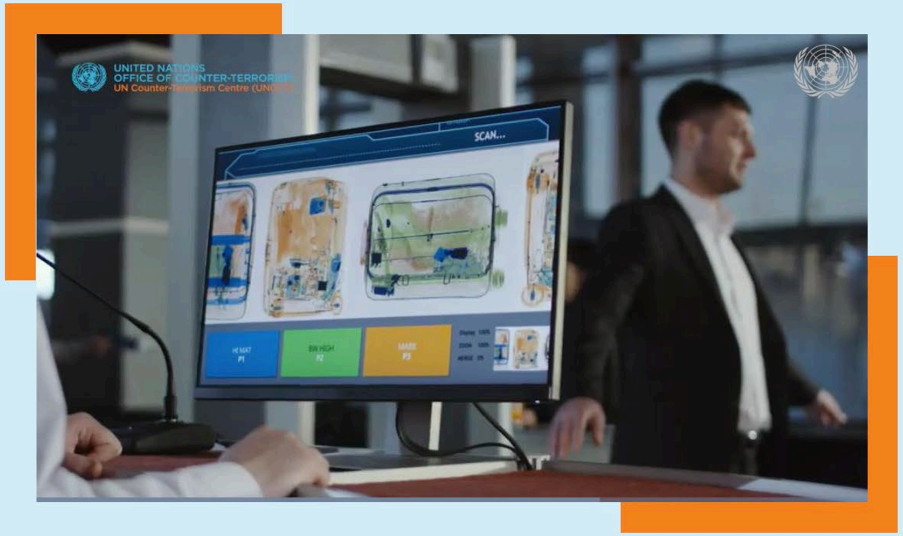
Responsible Use and Sharing of Biometric Data in the Counter-terrorism Context

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
UN Counter-Terrorism Centre (UNCCT)

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
UN Counter-Terrorism Centre (UNCCT)

SECURING BORDERS, BRIDGING PEOPLE

Ensuring effective border security and management is essential for preventing and countering the flow of suspected terrorists and foreign terrorist fighters (FTFs) across land, air and maritime borders, as well as the movement of illicit cargo, including weapons, arms and cash that may be used for terrorist purposes.



OUTLINE

I. The UN Compendium on Recommended Practices on the Responsible Use and Sharing of Biometrics

II. Security risks associated with Biometric technologies

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
UN Counter-Terrorism Centre (UNCCT)

I. Biometric Systems in the context of Border Security and Management

UNSCR 2396 (2017) *"Decides that Member 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 foreign terrorist fighters, in compliance with domestic law and* ***international human rights law****.*

Encourages Member States to share this data ***responsibly*** *among relevant Member States, as appropriate, and with INTERPOL and other relevant international bodies*

Calls upon other Member States, international, regional, and sub-regional entities to provide technical assistance, resources, and capacity building to Member States in order to implement such systems."

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
UN Counter-Terrorism Centre (UNCCT)

UNITED NATIONS SECURITY COUNCIL
COUNTER-TERRORISM COMMITTEE
EXECUTIVE DIRECTORATE (CTED)

