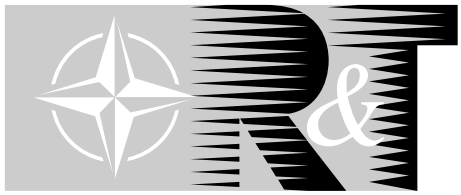
RTO-MP-101
AC/323(IST-033)TP/18

RTO-MP-101

NORTH ATLANTIC TREATY ORGANISATION



RESEARCH AND TECHNOLOGY ORGANISATION

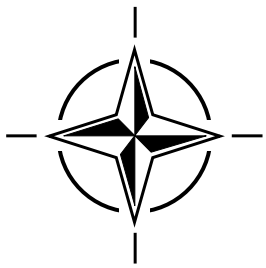
BP 25, 7 RUE ANCELLE, F-92201 NEUILLY-SUR-SEINE CEDEX, FRANCE

RTO MEETING PROCEEDINGS 101

Real Time Intrusion Detection

(La détection des intrusions en temps réel)

Papers presented at the RTO Information Systems Technology Panel (IST) Symposium held in Estoril, Portugal, 27-28 May 2002.



Published June 2003

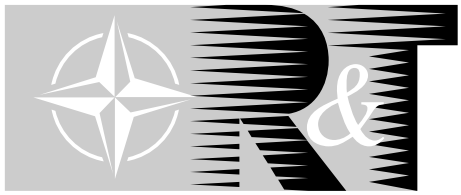
Distribution and Availability on Back Cover

This page has been deliberately left blank

Page intentionnellement blanche

RTO-MP-101
AC/323(IST-033)TP/18

NORTH ATLANTIC TREATY ORGANISATION



RESEARCH AND TECHNOLOGY ORGANISATION

BP 25, 7 RUE ANCELLE, F-92201 NEUILLY-SUR-SEINE CEDEX, FRANCE

RTO MEETING PROCEEDINGS 101

Real Time Intrusion Detection

(La détection des intrusions en temps réel)

Papers presented at the RTO Information Systems Technology Panel (IST) Symposium held in Estoril, Portugal, 27-28 May 2002.

The Research and Technology Organisation (RTO) of NATO

RTO is the single focus in NATO for Defence Research and Technology activities. Its mission is to conduct and promote cooperative research and information exchange. The objective is to support the development and effective use of national defence research and technology and to meet the military needs of the Alliance, to maintain a technological lead, and to provide advice to NATO and national decision makers. The RTO performs its mission with the support of an extensive network of national experts. It also ensures effective coordination with other NATO bodies involved in R&T activities.

RTO reports both to the Military Committee of NATO and to the Conference of National Armament Directors. It comprises a Research and Technology Board (RTB) as the highest level of national representation and the Research and Technology Agency (RTA), a dedicated staff with its headquarters in Neuilly, near Paris, France. In order to facilitate contacts with the military users and other NATO activities, a small part of the RTA staff is located in NATO Headquarters in Brussels. The Brussels staff also coordinates RTO's cooperation with nations in Middle and Eastern Europe, to which RTO attaches particular importance especially as working together in the field of research is one of the more promising areas of initial cooperation.

The total spectrum of R&T activities is covered by the following 7 bodies:

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

These bodies are made up of national representatives as well as generally recognised 'world class' scientists. They also provide a communication link to military users and other NATO bodies. RTO's scientific and technological work is carried out by Technical Teams, created for specific activities and with a specific duration. Such Technical Teams can organise workshops, symposia, field trials, lecture series and training courses. An important function of these Technical Teams is to ensure the continuity of the expert networks.

RTO builds upon earlier cooperation in defence research and technology as set-up under the Advisory Group for Aerospace Research and Development (AGARD) and the Defence Research Group (DRG). AGARD and the DRG share common roots in that they were both established at the initiative of Dr Theodore von Kármán, a leading aerospace scientist, who early on recognised the importance of scientific support for the Allied Armed Forces. RTO is capitalising on these common roots in order to provide the Alliance and the NATO nations with a strong scientific and technological basis that will guarantee a solid base for the future.

