy and robustness of AI-supported systems. The accuracy and robustness of a system will depend on various factors, but they are often not as high in practice as advertised. Bias is another issue that is associated with the use of AI. Issues with the accuracy and robustness of AI supported biometrics as well as the existence of bias risk violation of IHRL, in particular the right to privacy and the prohibition of discrimination. These issues may also lead to violations of IHL.

Professor Zwanenburg concluded his presentation by underlining that AI-supported biometrics offers important advantages, but that the applicable legal regimes pose various issues at different steps in the

biometric process that require attention from the development to the use of such biometric systems. For the most part, it seems the use of AI amplifies existing issues rather than introduce new ones.

3.3 Panel 1: Regional Approaches to the Military Use of Biometrics

3.3.1 Data Protection in military counter terrorism operations in Nigeria: a review of legal responses (Dr. Uchenna Orji, African Center for Cyber Law and Cybercrime Prevention)

The panel on regional perspectives was opened by an in-depth look at Nigeria's evolving legal and institutional landscape relevant for the utilization of biometric data in military counter-terrorism operations by Professor Orji. The Nigerian experience with biometrics is characterized by prolonged insurgencies, cross-border terrorism, and internal security operations that are increasingly relying on digital and biometric technologies. Professor Orji noted that Nigeria has several programs to collect biometric data, including mandatory registration of telecommunication subscribers.

He highlighted the importance of the Nigerian Data Protection Act (2023) as a cornerstone of the country's data protection framework which consolidated earlier regulations issued by the National Information Technology Development Agency. However, he highlighted that military and intelligence institutions remain largely outside the scope of such civilian data protection obligations, creating a significant gap for national security operations.

Nevertheless, as highlighted by Professor Orji, the Nigerian Armed Forces and other associated security agencies utilize biometric tools for a variety of tasks such as terrorist identification, detainee management, and border control. Consequently, these operations occur under a fragmented legal order consisting of Cybercrime legislation (Cybercrime Act of 2015), terrorism legislation (Terrorism Prevention and Prohibition Act of 2022), and various defense regulations. Professor Orji raised concerns regarding accountability, transparency and proportionality in the handling of biometric data under such a fragmented framework. Furthermore, he highlighted that Nigerian law does not provide independent review or judicial authorization for military access to biometric databases, nor impose limits on data retention.

In the conclusion to his presentation, Professor Orji called for the establishment of human right safeguards to regulate the utilization of biometric data for national security by the armed forces. Moreover, he emphasized the need to align domestic frameworks with international Human Right standards. Furthermore, he suggested closer coordination between the authorities involved in counter-terrorism operations, data protection regulators, and civil society to ensure responsible rights-based governance of military biometrics.

3.3.2 India's Approach to the Use of Biometrics in Military Operations (Dr. Harsha Rajwanshi, Gujarat National Law University and Commander Mahavir Arya, Indian Navy; and Masoom Sanyal, Gujarat National Law University)

The Indian part of the panel provided an intriguing look at the management of the world's largest biometric database and the legislative framework that surrounds it. The speakers emphasized how India's experience illustrates the opportunities and the regulatory challenges associated with utilizing biometrics in a large, diverse, and security-sensitive environment.

Dr. Rajwanshi outlined the legal framework that surrounds the biometric database developed under the Aadhar (literally meaning 'Foundation' or 'Base') programme, that contains the data of 1.3 billion people, under the Aadhar Act, 2016. Under the Aadhar programme, a 12-digit random number is issued by the Unique Identification Authority of India (UIDAI) to residents of India after collecting their demographic and biometric data. The use of Aadhar data is legally restricted only to civilian and welfare uses, such as accessing government and financial services, and its use by the military or intelligence services is subject to separate authorization, on a case to case basis, under the Aadhar Act only for purposes of 'national security'.

Continuing from a military perspective, Commander Mahavir Arya explained that under the Criminal Procedure Identification Act of 2022, fingerprints, iris scans, and biological samples may be collected from convicted or detained persons. This in turn forms the basis for the counterterrorism and law enforcement databases that are managed by the National Crime Records Bureau (NCRB). Inter-agency intelligence sharing, including in the context of military operations, border security, and counterterrorism is enabled by combining the aforementioned databases with the national Automated Fingerprint Identification System.