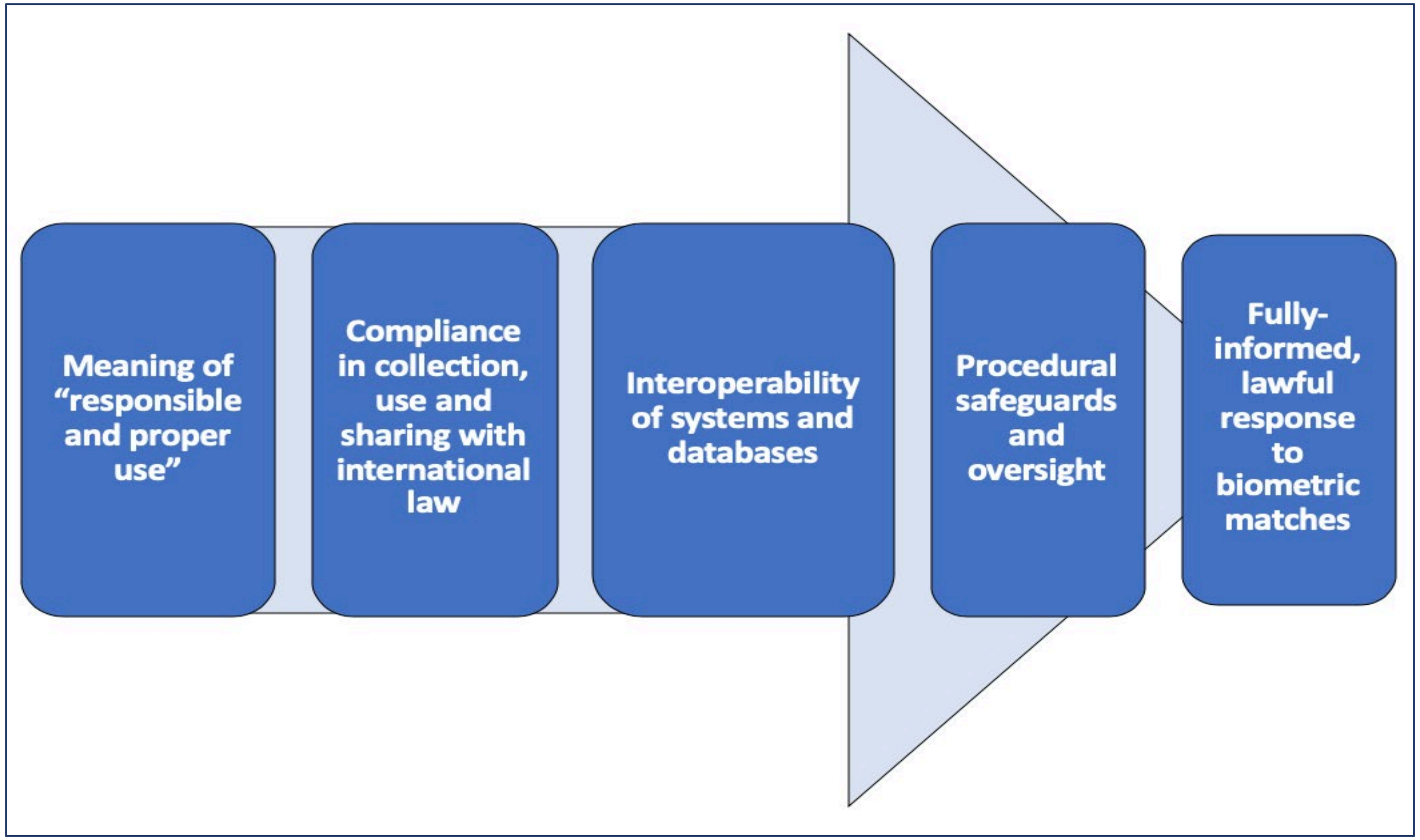
BIOMETRICS INSTITUTE

I. The UN Compendium

United Nations Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism

Compiled by CTED and UNOCT in 2018

offers the overall **framework of the procedural guidelines** for the acquisition, use and share of Biometric Data to counter terrorism



Meaning of "responsible and proper use"

Compliance in collection, use and sharing with international law

Interoperability of systems and databases

Procedural safeguards and oversight

Fully-informed, lawful response to biometric matches

I. **Recommended Practices** on the use of Biometrics to Counter Terrorism

- States should adopt **Human Rights based approaches to the use of biometrics technologies**, including the related procedural safeguards and effective oversight of its application

- Biometrics systems can be vulnerable to failure and many different forms of deliberate attacks. States are advised to conduct **regular risk assessments** at **every stage*** of the processing of biometric data

- It is recommended that States operate all their biometric systems **in compliance with international accuracy, safety and technical standards**

- The **procurement** and **management** of biometrics systems require long term **strategic planning** that addresses current and future resource requirements including public health associated concerns

II. Security Risks associated with Biometrics technologies

- Terrorist groups and FTFs may seek to take advantage of the disruption to the services that governments and law enforcement agencies usually conduct in the context of border security.

- The nexus between terrorists and transnational organized crime organisation might have strengthened to facilitate the traffic WMD, explosives, ammunition, firearms and SLAW, the smuggling dual-use items and the illegal movement of FTFs and returnees.

- Travel and trade restrictions have also impacted humanitarian organizations and in turns civilian populations increased their vulnerabilities.

- Terrorists might have exploit the possible misfunctions of digital surveillance systems (i.e. facemasks and biometrics) used for tracing purposes by Governments.