Published June 2003

ISBN 92-837-0032-5

Printed by St. Joseph Print Group Inc.
(A St. Joseph Corporation Company)
1165 Kenaston Street, Ottawa, Ontario, Canada K1G 6S1

Real Time Intrusion Detection

(RTO MP-101 / IST-033)

Executive Summary

Within NATO member nations and coalition partners there will be an increasing dependence on communication and information systems (CIS) to ensure the success of military operations, including mission critical operations. Also the interconnection of coalition CIS and the growing use of commercial-off-the-shelf software increases the risk of intrusions from external and internal sources. To minimize losses and ensure the continuous operation of CIS, there is a recognised need for a real-time, automated response to intrusions.

One of the important prerequisites for an appropriate response is the timely detection of intrusions, and this forms the background for the symposium.

The symposium includes two keynote addresses and seventeen papers discussing several aspects of the theme. The papers are presented in six technical sessions.

The first keynote address, entitled **Networked Systems Survivability Program**, is about the possibility of building survivable systems instead of continuing to correct the inadequacies of the systems being built today. The second keynote address, entitled **Building Secure Software**, is about taking security into account during all phases of development and ensuring that software developers get proper security training.

The first technical session, entitled **Real-time Intrusion Detection, Overview and Practical Experience** has 3 papers. They give an overview of the topics of the theme and point out some of the challenges of intrusion detection for the R&D community. In particular, practical experience illustrates the gap between actual needs and the state of intrusion detection systems.

The second technical session, entitled **Correlation and Fusion**, has 3 papers. They discuss technology for the correlation and fusion of intrusion detection information. The technology aims at faster and more reliable detection. One paper discusses fusion at the alert level.

The third technical session, entitled **Insider Threat Detection**, has 2 papers. The insider threat is a big challenge, because intrusion by authorized users may imply more severe consequences. Although several papers in the symposium deal with this aspect, the two papers selected for this session reflect the topic in specific environments.

The fourth technical session, entitled **Real-time Data Analysis and Processing** has 3 papers. It is obvious that a real time analysis of intrusion detection data is a very convenient way for real-time detection. The papers discuss anomaly detection techniques, clustering techniques, and data reduction techniques to increase speed of the analysis.

The fifth technical session entitled **Real Time Decision Support and Visualisation**, has 3 papers. The topics of this session are related to the fact that incident response will often include human decisions, thus intrusion detection systems must provide reliable information for decision making, e.g. appropriate visualisations of intrusions.

The sixth technical session, entitled **Intrusion Detection for Real Time and Time Service Dependent Applications**, has 3 papers. For real time applications, such as multimedia traffic and IP telephony, the detection of attacks on time dependency require special methods and technologies. Examples of real time applications are multimedia traffic and IP telephony. There is also a paper about a time-dependent service – thus attacks on time synchronisation can lead to unreliable service. Future intrusion detection systems must deal with this too.

The presentations at the symposium illustrate some R&D initiatives which will enable more reliable and timely detection of intrusions, but more improvements are still needed as basis for real-time automated response to intrusions. It is important for NATO to carefully monitor developments and apply the solutions so as to gain experience in military environments.

La détection des intrusions en temps réel

(RTO MP-101 / IST-033)

Synthèse

A l'avenir, la réussite des opérations militaires, y compris les opérations indispensables à la mission, conduites par les pays membres de l'OTAN et les partenaires d'une coalition, dépendra de plus en plus de l'efficacité des systèmes de communication et d'information (CIS). Aussi, l'interconnexion des systèmes CIS de coalition, associée au recours de plus en plus courant qui est fait à des composants du commerce (COTS), a pour effet d'accroître le risque d'intrusions de sources internes et externes. La nécessité de trouver une réponse automatisée aux intrusions, en temps réel, afin de réduire au minimum les pertes et d'assurer le fonctionnement ininterrompu des systèmes CIS, est largement admise.

