National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

A Standing Biometrics Capability for the Canadian Armed Forces

Major Rouslan Gouseinov

JCSP 48

Service Paper

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 48

Étude Militaire

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 48 – PCEMI 48
2021 – 2022

Service Paper – Étude militaire

A Standing Biometrics Capability for the Canadian Armed Forces

Major Rouslan Gouseinov

A STANDING BIOMETRICS CAPABILITY FOR THE CANADIAN ARMED FORCES

AIM

1. The ability to leverage biometrics represents a critical military capability in a modern complex operating environment that is characterized by the adversary's ability to remain hidden amongst the population. The purpose of this paper, therefore, is to demonstrate that the Canadian Armed Forces (CAF) current policies, directives, and capabilities relating to the use of biometrics in an expeditionary environment are inadequate for the modern battlefield.[1] This paper further suggests that to enable CAF preparedness for future deployed operations, which will likely involve the use of biometric capabilities by our allies, deliberate and coordinated action to develop a standing CAF biometrics capability is required.

INTRODUCTION

2. Biometrics is defined in the Canadian context as a process that enables the automated recognition of individuals based on their behaviour and biological characteristics.[2] The nature of the modern threat environment places a premium on a military's ability to detect and identify individual enemy combatants or local persons of interests. Moreover, threat actors are no longer contained by geographical boundaries, easily transitioning from one area of operations into another and in doing so leveraging anonymity to gain an operational advantage. Biometrics, as an intelligence function, can be used to identify individuals who may be attempting to conceal their true identities and who pose a threat to CAF personnel.[3] The value proposition of such a capability is that its application extends across the operational spectrum to include force protection, checkpoint operations, detainee management, recovery operations, targeting, sensitive site exploitation and Post-Improvised Explosive Device (IED) battlefield assessments.[4] The CAF's biometric capability was initially authorized by the Chief of Defence Staff (CDS) in December 2008 in order to provide operational support to Coalition Forces in the Afghanistan theatre of Operations.[5] The authority on the use of biometrics is governed by the *Chief of Defence Intelligence Interim Functional Directive: Guidance on the Collection, Use, Handling, Retention, and Disclosure of Biometric Data during Expeditionary Operations (*hereinafter referred to as the Interim Directive*).* Drafted in 2020 under the authority of the Chief of Defence

---

[1] The focus of this paper is strictly on the use of biometrics in an expeditionary operation by the CAF. The domestic use of biometrics by the CAF is legally constrained due to the nature of collecting personal data on Canadian citizens or permanent residents. Such collection is better served by security agencies with the necessary legal mandate to undertake such activity, i.e. , CSIS.

[2] Canadian Forces Intelligence Command, *Chief of Defence Intelligence Interim Functional Directive: Guidance on the Collection, Use, Handling, Retention, and Disclosure of Biometric Data during Expeditionary Operations* (Ottawa: DND Canada, 2020), 3.

[3] Ibid.

[4] Ibid.

[5] American, British, Canadian, Australian Armies, *Biometric Information Team Meeting – Canadian Response to Topics of Discussion: Biometric Policy and Sharing of Data outside of ABCA Militaries*, (Ottawa: DND Canada, 2013), 1. ABCA Armies (formally, the American, British, Canadian, and Australian Armies Program) is a program designed to enable and optimize interoperability and standardization of training and equipment between the armies of Australia, Canada, the United Kingdom, and the United States.