In order to balance the needs of national security against privacy, the speakers highlighted the emerging role of the Digital Personal Data Protection Act of 2023, which introduces comprehensive privacy rights and state responsibilities for data processing. However, currently its implementing rules are yet to be issued, and therefore its impact will remain to be seen. Nevertheless, the new legislation echoes the constitutional standard set in *Puttaswamy vs Union of India* (2018) which recognized privacy as a fundamental right.

The speakers observed that India's approach reflects a gradual convergence of civilian data-protection principles and security-sector practices. Even with the military's use of biometric data remaining under stringent limits, there are indications that the emerging Indian trend has been towards developing more tailored databases and biometric tools, particularly for tasks related to verification, controlled access, and certain analytical functions connected to national security and law-enforcement. These efforts are accompanied by oversight from judicial and administrative bodies to ensure lawful, proportionate, and purpose-specific use.

In conclusion, the speakers highlighted the evolving nature of India's biometric governance that is currently under development in order to prevent misuse and reinforce public trust in the use of biometric technologies in national defense. In this regard, the speakers highlighted the importance of institutional transparency, inter-agency coordination, and clear accountability mechanisms as key enablers of a successful legal framework governing the use of biometrics in national defense.

3.3.3 The Turkish Gendarmerie's Use of Biometrics and the Support Provided to the Army in the use of Biometrics for Border Control, Identification of Illegal Immigrants and Foreign Fighters (Colonel Özgür Ecevit Taşci, Deputy Director, NATO Stability Policing Centre of Excellence)

Located between Europe and the Middle East, the unique perspective of Türkiye in regard to the use of biometrics in the context of law enforcement and military support operations was provided by Colonel Taşci. The presentation highlighted the integration of biometrics by the Turkish Gendarmerie to overcome challenges related to border management, counterterrorism, and the identification of illegal immigrants and foreign fighters.

The legal framework surrounding the use of biometrics underwent a significant reform as the use of biometric data by law enforcement and border agencies was authorized under judicial supervision. Nevertheless, challenges similar to those faced in other NATO states still remain, such as the absence of specific ratified military directives on the use of biometrics in the armed forces, which increases dependence on the cooperation between the Gendarmerie and the Army for practical implementation.

Colonel Taşci emphasized the crucial role played by biometrics in 'defeating anonymity' and enabling the identification of adversaries that attempt to blend in with the civilian population. He further highlighted how biometrics serve as a strategic enabler of the NATO Stability Policing doctrine that promotes the integration of policing functions into military operations to restore and maintain public order in post-conflict or crisis environments through reliable identity management, intelligence analysis, and interagency information sharing and coordination. In order to safeguard this use of biometrics, the Colonel underlined the importance of judicial oversight and standardized procedures to address issues of data retention, privacy, and proportionality.

Colonel Taşci stressed that the acquisition of certain law enforcement capabilities – primarily biometrics – by militaries will be crucial for the success of military operations. This implies the need for domestic legislation regulating the use of such capabilities. In this context, he noted that many states do not have such legislation in place. He compared the legislation of two states that do, Italy and Türkiye.

Colonel Taşci concluded his presentation by reiterating that the effective use of biometrics in military and law enforcement contexts requires not only technological capacity but also robust legal authority, clear accountability, and continuous training. He called for deeper cooperation within NATO to harmonize biometric policies, operational standards, and information-sharing mechanisms, ensuring that the deployment of these tools remains consistent with international law and human rights obligations.

3.3.4 Discussion

As highlighted by the speakers in the panel, the use of biometrics is an essential component of modern military operations. Nevertheless, the legal framework has not yet caught up with the new operational realities and challenges posed by the widespread use of biometrics.

Several participants in their questions and comments brought up the risk that without clear legal mandates, the armed forces risk operating in a grey zone between the prerogatives of national security and human rights such as privacy. The presentation by Colonel Taşci prompted particular interest in

how NATO member states can align domestic frameworks with alliance-wide standards, ensuring consistent application of biometric technologies in joint operations.

Moreover, the reliance on the private sector, often foreign rather than domestic companies, for the technologies, and their development was raised by the audience. In order to meet this reality, contractual safeguards, ethical procurement policies, and export control mechanisms are necessary to combat misuse or unauthorized transfer of data and dual-use technologies. Furthermore, on the topic of cross-border transfer of data as well as data retention, the participants stressed the need for mutual legal assistance frameworks and standardized data governance protocols to facilitate cooperation in counterterrorism and combating hybrid threats, while safeguarding personal data.

The debate concluded with a recognition that, despite contextual differences, the experiences of Nigeria, India, and Türkiye collectively demonstrate an ongoing global shift toward integrating biometrics into national security architectures. However, achieving a responsible balance between security efficiency and rights protection requires not only advanced technology but also legislative clarity, independent oversight, and regional cooperation.

