WORKSHOP ANNOUNCEMENT
CALL FOR CONTRIBUTIONS

Cyber Attack Detection, Forensics and Attribution for
Assessment of Mission Impact

IST-128-RWS-019

to be held in
Istanbul, Turkey
15 - 17 June 2015

IF YOU WISH TO PRESENT A PAPER, SUBMIT BEFORE 1 April 2015

ENROL BEFORE 1 June 2015

The Workshop is NATO UNCLASSIFIED
OPEN to Partnership for Peace (PfP/EAPC) Nations
The NATO Science and Technology Organization

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

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

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

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

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

These Panels and Group are the powerhouse 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:

a) Architecture & Intelligent Information Systems (A2IS)
b) Communications and Networks (COM)
c) Information Warfare and Assurance (IWA)
PROGRAMME COMMITTEE

Programme Chair

Dr. Alexander KOTT
U.S. Army Research Laboratory
United States
Email: alexander.kott1.civ@mail.mil

COMMITTEE MEMBERS

Mr. Hüseyin TİRLİ
TÜBİTAK BİLGEM
Cyber Security Institute
Email: huseyin.tirli@tubitak.gov.tr
Turkey

Mr. Edmund N. MOXON
DSTL
Email: enmoxon@dstl.gov.uk
United Kingdom

Dr. Reginald SAWILLA
NATO-NCI Agency
Email: reginald.sawilla@ncia.nato.int
The Netherlands

Assoc. Prof. Dr. Maya BOZHILOVA
Defence Institute "Prof. Tsvetan Lazarov"
Email: m.bozhilova@di.mod.bg
Bulgaria

Dr. Dennis McCALLAM
Northrop Grumman
Email: dennis.mccallam@ngc.com
United States

Mr. Oğuzhan TOPGÜL
TÜBİTAK BİLGEM
Cyber Security Institute
Turkey

Col. Assoc. Prof. Dr. Nikolai STOIANOV
Defence Institute "Prof. Tsvetan Lazarov"
Email: n.stoianov@di.mod.bg
Bulgaria

Dr. Chris WILLIAMS
Dstl
Email: cwilliams@dstl.gov.uk
United Kingdom

Mr. Alfred MØLLER
Danish Defence Acquisition and Logistics Organization
Email: avm@mil.dk
Denmark
BACKGROUND

The success of a military mission is highly dependent on the Communications and Information Systems (CIS) that support the mission, and on their use in the cyber battle space. The inexorably growing dependency on computational information processing for weapons, intelligence, communication, and logistics systems continues to increase the vulnerability of missions to various cyber threats.

Attacks on CIS systems or other cyber incidents degrade or disrupt the usage of CIS systems, and the resulting mission capability, performance, and completion. Such incidents are expected to increase in frequency and sophistication. Therefore there is a need to address the technology and procedures to characterize the impact of cyber attacks on the mission. Such an impact analysis must necessarily include a broad range of cyber analysis activities: detect attacks in a mission-supporting manner, assess damages relevant to the mission, investigate impacts on mission elements, recover from attacks in order to continue missions to the maximum extent possible, and decide on how to respond to cyber attacks in a manner that maximizes mission success.

Additionally, forensics methods and tools are necessary to determine key facts relevant to assessing mission impact. Such tools are used for evidence collection, analysis of the attack, identification of the attacker, understanding the attack, damage assessment, and attribution of attackers. Dependent on the mission and the type of an attack - there may be different degrees of relative importance and resources attached to attack detection, continuity of the military mission, damage assessment, evidence collection, attribution, and other activities. Usage of related methods, procedures, tools or technology should depend largely on mission.

WORKSHOP OBJECTIVES:

The workshop will focus on identifying practice and research challenges, gaps and approaches – current and future -- to assessment of mission impact due to a cyber attack. Because such an assessment is inseparable from, and impossible without, attack detection, forensics and attribution, the workshop will explore how these activities and related technologies and methods should support the assessment of mission impact.

An example of a complex challenge to be explored by this workshop is achieving the right balance between computational, communication and information resources. Such a balance must be maintained between resources required for ongoing military operations and mission success, resources used for attack detection, battle damage assessment, and investigation - including forensics methods - and resources used to identify origin of attacker in order to determine the attack response, while optimizing the likelihood of mission success. An example of a potential opportunity that the workshop may explore is the question of whether principles known from the traditional military battle damage identification and assessment can be utilized in the cyber domain.

By examining such complex issues, the workshop will formulate a coherent structure of key research and development challenges and technology gaps, as well as recommendations for most promising research and development approaches to closing the gaps.

