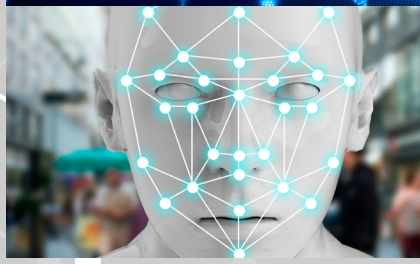
NEW DOCTRINAL CONCEPTS

# BIOMETRICS

*by* **WING COMMANDER MARK LUNAN**
Royal Air Force
Subject Matter Expert and Observer/Trainer
Joint Warfare Centre

***with additional contributions from***
Lieutenant Colonel Joel Moore, HQ SHAPE
Lieutenant Colonel John Moore, JWC
Major Wilko ter Horst, HQ SHAPE



**OXFORD ENGLISH DICTIONARY DEFINITION**
Relating to or involving the application of statistical analysis to biological data. Also known as Biometry and Biostatistics in North American English.

**NATO DEFINITION**
The automated recognition of individuals based on their behavioral and biological characteristics.

**JOINT DEFINITION**
The process of recognizing an individual based on measurable anatomical, physiological and behavioral characteristics. The U.S. places biometrics in the category of "Identity Intelligence (I2)" and is now a discrete category of intelligence products.[1]

**SO WHAT FOR NATO**
Biometrics is a capability that, together with intelligence, supports the identification of threats to NATO and assists in counter-threat operations conducted by NATO assets.

**In 2012, NATO Nations unanimously adopted the *"Concept of Biometrics in Support of Operations"* which highlights the broad cooperation required across the full spectrum of military and civilian entities for biometrics to take effect against threat anonymity. The practical use of biometrics in NATO operations first took place in Afghanistan.[2]**

**ABOVE:** Flowers posed in the impact of a Kalashnikov bullet in the bar hotel Le Carillon near the Bataclan theater after the terrorist attack in Paris, 13 November 2015. Photo by Frederic Legrand, Shutterstock

***DOCUMENTARY SOURCES***

Allied Intelligence Publication (AIntP) 15 (Countering Threat Anonymity: Biometrics In Support of Operations and Intelligence); NATO Concept for Biometrics in Support of Operations, 21 March 2012; U.S. Army, Joint Publication 2.0, "Joint Intelligence", 2013.

NATO's New Strategic Concept, and the 2014 Wales Summit Declaration identified an increase of that threat posed to the Alliance by individuals and non-state actors, who will act under the protection of anonymity to gain tactical, operational and strategic advantages. Among these increasing threat categories are terrorists[3], traffickers, foreign fighters, insurgents, hackers and pirates. These actors will seek to remain anonymous and conceal their activities when encountered by NATO forces. The need to identify such actors and mitigate their ability to remain anonymous is currently high on NATO's agenda, and to this end biometrics is considered one of NATO's top strategic and operational capabilities.

The quality of Biometrics Support to Operations is directly proportional to the size of its database used to remove the anonymity. Therefore, NATO Automated Biometrics Identification System (NABIS) was created to provide functionality to store biometrics data and facilitate multimodal biometrics searches. NABIS stimulates sharing of biometrics among the [NATO] nations in a controlled environment. It also provides the ability to create a repository to store biometric data for immediate verification that is available for NATO forces in a Joint Operations Area (JOA). In the context of NATO operations today, when NABIS becomes fully operational, it will give commanders the ability to more quickly and accurately discover, identify, and record the identities of threat actors. It will also enhance Command and Control (C2) by allowing commanders to be automatically informed of who is encountered by whom, where, and at what time. This, in turn, will support actionable intelligence at the operational (NATO Response Force (NRF)) and strategic (national agencies) levels.[4]

A biometric characteristic is a biological and behavioral signature of a person from which distinguishing, repeatable features can be extracted for the purpose of recognition. Each characteristic has a distinct set of advantages and disadvantages for use in support of military operations. Lessons Learned and Identified by best practices in ISAF by NATO Nations consistently highlighted that collection of certain human characteristics was essential,[5] which are:

