

# CALL FOR PAPERS

## IST-148/RSY-032 Symposium

## on

## “CYBER DEFENCE SITUATION AWARENESS”

**to be held in**

**Sofia, Bulgaria**

**3 – 4 October 2016**

## 

**DEADLINE FOR RECEIPT OF EXTENDED ABSTRACTS:**

**15 AUGUST 2016**

*(US Authors please check Annex A of this document)*

**This Symposium is Unclassified/Unlimited, open to PfP, Med Dialogue Nations**

**IST Panel Executive: Maj. Luc DETIENNE IST Panel Assistant: Mrs Aysegül APAYDIN**

Tel: +33(0)1 5561 2280 Tel: +33 (0)1 5561 2282

Fax: +33 (0)1 5561 9607 Fax: +33 (0)1 5561 9626

Email: [luc.detienne@cso.nato.int](mailto:luc.detienne@cso.nato.int) Email: [aysegul.apaydin@cso.nato.int](mailto:aysegul.apaydin@cso.nato.int)

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

Tel: +33 (0)1 55 61 22 00 - Fax: +33 (0)1 55 61 22 99 - E-Ma[il : mailbox@cso.nato.int](mailto:mailbox@cso.nato.int)

**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 NAT O’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 Groups 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 Information Systems Technology (IST) Panel**

The mission of the Information Systems Technology (IST) Panel is to implement, on behalf of the S&T Board, the STO 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 war fighters, 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:

* 1. Information Warfare and Assurance,
  2. Architecture and Intelligent Information Systems,
  3. Communications and Networks,

#### TECHNICAL PROGRAMME COMMITTEE

#### Programme Co-Chair men

**Mr. Douglas WIEMER Dr. Robert ERBACHER**

RHEA Group Army Research Laboratory

Canada United States

Email: [d.wiemer@rheagroup.com](mailto:d.wiemer@rheagroup.com) Email: [robert.f.erbacher.civ@mail.mil](mailto:robert.f.erbacher.civ@mail.mil)

**COMMITTEE MEMBERS**

|  |  |
| --- | --- |
| Col.Dr. Nikolai STOIANOV  Defence Institute “Professor Tsvetan Lazarov”  Bulgaria  E-mail: [n.stoianov@di.mod.bg](mailto:n.stoianov@di.mod.bg) | Assoc.Prof.Dr. Maya BOZHILOVA  Defence Institute “Professor Tsvetan Lazarov”  Bulgaria  E-mail: [m.bozhilova@di.mod.bg](mailto:m.bozhilova@di.mod.bg) |
| Prof. Wim MEES  Royal Military Academy  Belgium  E-mail: [wim.mees@rma.ac.be](mailto:wim.mees@rma.ac.be) | Prof. Bob MADAHAR  DSTL  United Kingdom  E-mail: [bkmadahar@dstl.gov.uk](mailto:bkmadahar@dstl.gov.uk) |
| Dr. Jens TÖLLE  Fraunhofer-FKIE  Germany  E-mail: [jens.toelle@fkie.fraunhofer.de](mailto:jens.toelle@fkie.fraunhofer.de) | Prof.Dr. Nazife BAYKAL  Middle East Technical University  Turkey  E-mail: [baykal@metu.edu.tr](mailto:baykal@metu.edu.tr) |
| Maj.Ing. Michal TURCANIK  Armed Forces Academy at Liptovsky Mikulas  Slovak Republic  E-mail: [michal.turcanik@aos.sk](mailto:michal.turcanik@aos.sk) | Dr. Alexander KOTT  US Army Research Laboratory  USA  E-mail: [alexander.kott1.civ@mail.mil](mailto:alexander.kott1.civ@mail.mil) |
| Dr. Margaret Varga  Seetru Ltd./ University of Oxford  United Kingdom  E-mail: [Margaret.varga@seetru.com](mailto:Margaret.varga@seetru.com) | Dr. Reginald Sawilla  NCI Agency  Canada  E-mail: [Reginald.sawilla@ncia.nato.int](mailto:Reginald.sawilla@ncia.nato.int) |
| Mr. Przemyslaw BEREZINSKI  Military Communications Institute  Poland  Email: [p.berezinski@wil.waw.pl](mailto:p.berezinski@wil.waw.pl) | Mr. Mauno PIHELGAS  NATO Cooperative Cyber Defence  Estonia  Email: [mauno.pihelgas@ccdcoe.org](mailto:mauno.pihelgas@ccdcoe.org). |

