Analysis of Interoperability Factors Involved in the Sharing of Biometric Data

(STO-TM-SAS-135)

Executive Summary

The adoption of security measures based on biometrics has proven to be extremely important for NATO Nations, especially in the Joint Operation Areas (JOAs). The possibility of using biometrics to screen employees when recruiting local personnel for a base or to identify criminals involved in the use of Improvised Explosive Devices (IED), has triggered some NATO Nations to create biometric databases and Biometrically Enabled Watch Lists (BEWLs). NATO itself has implemented the NATO Automated Biometric Identification System (NABIS)[1], developed as part of the Defence Against Terrorism Program of Work (DAT POW) managed by the Emerging Security Challenges Division (ESCD). Despite its potentially high value for NATO Nations and, indirectly, for some NON-MIL Entities (such as national law enforcement agencies), in very general terms and except for JOAs, the biometric data acquired by a NATO military force cannot be shared. This is mainly due to legal and constitutional constraints, but also technical problems related to interoperability. The primary goal of the SAS-135 Research Task Group (RTG) was the identification of such barriers and the promotion of the NATO biometric standard (STANAG 4715). STANAG 4715 is not probably sufficiently known outside of NATO and its adoption could boost collaboration between MIL and NON-MIL entities.

[1] Niculescu, B.R and Coman, C. (2017). NATO Automated Biometric Identification System (NABIS), MTA Review, Vol. 27(2), Dec.

Analyse des facteurs d'interopérabilité impliqués dans le partage des données biométriques

(STO-TM-SAS-135)

Synthèse

L'adoption de mesures de sécurité fondées sur la biométrie s'est révélée extrêmement importante pour les pays de l'OTAN, en particulier dans les zones d'opération interarmées (JOA). La possibilité d'utiliser la biométrie pour examiner les antécédents des employés pendant le recrutement du personnel local d'une base ou d'identifier les criminels impliqués dans l'utilisation d'engins explosifs improvisés (EEI) a poussé certains pays de l'OTAN à créer des bases de données biométriques et des listes de surveillance liées à la biométrie (BEWL, Biometrically Enabled Watch List). L'OTAN elle-même utilise le NABIS, système automatisé d'identification biométrique de l'OTAN,[2] développé dans le cadre du programme de travail pour la défense contre le terrorisme (DAT POW) géré par la Division Défis de sécurité émergents (ESCD). Malgré leur valeur potentiellement élevée pour les pays de l'OTAN et, indirectement, pour certaines entités non militaires (telles que les Forces de Sécurité Intérieure (FSI)), les données biométriques acquises par une force militaire de l'OTAN, en termes extrêmement généraux et à l'exception des zones d'opération interarmées (JOA), ne peuvent pas être partagées. Cela découle principalement de contraintes juridiques et constitutionnelles, mais également de problèmes techniques liés à l'interopérabilité. Le but principal du groupe de recherche (RTG) SAS-135 était d'identifier les obstacles de ce type et de promouvoir la norme biométrique de l'OTAN (STANAG 4715). La STANAG 4715 n'est probablement pas suffisamment connue en dehors de l'OTAN et son adoption pourrait stimuler la collaboration entre les entités militaires et non militaires.

[2] Niculescu, B.R et Coman, C. (2017). NATO Automated Biometric Identification System (NABIS), MTA Review, Vol. 27(2), déc 2017.