- **Topography:** Face, finger and hand.
- **Structure:** Iris, DNA[6] and hand-vein.
- **Dynamics:** Hand-writing, voice and keystroke.
- **Gait**[7]

Using biometrics as a means of identifying individuals within the operational environment presents distinct advantages over the traditional methods of using text-based identification processes. These advantages are as follows:

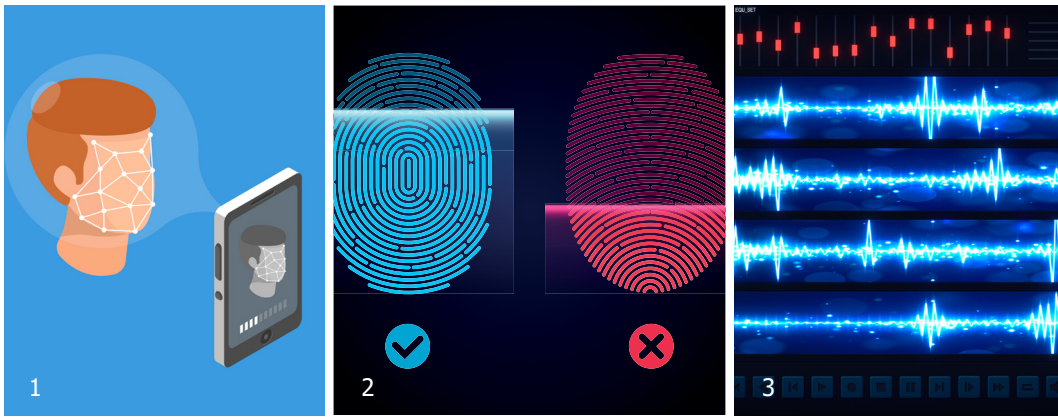
- **Scientific Accuracy:** Includes beyond reasonable doubt.

— **Real-Time Automation:** Enables quicker analytical turnaround time.
— **Technical Exploitation:** Links individuals to items recovered during operations.
— **Biometrically Enabled Watch Lists:** Force multiplier for commanders.[8]

Following best practice from Lessons Learned in Afghanistan, biometrics assisted NATO using the "F4" principles below:

— **Find:** Systematically captured and matched biometric samples from individuals in the battlespace as well as from improvised explosive devices (IEDs), weapons' caches, computers, mobile phones, documents and other sources. This in turn identified and linked anonymous persons to networks, places, items, and events.
— **Fix:** Allows NATO to positively identify (PID) the targets of operations more accurately, which increases fidelity in targeting.
— **Finish:** Biometrics allows the use of a Biometrics Enabled Watch List (BEWL), which allows the NATO commanders to provide specific guidance to operational as well as tactical elements on how to address specific individuals encountered during operations.[9]
— **Force Multiplier:** Biometric samples, captured across the comprehensive spectrum can be automatically matched, which empowers C2, force protection, counter-intelligence and targeting efforts. The additional use of BEWLs creates opportunities within operations to find, fix and finish threats.[10]

The interdependent purpose of NATO biometrics for capturing and using biometric data in support of NATO operations is the identification of threat actors. This is accomplished by one foundation (Enrolment), and two primary (Identification and Verification) biometric functions.[11] **Biometric Enrolment** is the act of creating and storing a biometric data record. It can be used to biometrically link an event record to an individual. Biometric Enrolment also takes place when a latent biometric sample is digitized for matching against a biometric database. Latent biometric samples are developed through technical exploitation and subsequent forensic processes, which are used to recover latent fingerprints or DNA from items.[12] **Biometric Identification** is the process when a biometric sample is compared against all records in a biometric repository or system of repositories to find and return the biometric reference identifier(s) attributable to an individual. It is used to associate that individual with previously collected biographic and situational information. Its primary focus is to identify anonymous threat persons.[13]




**ABOVE:** "Topography" collection examples. A smartphone scans a person's face for facial recognition (1), fingerprint capture to analyze fingerprint data (2), "Dynamics" collection example of voice sampling (3).

