NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(SAS-135)TP/1073

www.sto.nato.int

STO TECHNICAL MEMORANDUM **TM-SAS-135**

Analysis of Interoperability Factors Involved in the Sharing of Biometric Data

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

This report documents the findings of the SAS-135 Research Task Group.

Published December 2022

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(SAS-135)TP/1073

www.sto.nato.int

STO TECHNICAL MEMORANDUM **TM-SAS-135**

Analysis of Interoperability Factors Involved in the Sharing of Biometric Data

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

This report documents the findings of the SAS-135 Research Task Group.

Authors: A. Altomonte, R. Breen, L. Darke,

B. Greene, M. Savastano, E. Vaucher-Grondin,

The NATO Science and Technology Organization

Science & Technology (S&T) in the NATO context is defined as the selective and rigorous generation and application of state-of-the-art, validated knowledge for defence and security purposes. S&T activities embrace scientific research, technology development, transition, application and field-testing, experimentation and a range of related scientific activities that include systems engineering, operational research and analysis, synthesis, integration and validation of knowledge derived through the scientific method.

In NATO, S&T is addressed using different business models, namely a collaborative business model where NATO provides a forum where NATO Nations and partner Nations elect to use their national resources to define, conduct and promote cooperative research and information exchange, and secondly an in-house delivery business model where S&T activities are conducted in a NATO dedicated executive body, having its own personnel, capabilities and infrastructure.

The mission of the NATO Science & Technology Organization (STO) is to help position the Nations' and NATO's S&T investments as a strategic enabler of the knowledge and technology advantage for the defence and security posture of NATO Nations and partner Nations, by conducting and promoting S&T activities that augment and leverage the capabilities and programmes of the Alliance, of the NATO Nations and the partner Nations, in support of NATO's objectives, and contributing to NATO's ability to enable and influence security and defence related capability development and threat mitigation in NATO Nations and partner Nations, in accordance with NATO policies.

The total spectrum of this collaborative effort is addressed by six Technical Panels who manage a wide range of scientific research activities, a Group specialising in modelling and simulation, plus a Committee dedicated to supporting the information management needs of the organization.

- AVT Applied Vehicle Technology Panel
- HFM Human Factors and Medicine Panel
- IST Information Systems Technology Panel
- NMSG NATO Modelling and Simulation Group
- SAS System Analysis and Studies Panel
- SCI Systems Concepts and Integration Panel
- SET Sensors and Electronics Technology Panel

These Panels and Group are the power-house of the collaborative model and are made up of national representatives as well as recognised world-class scientists, engineers and information specialists. In addition to providing critical technical oversight, they also provide a communication link to military users and other NATO bodies.

The scientific and technological work is carried out by Technical Teams, created under one or more of these eight bodies, for specific research activities which have a defined duration. These research activities can take a variety of forms, including Task Groups, Workshops, Symposia, Specialists' Meetings, Lecture Series and Technical Courses.

The content of this publication has been reproduced directly from material supplied by STO or the authors.

Published December 2022

Table of Contents

List of Acronyms

AIntP	NATO Allied Intelligence Publication
COE	Centre of Excellence
CSO	NATO Science and Technology Organization Collaboration Support Office
ESCD	NATO Emerging Security Challenges Division
FCC	Five Countries Conference
IED	Improvised Explosive Devices
ISAF	International Security Assistance Force
LEA	Law Enforcement Agency
MIL	Military
MoD	Ministry of Defence
MCM	Military Committee Memorandum
NABIS	NATO Automated Biometric Identification System
NBPCG	NATO Biometrics Programme Coordination Group
NON-MIL	Non-Military
PBM	Panel Business Meeting
RTG	Research Task Group
SAS	System Analysis and Studies, one of the six STO Technical Panels.
SHAPE	NATO Supreme Headquarters Allied Powers Europe (Mons, BEL)
STANAG	Standardization Agreement.
STRATCOM	Strategic Communication
STO	NATO Science and Technology Organization

Glossary

Centre of Excellence	International military organisations that train and educate leaders and specialists from NATO member and partner countries.
International Security Assistance Force	NATO-led military mission in Afghanistan, established by the United Nations Security Council in December 2001 by Resolution 1386.
Military Committee Memorandum	A document in which the Military Committee issues views, guidance, requests, advice, or instructions for immediate or near-term use.
Non-Military	In the context of this document, any civilian entity potentially interested in the sharing of biometric data.
System Analysis and Studies	One of the six STO Technical Panels.
Standardization Agreement	A STANAG defines processes, procedures, terms, and conditions for common military or technical procedures or equipment between the member countries of the Alliance.
Strategic Communication	A term that refers to policy-making and guidance for consistent information activity within an organisation and between organisations.