3.4 Keynote on the Operational Use of Biometrics in a NATO Context (Mr. Sam Henze, NATO HQ)

Mr. Henze's presentation provided an overview of NATO's evolving policy guiding the use of biometrics, and the legal and ethical considerations that accompany their use in multinational operations. The use of biometrics has long been proven to be invaluable in an operational context, as demonstrated by previous operations. As a result, NATO is focused on developing a biometric capability that provides both operational efficiency and adherence to international law.

Mr. Henze underlined two key premises in his presentation. First, without an adequate legal framework NATO forces cannot use biometrics. Second, there is a need to know how forces want to use biometrics. It is important to acknowledge that many ideas on the latter are based on how NATO used to conduct military operations in the last decades, namely primarily in the context of counterterrorism. However, the situation is different now, with NATO preparing for possible large-scale combat operations in defence of NATO territory itself. This is a totally different context for the use of biometrics and raises the question whether the existing legal framework is fit for purpose.

Starting from a description of the different steps in the 'biometric process', Mr. Henze pointed out that some nations' forces are allowed to undertake activities in one step but not in another. He also underlined that different legal issues arise at different steps depending on what a force wishes to use biometrics for, which he referred to as 'modularity'.

Mr. Henze explained that NATO itself does not have an overarching database with biometric data. It is not NATO itself but NATO member states that have certain capabilities. NATO does however have a biometrics program, that aims to create the conditions for biometrics to operate. The program promotes capability development by NATO member states, and encourages them to learn from each other's experience and for the more capable to help the less capable. NATO also develops doctrine to support

the use of biometrics. A new version of the relevant document is currently pending ratification by NATO member states.

The presentation provided a reminder that biometric data is a sensitive form of personal information, the misuse of which could undermine public trust and operational legitimacy. Therefore, Mr. Henze emphasized the importance of secure data exchanges, resilience against cyber threats and interoperability when it comes to biometrical data. Moreover, he highlighted the importance of NATO's Centres of Excellence, such as the CCDCOE and the Stability Policing Centre of Excellence (SP COE) in conducting research and training on the legal and operational aspects of biometric technologies.

In his conclusion, Mr. Henze emphasized that NATO views biometrics as a strategic and cross-cutting capability essential to modern defence and deterrence. However, he cautioned that technological advancement should remain firmly anchored in the rule of law, data protection, and ethical governance. NATO's challenge, he noted, is to ensure that the use of biometrics enhances security while preserving the fundamental rights and democratic values that define NATO.

3.5 Biometrics and Border Control: Insights from eu-LISA (Dr. Javier Galbally, R&I team, eu-LISA)

Dr. Galbally began by outlining eu-LISA's operational mandate. eu-LISA provides Information Technology (IT) services to EU Member States so that they can share identity-related data of third country nationals within the Schengen Area. eu-LISA implements this service through a series of central large-scale IT systems. This includes the management of key biometric databases such as the Schengen Information System (SIS II), the Visa Information System (VIS), Eurodac, and the new Entry/Exit System (EES).

He explained that eu-LISA operates in three main domains: border management and migration, internal security and law enforcement and justice cooperation. In all those three domains, the key two objectives of the services provided by eu-LISA to MS are: increasing security and travel facilitation within the Schengen Area.

The large scale IT systems managed by eu-LISA collectively enable the identification, registration, and verification of individuals crossing external EU borders. The introduction of the interoperability architecture which links, when allowed by the regulation, the biometric and biographic databases managed by the Agency, marks a major step in improving the EU's capacity to detect identity fraud, monitor irregular migration, and strengthen the security of the Schengen Area.

He explained that the new interoperability framework, integrates the main component processing biometric data, the shared Biometric Matching Service (sBMS), which provides fingerprint and facial recognition capabilities across EU large-scale IT systems. This interoperable approach to managing the systems, compared to the previous "siloes-based" strategy, allows for more accurate identity checks while reducing duplication and inconsistencies between databases. Importantly, Dr. Galbally stressed that this integration is accompanied by robust data protection safeguards, including strict access control, purpose limitation, and independent oversight by the European Data Protection Supervisor (EDPS) and national authorities.