Ce symposium sur la détection d'intrusions en temps réel a pour origine le sujet de la détection d'intrusions en temps réel, qui est l'une des conditions préalables à l'obtention d'une réponse appropriée.

Le symposium comprend deux discours d'ouverture et dix-sept communications couvrant différents aspects du sujet. Les communications sont présentées en six sessions techniques.

Le premier discours d'ouverture, intitulé **La réalisation de systèmes résistant en réseaux**, examine la possibilité de réaliser des systèmes résistants, pour ne pas avoir à corriger les imperfections des systèmes en cours de fabrication aujourd'hui. Le deuxième discours d'ouverture, intitulé **La création de logiciels protégés**, concerne la prise en compte de la sécurité pendant toutes les phases du développement, ainsi que la nécessité de formation en matière de sécurité pour les réalisateurs de logiciels.

La première session, intitulée **La détection d'intrusions en temps réel : aperçu et expérience**, comporte trois communications. Elles résument les différents sujets du thème, en faisant ressortir certains défis en matière de détection d'intrusions qui seraient à relever par les chercheurs dans ce domaine. En particulier, l'expérience pratique montre l'écart qui existe entre les besoins réels et les performances actuelles des systèmes de détection d'intrusions.

La deuxième session technique, intitulée **La corrélation et la fusion**, comporte trois communications. Elles portent sur les technologies de la corrélation et la fusion des données de détection d'intrusions. Ces technologies visent une détection plus rapide et plus fiable. L'une d'entre elles concerne la fusion au niveau de l'alerte.

La troisième session technique, intitulée **La détection de la menace interne**, comporte deux communications. La menace interne représente un défi important, parce que l'intrusion par des utilisateurs autorisés peut avoir des conséquences plus graves. Bien que cet aspect soit traité par d'autres conférenciers, les deux communications choisies pour cette session examinent le sujet dans le contexte d'environnements spécifiques.

La quatrième session technique, intitulée **L'analyse et le traitement de données en temps réel**, comporte trois communications. Il est un fait certain que l'analyse en temps réel des données de détection d'intrusions est très importante pour la détection en temps réel. Les communications traitent des techniques de détection d'anomalies, des techniques d'agrégation, ainsi que des techniques destinées à accélérer l'analyse.

La cinquième session technique, intitulée **La visualisation et les aides à la prise de décisions**, comporte trois communications. Les sujets couverts par cette session témoignent du fait que la réponse aux incidents implique souvent des décisions humaines et que par conséquent, les systèmes de détection d'intrusions doivent fournir des données fiables, aux fins de la prise de décisions, par exemple des visualisations d'intrusions.

La sixième session technique, intitulée **La détection des intrusions pour applications temps réel et asservies au temps**, comporte trois communications. Pour les applications temps réel, telles que le trafic multimédia, la détection d'attaques sur les fonctions liées au temps, fait appel à des méthodes et à des technologies particulières. Le trafic multimédia et le téléphone Internet sont des exemples d'applications multimédia. Une autre communication présente un service asservi au temps : dans de tels cas, la fiabilité du service peut être compromise par d'éventuelles attaques sur la synchronisation. Les futurs systèmes de détection d'intrusion devront pouvoir traiter cet aspect également.

Les présentations qui seront données lors du symposium renseigneront les participants sur certaines initiatives R&D qui devraient permettre d'obtenir une détection d'intrusions plus prompte et plus fiable, mais la réponse aux intrusions automatisée en temps réel ne sera obtenue que suite à d'autres améliorations encore. Il est important pour les pays membres de l'OTAN de suivre de près les développements dans ce domaine et d'appliquer les solutions trouvées afin d'acquérir de l'expérience dans des environnements militaires.