**IST PANEL OFFICE & POINTS OF CONTACT**

Maj. Luc DETIENNE Mrs. Aysegul APAYDIN

IST Panel Executive IST Panel Assistant

Tel: +33 (0)1 5561 2280 Tel: +33 (0)1 5561 2282

Fax: +33 (0)1 5561 9607 Fax: +33 (0)1 5561 9626

Email: [luc.detienne@cso.nato.int](mailto:luc.detienne@cso.nato.int) E-mail: [aysegul.apaydin@cso.nato.int](mailto:aysegul.apaydin@cso.nato.int)

**BACKGROUND**

NATO 2020 states - Responding to the rising danger of cyber-attacks: NATO must accelerate efforts to respond to the danger of cyber-attacks by protecting its own communications and command systems, helping Allies to improve their ability to prevent and recover from attacks, and developing an array of cyber defence capabilities aimed at effective detection and deterrence.

An important requirement for cyber defence is improved Cyber Defence Situation Awareness (CDSA) of the cyber environment. Research has focused in the areas of situational awareness metrics, visualization and dynamic risk assessment for mission assurance. In addition, several projects have been established which are developing CDSA tools, techniques and technologies, and are at the point where nations can leverage each other’s efforts through international collaboration. The CDSA Symposium is proposed as an opportunity to present current state-of-the-art projects and research activities in the domain of CDSA.

**OBJECTIVE(S) of the Symposium**

The aim of the symposium is to bring together experts and practitioners from NATO member military agencies along with industry leaders and academic visionaries to present and discuss the state-of-the-art developments and hard challenges in cyber defence situational awareness, cyber security and the application and exploration of cyber security metrics, dynamic risk assessment, visualization and visual analytics in cyber defence. The meeting will result in a raised awareness of our common efforts and the development of collaborative opportunities.

**Symposium Topics**

The theoretical and empirical topics to be covered may include but are not limited to:

* Cyber Defence
* Cyber Resiliency
* Current Challenges in Cyber Security
* Cyber Situational Awareness
* Security Metrics
* Dynamic Risk Assessment
* Mission Assurance
* Continuous Monitoring
* Network Analysis and Monitoring
* Visual Analytics
* Case Studies, Best Practices and Lessons Learned
* Evaluation of Situation Awareness effectiveness in CD
* Cyber Security Models and Architectures
* Security Verification, Evaluations and Measurements

#### 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). Submissions are solicited on any of the listed topics, or on any other topic that illuminates any of the themes. 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 to this, we kindly ask each author to fill in a Questionnaire (Part I and II) that you will find in ***Annex B***. 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 contribution.

**EXCEPTION:** Authors from the United States must comply with US procedures. *(Refer to the Instructions in* ***Annex A****)*

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

Please send an electronic copy of the extended abstract and demonstration descriptions together with the completed Questionnaire (Parts I and II) herewith attached (***Annex B***) to the Technical Programme Committee Chairman Mr Douglas Wiemer ([d.wiemer@rheagroup.com](mailto:d.wiemer@rheagroup.com)), with a courtesy copy to the IST Panel Assistant ([aysegul.apaydin@cso.nato.int](mailto:aysegul.apaydin@cso.nato.int)) early enough to reach them by **15 AUGUST 2016**.

#### IMPORTANT DATES

**15 AUGUST 2016 ●** Submission of papers/extended-abstracts

**1 SEPTEMBER 2016 ●** Notification to authors by Chairman of Technical Programme Committee

**●** Authors to receive full «Instructions to Authors» package from CSO

**●** Authors to start national procedure to obtain the «Presentation/Publication   
 Release and Clearance Certificate (Form 13e)   
 *(this document will be attached to the “Instructions to Authors” document)*

**15 SEPTEMBER 2016 ●** Submission of «Presentation/Publication Release and Clearance Certificate»   
 (Form 13e) to CSO

**●** Submission of manuscripts to CSO (electronic by e-mail (Word & PDF)

**15 SEPTEMBER 2016 ●** Submission of the Oral Presentation (by e-mail to CSO)

#### PAPERS and PRESENTATIONS

Approximately 20 to 25 full papers will be presented at the plenary sessions, each author being allocated 30 minutes, with usually twenty minutes for the presentation of their paper and five minutes for discussion. All presented papers will be published. They should be written and presented in English. Authors whose extended abstracts are accepted will be asked to provide a full version of their paper electronically by e-mail. Detailed instructions (Authors Package) and necessary material will be sent to each “Lead” author of papers together with the acceptance notification.