Dr. Galbally discussed some challenges in the use of biometrics, including issues related to biometric accuracy as well as data quality. He emphasized the possibility of drawing best practices from civilian border management practices for the use of biometric technology within the armed forces. In this regard, eu-LISA's safeguards for privacy protection, data governance, and interoperability could inspire regulations and practices for military operations that increasingly rely on biometric technologies. In this vein, he suggested that future cooperation between civilian and defense actors between the EU and NATO could provide more secure, ethical and technology resilient frameworks in the use of biometrics.

3.6 Cooperation in the Use of Biometrics in the context of the Armed Forces (Mr. Willem Bochmann, Netherlands Ministry of Defense)

Mr. Bochmann's presentation outlined recent policy developments that address the practical and legal challenges related to data protection in a military context. In particular, his presentation emphasized the need for clear(er) cross-border data sharing frameworks, and standardized accountability mechanisms to ensure that personal and operational data is handled lawfully and securely during multinational operations.

He started his presentation with a hypothetical scenario, which highlighted questions and concerns that arise in the context of the sharing of data between armed forces. He noted that dealing with data protection in the military field is relatively new and poses novel legal challenges. This has led to internal discussions in national ministries of Defence as well as in NATO. These discussions have foregrounded staff and management concerns. They involve issues concerning not just data protection (law) including the EU General Data Protection Regulation (GDPR) and the Organisation for Security and Cooperation in Europe (OSCE) Convention 108+, but also human and fundamental rights. He referred to an initiative by Belgium, Denmark, Germany and the Netherlands to start an international conversation on military data protection.

Concerning the applicability of specific legal regimes to military data, he noted that there are questions around the scope of EU law and applicability of EU rules to the military. There is no doubt however that Convention 108+ is applicable. He pointed out that the implementation of data protection law differs per EU country.

Mr. Bochmann highlighted that while national defense activities are largely outside of the scope of the GDPR, the principles therein are increasingly influencing policies within the armed forces. As an example, he provided the Dutch approach of adopting a 'GDPR-aligned' data protection framework that incorporates privacy by design, data minimization, and independent oversight to defense systems and procurement. In this vein, he noted that the Dutch Ministry of Defense has also introduced Data Protection Impact Assessments and internal privacy governance mechanisms to ensure compliance from the earliest stages of capability development. This proactive approach is intended to implement privacy by design as a standard practice in military systems and technology procurement.

Mr. Bochmann then turned to identified challenges and main take-aways. In this context, he reiterated that military personal data protection is a relatively new, scarcely dealt with field. There are no formalized common understandings, principles or rules yet. Moreover, knowledge about relevant legislation in

different nation deserves attention, and there is legal uncertainty about, and large gaps between, domestic legislation. Against this background, work is being done toward a common Data Protection Framework within NATO and EU to ensure equality in legislation and legal interoperability.

The final part of Mr. Bochmann's presentation concerned the way ahead. In this regard, the NATO data protection working group has an important role to play. It is also important to standardize data protection clauses in international agreements and arrangements. Finally, bi- and multinational arrangements on the (joint) processing of Personal Data can provide more clarity.

3.7 Panel 2: The Use of Biometrics and the Private Sector

3.7.1 Biometric Bodies in armed Conflict: Private Sector Influence and the Boundaries of IHL (Dr. Anna Greipl, Geneva Academy of International Humanitarian Law and Human Rights, and Dr. Jonathan Andrew, Pufendorf Institute)

Dr. Greipl began the presentation by drawing attention to the increasing role of the private sector in the development and design of biometric technologies used by the armed forces. More specifically, she emphasized that, in this context, ensuring military biometric systems comply with IHL must begin at the earliest stage of their lifecycle, during procurement, rather than relying on investigations after deployment.

She shows how 'non-weapon' technologies, such as biometric identification tools, directly influence legally relevant military decisions through the design choices of private actors. Traditional IHL oversight has centered on regulating the development and acquisition of weapon systems or left it to post-conflict accountability. As a result, a narrow, weapon-focused approach risks overlooking how ostensibly "neutral" systems, such as biometrics, can shape conduct during hostilities.

Overall, she highlighted that today's defense landscape is dominated by private companies that develop and supply not only weapons but also the enabling technologies around them. Because these firms exercise significant influence through design choices, procurement contracts represent a critical opportunity to embed IHL safeguards and to assign accountability to suppliers before systems enter operational use. This shift toward proactive, procurement-based compliance offers meaningful advantages for early risk mitigation, while also raising practical challenges that her co-presenter then addresses.