SAS-135 Membership List

CO-CHAIRS

Mr. Alessandro ALTOMONTE
Secretariat General of Defence/National Armaments Directorate
ITALY
Email: r5finanziario@sgd.difesa.it

Mr. Mario SAVASTANO
IBB – CNR
ITALY
Email: mario.savastano@cnr.it

MEMBERS

Mr. Robert BREEN
Ministry of Defence Expertise Center
C-IED Biometrics
NETHERLANDS
Email: r.breen@mindef.nl

Mr Brian GREENE
DRDC
CANADA
Email: brian.greene@forces.gc.ca

Mr. Leonard DARKE
Headquarters, United States Marine Corps, C4
UNITED STATES
Email: leonard.darke@usmc.mi

ADDITIONAL CONTRIBUTOR

Mrs. Estelle VAUCHER-GRONDIN
Central Office for Combatting Crimes against Humanity, Genocides and War Crimes
FRANCE
Email: estelle.vaucher-grondin@gendarmerie.interieur.gouv.fr

PANEL/GROUP MENTOR

Mr. Alessandro ALTOMONTE
Secretariat General of Defence/National Armaments Directorate
ITALY
Email: r5finanziario@sgd.difesa.it

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.

ANALYSIS OF INTEROPERABILITY FACTORS INVOLVED IN THE SHARING OF BIOMETRIC DATA

1.0 INTRODUCTION

The SAS-135 Research Task Group on the "Analysis of interoperability factors involved in the sharing of biometric data" was created in 2017 with the explicit aim of:

1) Analysing the barriers to sharing biometric data among the Ministries (or Departments) of Defence of the NATO Nations and
2) Analysing the conditions for improving a dialogue between MIL and NON-MIL entities (such as Law Enforcement Agencies) on a possible biometric data sharing.

A group of experts from Canada, France, Italy, the Netherlands, and the United States of America contributed to the activities of the RTG and joined the meetings that were held in France at the STO CSO of Neuilly (Paris) and in Rome (Italy).

The present document highlights the main points of the RTG's activity. It was drafted during the last meeting held at the CSO in December 2019. The document was subsequently expanded and a revised version reflecting recommendations received at the April 2020 SAS PBM, was drafted in July 2020. The document was further amended in 2021 and 2022 in the light of further comments received.

1.1 Biometrics

Biometrics is the automated recognition of individuals based on their behavioural and biological characteristics. Using biometrics as a means of identifying individuals within the operational environment has various advantages if compared to the traditional methods of using text-based identification [1].

Common biometric characteristics are:

- Fingerprints;
- Face
- Iris;
- DNA; and
- Voice.

1.1.1 Behavioural Biometrics

Some biometric modalities are defined as "behavioural" since they are based on the recognition of behavioural characteristics of the individuals. The list includes the analysis of keystroke dynamics, gait, voice, and signature dynamics. The recognition of voice characteristics[1] is the only behavioural biometric in scope with the present document.

2.0 BACKGROUND AND JUSTIFICATION

"Terrorists (including foreign terrorist fighters, returnees and relocators) have developed the skills to move across borders without being detected or identified" [2]. This threat reinforces the necessity of increasing the sharing of biometric data, collected in the MIL and NON-MIL contexts.

[1] The biometric characteristics of voice include both physical and behavioural elements.

Biometric technologies, which embed an identity to a physical and/or behavioural characteristic of an individual, represent a powerful countermeasure to anonymity and have proved to be a robust and reliable tool in a wide number of applications.

In 2012 NATO adopted a Biometrics Framework (MCM 0050-2012), setting the stage for a capability that had been used in operations but lacked a NATO guidance, partnering capabilities, and training to solidify its use in multi-national operations.

To coordinate cooperation among NATO Nations, the NATO Emerging Security Challenges Division (ESCD) created a Coordination Group, the NATO Biometrics Programme Coordination Group (NBPCG).

On 7 December 2017, the SAS-135 RTG activity was presented at the NBPCG Senior Level Meeting held at the NATO Supreme Headquarters Allied Powers Europe (SHAPE) in Mons (BEL).