Click inside the blue boxes or on the titles to view the corresponding section

Contents

SESSION III: INSIDER THREAT DETECTION
Chairman: Dr H. STEINHEUER (GE)

SESSION IV: REAL TIME DATA ANALYSIS AND PROCESSING
Chairman: Dr J. LEFEBVRE (CA)

SESSION V: REAL TIME DECISION SUPPORT AND VISUALISATION
Chairman: Dr W. MEES (BE)

SESSION VI: INTRUSION DETECTION FOR REAL TIME AND TIME SERVICE DEPENDENT APPLICATIONS
Chairman: Prof. A. ZUQUETE (PO)

Theme

The extensive and increasing application and use of information and communication technology has created both new capabilities and new vulnerabilities. It is critical to the future of NATO that systems remain robust and retain the confidence of the users. The proliferation of threats to information systems has already been seen in the civil sector. These threats will also impact military operations, especially with the proliferation of commercial-off-the-shelf systems and technology. Probing of computer networks and penetration attacks have already been reported by NATO-member nations and are expected to increase. These threats originate not only from potential military adversaries and state-sponsored terrorists, but also from third parties whose only interest is to disrupt operations. Another problem may be the threat of internally originated attacks or misuse.

The widespread use of information systems for the collection, processing and dissemination of mission critical data and information requires appropriate defences. It is important to understand how to identify unauthorised activities in order to provide a real-time (or near-real-time) automated response to ensure the operation of information systems, which need to be continuously available, including mission critical systems. In this context, a key challenge is the development of systems for real-time detection of intrusions.

The main focus of this symposium is technologies/techniques and tools for real-time intrusion detection. This will include a state-of-the-art overview of research, experiments, and deployment of promising current and new intrusion detection technologies, which have the potential for real-time applications, thereby making it possible to see which technologies and tools could be deployed in the future within NATO and coalition networks.

TOPICS TO BE COVERED:

- Real-time decision support
- High-speed data processing, including pre-processing techniques, data reduction and adaptive filtering
- Advanced real-time data analysis
- Information fusion, including correlation, aggregation, and alignment techniques
- Insider threat detection and intruder profiling
- Expert systems or intelligent assistants for intrusion detection
- Pattern recognition, including Neural Nets (e.g. adaptive resonance techniques)
  On-line visualisation of intrusions and progress thereof

Thème

L'application et l'utilisation largement répandues et croissantes des technologies de l'information et des communications ont créé non seulement de nouvelles capacités mais aussi de nouvelles vulnérabilités. Il est indispensable pour l'avenir de l'OTAN que les systèmes conservent leur robustesse et continuent de mériter la confiance des utilisateurs. La prolifération des menaces sur les systèmes d'information a déjà été remarquée dans le secteur civil. Ces menaces auront également un impact sur les opérations militaires, qui sera amplifié par la prolifération des systèmes et technologies disponibles sur étagère (COTS). Le sondage des réseaux informatiques et des attaques de pénétration ont déjà été signalés par des pays membres de l'OTAN et deviendront sans doute plus nombreux. Ces menaces ont pour origine non seulement des adversaires militaires potentiels et le terrorisme parrainé par l'état, mais aussi des tiers dont le seul intérêt est de perturber les opérations. La menace d'attaques et d'usage abusif d'origine interne est un problème additionnel.

L'utilisation généralisée de systèmes d'information pour la collecte, le traitement et la diffusion de données indispensables à la mission exige des moyens de défense appropriés. Il est important de savoir identifier des activités non autorisées afin de fournir une réponse automatisée en temps réel (ou quasi-réel) pour secourir les systèmes d'information, qui doivent fonctionner en permanence, y compris les systèmes indispensables à la mission. Dans ce contexte, le développement de systèmes assurant la détection d'intrusion en temps réel est l'un des défis clés.