Continuing the presentation, Dr. Jonathan Andrew shared case studies which demonstrated how private companies often act as *de facto* custodians of sensitive biometric data, in regard to both the technological infrastructure and the analytical processes. This in turn raises questions about whether existing IHL obligations can be meaningfully applied when decision chains include private actors.

In order to address these concerns, procurement practices must be strengthened to bridge both IHL and human rights compliance, through a broader review mechanism that takes into account human rights obligations. He discussed certain practical limitations in applying human rights compliance. These include that law enforcement and military procurement of systems that integrate biometrics frequently encounter substantial structural impediments to human rights safeguarding; that temporal pressures

intensify these challenges; and that the opacity and complexity of supply chains further renders complete oversight and traceability especially difficult, potentially enabling procurement of problematic systems despite human rights due diligence.

He then turned to some institutional challenges to enabling human rights impact assessments (HRIA). In particular, the fact that procurement teams require specialized personnel trained in human rights due diligence methodologies; that ongoing instruction, resourcing, and institutional expertise is required: that information asymmetries between procuring entities and contractors create difficulties in assessing and monitoring human rights compliance in procurement of biometrics; that existing frameworks for conducting human rights impact assessments often provide insufficient clarity on the scope of responsibilities to review complex scenarios in which human rights infringements may manifest; and that horizon-scanning and scenario planning require investment of resources to develop credible frameworks for modelling potentialities in the development and deployment of biometrics.

Dr. Andrew then provided a number of specific examples of challenges in conducting HRIA. He concluded his presentation with a number of recommendations, while acknowledging potential resource limitations may impact these. Specific recommendations were:

1. Continuously update human rights training, ensuring that broader knowledge, contextual background and diverse information sources are made accessible during HRIAs and other evaluation processes.
2. Implement risk-tiered processes, proportionate to sensitivity, to optimize resource allocation so as not to compromise the scrutiny of high-risk systems.
3. Specialized training programmes should be institutionalized to develop capacity for identifying human rights risk indicators/metrics to better enable further evaluations.
4. Engage multilateral institutions to encourage international cooperation to develop more consistent approaches in research on human rights protection in the context of evolving biometric capabilities.
5. Procurement performance metrics must explicitly integrate human rights compliance indicators, ensuring accountability extends beyond traditional measures.

3.7.2 Human Rights by Design and by Contract: Embedding Legal Safeguards into the Development and Procurement of Dual-Use Biometric Technologies (Mr. Rok Bizjak, Legal Advisor for the Slovenian Ministry of Defense and PhD Candidate)

Mr. Bizjak's presentation provided a closer look at how contractual arrangements in military procurement can be utilized to ensure compliance with human rights in the context of biometric technologies. He noted how biometric systems serve both civilian and defense applications, which adds ethical, legal and security challenges owing to its dual-use character. As a solution, Mr. Bizjak suggests the use of "Human Rights by Design" as an approach to ensure respect for privacy, dignity, and proportionality.

Under the "Human Rights by Design" approach legal and ethical impact assessments are incorporated into the early stages of capability development. Safeguards such as data minimization, auditability, user access controls, and bias mitigation should be included in the technical specification of the system.

Moreover, continuous testing and verification of algorithmic fairness and accuracy should be used to complement the approach.

Secondly, Mr. Bizjak proposed integration of human rights by contract. More specifically, requiring contractors through contractual means to comply with relevant legal obligations, stemming from IHL, IHRL, and other relevant national law. Furthermore, the opacity associated with commercial biometric systems should similarly be remedied through contractual provisions that require transparency on the algorithm design, data handling, and subcontracting chains.

He also highlighted the role of EU-level initiatives, including the EU Artificial Intelligence Act, the Coordinated Plan on AI, and the European Defence Fund's ethical review requirements, which collectively encourage Member States to adopt "responsible innovation" frameworks. These initiatives, he argued, can guide defence ministries in aligning procurement practices with democratic values while maintaining strategic autonomy.

3.7.3 Emotional Surveillance in Security Action: Dissecting the IHRL-IHL Biometric Compliance Conundrum (Dr. Paolo Levantino, Sant'Anna School of Advanced Studies, Pisa)

Dr. Levantino delivered a presentation that focused on the emergence of emotional surveillance technologies and the implications of their use in a military context. Emotion recognition technologies (ERT) detect, record, and analyze human emotions or intentions through biometric and behavioral data. Emotional surveillance therefore exploits a variety of biometric features and other input data such as heart-rate, voice modulation, and facial micro-expressions to determine, interpret, or infer emotional states or intentions of natural persons. This in turn intrudes on what he referred to as the "last private frontier of the human being" by delving not only into the external characteristics, but rather the inner emotional and cognitive conditions of a person.