Intelligence, in his role as the functional authority for all matters related to biometrics in the CAF, the Interim Directive seeks to provide direction and guidance on all matters related to the execution of biometric activities when authorized by the CDS as part of mandated expeditionary operations.[6]

3. Although not directly referenced in *Strong, Secure, Engaged* (SSE), the establishment of a standing biometrics capability is instrumental in the success of the following SSE initiatives:

a. **Initiative 42**: Modernize land-based command and control and Intelligence, Surveillance, and Targeting (ISR) systems;

b. **Initiative 71**: Build the Canadian Forces Intelligence Command's (CFINTCOM) capacity to provide actionable intelligence to war fighters.

c. **Initiative 72**: Establish a CAF targeting capability to better leverage capabilities to support military operations.[7]

As such, this paper will investigate the current policies and capabilities governing the application of biometrics within the CAF to highlight how they currently do not enable success in an operational environment. The following paragraphs will outline the technological and legal shortcomings that must be addressed by the CAF prior to the establishment of a standing biometrics capability, a capability that the CAF must institutionalize if it hopes to remain effective in the future security environment.

DISCUSSION

4. Lessons learned from deployed operations in Afghanistan (Operation Athena) identified biometrics as a key enabler for defensive "force protection" and offensive "attack the network" operations.[8] The Afghanistan experience has taught the CAF that an effective biometric capability consists of three core components:

a. Collection: enables deployed CAF personnel to collect biometric data from both individuals and latent material for the purpose of screening against biometrically enabled watchlists and/or authoritative databases, and/or enrolling it into an authoritative database in order to enhance overall force protection.

b. Communication and Information Systems (CIS) framework and process architecture: This framework and architecture forms the authoritative biometric data source for operational use and include the electronic data storage capability, the necessary matching and retrieval processes, and be supported by a transport layer capable of providing information sharing capabilities and connectivity to and from deployed

[6] Canadian Forces Intelligence Command, *Chief of Defence Intelligence Interim Functional Directive*…, 1. Biometric activities include collection, screening, verification, enrolment, use, handling, retention, and disclosure.
[7] Department of National Defence, "Strong, Secure, Engaged: Canada's Defence Policy. Strong, Secure, Engaged. Canada's Defence Policy. (forces.gc.ca), 109-110.
[8] Department of National Defence, *Canadian Army Biometric Activity/Architecture,* (Ottawa: DND Canada, 2015), 3.

operations. It will be the system into which all collection capabilities and data will be fed and will enable the fusion and exploitation of that data; and

c. Exploitation – The exploitation capability is used on deployed operations to develop intelligence and enhance force protection through such measures as base or ship access control and local employment vetting, as well as augment offensive operations such as counterinsurgency and maritime interdiction operations.

5. All three components rely on the ability to gain access to a national or allied database that can effectively match biometric data to persons of interest (POI). During the war in Afghanistan, because of not having resident Canadian biometric storage architecture, the CAF agreed to utilize the US Department of Defense (DOD) Biometric architecture. The issue with that decision was that the CAF then no longer "owned" the biometric data it collected, and therefore under a legal context could not answer for what purposes that data had been used by the US or other allied nations[9]. The CAF needs to establish the technology to create its own biometric database, as well as leverage the databases of allies.

Technological Deficiencies

6. Biometric collection devices used by US and allied forces typically collect fingerprints, iris images, and facial images and then subsequently stores this data into national databases for further exploitation. As such, this data can then be searched upon and compared to other collected biometrics to be able to verify the identity of an individual. Using forensic processes such as lifting a latent fingerprint or collecting DNA from materials or evidence found through the examination of IED components after an explosion, can result in identifying biometric data. Through exploitation of these types of biometrics, individual identification and possible attribution can be made.[10] The ability to identify a positive match is based upon having access to a database of collected biometric data of non-Canadian citizens that can be cross matched to verify an identity.

7. The ability to transmit to the database becomes key in operationalizing the biometrics concept; without it, collected biometrics data would be rendered ineffective. The probability of identifying those who are tied to criminal or insurgent activity increases as the biometric database grows. The ability to link into authoritative databases is also critical for the development of a key product used to support tactical biometrics operations — the Biometric Enabled Watch List (BEWL), which would fall under the exploitation component. The BEWL is a collection of individuals whose biometrics have been collected and determined by analysts to be threats, potential threats, or who simply merit tracking.[11] However, the BEWL needs constant updating, and therefore for CAF personnel to have the latest intelligence on the status of

---

[9] Department of National Defence, *Canadian Forces Intelligence Liaison Officer to the US National Ground Intelligence Center Biometric Responsibilities*, (Ottawa: DND Canada, 2013), 2. The case of Maher Arar served as the most vivid example of how the sharing of personal information between allied security services could contribute to difficult legal circumstances.