Biometric records can originate through inter-agency sharing or from military activities. Sharing can originate from historic datasets provided by Allied, host, or Partner Nations. Biometric Enrolment records from a variety of military activities can be simultaneously checked against the database for Biometric Identification, while adding additional enrolment records to the database.[14]

**Biometric Verification**, meanwhile, is a one-to-one process in which an individual's biometric sample is matched against his stored biometric file. It is often used in processes associated with ID cards and is used to control access to bases, areas, facilities, assets, and events. Biometric Verification, supported by biometric Identification, is vital in detecting insider threat and preventing green on blue attacks.[15]

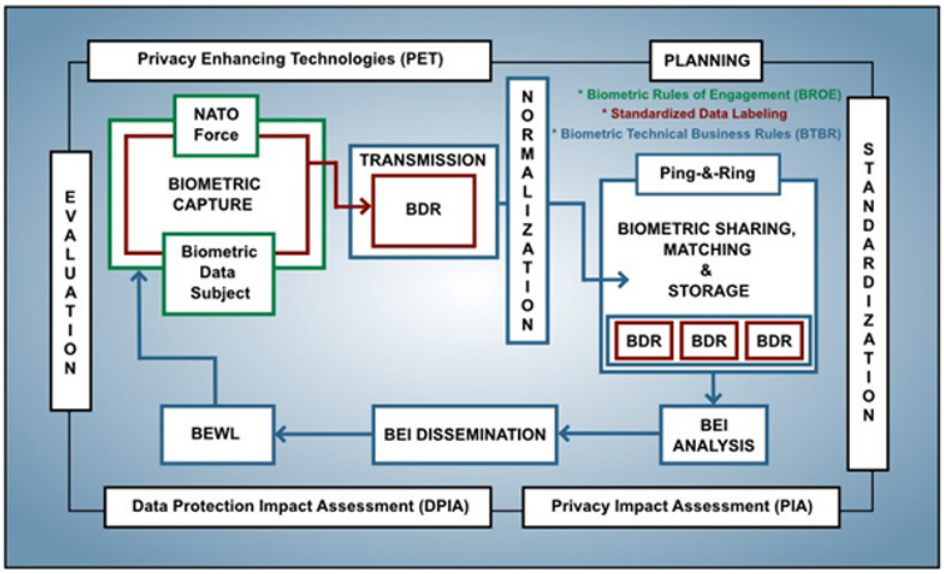
A NATO or Partner Nation's use of biometrics may be permitted or constrained by national laws and international agreements to which they are a party. These factors vary from one nation to another and these variances impact on how each nation might participate in NATO biometric activities. As such, the NATO Biometric Framework and Cycle was created to promote an interoperable and collaborative NATO standard.[16] The NATO Biometric Framework and Cycle sets a baseline of technical interoperability standards, concepts for national control[17] and processes for assessing and protecting privacy and data security; all of which underpins planning and evaluation. Here is an explanation of some of the abbreviations:

**BDR:** The Biometric Data Record contains those human characteristics of an individual listed above (Topography, Structure, Dynamics, Gait).[18]

**BDS:** A Biometric Data Subject is an individual person. This can be a volunteer, such as a locally employed civilian working inside a NATO deployed base or a threat individual/person of interest. A factor in determining the capture and use of biometric data is whether its capture is consensual or non-consensual. In certain instances, Biometric Series Rules of Engagement and national caveats may determine whether or not consent is required.[19]

**BEI:** Biometric Enrolled Identification is the intelligence resulting from the capture, processing, analysis, interpretation and dissemination of biometric data, the contextual information associated with that data and other associated information and intelligence. It aims to integrate the information from biometric capture and processing into all-source intelligence analysis.

**BEWL:** Biometric Enabled Watch List is an intelligence product, which assesses and categorizes biometrically identified individuals. The BEWL is key to the dissemination of biometric information throughout NATO commands.[20]




**ABOVE:** NATO Biometric Framework and Cycle.

**BTBR:** Biometric Technical Business Rules is a set of rules in a system developed to automate the requirements of sharing arrangements.