Ce symposium est principalement axé sur les technologies/techniques et outils de détection d'intrusion en temps réel. Le programme comprend un aperçu de l'état actuel des connaissances dans le domaine de la recherche, l'expérimentation et le déploiement des technologies de détection d'intrusion prometteuses actuelles et nouvelles, susceptibles d'être utilisées pour des applications temps réel, et laisse prévoir ainsi les technologies et les outils qui pourraient être déployés à l'avenir au sein des réseaux de l'OTAN et d'éventuelles coalitions.

SUJETS A TRAITER :

- Le soutien de la prise de décisions en temps réel
- Le traitement des données à grande vitesse, y compris les techniques du pré-traitement, la réduction des données et le filtrage adaptatif
- L'analyse des données avancée en temps réel
- La fusion des données, y compris les techniques de corrélation, d'agrégation et d'alignement
- La détection de menaces internes et l'établissement de profils d'intrusion
- Systèmes experts et assistants intelligents pour la détection d'intrusions
- Analyse typologique, y compris les réseaux neuronaux (par exemple les techniques de résonance adaptative)
  La visualisation en ligne d'intrusions et de leur progrès

Information Systems Technology Panel

Acknowledgements/Remerciements

The Panel wishes to express its thanks to the Portuguese members of RTA for the invitation to hold this Symposium in Estoril and for the facilities and personnel which made the Symposium possible.

Le Panel tient à remercier les membres du RTB du Portugal auprès de la RTA de leur invitation à tenir cette réunion à Estoril, ainsi que pour les installations et le personnel mis à sa disposition.

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	RTO-MP-101 AC/323(IST-033)TP/18	ISBN 92-837-0032-5	UNCLASSIFIED/ UNLIMITED

5. Originator Research and Technology Organisation
North Atlantic Treaty Organisation
BP 25, F-92201 Neuilly-sur-Seine Cedex, France

6. Title
Real Time Intrusion Detection

7. Presented at/sponsored by
the RTO Information Systems Technology Panel (IST) Symposium held in Estoril, Portugal, 27-28 May 2002.

8. Author(s)/Editor(s)	9. Date
Multiple	June 2003
10. Author's/Editor's Address	**11. Pages**
Multiple	236 (text) 634 (slides)

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

13. Keywords/Descriptors

Communications management
Communications networks
Computer networks
Computer security
Correlation techniques
Data fusion
Data processing security
Decision support
Denial of service attacks
Electronic security
IDS (Intrusion Detection Systems)
Information systems
Information warfare
Intrusion detectors
Monitors
Network security
Network traffic
Protocols
Real time operations
Reporting
Requirements
Secure communication
Software engineering
Surveillance
Threat evaluation
Traffic simulation
Visualization technologies
Vulnerability

14. Abstract

This volume contains the Technical Evaluation Report, the Keynote Addresses and 17 papers, presented at the Information Systems Technology Panel Symposium held in Estoril, Portugal from 27th to 28th May 2002.

The papers presented covered the following headings:

- Real-Time Intrusion Detection, Overview and Practical Experience
- Correlation and Fusion
- Insider Threat Detection
- Real-Time Data Analysis and Processing
- Real-Time Decision Support and Visualisation
- Intrusion Detection for Real-Time and Time-Service Dependent Applications

This page has been deliberately left blank

Page intentionnellement blanche

NORTH ATLANTIC TREATY ORGANISATION

RESEARCH AND TECHNOLOGY ORGANISATION
BP 25 • 7 RUE ANCELLE
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@rta.nato.int

DIFFUSION DES PUBLICATIONS
RTO NON CLASSIFIEES

L'Organisation pour la recherche et la technologie de l'OTAN (RTO), détient un stock limité de certaines de ses publications récentes, ainsi que de celles de l'ancien AGARD (Groupe consultatif pour la recherche et les réalisations aérospatiales de l'OTAN). Celles-ci pourront éventuellement être obtenues sous forme de copie papier. Pour de plus amples renseignements concernant l'achat de ces ouvrages, adressez-vous par lettre ou par télécopie à l'adresse indiquée ci-dessus. Veuillez ne pas téléphoner.

