CTED Analytical Brief: Biometrics and Counter-Terrorism

United Nations Security Council
Counter-Terrorism Committee
Executive Directorate (CTED)

Photo Credit: iStock.com/ktsimage

BACKGROUND

The present Analytical Brief was prepared by CTED in accordance with Security Council resolution 2395 (2017), which directs CTED to conduct analytical work on emerging issues, trends, and developments and to make its analytical products available throughout the United Nations system.

CTED Analytical Briefs aim to provide the Security Council Counter-Terrorism Committee, United Nations agencies, and policymakers with a concise analysis of specific issues, trends, and developments, as identified through CTED's engagement with Member States on their implementation of the relevant Council resolutions. They also include relevant data gathered by CTED, including through engagement with its United Nations partners; international, regional, and subregional organizations; civil society organizations (CSOs); and members of the CTED Global Research Network (GRN).

INTRODUCTION

Biometrics are the use of a person's physical characteristics or personal traits to identify or verify the claimed identity of that individual.[1] These can include fingerprints, face, vein pattern, eye, iris print, DNA, blood, voice, gait, or signature.[2] Private entities and public authorities have increasingly used biometrics to validate and identify individuals, granting or restricting access to locations, services, or devices. Public sector users include law enforcement and security agencies, criminal justice, immigration, and social welfare processes (including to prevent identity fraud and theft) and the authentication of beneficiaries of humanitarian aid.[3]

Since the adoption of Security Council resolutions 2322 (2016) and 2396 (2017), the use of biometrics for counter-terrorism purposes – notably in the context of border management and security – has become increasingly widespread. Council resolution 2322 (2016) calls on Member States to share information about foreign terrorist fighters (FTFs) and other individual terrorists and terrorist organizations, including biometric and biographic information.

In its resolution 2396 (2017), the Council decides that States shall develop and implement systems to collect biometric data, which could include fingerprints, photographs, facial recognition, and other relevant identifying biometric data, in order to responsibly and properly identify terrorists, including FTFs, in compliance with domestic law and international human rights law. The Council also encourages Member States to share this data responsibly among relevant Member States and with relevant international bodies, including the International Criminal Police Organization (INTERPOL).

In promoting implementation of these resolutions by Member States, CTED has identified effective practices, issues, gaps, and challenges in their use of biometrics for counter-terrorism purposes. The present Analytical Brief will explore trends in the use of this technology in counter-terrorism, key challenges, and guidance developed to ensure that relevant stakeholders use the technology responsibly. The use of biometrics in counter-terrorism has been raised in the context of numerous assessment visits and desk assessment reviews conducted by CTED

[1] Woodward, J.D., Biometrics: Facing Up to Terrorism (2001).
[2] Biometrics Institute, What are biometrics?
[3] Zureik, E. and Hindle, K. Governance, Security and Technology: The Case Of Biometrics (2004).

on behalf of the Counter-Terrorism Committee. The following analysis represents key developments identified by CTED through its engagement with Member States and its interaction with CSOs (in particular the Biometrics Institute, in accordance with the Arrangement on Cooperation signed by the two entities).

KEY TRENDS

Biometrics in counter-terrorism

The rapidly expanding range of counter-terrorism-related applications for biometric systems includes authentication and verification equipment – e.g., biometric passports ("e-passports"), biometric smart gates, and passport readers – and digital forensics.[4]

The COVID-19 pandemic presented States with unique challenges regarding the use of biometrics to facilitate international travel, with the widespread use of masks and fear of transmitting the disease via touch limiting the effectiveness of established identification methods, including facial recognition and fingerprint scanners. As a result, many States have begun to introduce touchless devices and iris scanners that can verify identity even when masks are worn.[5]

Biometrics have become more prevalent in efforts to detect criminals, known terrorists, and individuals suspected of terrorist offences, including in public spaces, with facial recognition systems used in conjunction with CCTV video surveillance. Recognition technology has also been coupled with unmanned aircraft systems (UAS) in a law enforcement and border control context, helping to control large crowds and assist in the identification of individuals in public spaces (as identified in CTED's related Trends Alert).[6]