While the deployment of such technologies in the military domain may offer opportunities to ensure better adherence to basic rules of IHL (e.g., distinction) in complex operational environments (OEs), such deployments also generate a "compliance conundrum" between IHL and IHRL as both regimes may be applicable and provide relevant rules. In this sense, applying both IHL and IHRL in this context leads to ambiguity, especially in the context of counterterrorism or the countering of hybrid threats. In particular, considering the definitional and regulatory inconsistencies characterizing the only legal framework currently addressing the processing of data by ERT that, although not directly applying in military contexts, nevertheless offers some guidance in this respect (i.e., the EU AI Act), identifying what is the law applicable to the processing of such data through ERT by armed forces becomes an even more complex task.

In order to address these challenges, Dr. Levantino proposes a multi-layered framework mindful of the disputed scientific theories used as a basis for the development of such tools, data protection considerations, and context-dependent assessments on the concurrent application of IHL and IHRL in any given OE. Finally, Dr. Levantino reminded that emotional surveillance should be recognized as a high-risk and exceptional capability, the use of which needs to be justified based on military necessity and accompanied by robust safeguards. In his concluding remarks, Dr. Levantino cautioned that the

rise of emotional biometrics signals a paradigm shift from surveillance of bodies to surveillance of cognitive life, and the applicable legal frameworks must adjust to meet this change.

3.7.4 Discussion

A key theme emerging from the discussion was the accountability gap created by the widespread outsourcing of biometric and artificial intelligence (AI) systems to private contractors. Several participants observed that private companies now design and maintain many of the data-processing and identity-verification systems employed in military operations, often beyond the scope of direct governmental or judicial oversight. Questions were raised about how state responsibility under international law interacts with corporate accountability, particularly when private entities collect or analyze biometric data in conflict zones.

Referring to Dr. Greipl's and Dr. Andrew's presentation, participants highlighted that violations of international law could occur through contractual relationships with private contractors rather than through direct state action. Participants agreed that clarifying attribution and liability standards for private biometric activities under IHL IHRL should become a policy priority.

Inspired by Mr. Bizjak's presentation, further discussions focused on how procurement frameworks could be adapted to include enforceable human rights clauses, independent audits, and transparency obligations when handling biometric data. Several attendees stressed that such mechanisms would enhance operational legitimacy and public trust, particularly in dual-use projects where military and civilian applications overlap.

Furthermore, the emerging risks related to emotional surveillance generated comments and discussion from the audience. Participants echoed Dr. Levantino's sentiment that these technologies represent a unprecedented challenge for privacy, autonomy, and human dignity as they intrude upon the cognitive state of a person. Agreeing with Dr. Levantino, participants concurred that emotional surveillance is a high risk technology that should be utilized with strict legal and ethical oversight. The discussion reaffirmed that private-sector engagement in defence biometrics is both inevitable and indispensable, but it must be accompanied by a corresponding evolution in legal doctrine, procurement practice, and institutional ethics.

4. Day 2, 24th of October 2025

4.1 Panel 3: Biometrics in Criminal Accountability Processes

4.1.1 Biometrics as Battlefield Evidence (Professor Joris van Wijk, Vrije Universiteit Amsterdam)

Professor van Wijk's presentation highlighted the growing importance of biometrics when it comes to battlefield evidence. With advances in biometric and sensory technologies the evidentiary toolkit available to investigators has significantly increased. However, the use of such technologies has raised issues in regard to the authenticity, chain of custody and procedural safeguards associated with the evidence.

As noted by Professor van Wijk, modern conflicts generate a significant amount of biometric data and digital traces, which while initially collected for operational purposes may later be repurposed for judicial proceedings. An example of this is the use of biometric registries, originally for counterterrorism or border security later being used to verify the identity of detainees, victims, or witnesses in a post-conflict setting.

This transfer of operational data to admissible evidence is wrought with technical, legal, and ethical challenges. The absence of standardized protocols for data authentication, retention and verification may all undermine the evidentiary value of such material in court. Furthermore, questions of jurisdiction, consent and legality of collection of the evidence may occur when the evidence is collected by military personnel rather than law enforcement authorities. These concerns became even more pronounced when evidence is obtained through coalition or intelligence-sharing announcement from other jurisdictions with differing national laws and procedures.