**"Ping and Ring":** A slang term for NATO and national inter-agency coordination, cooperation and biometrics information exchange.[21] This term is also extended to the biometrics user community at the operational and tactical levels within a JOA. A typical Ping and Ring graphic is depicted below, which highlights information sharing between two nations resulting in a **Multi-Biometric Match Report (MBMR)**. MBMRs contain biometric encounters by multiple NATO nations, and as such, each of those nations potentially has valuable information regarding the individual. The nation that last encounters an individual is the necessary customer of information and intelligence regarding that individual. This is known as the **Principle of Last Encounter**.[22]

**Legal Concerns:** The main legal issues in biometrics involve the sharing of identity intelligence activities, data and techniques between the NATO Nations. Concept Papers and reports of Biometrics Working Groups generally state that biometric information is Personally Identifiable Information (PII) that must be handled "in accordance with the applicable national laws of the collecting nation."[23]

In the near future, *The Three Swords Magazine* expects to feature an article explaining the legal aspects of biometrics in detail.

## So what for NATO

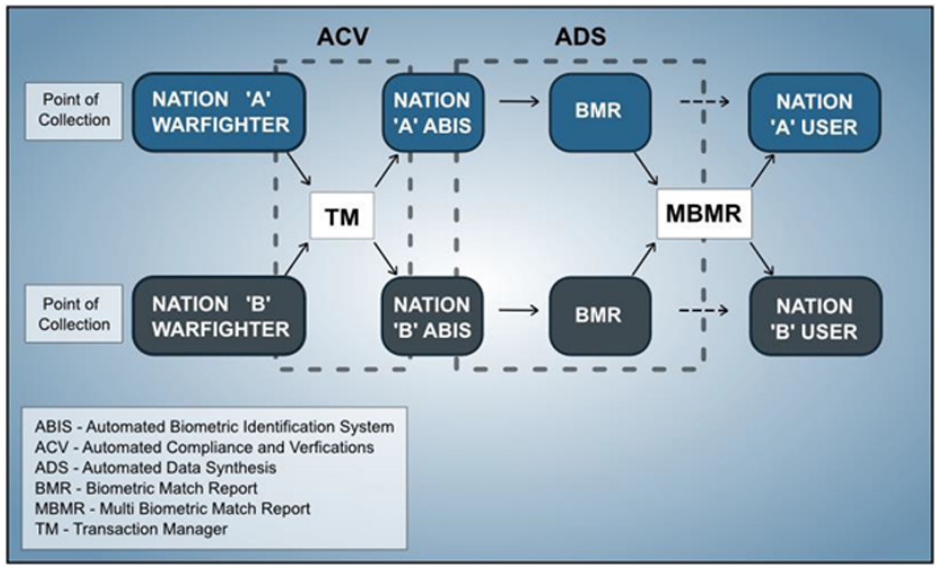
Within the context of the NRF operations, here are two examples of Biometrics Support:

**1/ Inter-Agency Cooperation:** The NRF is supporting a foreign nation's re-building process, which is being undermined by arms smuggling into that state. All biometric operations are conducted using ABIS.[24] A civilian truck driver provides biometric samples to the nations' border police, who are supported by the NRF elements. The biometric samples and contextual information are transmitted to the JOA ABIS, and subsequently compared to the locally stored biometric files. The truck driver's biometric data does not match any file in the JOA ABIS, and a negative response is provided back to the border police. The truck driver is also checked against local and national criminal records. The border police review the match result and clear the truck driver to continue.

The biometric file is enrolled and stored in the JOA ABIS, and is then shared with other agencies (where information sharing agreements are already in force). Two weeks later, the host nation's national police, supported by the NRF, conduct a raid on the arms-smuggler's safe house and seize numerous documents and computer hardware. Biometric samples are collected from this evidence, and compared to the JOA ABIS. A match is made between the latent samples collected during the raid and the truck driver's biometric file. An analysis of the data collected from the raid and associated information is completed and the truck driver's non-biometric reference information is updated with these new samples, red-flagged for future matches, placed on the JOA BEWL and shared with all biometric system operators within the country.