3.0 OBJECTIVES

The objectives of the SAS-135 RTG were:

1) To disseminate in the NON-MIL area information about standards for biometrics interoperability developed in the MIL context (STANAG 4715); and
2) To increase awareness in the NON-MIL context about the activities on biometrics carried out by NATO.

4.0 TECHNICAL TEAM LEADER AND LEAD NATION

Chair: Lieutenant Colonel, Alessandro Altomonte, Italy

Lead Nation: Italy.

5.0 PARTICIPATING NATIONS

NATO Nations and Bodies: Canada, France, Italy, Netherlands, United States.

PfP Nations: None.

MD Nations: None.

ICI Nations: None.

Global Partners: None.

Contact/Other Nations: None.

6.0 STATUS OF ACTIVITIES

The status of the RTG's initiative is complete. This Technical Memorandum reports on the activities of the Group.

7.0 LIAISON WITH OTHER BODIES

There were no formal liaisons with other bodies, but the objectives and progress of the SAS-135 RTG were periodically presented to NATO Biometrics Programme Coordination Group (NBPCG) meetings.

8.0 LOCATION AND DATES

Activity Start: December 2017.

Activity End: December 2019 (effective August 2020).

Location: The SAS-135 RTG meetings were held at the NATO CSO in Neuilly-sur-Seine (FRA) and in Rome (ITA).

9.0 RECOMMENDATIONS OR FEEDBACK FOR THE ACTIVITY CHAIR

During the April 2020 45th SAS PBM, the Review Groups produced an Activity Review Feedback on the SAS-135 RTG. It recommended converting the activity report into a Technical Memorandum with additional details on the following points.

9.1 Clarify Whether Behavioural Characteristics Are in Scope or Not

Section 1.1.1 on Behavioural Biometrics (see p. 1 of the present document) provides a clarification about this issue.

9.2 Report is Short on Detail: Clarify What Work Was Done by the Group

The basis for the creation of the SAS-135 RTG was the assumption that the sharing of MIL biometric data among NATO Nations presents a significant level of complexity.

The RTG tried to identify how it would be possible to increase the biometric data sharing and started to analyse the agreements to be proposed in order to achieve better cooperation among the concerned Entities.

Particular emphasis was given to the most appropriate modalities (i.e., an ad hoc STRATCOM) to stress the importance of adopting a common technical language to share data.

The two identified macro-areas of difficulty for the biometric data sharing are mainly of technical (i.e., lack of adherence to STANAG 4715) and legal/juridical nature (i.e., data protection issues and the nature of national constitutional frameworks).

While technical issues appear possible to resolve thanks to the adoption of common standards, legal and juridical aspects look particularly intricate. For example, the ownership of the biometric data, in case of sharing and the inherited responsibilities of the national entity receiving the data from another national entity represent two difficult areas requiring further clarification.

In the course of the activities, the RTG considered various effective biometric data-sharing scenarios, (in the MIL as NON-MIL contexts) and for these analysed the solutions found and the inhibiting factors.

Outcomes

The main outcomes of the RTG were:

- The advantages offered by the sharing of biometric data among NATO Nations are evident, but the number of Nations actively involved in the discussion is still limited.
- NATO Nations involved in joint operations and missions (such as NTM-I, NMI, ISAF, RSM, KFOR) are more interested in addressing the difficulties associated with the use of biometrics and biometric data sharing (the sharing of biometric data is currently only permitted in JOAs).

- The rotation policy that interests the MIL is a crucial factor because quite often the skill of a group involved in biometrics is reduced or, in some cases, lost when some key persons have to be deployed to another duty.
- While there are NON-MIL networks that allow international biometric data sharing (e.g., the Prüm Convention in force among several EU Nations and the Five Country Conference (FCC) involving the immigration authorities of Australia, Canada, New Zealand, the United Kingdom, and the United States), there are no similar capabilities in the MIL area. To the aim of increasing the circulation of biometric data among the MoD of the NATO Nations, it would be particularly interesting to carefully analyse the juridical and constitutional premises that made possible the biometric data sharing in the above-mentioned NON-MIL programmes.
- NATO has created its own database for the common management of biometric data (NATO Automatic Biometrics Identification System – NABIS). It became immediately clear that: i) The adoption of a common standard (STANAG 4715) is a key issue; and ii) The modality of how to share data is a fundamental point.
- The interaction between MIL and NON-MIL data is also a problem in relations with international organisations. For example, Interpol is an international law enforcement organisation that runs on LEA data. MIL data is connected to INTEL issues, and it is not common for Interpol to be allowed to use MIL data (only on special request).
- As concerns the convergence between MIL and NON-MIL biometric data, the adoption of common standards is a crucial point and the advantages offered by the adoption of STANAG 4715 should be highlighted to NON-MIL entities.
- Dialogue among the MIL and NON-MIL communities is a fundamental step to opening a discussion on how to approach the existing legal and constitutional barriers. An appropriate STRATCOM should be prepared.