In order to remedy these concerns, Professor van Wijk proposed clear international standards for the collection, preservation, and biometric battlefield evidence based on existing best practices in forensics. In addition, the training of military personnel in correctly collecting and documenting evidence is crucial in order to ensure judicial admissibility later. He underlined that gendarmerie-type forces may play an important role. These forces, such as the Royal Netherlands Marechaussee in the Netherlands, occupy a dual institutional position with a civilian and military mandate. This potentially gives them an important 'bridging' function.

4.1.2 The use of Biometrics during Investigations and Biometric Data as Evidence in (Domestic) War Crimes Trials (Dr. Karolina Aksamitowska, Tallinn University)

Dr. Aksamitowska continued conveying the importance of biometric evidence in modern war crimes trials in her presentation. She demonstrated this by reference to case law originating from the post-Syrian conflict era where courts in European states began to process war crimes committed abroad under universal jurisdiction. Moreover, following Russia's full-scale invasion of Ukraine in 2022, the collection and authentication of digital and biometric evidence intensified both domestically and with international partners.

She emphasized the crucial role of migration authorities in verifying the identity of potential suspects, victims and witnesses. The co-operation between war crimes prosecutors and migration authorities has proven essential as the latter are often the first to detect potential perpetrators or witnesses, whereby it is crucial that they transfer that information to the prosecutors.

In order to demonstrate these prosecutions in practice, Dr. Aksamitowska presented cases where biometric and digital evidence were crucial in obtaining a conviction. Evidence used in these cases included facial recognition and voice comparison to credibly establish the identity of the suspect in, for example, execution videos. Here too, the role of the private sector is pronounced as often national forensic institutes collaborate with the private-sector technology providers to authenticate evidence.

Dr. Aksamitowska also discussed the establishment of cooperative mechanisms such as the EU Analysis Project on Core International Crimes, Europol's Siena information system, and the Joint Investigation Teams (JITs), which facilitate secure information-sharing between national prosecutors. She explained that this networked approach enables domestic courts to use biometric and digital evidence gathered in multiple jurisdictions while maintaining the chain of custody and ownership of data.

In examining the Ukrainian context, she noted that Eurojust and national war crimes units are assisting Ukraine's Prosecutor General in integrating digital evidence, such as imagery, satellite data, and forensic samples, into domestic proceedings. While international support has accelerated evidence collection, she cautioned that foreign-gathered biometric data is not always admissible under Ukrainian law, underscoring the importance of developing harmonized standards across jurisdictions.

Dr. Aksamitowska concluded by identifying key legal and procedural opportunities and challenges in using biometric evidence domestically. First, technical capacity translates into operational opportunities. Second, evidentiary challenges. Third, issues surrounding technical accuracy of biometric systems and bias in AI-driven identification tools. Finally, a blurring may occur between migration protection and criminal justice. She stressed that domestic war crimes prosecutions must strike a balance between technological innovation and due process, ensuring that the use of biometrics enhances accountability without undermining fair-trial guarantees.

4.1.3 The Use of Biometrics during Investigations and Biometric Data as Evidence in (International) War Crime Trials (Dr. Rogier Bartels, International Criminal Court)

Dr. Bartels began by outlining the conceptual and institutional distinction between domestic and international use of biometric evidence. Whereas national courts often handle direct perpetrators and can rely on evidence gathered by domestic law enforcement agencies, international tribunals typically prosecute commanders and senior officials far removed from the crime scenes. Consequently, the types of biometric evidence available, and the standards for its collection and admissibility, differ substantially.

He explained that, despite advances in technology, the ICC's evidentiary framework remains largely traditional, relying on witness testimony, documentary evidence, and expert reports. The Rome Statute and Rules of Procedure and Evidence, which were drafted more than 25 years ago, at present do not contain specific provisions on biometric data, and admissibility is assessed under general criteria such as relevance, probative value, and absence of prejudice to the accused. Moreover, the ICC does not operate its own forensic or biometric laboratories and thus depends on state cooperation and partner organizations for evidence collection and verification.

As a result, there may be both legal and practical obstacles in presenting or relying on biometric evidence in ICC proceedings. Firstly, as with any evidence, the Court must verify that the evidence was lawfully obtained in accordance with applicable human rights standards (e.g., without coercion). Secondly, as many biometric datasets are created by non-judicial actors or in a conflict environment, their accuracy may be compromised or the chain of custody may be (partially) unknown. Thirdly, owing to its sensitivity, the use of biometric data must comply with strict confidentiality and data protection, especially when dealing with victims or witnesses.