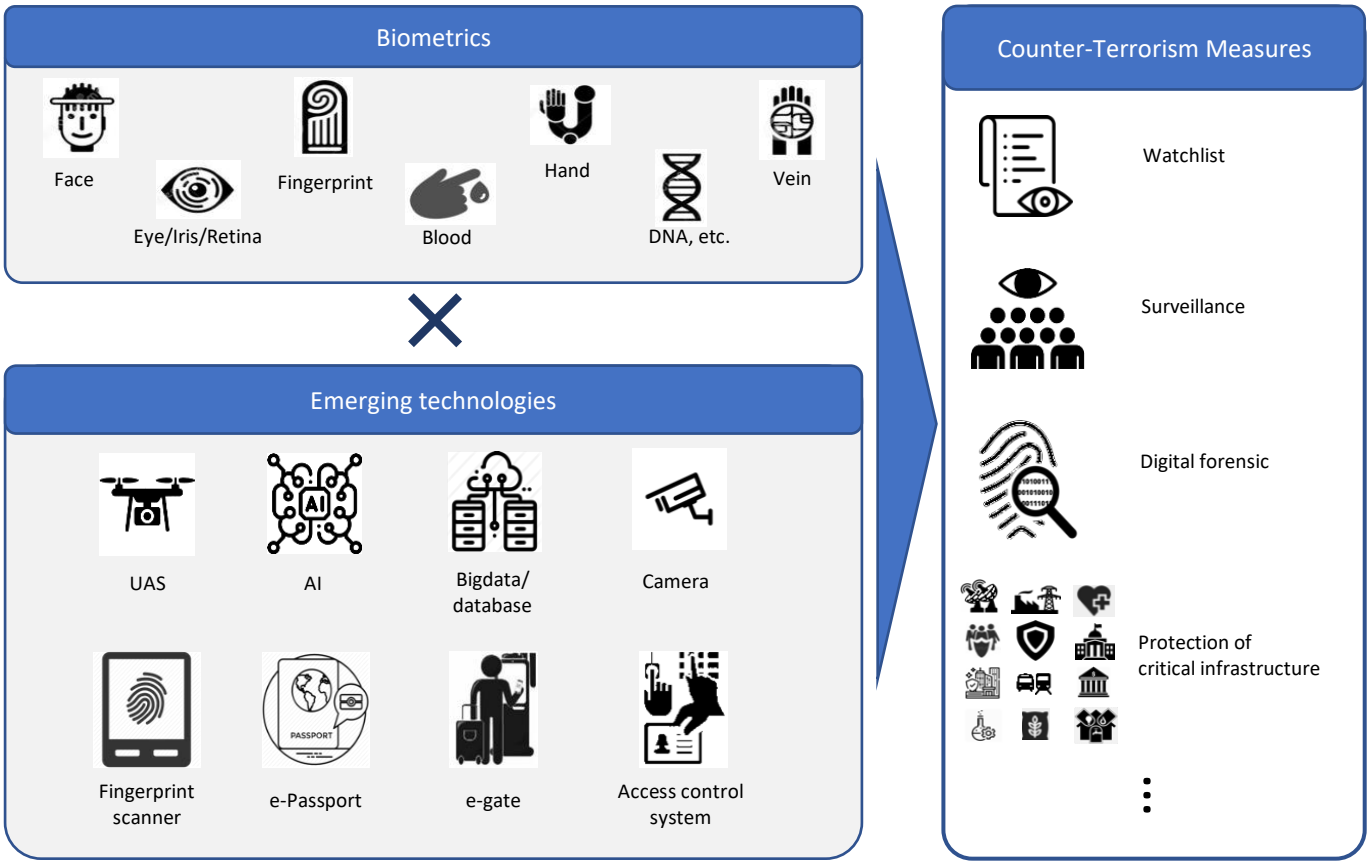
The use of biometrics in counter-terrorism is often connected to the development and utilization of emerging technologies. This has included techniques to identify individuals of interest – for example high-definition cameras, matching algorithms, and artificial intelligence (AI), sometimes in conjunction with a linked database (e.g., terrorist watchlists) – and the use of biometrics (including multi-biometrics access control systems) to protect critical infrastructure sites and facilities, as well as "soft" targets, from terrorist attacks.[7]

As noted in a recent Financial Action Task Force (FATF) report,[8] biometric technologies may also be increasingly helpful for countering the financing of terrorism, offering enhancements to know-your-client (KYC) and customer due diligence (CDD) processes and alternatives to financial institutions' monitoring of banking relationships.