9.3 A Summary of National Biometric Data Sharing Policies Would Be Useful

A summary of national biometric data sharing policies will be provided if a new study in the area of biometrics is proposed at the next PBM.

9.4 If Possible, Develop a Short Paper on Observed NATO Policy Gaps to Enable Exploitation of the Awareness Created

A short paper on observed NATO policy gaps will be provided if a new study in the area of biometrics is proposed at the next PBM.

10.0 RECOMMENDATIONS TO THE PANEL/GROUP OR THE SCIENCE AND TECHNOLOGY BOARD (STB)

Activity Chair to the Panel

The activity carried out by the SAS-135 RTG represents a starting point in a complex area crucial for NATO Nations. Several lessons have been learned during the activity, mainly that there is a gap between the military and the civilian contexts in the area of biometrics and that this gap is very difficult to fill. This is due to a number of factors, such as the level of confidentiality that characterizes the MIL data and the dependence of the data sharing on national juridical frameworks. The role of the civilians is fundamental because they have the potential power to trigger a parliamentary discussion and consequently the creation of new legal frameworks for the sharing of data, with particular reference to biometrics. A second lesson learned is that an activity on so complex an area requires large participation of NATO Nations, so a large consensus will be a necessary condition if a proposal for a continuation of the activity on biometrics is to be approved.

11.0 REFERENCES

[1] NATO. AINTP-15 (23 Feb 2016). Countering Threat Anonymity: Biometrics in Support of NATO Operations and Intelligence.

[2] Biometrics Insitute. (2018). A Summary of the United Nations Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism. https://www.biometricsinstitute.org/wp-content/uploads/UNOCT-Biometrics-Summary-Bro_WEB.pdf

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	STO-TM-SAS-135 AC/323(SAS-135)TP/1073	ISBN N/A	PUBLIC RELEASE

5. Originator

Science and Technology Organization
North Atlantic Treaty Organization
BP 25, F-92201 Neuilly-sur-Seine Cedex, France

6. Title

Analysis of Interoperability Factors Involved in the Sharing of Biometric Data

7. Presented at/Sponsored by

This report documents the findings of the SAS-135 Research Task Group.

8. Author(s)/Editor(s)	9. Date
A. Altomonte (Editor), R. Breen, L. Darke, B. Greene, M. Savastano (Co-Editor), E. Vaucher-Grondin	December 2022

10. Author's/Editor's Address	11. Pages
Multiple	20

12. Distribution Statement

There are no restrictions on the distribution of this document. Information about the availability of this and other STO unclassified publications is given on the back cover.

13. Keywords/Descriptors

Biometrics; Data sharing; NATO Biometrics Programme Coordination Group (NBPCG); Standardization

14. Abstract

Data oriented to the fight against terrorism and criminality should represent a common resource to be shared among all concerned parties. In reality, as shown in the aftermath of several terrorist attacks, the sharing of such kind of data, at international level, is difficult. In particular, biometric data is especially valuable given its role in identifying persons of interest. The MIL Forces of several NATO Nations have acquired a considerable experience in the use of biometrics and an amount of biometric data has been collected. Although it would be helpful if this data could be shared, national legislations pertaining data collected in a military operation, along with a technical fragmentation in terms of standardization, currently, make biometric data sharing a complex task.

NORTH ATLANTIC TREATY ORGANIZATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

SCIENCE AND TECHNOLOGY ORGANIZATION

DIFFUSION DES PUBLICATIONS
STO NON CLASSIFIEES

Les publications de l'AGARD, de la RTO et de la STO peuvent parfois être obtenues auprès des centres nationaux de distribution indiqués ci-dessous. Si vous souhaitez recevoir toutes les publications de la STO, ou simplement celles qui concernent certains Panels, vous pouvez demander d'être inclus soit à titre personnel, soit au nom de votre organisation, sur la liste d'envoi.

Les publications de la STO, de la RTO et de l'AGARD sont également en vente auprès des agences de vente indiquées ci-dessous.