He noted that biometric evidence, if improperly collected or verified, could undermine rather than enhance accountability efforts. For that reason, the ICC prioritizes multi-source corroboration, ensuring that biometric information is supported by other types of evidence before being introduced at trial. He suggested that as international courts adapt to the digital age, biometric data will increasingly be used as evidence, especially in contexts where physical witnesses or traditional forensic evidence are unavailable. Such data will also be used as a starting point to obtain other, more traditional evidence. Using facial recognition, for example, to identify persons who may act as witnesses.

The ICC's challenge, he observed, is to embrace technological innovation without compromising procedural integrity or the rights of the accused. Establishing standardized protocols for the collection, verification, and use of biometric data, potentially through joint international guidelines, would be a critical step toward ensuring consistent and ethical practice across international courts and tribunals.

4.1.4 Discussion

Several participants voiced their agreement with Dr. Bartels's observation that the Rome Statute and ICC Rules of Procedure and Evidence were drafted before the digital revolution and therefore lack specific provisions governing biometric evidence. As a result, the admissibility of such data is assessed case by case, often leading to procedural uncertainty and inconsistency.

On the topic of battlefield evidence, participants discussed that when evidence is collected in a combat environment or transferred between states, the maintaining of the integrity of the evidence becomes challenging. A number of speakers emphasized the need for standardized documentation and verification protocols to ensure that biometric evidence collected on the battlefield can be later used in judicial proceedings without compromising fairness or reliability.

In regard to the close cooperation between war crimes prosecutors and migration authorities, participants raised concerns about the potential misuse of asylum-related biometric data for prosecutorial purposes. In particular, participants noted that the distinction between administrative and criminal use of such data must remain clear to protect the rights of vulnerable individuals.

Participants discussed the legal implications of evidence obtained from private or non-judicial actors, emphasizing that international courts must verify the legality of data acquisition under both domestic and international law. Some suggested that international guidelines or a common evidentiary framework could help harmonize these practices across jurisdictions.

Furthermore, participants highlighted the risk that algorithmic bias, unreliable recognition software, or coercive data collection could undermine due process and fairness in criminal trials. Several attendees

argued that the introduction of biometric evidence must always be accompanied by expert testimony explaining its reliability, limitations, and margin of error.

4.2 Human Rights During an Armed Conflict: The Right to Privacy (Dr. Aleksi Kajander, NATO CCDCOE)

Dr. Kajander began his presentation by outlining the growing importance of human rights during armed conflicts by filling gaps left by IHL in the protection of civilians. In addition, he noted that as human rights are applicable during peacetime, while IHL is not, they have must be considered especially in the cases where the armed forces provide assistance to law enforcement or respond to internal disturbances below the threshold of an (non)international armed conflict.

Furthermore, he emphasized that while certain human rights are absolute and non-derogable, many rights including the right to privacy may be subject to lawful limitations ordinarily, as well as derogations during an emergency. His presentation highlighted the importance of providing practical guidelines to practitioners on how the derogations should be limited to what is strictly necessary during an armed conflict. He provided practical examples from the CCDCOE's upcoming Handbook on the Right to Privacy of factors a practitioner should consider, such as the extent and type of hostilities, effective control of territory, and the density of civilian populations in the area.

Continuing on the right to privacy, Dr. Kajander discussed how the right to privacy is increasingly at risk of being violated during military operations owing to the proliferation of biometric and other surveillance technologies. Furthermore, owing to time of their time of drafting, existing human rights instruments do not offer specific guidance on the use of such technologies whereby there is a risk of loopholes and grey zones forming that may compromise the right to privacy for civilians during armed conflicts.

Moreover, he emphasized the importance of preparing the domestic legal framework of a state before a conflict occurs by clarifying how and under which safeguards biometric data can be utilized during an armed conflict. As an example, he brought to the audience's attention the growing number of databases containing biometric data resulting from changes in domestic legislation, such as online age verification laws. Utilizing the recent data breach of 70 000 ID photos from such a database, he raised the issue of not only their cybersecurity, but also of whether the current domestic legislations have considered their potential use by the armed forces during an armed conflict. Consequently, he finished his presentation by emphasizing the importance of both preparation and raising awareness when it comes to human rights, and the privacy in particular during an armed conflict, even before a conflict arises.

4.3 Closing

Prof. Marten Zwanenburg and Dr. Aleksi Kajander made closing remarks and used the opportunity to invite participants to continue the conversation and to share their ideas for follow-up activities.