---

[4] United Nations, United Nations Compendium of Recommended Practices for the Responsible Use & Sharing of Biometrics in Counter-Terrorism (2018).
[5] CTED, The impact of the COVID-19 pandemic on terrorism, counter-terrorism and countering violent extremism (2020).
[6] CTED, CTED Trends Alert: Greater Efforts Needed to Address the Potential Risks Posed by Terrorist Use of Unmanned Aircraft Systems (2019).
[7] Chaurasiaa,P., Yogarajaha, P., Condella, J., Prasada, G., McIlhattonb, D., and Monaghanc, R., Countering terrorism, protecting critical national infrastructure and infrastructure assets through the use of novel behavioral biometrics (2016).
[8] http://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf (June 2021). See also FATF Guidance on Digital ID.

Table 1: Trends in use of biometrics in counter-terrorism



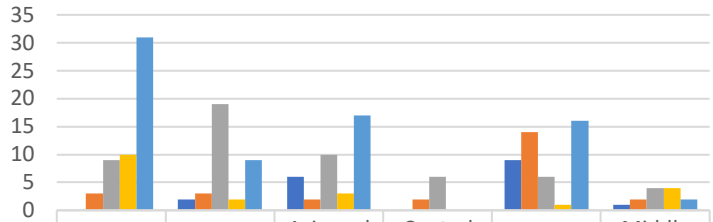
Member States' use of biometrics

CTED's dialogue with Member States, conducted on the Committee's behalf, has revealed that, although the extent of biometrics use and expertise varies significantly, 118 of the 193 United Nations Member States have made at least marginal progress in introducing biometrics for counter-terrorism purposes[9] *(see table 2, below).*

There are clear regional trends in this usage. Biometrics are widely used in nearly half of European Member States but only marginally introduced across the Middle East. More than half of African Member States have yet to introduce biometrics at all.

[9] On behalf of the Committee, CTED has provided all 193 United Nations Member States with its desk reviews on their implementation of the relevant Council resolutions (as of 18 November 2021).

Table 2: States using biometrics in counter-terrorism (as of 30 November 2021)



	Africa	Americas	Asia and Pacific	Central Asia	Europe	Middle East
Yes	0	2	6	0	9	1
Largely	3	3	2	2	14	2
Partially	9	19	10	6	6	4
Marginally	10	2	3	0	1	4
No/ Insufficient information	31	9	17	0	16	2

CTED's engagement with relevant stakeholders has identified the following trends in Member States' use of biometric technologies for counter-terrorism purposes:

- States are expanding the range of physical spaces (e.g., border crossing, public spaces, etc.) and digital spaces (e.g., social media) where they are validating biometric data.
- States are employing new and more sophisticated technologies to capture, collect, process, and analyse biometric data.
- A wider range of government officials (e.g., intelligence agencies, national and local police forces, border guards, immigration officers) and some private-sector actors (e.g., contractors) have been authorized to access biometric data.
- Some States have begun to accelerate the sharing of biometric data as part of counter-terrorism cooperation and information-sharing measures.
- States have increasingly developed terrorist watch lists and databases that link or cross-check with biometric databases, including by carrying out biometric checks against INTERPOL notices and databases in order to identify and detect criminals and terrorists.

CHALLENGES

CTED's analysis and engagement with relevant stakeholders has identified a range of challenges relating to the responsible use of biometric technologies in counter-terrorism. These include:

- Technological weakness and limitations
- Insufficient capacity
- Insufficient legal and administrative frameworks
- Insufficient oversight, safeguards, and protection of privacy and data, and the duration of data retention
- Reinforcement of existing discrimination and inequalities
- Potential misuse and challenges to protected freedoms of religion, expression, and association
- Limited sharing of biometric data and information

- Lack of effective remedies in case of violations
- Risk of fraud and abuse of biometric data

Although advances in biometric technology have significantly improved its accuracy and reliability, technological shortfalls can still negatively impact its effectiveness. Environmental factors – such as camera angle, lighting, and facial expression – can affect the operating conditions of biometric systems, thus potentially causing a false match (incorrectly matched to another person's template) or non-match (not matched to a correct template).[10] While best-in-market systems have overcome many of these issues, few States currently have access to such systems. Developing an expert user base can also help minimize these errors but delivering the necessary training often requires significant resources and expertise.

However, CTED's dialogue with Member States, including in the context of the Committee's country assessment visits, suggest that, although these technological capacity issues (including the cost of acquiring and running the systems) are not insignificant, they can and are being addressed. In contrast, more significant challenges relate to the development of governance, institutional, and legal and regulatory frameworks.