WORKSHOP TOPICS:

All example topics focus on the goal of assessment of mission impact. They include but are not limited to:

- Analysis and modeling of mission and mission dependencies of CIS assets;
- Prediction of mission impact, including cascading impacts;
- Quantification and qualification of predicted mission risks and impacts;
- Quantification of the criticality of assets in accordance with mission dependencies;
- Methods and techniques for assessing mission dependencies and cyber risks;
• Incident analysis from mission impact perspective - methods, tools and technology;
• Mission-focused attack detection with prioritization for mission needs, including early warning;
• Advanced data analysis tools for characterizing attackers tools used in the incident;
• Automated damage assessment;
• Mission-focused forensics of information, computers and networks;
• Automation of mission-focused forensics triage;
• Tools and methods for visualization of damage and the impact on mission dependencies;
• Correlation and fusion of damage and evidence data;
• Mission impact focused attribution and trace back;
• Current and future trends, including potential for real-time or large scale forensics and other analysis that characterizes impact on a particular mission. Emerged/emerging “disruptive” technology developments;
• Metrics for mission impact assessments;
• Use of simulation, e.g., event (re)construction methods and tools, and simulation of impact on mission, such as dependencies propagation.

WORKSHOP FORMAT AND ORGANIZATION

The workshop will bring together military and civilian cyber security researchers, technologists, and practitioners. The workshop provides an excellent opportunity to increase participants' insight in civil as well as military cyber security problem space, and to influence the future research in cyber security, especially as it relates to mission impact assessment and related detection, forensics and attribution. The workshop will comprise a series of topical sessions – see Attachment 1. Each session will include several presentations of papers – some of which will be full papers and others will be shorter position papers – and a discussion open to all participants. The Programme Committee will utilize both the papers and the oral discussions at the workshop to formulate the final report of the workshop, including a set of recommendations.

CALL FOR PAPERS

Although submission of a paper is not required for participating in the workshop, it is encouraged. The Programme Committee invites two types of papers: full papers and position papers. A full paper is a technical paper (between 2500-5000 words) that presents results of a novel research and is subject to evaluation criteria of a typical technical conference. A position paper is short (between 500-1500 words) and reflects the views of the author – usually a discussion of research challenges, gaps and approaches -- without necessarily presenting a supporting research. Papers must address one or more of the aforementioned topics and focus on assessment of mission impact due to a cyber attack.

All (NATO UNCLASSIFIED-Releasable to PfP) papers must be submitted and sent by e-mail to the Workshop Chairman (alexander.kott1.civ@mail.mil) and to the Chairman’s Assistant (ana.a.santiesteban.civ@mail.mil) by the deadline set in the schedule (see below). US authors and non-US Citizen affiliated with a US organization, please see Attachment 2.

The paper must include the following information, in the beginning:
• IST-128 Workshop on Cyber Attack Detection, Forensics and Attribution for Assessment of Mission Impact
• TITLE OF THE PAPER
• Name of the principle Author, followed by the names of the Co-Author(s) if any, and then Company/Affiliation, complete mailing addresses, telephone, fax and e-mail addresses.
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 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 papers. For further information, authors may contact any of the Programme Committee Members listed in this document or their National STO Coordinator. Please allow sufficient time for the clearance to be issued before deadline. In this case, the NATO classification for the Workshop has been declared as NATO UNCLASSIFIED – Releasable to Partner for Peace (PfP) nations.

US Authors: Authors from the United States must comply with US procedures. (Refer to the Instructions in Attachment 2)

The Programme Committee will select a number of papers that are considered suitable for presentation at the Workshop. Authors will be notified by the date indicated in the schedule whether or not their papers are selected. Authors of selected papers will also be provided with information in the Instructions for Authors, which contains detailed instructions for the final formatting, presentation, transmission, etc. of papers.

The time allowed for each presenter of a full paper is 20 minutes, for a position paper - 10 minutes. Equipment will be available for PowerPoint presentations. Paper presentation times will be given in the Programme Announcement included with General Information Package. All papers accepted for presentation at the workshop will appear in the Workshop’s Report and published electronically on the CSO Website.

Please note that the authors of papers selected for presentation will not be financially supported by this organization. You are fully responsible for your own hotel and travel.

Schedule

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 April</td>
<td>Deadline for submission of your paper (not required for attendance but encouraged)</td>
</tr>
<tr>
<td>15 May</td>
<td>Author is notified whether the paper has been accepted</td>
</tr>
<tr>
<td>1 June</td>
<td>Deadline for enrolment (whether you present a paper or not)</td>
</tr>
</tbody>
</table>

GENERAL INFORMATION

Classification

All material and discussion in this workshop will be unclassified.

Participation and Enrolment

You can attend and participate in the workshop even if you do not present a paper. However, enrolment is required in order to attend the workshop. Whether you present a paper or not, you must enrol for the workshop on the CSO website (www.cso.nato.int) before 1st June 2015. The enrolment web page will become available on March 15. We encourage you to enrol early. Attendance will be limited to a number of people to be determined by the Programme Committee.