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
UN Counter-Terrorism Centre (UNCCT)

II. Security Risks associated with **Biometrics technologies**

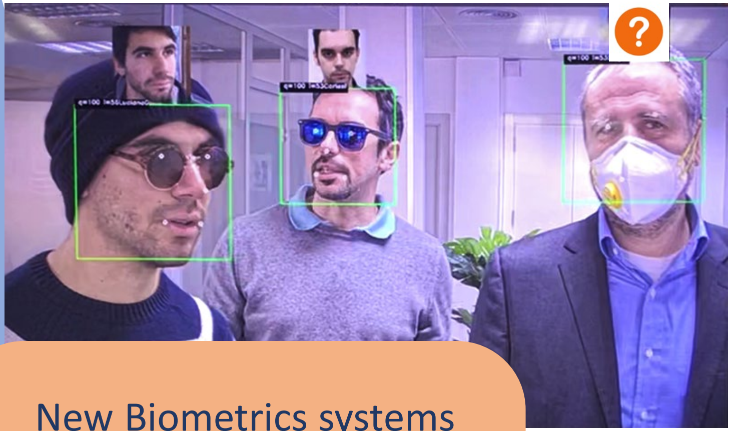
- Biometrics systems are the most accurate tools in border security but also present technological weaknesses and operational challenges

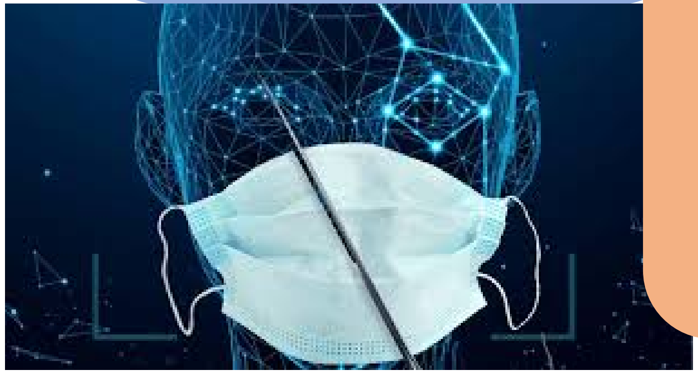
- COVID19-related **Public Health** and **Safety Measures** added a layer to the current screening and risk assessment procedures at borders

Facial recognition systems are exposed to *Face Morphing Attacks* or *Presentation Attacks*.

!!!

IN 2020: the difficulty in detecting the entire face given the use of mask **only compounds existing risks**.





New Biometrics systems should take into consideration possible algorithm **bias** to avoid security breaches and Human Rights violations..

II. Security Risks associated with Biometrics technologies

A **Human Rights-compliant approach** to biometrics is not possible without safeguarding the **right to privacy** and recognized **data protection principles**

Human Rights implications are much broader and addressing them requires considering the universal, indivisible, interdependent, and interrelated nature of all human rights.

- The lawfulness* of interference with human rights needs to be assessed at each stage of data handling and usage, including collection, retention, processing, sharing

- A human-rights-minded approach should govern **all phases of design, development and deployment** of biometric tools = "human rights by design"

II. Security Risks associated with Biometrics technologies

UN Guiding Principles on Business and Human Rights require:

.

- adoption of explicit and public **policy commitment** to meet stakeholder's responsibility to respect human rights (to also be reflected in operational policies – i.e. **authorization and licensing systems covering all stages of the processes**);

- conducting **risk assessments** examining actual and potential human rights impacts, both direct and indirect, of the operations;

  (Note: due diligence responsibilities **cover all phases of technology development and deployment**, including in relation to sale or transfer of the product, as well as after-sales support and maintenance)

- set up **internal accountability mechanisms** for the implementation of human rights policies; and

- **communicate externally how human rights impacts linked to their operations are addressed**, particularly when concerns are raised by or on behalf of affected stakeholders.

Biometrics are <u>high risk technologies</u> : processes must be set up in a way to protect against misuse, including **independent oversight** and **transparency** requirements.

Thank you | Merci beaucoup | شكرا جزيلا | Спасибо | Gracias | 谢谢

Rocco Messina

Head BSM Unit

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
UN Counter-Terrorism Centre (UNCCT)

BORDER SECURITY AND MANAGEMENT (BSM)

@UN_OCT

#UniteToCounterTerrorism