#### GENERAL INFORMATION

The Bulgarian authorities have graciously invited the IST Panel to hold this event in their country. The audience will include the STO/IST Panel Members, experts from NATO nations, as well as potential participants from Partner for Peace or Med. Dialogue nations.

This symposium will bring together both military and civilian users, practitioners, researchers and technologists, with big picture ideals blended with appropriate level of detail. It will also feature invited presentations and keynote speeches.

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

A Meeting Announcement as well as a General Information Package giving further details on the meeting site where the symposium will take place, including Hotel Booking Forms will be available from the CSO website.

Authors will be notified by the IST Panel Office of the opening of on line enrolment on the CSO web site ([www.cso.nato.int](http://www.cso.nato.int/)). It is mandatory for all participants to enrol on this website using the reference IST-148 to get access to the meeting site. The General Information Package (GIP) will be automatically sent once the enrolment is validated, giving further details about the meeting venue, hotel bookings and other necessary information.

#### PUBLICATION OF MEETING PROCEEDINGS

Complete instructions will be sent by the IST Panel Assistant to the lead authors of the selected papers who will be providing a full paper. The Guidelines for authors will detail all requirements and deadlines for the preparation of the final manuscripts and presentations.

All authors will need to provide CSO with a final version of their Paper by **15 SEPTEMBER 2016**, together with the Presentation/Publication Release and Clearance Certificate (Form 13e). Please be reminded that all papers must be written and presented in English.

A week before the Symposium, CSO will pre-release the papers on the CSO website. These papers will be available under a login and password which will be provided by the IST Panel Office.

The final publication (Meeting Proceedings) will be at a URL address which will be given later, together with a login and password. This will represent the official reference of the Meeting Proceedings of this Symposium including the presentations, papers, posters (if any), demonstration videos (if any), an Executive Summary, abstract and the TER (Technical Evaluation Report). Please take note that CSO reserves the right to print in the Proceedings any paper or material presented at the meeting.

Any questions on the technical aspects of the scientific programme or the contents of papers should be addressed to the Programme Committee Chairman and/or members.

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

**Attn:** **Mrs Aysegül APAYDIN**

Information Systems Technology Panel Assistant

Science & Technology Organization/Collaboration Support Office (CSO)

BP 25, 922001 Neuilly sur Seine

France

Tel: +33 (0)1 5561 2282

Fax: +33 (0)1 5561 9626

E-mail: [aysegul.apaydin@cso.nato.int](mailto:aysegul.apaydin@cso.nato.int)

#### SECURITY LEVEL AND CLEARANCE FOR PRESENTATIONS AND PAPERS

It is the responsibility of each contributor to fulfil the publication release and clearance requirements of his/her organization/company and country to obtain clearance of abstracts and papers as needed. An official clearance is mandatory in the United States and there may also be a requirement in other countries to obtain clearance for unclassified as well as classified papers. For further information, authors should contact the appropriate Programme Committee Member listed in this document or their National STO Coordinator. To assist with this process, the IST Panel Assistant will send further detailed instructions to the authors of the papers selected.

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

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

#### IST PANEL EXECUTIVE IST PANEL ASSISTANT

Maj. Luc DETIENNE Mrs. Ayşegül APAYDIN

E-mail: [luc.detienne@cso.nato.int](mailto:luc.detienne@cso.nato.int) E-mail: [aysegul.apaydin@cso.nato.int](mailto:aysegul.apaydin@cso.nato.int)

Tel: +33 (0)1 5561 2280 Tel: +33 (0)1 5561 2282

Fax: +33 (0)1 5561 9607 Fax: +33 (0)1 5561 9626

*From Europe: From the USA or CANADA:*

CSO/NATO CSO-NATO

Attention: IST Panel Attention: IST Panel

BP 25, 7 rue Ancelle PSC 116

92201 Neuilly-sur-Seine Cedex, France APO AE 09777

# SPECIAL NOTICE TO U.S. AUTHORS AND

#### ANNEX A

**NON-U.S. CITIZENS AFFILIATED WITH U.S. ORGANISATIONS**

Ref.: Symposium (IST-148-RSY-032) on “CYBER DEFENCE SITUATION AWARENESS”

