



AC/323(IST-049)TP/193



www.rto.nato.int

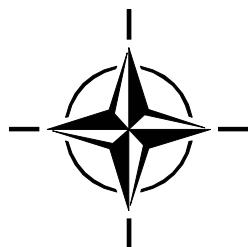
RTO TECHNICAL REPORT

TR-IST-049

Improving Common Security Risk Analysis

(Amélioration d'un processus commun
d'analyse de risques sécurité)

Final Report of Task Group IST-049.



Published September 2008





AC/323(IST-049)TP/193



www.rto.nato.int

RTO TECHNICAL REPORT

TR-IST-049

Improving Common Security Risk Analysis

(Amélioration d'un processus commun
d'analyse de risques sécurité)

Final Report of Task Group IST-049.

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 co-operative 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 co-ordination 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 co-ordinates RTO's co-operation 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 co-operation.

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 System Analysis and Studies 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 co-operation 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.

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

Published September 2008

Copyright © RTO/NATO 2008
All Rights Reserved

ISBN 978-92-837-0045-6

Single copies of this publication or of a part of it may be made for individual use only. The approval of the RTA Information Management Systems Branch is required for more than one copy to be made or an extract included in another publication. Requests to do so should be sent to the address on the back cover.

Table of Contents

	Page
List of Figures/Tables	vi
Membership of Task Group	vii

Executive Summary and Synthèse	ES-1
---------------------------------------	-------------

Chapter 1 – Versions	1-1
-----------------------------	------------

Chapter 2 – Introduction	2-1
2.1 Rationale	2-1
2.2 References to Risk Assessment and Risk Analysis within NATO Documentation	2-1
2.3 Role of Risk Analysis	2-1
2.4 Glossary	2-5
2.5 References	2-7
2.6 Reference Web Sites	2-8
2.7 Scope and Objectives	2-8
2.8 Acknowledgment	2-8

Chapter 3 – Review of Existing Methodologies	3-1
---	------------

3.1 Overview of the Selected Methodologies	3-1
3.1.1 CRAMM	3-1
3.1.1.1 Introduction	3-1
3.1.1.2 Description	3-1
3.1.2 EBIOS ®	3-3
3.1.2.1 History	3-3
3.1.2.2 Description	3-4
3.1.3 Overview of Canadian TRA Methodology	3-9
3.1.3.1 Using TRA in Risk Management	3-9
3.1.3.2 Risk Management Tools	3-10
3.1.4 US	3-15
3.1.4.1 Introduction	3-15
3.1.4.2 Objective	3-15
3.1.4.3 Basic Risk Management	3-15
3.1.4.4 Department of Defense (DoD) Information Technology Security Certification and Accreditation Process (DITSCAP)	3-21
3.1.4.5 Conclusion	3-21
3.1.5 Czech Methodology	3-22
3.1.6 Spanish Method MAGERIT	3-23
3.1.6.1 Step 1: Assets	3-24

3.1.6.2	Step 2: Threats	3-24
3.1.6.3	Step 4: Determination of the Impact	3-25
3.1.6.4	Step 5: Determination of the Risk	3-26
3.1.6.5	Step 3: Safeguards	3-27
3.1.6.6	Revision of Step 4: Residual Impact	3-27
3.1.6.7	Revision of Step 5: Residual Risk	3-28
3.2	Comparative Analysis	3-28
3.3	Alternative Methods	3-35

Chapter 4 – Common Criteria and Risk Analysis **4-1**

4.1	Common Method Using Common Criteria	4-1
4.1.1	Similarities and Differences Between CC and TRA	4-2
4.1.2	Using CC with TRA	4-2
4.1.3	Protection Profile and TRA	4-4
4.2	Critical Aspects of Common Criteria Evaluation	4-4
4.2.1	CC and TRA Summary	4-6
4.3	Security Requirements and CC	4-7

Chapter 5 – Risk Analysis Tools **5-1**

5.1	Existing Tools	5-1
5.1.1	EBIOS Tool	5-1
5.1.2	CRAMM	5-1
5.1.3	RISKAN	5-1
5.1.4	PILAR / EAR	5-1
5.1.5	Comparative Analysis	5-1

Chapter 6 – Definition of a Common Methodology **6-1**

6.1	The Different Components of Risk Analysis	6-1
6.2	Generic Risk Assessment Framework	6-1

Chapter 7 – Recommendations **7-1**

7.1	Dynamic Risk Analysis	7-1
7.2	Information Exchange Requirements	7-1
7.2.1	For Systems Interconnections	7-1
7.2.2	To Update a Common Threat and Vulnerability Repository	7-1
7.2.3	Within a Coalition	7-1
7.3	Proposed Evolutions of Existing Methods and Tools	7-3
7.4	Follow on Activities	7-3
7.4.1	Within RTO/IST	7-3
7.4.2	Within Other NATO Entities	7-4

Annex A – Composed Systems **A-1**

A.1	Composed Systems	A-1
-----	------------------	-----

A.2	Vertical Assurance	A-2
A.3	Structural Assurance	A-2
A.4	A Note on Complexity Theory	A-3

Annex B – Examples of Attack Methods (from EBIOS) **B-1**

Annex C – Examples **C-1**

C.1	Asset Types	C-1
C.2	Threats Description	C-12
C.3	Vulnerabilities Description	C-12

List of Figures/Tables

Figure		Page
Figure 2-1	Risk Management Process	2-2
Figure 3-1	High Level Structure of CRAMM Methodology	3-2
Figure 3-2	Risk Management Model	3-10
Figure 3-3	Risk Assessment Methodology Flow Chart	3-16
Figure 3-4	Risk Decision Flow Chart	3-19
Figure 3-5	Risk Management Process	3-20
Figure 3-6	Risk Management Cycle	3-20
Figure 3-7	MAGERIT Main Steps	3-23
Figure 3-8	MAGERIT Main Steps, including Safeguards	3-27
Figure 7-1	DRA, Alternative Architectures for Coalitions	7-2

Table

Table 3-1	Potential of the Attacker	3-8
Table 3-2	TRA Process Tasks	3-12
Table 3-3	Likelihood Definitions	3-17
Table 3-4	Magnitude of Impact Definitions	3-18
Table 3-5	Comparative Analysis	3-29
Table 4-1	CC V 2.1 Documents Useful for TRA	4-3
Table 5-1	Comparative Analysis	5-2
Table 6-1	Generic Risk Assessment Framework	6-2

Membership of Task Group

Task Group Chairman

Dip. Eng Jean-Pierre LEBEE
DGA/DCE/CELAR
BP 7, 35998 RENNES Armées
France

Jean-Pierre.lebee@dga.defense.gouv.fr
Tel: +33 (0) 2 99.42.98.68
Fax: +33 (0) 2 99.42.64.50

Task Group Members

BELGIUM

Maj. Dr. Wim MEES
Ecole Royale Militaire
Computer Science Department
30 Renaissancelaan
B-1000 Brussels
[Email: Wim.Mees@rma.ac.be](mailto:Wim.Mees@rma.ac.be)
Tel: +32 (2) 737.65.13
Fax: +32 (2) 737.65.12

CANADA

Dr. Jean SAVOIE
Defence R&D Canada – Ottawa
3701 Carling Ave
Ottawa, Ontario K1A 0Z4
[Email: Jean.savioie@drdc-rddc.gc.ca](mailto:Jean.savioie@drdc-rddc.gc.ca)
Tel: +1 (613) 993-5132
Fax: +1 (613) 993-9940

CZECH REPUBLIC

Dip. Ir. Michal VANECEK
T-SOFT s.r.o., Novodvorská 1010/14
142 01 Prague 4
[Email: vanecek@tsoft.cz](mailto:vanecek@tsoft.cz)
Tel: +420 (2) 61.34.87.38
Fax: +420 (2) 61.34.87.91

UNITED STATES

Ms. Phyllis JENKET
Code 5544, Naval Research Laboratory
4555 Overlook Ave SW
Washington DC, 20375-5337
[Email: phyllis.jenket@navy.mil](mailto:phyllis.jenket@navy.mil)
Tel: 001.843.218.5444

Mr. Rodney STALKER
Code 5541
Naval Research Laboratory
4555 Overlook Ave SW
Washington, DC 20375-5337
[Email: rodney.stalker@navy.mil](mailto:rodney.stalker@navy.mil)
Tel: 001.301.757.2986

NATO C3 AGENCY

Dip. Eng Frederic JORDAN
INFOSEC & Cyber Defence
Senior INFOSEC Engineer
NATO C3 Agency, PO Box 174
2501 CD, The Hague
Netherlands
[Email: Frederic.JORDAN@nc3a.nato.int](mailto:Frederic.JORDAN@nc3a.nato.int)
Tel: 31-70-374-3486

NHQC3S

Dip. Eng Franck ROUSSET
Staff Officer
Boulevard Léopold III
B-1110 Brussels
Belgium
[Email: f.rousset@hq.nato.int](mailto:f.rousset@hq.nato.int)
Tel: +32 (0)2 707 54 24
Fax: +32 (0)2 707 58 34



REPORT DOCUMENTATION PAGE																					
1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document																		
	RTO-TR-IST-049 AC/323(IST-049)TP/193	ISBN 978-92-837-0045-6	UNCLASSIFIED/ UNLIMITED																		
5. Originator	Research and Technology Organisation North Atlantic Treaty Organisation BP 25, F-92201 Neuilly-sur-Seine Cedex, France																				
6. Title	Improving Common Security Risk Analysis																				
7. Presented at/Sponsored by	Final Report of Task Group IST-049.																				
8. Author(s)/Editor(s)	Multiple		9. Date September 2008																		
10. Author's/Editor's Address	Multiple		11. Pages 100																		
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	<table> <tbody> <tr> <td>Communications networks</td> <td>Network security</td> <td>Surveillance</td> </tr> <tr> <td>Computer networks</td> <td>Risk</td> <td>Systems analysis</td> </tr> <tr> <td>Computer security</td> <td>Risk analysis</td> <td>Threat and risk analysis</td> </tr> <tr> <td>Data processing security</td> <td>Secure communication</td> <td>Threat evaluation</td> </tr> <tr> <td>Information systems</td> <td>Software engineering</td> <td>Vulnerability</td> </tr> <tr> <td>Monitors</td> <td>Standards</td> <td></td> </tr> </tbody> </table>			Communications networks	Network security	Surveillance	Computer networks	Risk	Systems analysis	Computer security	Risk analysis	Threat and risk analysis	Data processing security	Secure communication	Threat evaluation	Information systems	Software engineering	Vulnerability	Monitors	Standards	
Communications networks	Network security	Surveillance																			
Computer networks	Risk	Systems analysis																			
Computer security	Risk analysis	Threat and risk analysis																			
Data processing security	Secure communication	Threat evaluation																			
Information systems	Software engineering	Vulnerability																			
Monitors	Standards																				
14. Abstract	<p>This report is the final report resulting from the four meetings of the working group called "Improving Common Security Risk Analysis" (IST-049 – RTG-021). The report describes the different methods used by various NATO countries. As a first conclusion, the report shows that these methodologies, even if based on similar principles, differ in their knowledge bases or type of results. This makes the risk assessments difficult or impossible to compare when different methods have been used. In a second part, the report identifies the main steps which are considered as mandatory for a method to be used by NATO. Then the report identifies recommendations which should be taken into account by the existing methods and tools in order to solve the interoperability problem identified in the first part of the document but also to be able to take into account the new NATO concepts such as NNEC. The final chapter of the report identifies the follow on activities to be conducted within RTO/IST or within other NATO entities.</p>																				





BP 25
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

Les publications de l'AGARD et de la RTO peuvent parfois être obtenues 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 soit à titre personnel, soit au nom de votre organisation, sur la liste d'envoi.

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

Les demandes de documents RTO ou AGARD doivent comporter la dénomination « 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 RTO au fur et à mesure de leur publication, vous pouvez consulter notre site Web (www.rto.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 RTO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30, 1000 Bruxelles

CANADA

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

DANEMARK

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

ESPAGNE

SDG TECEN / DGAM
C/ Arturo Soria 289
Madrid 28033

ETATS-UNIS

NASA Center for AeroSpace Information (CASI)
7115 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

NASA Center for AeroSpace Information (CASI)

7115 Standard Drive
Hanover, MD 21076-1320
ETATS-UNIS

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

HONGRIE

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

ITALIE

General Secretariat of Defence and
National Armaments Directorate
5th Department – Technological
Research
Via XX Settembre 123
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

Centralny Ośrodek Naukowej
Informacji Wojskowej
Al. Jerozolimskie 97
00-909 Warszawa

PORTRUGAL

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

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 K1A 0S2, CANADA

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)



BP 25

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



DISTRIBUTION OF UNCLASSIFIED RTO PUBLICATIONS

AGARD & RTO publications are sometimes available from the National Distribution Centres listed below. If you wish to receive all RTO reports, 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 reports may also be purchased from the Sales Agencies listed below.

Requests for RTO or AGARD documents should include the word '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 RTO reports as they are published, please visit our website (www.rto.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 RTO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30
1000 Brussels

CANADA

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

CZECH REPUBLIC

LOM PRAHA s. p.
o. z. VTÚLaPVO
Mladoboleslavská 944
PO Box 18
197 21 Praha 9

DENMARK

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

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

NASA Center for AeroSpace Information (CASI)

7115 Standard Drive
Hanover, MD 21076-1320
UNITED STATES

HUNGARY

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

ITALY

General Secretariat of Defence and
National Armaments Directorate
5th Department – Technological
Research
Via XX Settembre 123
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

Centralny Ośrodek Naukowej
Informacji Wojskowej
Al. Jerozolimskie 97
00-909 Warszawa

PORTUGAL

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

SALES AGENCIES

The British Library Document Supply Centre

Boston Spa, Wetherby
West Yorkshire LS23 7BQ
UNITED KINGDOM

ROMANIA

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

SLOVENIA

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

SPAIN

SDG TECEN / DGAM
C/ Arturo Soria 289
Madrid 28033

TURKEY

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

UNITED KINGDOM

Dstl Knowledge and Information
Services
Building 247
Porton Down
Salisbury SP4 0JQ

UNITED STATES

NASA Center for AeroSpace
Information (CASI)
7115 Standard Drive
Hanover, MD 21076-1320

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 2216
UNITED STATES
(also available online in the NTIS Bibliographic Database or on CD-ROM)