Des exemplaires supplémentaires peuvent parfois être obtenus auprès des centres nationaux de distribution indiqués ci-dessous. Si vous souhaitez recevoir toutes les publications de la RTO, ou simplement celles qui concernent certains Panels, vous pouvez demander d'être inclus sur la liste d'envoi de l'un de ces centres.

Les publications de la RTO et de l'AGARD sont en vente auprès des agences de vente indiquées ci-dessous, sous forme de photocopie ou de microfiche. Certains originaux peuvent également être obtenus auprès de CASI.

CENTRES DE DIFFUSION NATIONAUX

ALLEMAGNE
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr, (FIZBw)
Friedrich-Ebert-Allee 34
D-53113 Bonn

BELGIQUE
Etat-Major de la Défense
Département d'Etat-Major Stratégie
ACOS-STRAT-STE – Coord. RTO
Quartier Reine Elisabeth
Rue d'Evère, B-1140 Bruxelles

CANADA
DSIGRD2
Bibliothécaire des ressources du savoir
R et D pour la défense Canada
Ministère de la Défense nationale
305, rue Rideau, 9e étage
Ottawa, Ontario K1A 0K2

DANEMARK
Danish Defence Research Establishment
Ryvangs Allé 1, P.O. Box 2715
DK-2100 Copenhagen Ø

ESPAGNE
INTA (RTO/AGARD Publications)
Carretera de Torrejón a Ajalvir, Pk.4
28850 Torrejón de Ardoz - Madrid

ETATS-UNIS
NASA Center for AeroSpace Information (CASI)
Parkway Center
7121 Standard Drive
Hanover, MD 21076-1320

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
Department for Scientific Analysis
Institute of Military Technology
Ministry of Defence
H-1525 Budapest P O Box 26

ISLANDE
Director of Aviation
c/o Flugrad
Reykjavik

ITALIE
Centro di Documentazione Tecnico-Scientifica della Difesa
Via XX Settembre 123a
00187 Roma

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
Armament Policy Department
218 Niepodleglosci Av.
00-911 Warsaw

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

REPUBLIQUE TCHEQUE
DIC Czech Republic-NATO RTO
VTÚL a PVO Praha
Mladoboleslavská ul.
Praha 9, 197 06, Česká republika

ROYAUME-UNI
Dstl Knowledge Services
Kentigern House, Room 2246
65 Brown Street
Glasgow G2 8EX

TURQUIE
Millî Savunma Başkanliği (MSB)
ARGE Dairesi Başkanliği (MSB)
06650 Bakanliklar - Ankara

AGENCES DE VENTE

NASA Center for AeroSpace Information (CASI)
Parkway Center
7121 Standard Drive
Hanover, MD 21076-1320
Etats-Unis

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 K1A 0S2, Canada

Les demandes de documents RTO ou AGARD doivent comporter la dénomination "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 RTO et AGARD figurent dans les journaux suivants:

Scientific and Technical Aerospace Reports (STAR)
STAR peut être consulté en ligne au localisateur de ressources uniformes (URL) suivant:
http://www.sti.nasa.gov/Pubs/star/Star.html
STAR est édité par CASI dans le cadre du programme NASA d'information scientifique et technique (STI)
STI Program Office, MS 157A
NASA Langley Research Center
Hampton, Virginia 23681-0001
Etats-Unis

Government Reports Announcements & Index (GRA&I)
publié par le National Technical Information Service
Springfield
Virginia 2216
Etats-Unis
(accessible également en mode interactif dans la base de données bibliographiques en ligne du NTIS, et sur CD-ROM)