Language

Presentations and discussions will be in English.

Workshop site, lodging and social programme

The workshop will be held in Istanbul, Turkey.

There is no workshop registration fee.

Attendees and accompanying persons will be responsible for their own accommodation arrangements and any travel expenses.
Once you have enrolled on the CSO website and your enrolment has been validated, you will automatically receive a General Information Package (GIP), giving you further details about the meeting site, the hotels and other general information.

Any questions on the technical aspects of the scientific programme or the participation process should be addressed to the Workshop Chair.

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

(Interim) IST Panel Executive
Mr. Philippe SOÈTE
E-mail: philippe.soete@cso.nato.int
Tel: +33 (0)1 5561 2280

IST Panel Assistant
Mrs. Ayşegül APAYDIN
E-mail: aysegul.apaydin@cso.nato.int
Tel: +33 (0)1 5561 2282

Science & Technology Organization/Collaboration Support Office (CSO)
Information Systems Technology (IST) Panel
BP 25, 922001 Neuilly sur Seine, France

Questions on the local arrangement and facilities should be addressed to Mr. Hüseyin TİRLİ
(huseyin.tirli@tubitak.gov.tr)
The Programme and Organization of the Workshop

The Tentative Programme and Organization of the Workshop

**MONDAY, 15 June 2015**

09h00 – 12h00  Session 1: Mission Impact Assessment and Attack Detection

In this session we explore the complex relations between the assessment of mission impact and the various aspects of detection of malicious cyber activities. Understanding of potential nature of mission impact, and priorities associated with mission impact, can guide the process of detection. Conversely, the information gleaned in the process of detection informs assessment of the mission impact and helps its automation.

13h00 – 16h00  Session 2: Mission Impact Assessment and Forensics

Cyber forensics is a key process that yields insights into the nature of the impact that a cyber incident induces on the mission. As such, the forensics itself should be informed by the mission structure and dynamics. Here we explore mission-focused forensics of information, computers and networks; automation of mission-focused forensics triage; characterizing attackers tools; real-time or large scale forensics analysis that characterizes impact on a particular mission.

**TUESDAY, 16 June 2015**

09h00 – 12h00  Session 3: Mission Impact Assessment and Attribution

The challenge of attribution and trace-back for cyber incidents continues to grow in importance and complexity. Mission impact assessment can provide clues regarding the intent and the identity of potential perpetrators of the cyber attack. At the same time, any information about the attacker can help guide and focus the impact assessment. We also explore correlation and fusion of related data.

13h00 – 16h00  Session 4: Modeling, Simulations and Visualization for Mission Impact Assessment

In this session we explore analysis and modeling of mission and mission dependencies of CIS assets; use of event reconstruction methods and tools, and simulation of impact on mission, such as dependencies propagation. Also of interest are tools and methods for visualization of damage and the impact on mission; and metrics for mission impact assessments.

**WEDNESDAY, 17 June 2015**

09h00 – 12h00  Session 5: Opportunities, Priorities and Recommendations

In a structured brainstorming process, this session will integrate and analyze the overall results and findings of the workshop; it will yield key clusters of technical gaps and barriers, promising approaches to overcoming the gaps, and prioritization of directions in research and development of methods, technologies and tools for mission impact assessment. Recommendations for follow-on NATO IST activities, if any, will be formulated as well.
SPECIAL NOTICE FOR US AUTHORS AND NON-US CITIZENS AFFILIATED WITH US ORGANIZATIONS

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
E-mail: david.r.uribe.ctr@mail.mil or usnatcor@osd.mil
Tel: +1 571 372 6539 / 6538
Fax: +1 571 372 6471

PLEASE NOTE THE FOLLOWING:

All U.S. Authors must submit one electronic copy to this P.O.C. by 1 APRIL 2015

All US Authors must include the following statement in a covering letter:
• The work described in this paper is cleared for presentation to NATO audiences (i.e., Approved for public release)
• The paper is technically correct
• If work is sponsored by a government agency, identify the organization and attest that the organization is aware of submission
• The paper is NATO/PfP Unclassified; and
• The paper does not violate any proprietary rights.

NOTE:
1. Only complete packages (paper plus all items listed above) will be accepted by the US P.O.C.
2. After review and approval, the US POC will forward all US papers with the Details of Authors Form to the Panel Assistant. All US papers must be received directly from the US POC. US papers will not be accepted directly from authors.
3. In the event there are any questions or concerns with these requirements, U.S. authors are encouraged to contact the US POC as early as possible. Delays in meeting POC deadlines will impact the timely submission of your paper.