Such legal and regulatory frameworks – which must be developed prior to the implementation of biometric systems – are a critical pre-requisite for the effective and responsible use of biometrics at the national level.[11] Failure to introduce safeguards that prevent the abuse or misuse of biometric technologies and data (including violations of human rights) can also negatively impact international cooperation, potentially undermining regional and international counter-terrorism efforts.

CTED's analysis indicates that many States have faced significant human rights-related challenges in their use of biometric tools and their data-sharing protocols. These challenges have included inadequate privacy and data-protection frameworks under domestic law and lack of clear procedural safeguards for, and effective oversight of, the application of biometric technology.[12][13] In the absence of such frameworks, biometric technologies can pose threats to privacy and personal security, including through their use for broader purposes such as mass surveillance, which can facilitate profiling and discrimination, often against marginalized groups, including women, minorities and asylum seekers.

There are also growing concerns about racial discrimination in the design and use of these technologies, particularly when they are combined with other emerging digital technologies such as machine-learning and algorithms, which have been shown to reinforce existing inequities based on racial, ethnic, and national origin grounds. The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has emphasized that the discriminatory impacts of the use of new technologies in counter-terrorism are both direct and indirect and that this is particularly true for the underlying algorithmic functions of such technologies.[14]

---

[10] Lukasik, K., The Physiognomy Of Biometrics: The Face Of Counterterrorism (2004).
[11] See United Nations Compendium of Recommended Practices for the Responsible Use & Sharing of Biometrics in Counter-Terrorism (2018).
[12] Huszti-Orbán, K. and Ní Aoláin, F. Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business? (2020)
[13] In the context of its assessment visits on behalf of the Counter-Terrorism Committee, CTED has recommended that some States ensure the development and implementation of biometric tools in a responsible manner and consider appropriate safeguards, such as protection of privacy and data, in accordance with resolution 2396 (2017).
[14] See statement of 25 June 2021.

FATF has also recently highlighted that the use of biometrics for financial-inclusion purposes – including remote onboarding and financial services delivery (demand for which has been heightened by the COVID-19 crisis) – may exacerbate financial exclusion among sectors of the population (frequently women, because of the gender digital divide) that do not have access to electronic devices, do not trust the authorities, or are unaware of the potential of such devices. In view of these concerns, and the broader risk that biometric technologies may be used to violate the rights to privacy and data protection, human dignity, self-determination and access to an effective remedy, CSOs have raised a number of concerns and called for a moratorium on the development and deployment of all biometric technologies until vital human rights safeguards are in place.[15]

Perhaps because of these significant challenges to the responsible use of biometrics, the sharing of biometric data relating to counter-terrorism remains inconsistent, even though resolution 2396 (2017) encourages States to share this data responsibly with each other, as appropriate; with INTERPOL; and with other relevant international bodies. CTED's engagement with Member States has also revealed that the sharing of FTFs' biometric data and information tends to be limited, even among Member States with sufficient capacity. It has also revealed that the sharing of such information and access to databases among relevant domestic entities is limited in some Member States.

Furthermore, the risk that biometric data may be stolen or tampered with, especially through cyberattacks, is a major concern. Although the use of biometrics makes forging credentials more difficult, the reading (and illicit capture) of data and the need to store biometric templates in remote databases does present a risk of theft and tampering, making biometric data potentially vulnerable to misuse or malicious use. Moreover, biometric information (e.g., voice, face, and fingerprint data) is easily collectable and accessible (unlike passwords or PINs). As artificial intelligence (AI) continues to advance, "deep fakes" (hyper-realistic videos that depict someone saying or doing things that never happened) are more likely to be accessible to organized criminals and traffickers.[16]

These multifaceted challenges illustrate the need for coordinated delivery of technical assistance and capacity-building for Member States (notably States of Africa, Central and South East Asia, and South America) that are struggling with the introduction and use of biometrics, as well as the need for States with expertise in the responsible use of biometrics to support such initiatives.[17] The private sector also has a critical role to play in the development of biometric systems in a responsible, human rights-compliant manner, including cybersecurity measures to protect the data collected. Many related public-private partnerships have already been developed, and those initiatives should be supported and promoted at the national, regional, and international levels, recognizing the importance of ensuring that such partnerships respect human rights and promote a gender-sensitive approach.

[15] See e.g., Article 19's website.
[16] Westerlund, M., The Emergence of Deepfake Technology: A Review (2019).
[17] In the context of the assessment visits conducted on behalf of the Counter-Terrorism Committee, CTED has recommended that States with the relevant capacity and capability provide technical assistance and capacity-building support to States in need.