to be held in Sofia, Bulgaria, 3 – 4 October 2016

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

**NATO STO U.S. National Coordinator OASD(R&E)/International Technology Programs 4800 Mark Center Drive**

#### Suite 17D08 Alexandria, VA 22350-3600

**Tel: +1 (571) 372 6539 / 6538**

**E-mail:** [**usnatcor@osd.mil**](mailto:usnatcor@osd.mil)

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

**1 AUGUST 2016**

**THE P.O.C. WILL FORWARD ALL US ABSTRACTS AS REQUIRED BY THE TECHNICAL PROGRAM COMMITTEE. (Deadline 15 AUGUST)**

IN ADDITION TO THEIR ABSTRACT, ALL U.S. AUTHORS MUST PROVIDE:

1. A CERTIFICATION (CAN BE SIGNED BY THE AUTHOR) THAT THERE ARE NO PROPRIETARY OR COPYRIGHT LIMITATIONS;
2. INTERNAL DOCUMENTATION FROM THEIR LOCAL PUBLIC AFFAIRS OR FOREIGN DISCLOSURE OFFICE (OR EQUIVALENT) THAT CLEARLY SHOWS:
   * TITLE OF THE PAPER OR PRESENTATION
   * LEVEL OF CLEARANCE (I.E. APPROVED FOR PUBLIC RELEASE)
   * NAME, TITLE AND ORGANIZATION OF THE APPROVAL AUTHORITY

-

1. FULL DETAILS OF AUTHORS

NOTE THAT ONLY COMPLETE PACKAGES (ABSTRACTS + ITEMS LISTED ABOVE) WILL BE ACCEPTED BY THE U.S. POC. AFTER REVIEW AND APPROVAL, THE U.S. POC WILL FORWARD ALL U.S. ABSTRACTS TO THE IST PANEL OFFICE, WHO WILL SEND THEM TO THE PROGRAMME COMMITTEE. U.S. AUTHORS ARE ENCOURAGED TO ADDRESS QUESTIONS AND CONCERNS TO THE POC AS EARLY AS POSSIBLE. DELAYS IN MEETING DEADLINES WILL IMPACT THE TIMELY SUBMISSION OF YOUR ABSTRACT.

Page 1

#### QUESTIONNAIRE

For consideration of a paper submitted for the Information Systems Technology Panel Symposium on:

#### CYBER DEFENCE SITUATION AWARENESS

#### (IST-148/RSY-032)

**Sofia, Bulgaria, 3 - 4 October 2016**

**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*** *having the major responsibility regarding the content of the paper)*

***(A Word copy of the questionnaire is attached to this PDF file)***

#### PART I

**TITLE OF PAPER:**

**What is the nature of the paper/presentation?**

|  |  |
| --- | --- |
| A researched vision with respect to one of three Cyber Security topics |  |
| A researched vision with respect to the combination of the Cyber Security topics |  |
| Report on experiences in implementing the vision of Cyber Security |  |
| Cyber Security lessons identified but not learned (yet) |  |

**Symposium Topic Areas:** *(please click 1 or several boxes as appropriate)*

|  |  |
| --- | --- |
| Cyber Defence |  |
| Cyber Resilience |  |
| Current Challenges in Cyber Security |  |
| Cyber Situational Awareness |  |
| Security Metrics |  |
| Dynamic Risk Assessment |  |
| Mission Assurance |  |
| Continuous Monitoring |  |
| Network Analysis and Monitoring |  |
| Visual Analytics |  |
| Evaluation of Situation Awareness Effectiveness in CD |  |
| Case Studies, Best Practices and Lessons Learned |  |
| Cyber Security Models and Architectures |  |
| Security Verification, Evaluations and Measurements |  |

Page 2

#### Please provide one or two sentences in response to the following questions:

1. What is the operational relevance of your technical work for defence?
2. What do you believe is a new idea or development in your technical work?

Page 3

#### 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:**

**AUTHORSHIP** *(Please list full names of authors and affiliations)*:

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

#### Lead Author:

**Nationality:**

**Position in organisation:**

|  |  |  |
| --- | --- | --- |
| **Telephone: Country code:** | ***Area/town code:*** | **Number:** |
| **Fax No: Country code:** | ***Area/town code:*** | **Number:** |
| **E-mail:** | | |