Several days later, the truck driver attempts to cross into the host nation at a different border checkpoint. He submits his individual identification and a biometric sample for verification. The sample is com-

**BELOW:** Inter-Nation Biometric Coordination and Information Exchange.



**ABOVE:** Iris scanning during a biometrics course at the Joint Readiness Training Center. "Biometrics is the science of using physiological features, such as fingerprints or irises, as a method of identification," said the class instructor, adding: "The good thing about using biometrics is that it's real time. That means if you're scanning someone, it will give you an answer within a couple seconds." Photo by Pvt. Luke Rollins, U.S. Army. (https://www.army.mil/article/23942/fort_lewis_soldiers_learn_about_biometrics_at_jrtc)

pared against the JOA BEWL, which alerts the border police to the red flag stored in the JOA ABIS. The truck driver is detained for questioning and his biometric file is updated with the newly collected biometric sample and contextual data.

**2/ Humanitarian Assistance Relief:** The NRF is responding as part of an international disaster relief effort. Thousands of injured are being treated and awaiting further treatment as soon as field medical hospitals are assembled and operational. All individuals who receive medical attention within the disaster area are immediately enrolled in a NATO biometric local ABIS that has been established for management of the Internally Displaced Persons (IDPs). All treatment records are linked to their respective biometric files. Many of the injured, after being initially treated, voluntarily relocate within the disaster area. However, this movement is making it difficult for medical personnel to efficiently provide medical services or track patients for follow-up treatment.

The NRF medical personnel are performing triage for IDPs arriving by buses at one of the newly established field hospitals. They collect biometric samples from each IDP for identification purposes as part of the initial medical assessment process. The biometric files are then sent for matching against the local ABIS to assist with the identification of the individual and retrieve any available medical treatment history. An IDP who cannot be matched against the local ABIS is enrolled as a new biometric file. All subsequent medical treatment will later be linked to that file.

When an IDP is positively matched against the local ABIS, links to his/her medical history are accessed and any prior treatment records are retrieved. Subsequent treatment is updated in the IDPs medical record so that information can be accessed by others again in the future by using the established net-centric links between the non-biometric repository (medical files) and his/her biometric file. The NRF medical personnel use these medical records to aid in triage.

Biometrics is used the world over by everyone, not just NATO, including humanitarian relief organizations or law enforcement agencies. From the moment you apply for a driving license or passport perhaps, you are "in the system"—therefore biometrics is nothing new.

Within the NATO context, biometrics has proven to be a significant theatre-level force multiplier in supporting a host nation in their fight against organized crime and terrorism and in humanitarian relief. Afghanistan was a typical example of how the International Security Assistance Force (ISAF) was able to do this. Future NRF operations are highly likely to use biometrics, dependent upon the mission, legal considerations and, of course, constraints or restraints stipulated by the relevant host nation. ✦

Photo by vlada93, Shutterstock

**BIOMETRICS IS REAL TIME**

## END NOTES:

1 U.S. Army, Joint Publication 2.0, "Joint Intelligence" (2013).
2 International Security Assistance Force (ISAF) used biometrics across Afghanistan 2010-2014.
3 Some NATO Nations do not regard counter-terrorism as a military function; however, intelligence collected in military operations can be essential to national operations.
4 Allied Intelligence Publication 15, "Countering Threat Anonymity: Biometrics in Support of NATO Operations and Intelligence (NATO Standardization Office 2016) [hereinafter AInt-15].
5 Id.
6 Deoxyribonucleic Acid.
7 AInt-15, F-5: "a biometric characteristic based on walking pattern".
8 AInt-15
9 AInt-15
10 Id.
11 Id.
12 Id.
13 Id.
14 Id.
15 Id.
16 Id.
17 NATO can only suggest or recommend to nations on matters of national control.
18 AInt-15
19 Id.
20 Id.
21 Subject to national caveats and NATO constraints and restraints.
22 AInt-15
23 NATO & Int'l Military Staff, Concept for Identity Intelligence (I2) (2017).
24 Automated Biometric Identification System.