[10] US Department of Defense, " Commander's Guide to Biometrics in Afghanistan" CALL-AfghanBiometrics.pdf (publicintelligence.net), 5.

[11] Ibid.

individuals, the devices need to be able to be connected to a network to receive the BEWL, which the CAF currently lacks.

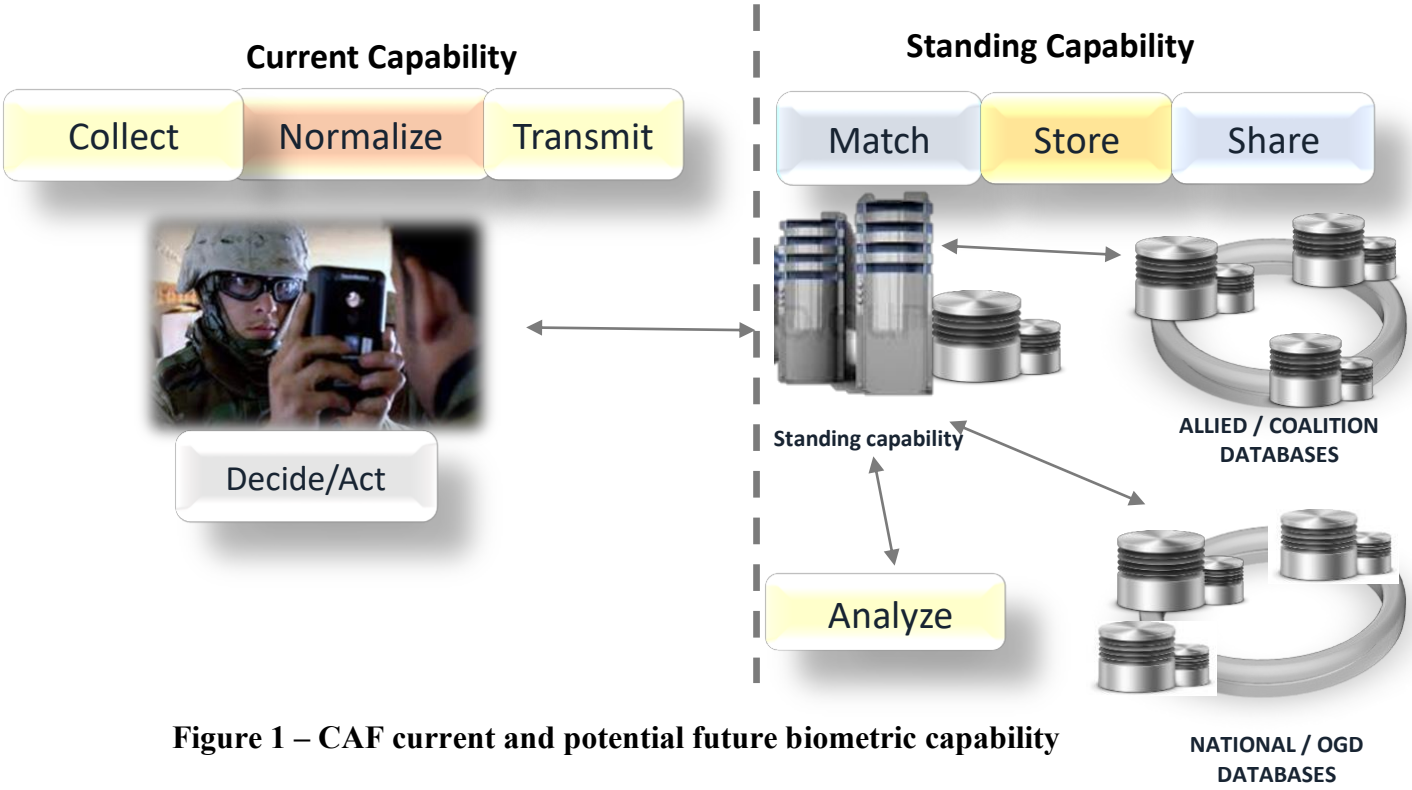

Figure 1 – CAF current and potential future biometric capability

8. With regards to the CAF's current biometrics capability, it is limited to the Army, the Royal Canadian Navy, and Canadian Special Operations Forces Command each having their own biometrics kits, which at this stage are not connected to any database that can house or match biometric data. Hence, the current capability can be summarized as the ability to do collection in a deployed environment and some first-line analysis only. In most cases, these tasks are contracted out to US industry for support due to the CAF lacking the ability to both access and share data.[12] Hence, the current CAF capability deficiency is described as the inability to identify adversaries who can deliberately engage in tactics to conceal their identities. This inability to verify and share the identity of potential adversaries poses a serious risk for force protection, especially in areas high in threat of espionage and sabotage like Eastern Europe. What is needed is the ability to transmit to an authoritative database, maintain and update the files, and allow for matching with previously collected data.

9. Another deficiency is the inability to obtain, and share collected biometric data with international partners, other government departments, and even other CAF environments.[13] Whatever biometric data is collected by the CAF, it currently has no ability to be cross-matched

[12] Canadian Forces Intelligence Command, *Biometrics – DND/CAF and the role of the Release and Disclosure Office,* (Ottawa: DND Canada, 2021), 4.
[13] Ibid.

to other databases and thereby unable to access identity information stored in international and national partner databases. This inability to share biometric information on POIs also impedes the ability for each environment to cooperate with each other. This becomes more pressing when environments operate in the same country, i.e., the Canadian Army and CANSOFCOM in Iraq.

Legal Considerations