Imprimé par Groupe d'imprimerie St-Joseph inc.
(Membre de la Corporation St-Joseph)
1165, rue Kenaston, Ottawa (Ontario), Canada K1G 6S1

NORTH ATLANTIC TREATY ORGANISATION

RESEARCH AND TECHNOLOGY ORGANISATION
BP 25 • 7 RUE ANCELLE
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Telefax 0(1)55.61.22.99 • E-mail mailbox@rta.nato.int

DISTRIBUTION OF UNCLASSIFIED
RTO PUBLICATIONS

NATO's Research and Technology Organisation (RTO) holds limited quantities of some of its recent publications and those of the former AGARD (Advisory Group for Aerospace Research & Development of NATO), and these may be available for purchase in hard copy form. For more information, write or send a telefax to the address given above. **Please do not telephone**.

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

RTO and AGARD publications may be purchased from the Sales Agencies listed below, in photocopy or microfiche form. Original copies of some publications may be available from CASI.

NATIONAL DISTRIBUTION CENTRES

BELGIUM
Etat-Major de la Défense
Département d'Etat-Major Stratégie
ACOS-STRAT-STE – Coord. RTO
Quartier Reine Elisabeth
Rue d'Evère, B-1140 Bruxelles

CANADA
DRDKIM2
Knowledge Resources Librarian
Defence R&D Canada
Department of National Defence
305 Rideau Street, 9th Floor
Ottawa, Ontario K1A 0K2

CZECH REPUBLIC
DIC Czech Republic-NATO RTO
VTÚL a PVO Praha
Mladoboleslavská ul.
Praha 9, 197 06, Česká republika

DENMARK
Danish Defence Research Establishment
Ryvangs Allé 1, P.O. Box 2715
DK-2100 Copenhagen Ø

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)
Friedrich-Ebert-Allee 34
D-53113 Bonn

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

HUNGARY
Department for Scientific Analysis
Institute of Military Technology
Ministry of Defence
H-1525 Budapest P O Box 26

ICELAND
Director of Aviation
c/o Flugrad
Reykjavik

ITALY
Centro di Documentazione Tecnico-Scientifica della Difesa
Via XX Settembre 123a
00187 Roma

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
Armament Policy Department
218 Niepodleglosci Av.
00-911 Warsaw

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

SPAIN
INTA (RTO/AGARD Publications)
Carretera de Torrejón a Ajalvir, Pk.4
28850 Torrejón de Ardoz - Madrid

TURKEY
Millî Savunma Başkanliği (MSB)
ARGE Dairesi Başkanliği (MSB)
06650 Bakanliklar - Ankara

UNITED KINGDOM
Dstl Knowledge Services
Kentigern House, Room 2246
65 Brown Street
Glasgow G2 8EX

UNITED STATES
NASA Center for AeroSpace Information (CASI)
Parkway Center
7121 Standard Drive
Hanover, MD 21076-1320

SALES AGENCIES

NASA Center for AeroSpace Information (CASI)
Parkway Center
7121 Standard Drive
Hanover, MD 21076-1320
United States

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 K1A 0S2, Canada

Requests for RTO or AGARD documents should include the word '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 RTO and AGARD publications are given in the following journals:

Scientific and Technical Aerospace Reports (STAR)
STAR is available on-line at the following uniform resource locator:
http://www.sti.nasa.gov/Pubs/star/Star.html
STAR is published by CASI for the NASA Scientific and Technical Information (STI) Program
STI Program Office, MS 157A
NASA Langley Research Center
Hampton, Virginia 23681-0001
United States

Government Reports Announcements & Index (GRA&I)
published by the National Technical Information Service
Springfield
Virginia 22161
United States
(also available online in the NTIS Bibliographic Database or on CD-ROM)

Printed by St. Joseph Print Group Inc.
(A St. Joseph Corporation Company)
1165 Kenaston Street, Ottawa, Ontario, Canada K1G 6S1

ISBN 92-837-0032-5