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivi du numéro de série. Des informations analogues, telles que le titre est la date de publication sont souhaitables.

Si vous souhaitez recevoir une notification électronique de la disponibilité des rapports de la STO au fur et à mesure de leur publication, vous pouvez consulter notre site Web (http://www.sto.nato.int/) et vous abonner à ce service.

CENTRES DE DIFFUSION NATIONAUX

ALLEMAGNE
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7, D-53229 Bonn

BELGIQUE
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research
for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30, 1000 Bruxelles

BULGARIE
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

CANADA
DGSIST 2
Recherche et développement pour la défense Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

DANEMARK
Danish Acquisition and Logistics Organization
(DALO)
Lautrupbjerg 1-5
2750 Ballerup

ESPAGNE
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

ESTONIE
Estonian National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

ETATS-UNIS
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc
BP 72
92322 Châtillon Cedex

GRECE (Correspondant)
Defence Industry & Research General
Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HONGRIE
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

ITALIE
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301
00175, Rome

LUXEMBOURG
Voir Belgique

NORVEGE
Norwegian Defence Research
Establishment
Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

PAYS-BAS
Royal Netherlands Military
Academy Library
P.O. Box 90.002
4800 PA Breda

POLOGNE
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

REPUBLIQUE TCHEQUE
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18
197 06 Praha 9

ROUMANIE
Romanian National Distribution
Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

ROYAUME-UNI
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down
Salisbury SP4 0JQ

SLOVAQUIE
Akadémia ozbrojených síl gen.
M.R. Štefánika, Distribučné a
informačné stredisko STO
Demänová 393
031 01 Liptovský Mikuláš 1

SLOVENIE
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

TURQUIE
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi
Başkanlığı
06650 Bakanliklar – Ankara

AGENCES DE VENTE

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
ROYAUME-UNI

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2
CANADA

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivie du numéro de série (par exemple AGARD-AG-315). Des informations analogues, telles que le titre et la date de publication sont souhaitables. Des références bibliographiques complètes ainsi que des résumés des publications STO, RTO et AGARD figurent dans le « NTIS Publications Database » (http://www.ntis.gov).

NORTH ATLANTIC TREATY ORGANIZATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

SCIENCE AND TECHNOLOGY ORGANIZATION

DISTRIBUTION OF UNCLASSIFIED STO PUBLICATIONS

AGARD, RTO & STO publications are sometimes available from the National Distribution Centres listed below. If you wish to receive all STO reports, or just those relating to one or more specific STO Panels, they may be willing to include you (or your Organisation) in their distribution.

STO, RTO and AGARD reports may also be purchased from the Sales Agencies listed below.

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number. Collateral information such as title and publication date is desirable.

If you wish to receive electronic notification of STO reports as they are published, please visit our website (http://www.sto.nato.int/) from where you can register for this service.

NATIONAL DISTRIBUTION CENTRES

BELGIUM
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30
1000 Brussels

BULGARIA
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

CANADA
DSTKIM 2
Defence Research and Development Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

CZECH REPUBLIC
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18
197 06 Praha 9

DENMARK
Danish Acquisition and Logistics Organization (DALO)
Lautrupbjerg 1-5
2750 Ballerup

ESTONIA
Estonian National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc – BP 72
92322 Châtillon Cedex

GERMANY
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7
D-53229 Bonn

GREECE (Point of Contact)
Defence Industry & Research General Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HUNGARY
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

ITALY
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301
00175, Rome

LUXEMBOURG
See Belgium

NETHERLANDS
Royal Netherlands Military Academy Library
P.O. Box 90.002
4800 PA Breda

NORWAY
Norwegian Defence Research Establishment, Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

POLAND
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

ROMANIA
Romanian National Distribution Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

SLOVAKIA
Akadémia ozbrojených síl gen M.R. Štefánika, Distribučné a informačné stredisko STO
Demänová 393
031 01 Liptovský Mikuláš 1

SLOVENIA
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

SPAIN
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

TURKEY
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi Başkanlığı
06650 Bakanliklar – Ankara

UNITED KINGDOM
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down, Salisbury SP4 0JQ

UNITED STATES
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

SALES AGENCIES

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
UNITED KINGDOM

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2
CANADA

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number (for example AGARD-AG-315). Collateral information such as title and publication date is desirable. Full bibliographical references and abstracts of STO, RTO and AGARD publications are given in "NTIS Publications Database" (http://www.ntis.gov).