10. The use of biometrically enabled technology in the operational spheres can be expected to raise several varied and complex legal issues that will need to be navigated through in the establishment of a standing CAF biometric capability. Different legal regimes govern the collection, storage, and use of biometric data in Canada at the federal, provincial, territorial, and municipal level. Across federal government departments, the collection, storage, and use of biometric information may be governed by the *Canadian Charter of Rights and Freedoms* as well as cross-cutting legislation such as the *Privacy Act*, *Access to Information Act,* and *Library and Archives of Canada Act.*

11. The Interim Directive classifies biometric data as personal information as defined in the *Privacy Act;* as such, CAF biometrics activities must be conducted in a manner that is consistent with the provisions of the *Privacy Act.*[14] Hence, one of the legal obstacles that the CAF will need to consider as it strives to establish a standing biometric capability is the legal authority to store personal data from a network associated to a POI, i.e., friends or acquaintances of a particular POI. Such information has proven very useful for understanding and dismantling adversary networks in counterinsurgencies as demonstrated in both Afghanistan and Iraq. The current challenge from a legal perspective, however, will be to acquire a legal mandate to capture and store biometric data on individuals who "might" become useful.

12. Another factor that complicates the CAF's use of biometrics is the nebulous legal framework under which such activity can be conducted. The Interim Directive specifies that it does not provide any legal authority for the conduct of biometric activities for current of future expeditionary operations.[15] That authority, in the context of the CAF, currently solely resides in the CDS, who must be the one to authorize any biometric activity during expeditionary operations.[16] This means that in the absence of a standing biometrics capability, CDS authority will have to be sought every time biometrics are to be used. Such a process can become lengthy and may not be appropriate for the dynamic modern operating environment, which is characterized by uncertainty and the ability to quickly react to unforeseen circumstances.