INTERNATIONAL GUIDANCE AND INITIATIVES

- The adoption of resolution 2322 (2016) marked the first time that the Security Council had called on Member States to share biometric data to detect and identify terrorists, including FTFs. Council resolution 2396 (2017) made that call a requirement under Chapter VII of the United Nations Charter.

- The Addendum to the guiding principles on foreign terrorist fighters (2018) (S/2018/1177) provides States with further guidance on effective response and implementation, focusing especially on the new requirements introduced by resolution 2396 (2017). The guidance can be utilized and referenced by States in their efforts at the national level. Guiding Principle No. 38 elaborates on those elements that constitute the "responsible" use and sharing of biometrics.

- In December 2019, the Council issued the Counter-Terrorism Committee's Technical guide to the implementation of Security Council resolution 1373 (2001) and other resolutions (S/2019/998), which also addressed the use of biometrics in the context of the relevant Council resolutions on counter-terrorism.

- In June 2021, following its Seventh Review of the United Nations Global Counter-Terrorism Strategy (A/RES/60/288), the United Nations General Assembly reaffirmed the Strategy by its adoption of resolution A/RES/75/291. Pursuant to the Strategy, all Member States are encouraged to address the threat of the increasing flow of international recruits to terrorist organizations, including through the implementation of obligations on the use of biometric data, with full respect for human rights and fundamental freedoms.

- CTED and the United Nations Office of Counter-Terrorism (UNOCT), acting in association with the Biometrics Institute and within the framework of the Global Counter-Terrorism Coordination Compact, has compiled the "The United Nations Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism", which was released in June 2018. The Compendium was developed to serve efforts to enhance implementation of biometric systems and to promote the use and sharing of biometrics in a responsible and proper manner, as required by resolution 2396 (2017).

- In 2020, the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism issued a report entitled Use of Biometric Data to identify Terrorists: Best practice or Risky business?

- INTERPOL has developed Project First, which aims to help States share biometric data on FTFs and other terrorist suspects, promotes the move from a "need to know" to a "need to share" culture, and aims to improve the identification and detection of terrorists and their affiliates by using the latest digital image-processing and facial-recognition technologies. It has also developed Project Hotspot, which aims to increase the amount of data that States contribute to border-related databases.

- The International Civil Aviation Organization (ICAO) has developed the ICAO Public Key Directory (PKD), a central repository for the exchange of information required to authenticate e-Passports, which provides an efficient way for States to upload their own information and download that of other States. By acting as a central broker, the PKD ensures that information adheres to the technical standards required to achieve and maintain interoperability.

- FATF has developed a detailed Guidance on Digital ID [18] to help Governments, financial institutions, virtual asset service providers (VASPS) and other regulated entities determine whether a digital ID is appropriate for CDD purposes. In its June 2021 Report on Opportunities and Challenges of New Technologies for AML/CFT, FATF also notes that mixed approaches (wherein official IDs are provided in tandem with biometric identification) may offer more robust identification and verification processes. The report emphasizes that biometric information collected by private parties should be recognized as protected information and subject to the legal standards required for such data under international legal instruments, and that its use should be limited by the proportionality and necessity principles.

- In partnership with the United Nations Counter-Terrorism Centre (UNCCT), the Global Counterterrorism Forum (GCTF) developed the "Good Practices in the Area of Border Security and Management in the Context of Counterterrorism and Stemming the Flow of "Foreign Terrorist Fighters", which were endorsed at the Seventh GCTF Ministerial Plenary Meeting held in September 2016. The Good Practices are intended to inform and guide Governments as they develop policies, programmes, and approaches for effective border-security management, cross-border cooperation, and border surveillance in a counter-terrorism context.

- In 2020, the United Nations Counter-Terrorism Centre (UNCCT) developed the Handbook on Children Affected by the Foreign-fighter Phenomenon: Ensuring a Child Rights-based Approach.

- UNCCT and CTED have also organized a series of regional expert workshops to raise awareness and enhance the capacity of Member States to ensure the responsible use and sharing of biometric data to detect, prevent, investigate, and prosecute terrorist offences and other serious crimes at borders.

CTED will continue to engage with these various initiatives and to develop and share its expertise on the issue of the responsible use of biometric technologies, acting in partnership with Member States; other United Nations entities; international, regional, and subregional organizations; local authorities; CSOs; the private sector; and the research community (through the GRN).

[18] https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf.