



North Atlantic Treaty Organization

Research and Technology Agency

CALL FOR PAPERS

INFORMATION SYSTEMS TECHNOLOGY PANEL SYMPOSIUM (IST-086/RSY-019)

C3I FOR CRISIS, EMERGENCY AND CONSEQUENCE MANAGEMENT

UNCLASSIFIED/UNLIMITED
Open to PfP nations



to be held in

Bucharest, Romania, 11-12 May 2009

DEADLINE FOR EXTENDED ABSTRACTS or RECEIPT OF PAPERS: 15 February 2009

RTA Headquarters -BP 25 -F-92201 Neuilly-sur-Seine Cedex - France

IST Panel Executive: Tel: +33 (1) 55 61 22 80 - Fax: +33 (1) 55 61 96 07 -E-Mail: maestriv@rta.nato.int

IST Panel Assistant: Tel: +33 (1) 55 61 22 82 -Fax: +33 (1) 55 61 96 26 - E-Mail: apaydina@rta.nato.int

THEME

The events of September 11, 2001 moved the issues of anti- and counter-terrorism, national/public security, and collective emergency response (both crisis and consequence management) to the fore of concerns of many nations. Critical infrastructures, major events (e.g. Olympics), harbours and airports protection against terrorist attack are examples of kinds of complex situations typical of the post 9/11 new security paradigm. In the event of a large-scale terrorist emergency situation, that would necessitate the ability to coordinate multi-agency and multi-national operations and during peace support operations, advanced decision support, knowledge exploitation, information fusion and knowledge management tools can significantly improve the ability to respond to such emergency. Among key issues are national security policies and the roles of NATO. Approaches and technologies aiding military experts to work together effectively with other civil authorities at all levels, and international allies shall be conceptualized. This shall yield to a collaborative environment that would support the fusion of various perspectives to better interpret the situation and the problem, identify candidate actions, formulate evaluation criteria, decide on what to do, and synchronize a diverse set of plans and actions .

The military viewpoint alone is not sufficient to meet the increase in terrorist threat that is diverse and unpredictable; as such threat requires a consideration of collective security that expands to cooperation with multiple non-military organisations (e.g. major events, harbour protection). Actually, working effectively in terrorist emergency situations requires the ability to communicate and to coordinate multi-national and multi-agency operations in a seamless environment. There are vast quantities of data and information requiring weeding, sorting, and analysis. Clearly, advanced information and knowledge management technology, for example, is required to enable the emergency response communities to timely and securely access data, information, services, etc. relevant to their roles and responsibilities, regardless of what agency operates the facilities where the critical data and services reside.

Domain characteristics: (non-exhaustive)

Thinking about the collective response to large-scale emergencies caused by terrorism, one can identify a number of characteristics of this domain:

- Diversity in the nature of operations involving different civilian organisations with different doctrines.
- Geographically dispersed operations.
- Large number and diversity of data, information and knowledge types and sources.
- Large number and diversity of services, applications, tools and products types and sources.
- The environment continually adjusts to expanding information technology capabilities.

Needs: (non-exhaustive)

In response to a crisis, emergency, the decision makers at all levels (e.g., incident commanders) and their staff need:

- to rapidly develop situational awareness (e.g., understand how a situation has developed and is expected to develop);
- to rapidly develop shared understandings of the operational environment;
- to plan operations considering the existence of different emergency plans and/or procedures used by different organisations or parties ;
- to timely disseminate plans (complete or partial) to the appropriate parties to allow immediate or short-term execution as required by the criticality of the situation;
- to monitor the situation and the execution of the plans
- to modify dynamically the plans according to the evolution of the situation;
- to ensure that each individual worker is productive and concentrated in its assigned roles and tasks;
- to ensure that the workers (participants) have the ability to consider and handle the different organisational cultures, processes and leaderships coming from the organisations involved;

- to deal with complex crises;
- to deal with multiple, simultaneous crises (e.g., multiple operations monitoring).

Limitations: (non-exhaustive)

- The required data, information and knowledge and the services, applications, tools and products originate from various stovepipe systems that are technically and semantically heterogeneous.
- The information is not provided or accessed in a timely fashion because of the high operational tempo.
- There is a significant information overload (e.g., a huge quantity of messages at a high rate of message reception).
- There are limitations in timely fusing the information of different natures.
- There are information management constraints because of different security domains.
- There is a lack of tools to understand how a situation has developed and is expected to develop.
- There are limited visualization capabilities.
- There are limited decision-aid / planning tools.
- Decisions are being made on incomplete / unreliable information
- Lack of collaborative tools,
- Lack of common ontology of the domain,
- Lack of upper ontologies that bridge the gap between partly similar domains,
- Lack of information exchange model
- Lack of knowledge management capabilities to capture and exploit corporate knowledge

Objective:

The objective of this Symposium is to address key issues and concepts that could overcome the limitations listed above taking into account the complexity of the domain (see the domain characteristics). The main topics to be covered to help military organisations working together effectively with other civil authorities at all levels, National and International allies for the management of a Collective Response to a Crisis/Emergency are:

- Decision-support;
- Information management;
- Human systems integration;
- Knowledge management in crisis and emergency situations;
- Distributed collaborative planning.

The Symposium will address a number of current NATO priorities, including NATO Rapid Response, and Defence against terrorism (DAT).

SYMPOSIUM TOPICS

The Symposium will examine the systems, technology and C2 issues for Crisis, Emergency and Consequence Management of a multi-national force operating in multi-jurisdiction multi-national military and civil environments. Its topics will include:

1. Scenarios for and threats to responders operating for anti- and counter-terrorism, national/public security, collective emergency response (both crisis and consequence management) and peace support operations. Critical infrastructures, major events (e.g. Olympics), harbours and airports protection against terrorist attack are examples of kinds of complex situations typical of the post 9/11 new security paradigm.

2. Advanced information and knowledge management technologies to enable the emergency response communities to timely and securely access data, information, services, etc. relevant to their roles and responsibilities, regardless of what agency operates the facilities where the critical data and services reside.
3. Advanced decision support and human system integration concepts to enhance the ability to coordinate multi-agency and multi-national operations responding to an emergency.
4. Knowledge exploitation, information fusion and knowledge management tools to enhance situation awareness of complex situations.
5. Collaborative approaches and technologies to support the development and execution of a collective response (plans) to a crisis and emergency situation in multi-jurisdiction environment.

THEME

Les événements du 11 septembre, 2001 ont porté au premier plan pour beaucoup de pays, les questions du contre-terrorisme, de la sécurité publique, de la réponse et de la gestion des crises et des urgences. Les infrastructures critiques, les événements majeurs, la protection des ports et des aéroports contre des attaques terroristes sont des exemples de situations complexes auxquelles ont doit faire face suite au 11 sept.

Dans l'éventualité d'un acte terroriste créant une situation d'urgence à grande échelle, ainsi que durant les opérations de soutien pour la paix, on aurait besoin de systèmes d'aide à la décision et d'outils d'exploitation de connaissances, de fusion d'information et de gestion de connaissances. Ceci faciliterait la coordination des opérations entre les différentes agences nationales et autres pour répondre à telle urgence.

Parmi les questions importantes sont les politiques nationales de sécurité et les rôles de l'OTAN. Il faut identifier des approches et technologies pour aider les experts militaires à travailler en collaboration de façon efficace à tous les niveaux avec des autorités civiles et alliées. On devrait viser un environnement de collaboration où la fusion de perspectives diverses amènerait une meilleure compréhension de la situation et du problème pour ainsi faciliter la formulation de plans d'actions coordonnés.

Le seul point de vue militaire n'est pas suffisant pour adresser la menace terroriste grandissante. Cette menace qui se présente sous formes diverses et imprévisibles. Il faut considérer une approche collective impliquant la coopération avec de multiples organisations civiles facilitée par un environnement où la communication et la coordination des opérations se fait sans heurts entre les différents intervenants. Il y a une énorme quantité d'information et de données qui nécessite d'être analysées et triées. A titre d'exemple, il est certain que les technologies de gestion de l'information et de la connaissance aideraient les communautés devant répondre à une urgence à avoir accès à temps et de façon sécuritaire aux données, à l'information, aux services, ...etc, relevant de leurs rôles et responsabilités nonobstant l'agence où ces services et données résident.

Les caractéristiques du domaine: (non-exhaustif)

Les caractéristiques du domaine parlant d'une réponse collective à une situation de crise provoquée par un incident terroriste sont:

- *La nature diverse des opérations impliquant les différentes organisations civiles de doctrines diverses.*
- *Les opérations sont géographiquement distribuées.*
- *Une grande quantité et diversité de types, de sources de données, d'information et de connaissances.*
- *Une grande quantité et diversité de types, de sources de services, d'applications, d'outils et de produits.*

- L'environnement s'ajuste continuellement à l'évolution des technologies de l'information.

Les besoins: (non-exhaustif)

Pour répondre à une urgence, une crise, les décideurs à tous niveaux et leurs équipes ont besoin de:

- Rapidement acquérir un éveil situationnel (ex. de comprendre rapidement comment une situation est en train d'évoluer et de prédire l'aboutissement);
- Rapidement acquérir une compréhension commune et partagée de l'environnement opérationnel;
- De planifier des opérations considérant l'existence des différents plans d'urgence et procédures utilisés par les différents intervenants;
- De distribuer les plans à temps aux différents intervenants pour action immédiate requise par l'urgence de la situation;
- De surveiller la situation et l'exécution des plans;
- De modifier de façon dynamique les plans selon l'évolution de la situation;
- De s'assurer que chaque travailleur individuel est productif et concentre sur ses tâches et rôle;
- De s'assurer que chaque participant peut faire face aux cultures, processus et leaderships provenant des différentes organisations;
- De faire face à la complexité des crises;
- De faire face à de multiples crises simultanées (ex., le monitoring de plusieurs opérations simultanées).

Limites: (non-exhaustif)

- Les données, l'information, les connaissances, les services, les applications, les outils et les produits proviennent de systèmes isolés variés qui sont techniquement et sémantiquement hétérogènes.
- L'accès à l'information ne se fait pas à temps à cause du tempo des opérations.
- Il y a une surcharge d'information (une très grande quantité de messages).
- Des limites pour fusionner l'information de nature diverses.
- Des contraintes liées à la gestion d'information provenant de différents domaines de sécurité.
- Un manque d'outils pour supporter la compréhension de comment une situation se développe et évolue.
- Des limites en visualisation, aides à la décision, planification et outils collaboratifs.
- Manque d'une ontologie du domaine et d'un modèle d'échange d'information.
- Manque de capacités en gestion de la connaissance pour capturer et exploiter la connaissance corporative.

Objectif:

L'objectif de ce symposium est d'adresser comment on pourrait surmonter les limites d'une réponse collective à une situation de crise provoquée par un incident terroriste prenant en compte les caractéristiques et des besoins listés plus haut. Les principaux sujets à être couverts pour aider les organisations militaires à travailler efficacement avec les autorités civiles à tous les niveaux, national, international pour la gestion d'une réponse collective à une situation de crise/urgence sont :

- Aide à la décision;
- Gestion de l'information;
- Intégration humains-machines;
- Gestion des connaissances pour les situations d'urgences et de crises;
- Planification collaborative distribuée.

Le symposium adressera un nombre de priorité de l'OTAN dont la 'défense et réponse rapide à des actes terroristes'.

SUJETS DU SYMPOSIUM

Le Symposium étudiera les problèmes reliés aux systèmes et technologies du C2 pour la gestion des urgences, crises et conséquences pour une force multinationale opérant dans un environnement multinational, multi-juridiction, civil-militaire. Les thèmes suivants seront abordés :

1. Les scénarios et menaces dans le cadre – une réponse collective à anti et contre terrorisme, sécurité nationale et publique, situations de crise, protection des infrastructures critiques, événements majeurs (ex. olympiques), ports et aéroports.
2. Les technologies de gestion de l'information et de la connaissance aidant les communautés devant répondre à une urgence à avoir accès à temps et de façon sécuritaire aux données, à l'information, aux services, ...etc., relevant de leurs rôles et responsabilités nonobstant l'agence où ces services et données résident.
3. Concepts d'intégration humain-machine et systèmes d'aide à la décision pour améliorer la coordination des opérations multi-agences multinationales répondant à une crise ou urgence.
4. Outils d'exploitation et de gestion des connaissances, de fusion d'information, pour améliorer l'éveil situationnel de situations complexes.
5. Approches et technologies de collaboration pour supporter le développement et l'exécution d'une réponse collective à une crise ou urgence dans un environnement multi-juridiction.

SUBMISSION INSTRUCTIONS

Authors are invited to submit completed papers or extended abstracts which should provide an explicit statement of the content of the paper and its relevance to the symposium (abstracts should be at least two pages, 1000-1200 words in English). An indication of which symposium topic the paper would logically fit would be of assistance to the Technical Programme Committee who will adjudicate on the papers selected.

In addition, the attached **Questionnaire** (*Annex C*), should be completed and submitted together with the abstract.

This will give the maximum amount of information on the status of feasibility of any project concerned, so that the Technical Programme Committee is able to make clear and complete evaluation of the appropriateness and timely interest of the proposed paper.

First page to include the Title of the Paper followed by the full name of the principal author and co-authors with the respective e-mail addresses. This will assist the administrative process and ensure further communication.

Abstracts and Questionnaires should be sent electronically in PDF, or MS Word format to the Co-Chairmen of the Technical Committee, Dr Eloi Bossé (eloi.bosse@drdc-rddc.gc.ca) and Mr Stéphane Paradis (Stephane.Paradis@drdc.rddc.gc.ca) with a copy to the IST Panel Assistant, Mrs Aysegül Apaydin (apaydina@rta.nato.int). Abstracts may also be lodged via url.

<http://www.rta.nato.int/cfp/IST-086-3090.pdf>

Authors will be notified of the decision by **20 February 2009**.

It is the responsibility of the author to ensure that the paper/abstract receives the necessary clearances before it is forwarded. Please allow sufficient time for the clearance to be issued before the deadline.

EXCEPTION: Authors from the United States must comply with US procedures. (Refer to Annex B)

Authors submitting abstracts should ensure that financial support for attending the Symposium will be available.

IMPORTANT DATES

15 Feb 2009	Submission of papers/extended-abstracts
20 Feb 2009	Notification to authors by Chairman of Technical Programme Committee
20 Feb 2009	Authors to receive full «Instructions to Authors» package from RTA
20 Feb 2009	Authors to start national procedure to obtain the «Presentation/Publication Release and Clearance Certificate (<i>this document will be attached to the «Instructions to Authors» document</i>)
10 Apr 2009	Submission of manuscripts to RTA (electronic by e-mail (Word & pdf), and paper copy by mail)
10 Apr 2009	Submission of «Presentation/Publication Release and Clearance Certificate» to RTA
20 Apr 2009	Submission of the Oral Presentation (by e-mail to RTA)

PAPERS AND PRESENTATIONS

Approximately 15 papers will be presented at the plenary sessions, each author being allocated 40 minutes, with usually thirty minutes for the presentation of their paper and ten minutes for discussion. All papers will be published regardless of their presentation. They should be written and presented in English or in French, the official NATO languages. Simultaneous interpretation will be provided between these two languages at all plenary sessions of the Symposium.

Authors whose papers are accepted will be asked to provide a full version of their paper electronically by e-mail together with a paper copy to be sent by mail to RTA no later than 1 month prior to the symposium. Papers are generally not longer than 15 pages. Detailed instructions (Authors Package) and necessary material will be sent to each "Lead" author of papers by **20 February 2009**.

The oral presentations at the plenary sessions should be an extract of the paper and not a reading of it. Authors are requested to send a copy of the oral presentation (text and visual aids) by e-mail to the IST Panel Assistant well in advance as this copy will be used by the interpreters for simultaneous interpretation as well as downloaded to the laptop or PC at the meeting site before the beginning of the event, allowing a technical check of the equipment as well as putting the presentations in the necessary order. The deadline will be **20 April 2009**.

GENERAL INFORMATION

The Romanian Research & Technology Board (RTB) members have graciously invited the IST Panel to hold this event in their country. The audience will include the RTO/IST Panel Members as well as experts from NATO and Partners for Peace (PfP) nations. The meeting will be Unclassified/Unlimited, open to PfP nations.

The conference will provide a forum for the presentation of research and technological advances by scientists and engineers working in all aspects of C3I technologies. The conference will also feature invited presentations and keynote speeches.

A Meeting Announcement as well as a General Information Package on Bucharest including Hotel Booking Forms will be distributed by RTA in the **beginning of March 2009**.

At the end of the symposium a «**Best Paper Award**» will be assigned by the Technical Programme Committee (TPC) and the IST Panel.

NEW POLICY ON CONFERENCE PROCEEDINGS

Once RTA receives the full version of accepted papers together with their proper Clearance Certificate, these papers will first be available on the RTO website under a Login and password, prior to the meeting.

The final publication will be at a URL address which will be given later together with a login and password, and which will be the official reference of the Meeting Proceedings of this Symposium including the Presentations, Posters, Executive Summary, Abstract and the TER (Technical Evaluation Report). Please take note that RTA reserves the rights to print in the Proceedings any paper or material presented at the meeting.

Enrolments will be made on the RTO web site: www.rto.nato.int (Ref. IST-086)

SYMPOSIUM WEBSITE

A Symposium Website will be created to inform the participants and to advertise the symposium papers and presentations. Once you're enrolled and it has been validated, you will receive a login and password to access the collaborative workspace for this event which will be created on the RTO website.

ADDITIONAL INFORMATION

Authors will be notified by the RTA of the opening of on line enrolment and receive a General Information Package about the Symposium site and the host country by **March 2009**.

Any **questions on the technical aspects of the scientific programme** or the contents of papers should be addressed to the **Programme Committee Co-Chairmen and members**.

Questions on the administrative aspects of this symposium or requests for further information on RTO activities should be addressed to the **IST Panel Office**:

Attn: Mrs Aysegul APAYDIN
IST Panel Assistant
R.T.A.
BP 25, 92201 Neuilly sur Seine, France
Tel: +33 (1) 55 61 22 82
Fax: +33 (1) 55 61 96 26
E-mail: apaydina@rta.nato.int

Authors of papers selected for presentation will not be financially supported by this organisation. You are responsible for your own hotel and travel reservations based on suggestions provided in the General Information Package which we will provide. Expenses for travel and per diem costs are the responsibility of each author's nation.

Thank you for your contributions which are very appreciated by the NATO community.

ADMINISTRATIVE INFORMATION

(Ref.: Symposium (IST-086/RSY-019 on "C3I for Crisis, Emergency and Consequence Management" to be held in Bucharest, Romania, 11-12 May 2009)

For each paper you are submitting, please send a copy of the abstract and of the completed Questionnaire (Parts I and II) to the Technical Programme Committee Co-Chairmen and IST Panel Assistant, early enough to reach them by:

15 FEBRUARY 2009

US AUTHORS: SEE INSTRUCTIONS IN ANNEX B

TECHNICAL PROGRAMME COMMITTEE

Co-Chairmen

Dr. Éloi BOSSE
Defence R&D Canada (DRDC) Valcartier
Head- C2 Decision Support Systems (C2DSS) Section
2459 Pie-XI Blvd North, Val-Bélair,
Quebec G3J 1X5, Canada
Tel: +1 (418) 844 4000 ext. 4478
Blackberry: +1 (418) 454 7359
Fax: +1 (418) 844 4538
E-mail: eloi.bosse@drdc-rddc.gc.ca

Mr. Stéphane PARADIS
Defence R&D Canada-Valcartier
Head/Intelligence & Information (I2) Section
2459 Pie-XI Blvd North
Québec, (Québec), G3J 1X5, Canada
Tel.: +1 (418) 844 4000 ext. 4384
Blackberry: +1 (418) 561 8271
Fax: +1 (418) 844 4538
Email: Stephane.Paradis@drdc-rddc.gc.ca

Members:

CZECH REPUBLIC

Col.Assoc.Prof. Vlastimil MALY
Military Technologies Faculty
Head, of Communication and Information Systems Dept.
Tel: +420 (973) 443 572
E-mail: vlastimil.maly@unob.cz

GERMANY

Dr.-Ing. Michael WUNDER
FGAN/FKIE
(Research Establishment for Communication, Information Processing and Ergonomics)
Head of Department ITF
Tel: +49 (228) 9435 511
E-mail: wunder@fgan.de

THE NETHERLANDS

Ir. Marcel VAN DER LEE
TNO Defence and Security
C4I Expert
Tel: +31 (70) 374 0209
E-mail: marcel.vanderlee@tno.nl

SPAIN

Dr. Manuel ESTEVE
Universidad Politécnica de Valencia
Communications Dept.
Tel: +34 (9) 6387 7305
E-mail: mesteve@com.upv.es

TURKEY

Prof.Dr. Nazife BAYKAL
Middle East Technical University (ODTU)
Informatics Institute
Tel: +90 (312) 210 3742
E-mail: baykal@ii.metu.edu.tr

Mr. Fatih OZCAN
Systems Engineering Division
ASELSAN Inc.
E-mail: fozcan@aselsan.com.tr

UNITED KINGDOM

Prof. Bob MADAHAR
DSTL
Information Dept.
Chief Technologist
Tel: +44 (2392) 21 7369
E-mail: bkmadahar@dstl.gov.uk

UNITED STATES

Dr. Erik BLASCH
AFRL/SNAA
Fusion Evaluation Program Manager
Tel: +1 (937) 904 9077
E-mail: erik.blasch@wpafb.af.mil

INFORMATION SYSTEMS TECHNOLOGY PANEL

IST PANEL EXECUTIVE:

Maj. Vincent MAESTRI, FAF
E-mail: maestriv@rta.nato.int
Tel: +33 (1) 55 61 22 80
Fax: +33 (1) 55 61 96 07

IST PANEL ASSISTANT:

Mrs. Ayşegül APAYDIN
E-mail: apaydina@rta.nato.int
Tel: +33 (1) 55 61 22 82
Fax: +33 (1) 55 61 96 26

From Europe:

RTA/NATO
Attention: IST
BP 25, 7 rue Ancelle
92201 Neuilly-sur-Seine Cedex, France

From the USA or CANADA:

RTA-NATO
Attention: IST
PSC 116
APO AE 09777

**SPECIAL NOTICE TO U.S. AUTHORS
AND
NON-U.S. CITIZENS AFFILIATED WITH U.S. ORGANISATIONS**

(Ref.: Symposium (IST-086/RSY-019) on "C3I for Crisis, Emergency and Consequence Management to be held in Bucharest, Romania, 11-12 May 2009)

**ABSTRACTS OF PAPERS FROM THE U.S. MUST BE SENT ONLY TO THE FOLLOWING
P.O.C.:**

**NATO RTO U.S. National Coordinator
William McCluskey
ODDR&E/International Technology Programs
201 12th St South
Arlington, VA 22202
United States**

Tel: +1 (703) 604-0283

Fax: +1 (703) 604-0293

**E-mail: usnatcor@osd.mil
william.mccluskey@osd.mil**

- 1. ALL U.S. AUTHORS MUST SUBMIT ONE ELECTRONIC COPY TO THIS P.O.C. BY
15 FEBRUARY 2009**

THE P.O.C. WILL FORWARD ALL US ABSTRACTS AS REQUIRED BY THE TECHNICAL PROGRAM COMMITTEE.

- 2. ALL U.S. AUTHORS MUST INCLUDE THE FOLLOWING STATEMENT IN A COVERING LETTER TO THE P.O.C.:**
 - THE WORK DESCRIBED IN THIS ABSTRACT IS CLEARED FOR PRESENTATION TO NATO AUDIENCES;**
 - THE ABSTRACT IS TECHNICALLY CORRECT;**
 - IF WORK IS SPONSORED BY A GOVERNMENT AGENCY, IDENTIFY THE ORGANIZATION AND ATTEST THAT THE ORGANIZATION IS AWARE OF SUBMISSION;**
 - THE ABSTRACT IS NATO/PFP Unclassified; AND**
 - THE ABSTRACT DOES NOT VIOLATE ANY PROPRIETARY RIGHTS.**

This letter or email stating that the above conditions have been met must accompany the abstract submittal to the Programme Committee Acting Co-Chairmen and the appropriate RTA Panel Assistant.

QUESTIONNAIRE

For consideration of a paper submitted for
the Information Systems Technology Panel Symposium on:
C3I FOR CRISIS, EMERGENCY AND CONSEQUENCE MANAGEMENT
(IST-086/RSY-019)
(UNCLASSIFIED/UNLIMITED) Partners for Peace (PfP) nations invited
Bucharest, Romania, 11-12 May 2009

Please attach a copy of this Questionnaire to each copy of abstract

*On each Abstract, authors should be listed in the order they will appear on the programme. Unless specified otherwise, the first listed author will be presumed to be the **LEAD AUTHOR** (i.e. the author having the major responsibility regarding the content of the paper).*

(Please use the TAB key to scroll from one section to the other)

PART 1

TITLE OF PAPER:

Anticipated Security Classification: (*Please choose as appropriate*):

- ORAL PRESENTATION:
- **FINAL MANUSCRIPT:**

TECHNICAL CONTENT

(Please tick the appropriate boxes):

What is the nature of the work reported in the paper?

A. EXPLORATORY DEVELOPMENT

- a. Theoretical research study
- b. Theoretical system or subsystem design

B. ADVANCED DEVELOPMENT

- a. Theoretical study with comparison with practical results
- b. Experimental investigation

**C. PROTOTYPE DEVELOPMENT
or
PRELIMINARY DEVELOPMENT**

D. ENGINEERING DEVELOPMENT

- a. Full scale system development
- b. System trials

PART II: DETAILS OF AUTHORS

CO-AUTHORED PAPERS: Authors should be listed in the order they will appear on the program. Unless specified otherwise, the first listed author will be presumed to be the LEAD AUTHOR (i.e. the author having the major responsibility regarding the content of the paper).

TITLE OF PAPER :

CONCISE BUSINESS MAILING ADDRESS (*include title (Mr, Mrs, Dr, etc.) full name & zip code*)

<p><u>Lead Author:</u></p>

Nationality:

Position in organisation:

Telephone: *Country code:* *Area/town code:* *Number:*

Fax No: *Country code:* *Area/town code:* *Number:*

E-Mail:

[Click here to download the Questionnaire in Word](#)

NATO'S RESEARCH & TECHNOLOGY ORGANIZATION (RTO)

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 Partnership for Peace nations, 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 seven bodies:

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

These bodies are made up of national representatives as well as generally recognized '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 organize 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 recognized the importance of scientific support for the Allied Armed Forces. RTO is capitalizing 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 mission of the Information Systems Technology (IST) Panel is to implement, on behalf of the R&T Board, the RTO Mission with respect to Information Systems Technology. The advancement and exchange of techniques and technologies to provide timely, affordable, dependable, secure and relevant information to warfighters, planners and strategists, as well as enabling technologies for modelling, simulation, and training are the focus of this Panel.

The **Information Systems Technology Panel (IST)** covers the fields of:

- (a) Information Warfare and Assurance,
- (b) Information and Knowledge Management,
- (c) Communications and Networks,
- (d) Architecture and Enabling Technologies.