13. The ability to share biometric data with other Canadian security partners, however, has been clearly established as being entirely within legal parameters. Other government security agencies such as the Communications Security Establishment (CSE), as well as the Royal Canadian Mounted Police and the Canadian Security Intelligence Service (CSIS), regularly exchange information under the Security of Canada Information Disclosure Act (SCIDA) of a

[14] Canadian Forces Intelligence Command, *Chief of Defence Intelligence Interim Functional Directive*…, 4.
[15] Canadian Forces Intelligence Command, *Chief of Defence Intelligence Interim Functional Directive*…, 2.
[16] Ibid, 4.

nature and in a manner that warrants information sharing arrangements, as encouraged by subsection 4(c) of the Act, including biometric data.[17]

14. The Interim Directive also does not mention the need for any oversight and compliance. However, since 2019, the National Security and Intelligence Committee of Parliamentarians (NSICOP) has been mandated to provide a framework review of how the government sets, reviews, and implements its intelligence priorities, as well as providing an activity review of the Department of National Defence's intelligence functions, which includes biometrics. [18] If the CAF is to establish a standing biometrics capability, it will need to consider a mechanism to undertake oversight and compliance over such a legally sensitive issue as the collection of biometric data.

CONCLUSION

15. Over the last 20 years, biometrics has proven to be a critical capability in the modern operating environment. Its value proposition primarily stems from being an effective method of eliminating the adversary's greatest asset: their ability to remain anonymous while exercising global mobility. Although the CAF currently possesses an interim framework to conduct biometric activities in an expeditionary environment, it still lacks the proper legal interpretations and technological guardrails to effectively operate in the future security environment and enable interoperability with coalition and allied partners. Unless these shortcomings are addressed, the CAF will continue to operate with a limited biometric capability and without the supporting infrastructure to transmit, match, jointly store, and share data. These deficiencies render it difficult for biometric information to be accessible to deployed forces, other government departments and agencies as well as international partners, leading to reduced operational effectiveness and increased risk to our forces. Moreover, if the CAF is unable to establish a standing biometric capability, it is very likely that SSE initiatives 42,71, and 72 will not be operationalized to their fullest extent.

RECOMMENDATIONS

16. With consideration to the preceding discussion, and in addressing the CAF's deficiencies concerning biometric activities, this paper puts forth the following recommendations:

a. Create a dedicated centralized authoritative source of operational biometric data, capable of delivering an automated, comprehensive end –to-end biometric capability that will be responsible for establishing common standards across the CAF and implement the capabilities necessary to share with partners and allies. This will also eliminate the need to seek CDS authority to conduct every single biometric activity other than in the most sensitive of cases.

---

[17] National Security and Intelligence Review Agency, *NSIRA and OPC's Review of Federal Institutions' Disclosures of Information under the Security of Canada Information Disclosure Act in 2020* (Ottawa: NSIRA Canada, 2021), 34.
[18] National Security and Intelligence Committee of Parliamentarians, 2019 *Annual Report,* annual_report_2019_public_en.pdf (nsicop-cpsnr.ca)

b. Refresh the Interim Functional Directive on Biometrics to provide further clarification on how to interpret the *Privacy Act* with regards to storing and potentially sharing biometric data.

c. Establish a closed network that will enable automated sharing of identity information amongst different environments and commands.

d. Establish a biometric centralized database, in full compliance of the *Privacy Act*, to be able to transmit to an authoritative allied database, maintain and update the files, and allow for matching with previously collected data.

e. Implement North American Treaty Organization (NATO) Standardization Agreement (STANAG) 4715 on Biometric data Interchange. This STANAG specifies the common technical requirements and formats for biometric store, match, and share Information Technology Systems. Implementation and conformance to the STANAG provides for interoperability amongst disparate biometric technology solutions by providing a common biometric data interchange format for coalition data sharing.[19]

f. Establish a body to assist with implementation oversight. Such a body may be leveraged to screen requests for the sharing of biometric information, to develop data safeguarding policies, to track biometric use in the CAF, and to provide other oversight as required.

Annexes:

Annex A: Bibliography
Annex B: Definitions

[19] North American Treaty Organization, *Standardization Agreement 4715: Biometrics Data Exchange,* (Brussels: NATO Standardization Office, 2021), 2.

BIBLIOGRAPHY

American, British, Canadian, Australian Armies. *Biometric Information Team Meeting – Canadian Response to Topics of Discussion: Biometric Policy and Sharing of Data outside of ABCA Militaries*. Ottawa: DND Canada, 2013.

Canada. Canadian Forces Intelligence Command. *Chief of Defence Intelligence Interim Functional Directive: Guidance on the Collection, Use, Handling, Retention, and Disclosure of Biometric Data during Expeditionary Operations.* Ottawa: DND Canada, 2020.

Canada. Department of National Defence. "Strong, Secure, Engaged: Canada's Defence Policy. Strong, Secure, Engaged. Canada's Defence Policy. (forces.gc.ca).

Canada. Department of National Defence. *Canadian Army Biometric Activity/Architecture.* Ottawa: DND Canada, 2015.

Canada. Department of National Defence. Canadian Forces Intelligence Liaison Officer to the US National Ground Intelligence Center Biometric Responsibilities. Ottawa: DND Canada, 2013.

Canada. Canadian Forces Intelligence Command. *Biometrics – DND/CAF and the role of the Release and Disclosure Office.* Ottawa: DND Canada, 2021.

Canada. National Security and Intelligence Review Agency. *NSIRA and OPC's Review of Federal Institutions' Disclosures of Information under the Security of Canada Information Disclosure Act in 2020*. Ottawa: NSIRA Canada, 2021.

Canada. National Security and Intelligence Committee of Parliamentarians. 2019 *Annual Report.* annual_report_2019_public_en.pdf (nsicop-cpsnr.ca)

North American Treaty Organization. *Standardization Agreement 4715: Biometrics Data Exchange.* Brussels: NATO Standardization Office, 2021.

United States. US Department of Defense. "Commander's Guide to Biometrics in Afghanistan" CALL-AfghanBiometrics.pdf (publicintelligence.net).

DEFINITIONS

1. **Biometrics**: A process that enables the automated recognition of individuals based on their behavioural and biological characteristics

2. **Biometric collection**: The physical process of obtaining biometric data and related contextual data from an individual. This term does not imply either retention or deletion of that data. NATO uses the term “capture” to denote this process.

3. **Biometric data**: A biometric sample or aggregation of biometric samples at any stage of processing. Note: Biometric data includes, but is not limited to, fingerprints, facial images, iris scan, voice recognition, keystroke, handprint, and deoxyribonucleic acid (DNA).

4. **Enrolment**: The process of collecting biometric and contextual data from an individual, converting it into a biometric reference, and retaining it in a database for later comparison and sharing.

5. **Intelligence**: The product resulting from the collection, processing, analysis, integration, and interpretation of available information concerning foreign states, hostile or potentially hostile forces or elements, geography and social and cultural factors that contributes to the understanding of an actual or potential operating environment. Note 1: The term “intelligence” also applies to the activities that result in the product and to the organizations engaged in such activities.

6. **Latent Biometric Collection**: The acquisition of biometric samples that originate from residue that is dormant, inactive, non-evident and not directly obtained from living beings. Also referred to as Forensic.

7. **Screening**: The one-to-many process of comparing a piece of collected biometric data against all of the biometric data on file to determine whether it matches any of the data and, if so, the known identity of the individual whose data was matched. Practically, this is accomplished by comparing to either a Biometrically Enabled Watchlist (BEWL), or an authoritative database.

8. **Verification**: The one-to-one process of comparing an individual’s biometric data against their stored biometric data on file to determine whether it matches.