NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

LECTURE SERIES
IST-143

on "Cyber Security Science and Engineering"

sur "Science et ingénierie de la cybersécurité"

organized by the

Information Systems and Technology Panel

to be held in

Talence (FRA) – 13-14 March 2017

Ecole Nationale Supérieure de Cognitique

This Lecture Series is open to citizens

from NATO Nations, Australia, Finland and Sweden

Latest Enrollment Date: 28 February 2017

Enroll on-line at:
https://events.sto.nato.int/index.php/upcoming-events/event-list/event/0/19-lecture-series/18-ist-143-cyber-security-science-and-engineering-bordeaux-talence-fra

All presentations and discussions will be held in EN, with simultaneous translation into FR.

Background

The mission of STO is to conduct and promote co-operative research and information exchange. STO consists of a three-level organization: the Science and Technology Board (STB), the Panels and the Technical Teams. The Information Systems Technology (IST) Panel is one of the seven Panels under the STB.
The Mission of the Information Systems Technology (IST) Panel is to advance and exchange appropriate technologies in order to provide timely, affordable, dependable, secure and relevant information and to improve C3I systems including special focus on Interoperability and Cyber Security.

Theme

The ubiquitous application and pervasive use of Information Communications Technologies (ICT) and emerging web sciences is being driven by the so far insatiable commercial demand for global computing, telecommunications and multi-media services. These developments have had a profound impact on both the commercial and military sectors to the point where the majority – if not all – critical functions, networks and systems depend on ICT. Military staffs rely on these infrastructures as well as specialised critical infrastructures and CIS (Communication and Information Systems) to support operations and deliver network enabled capabilities (NEC). The common point, and weakness, is the functional space that such ICT-based infrastructure and systems operate in. Any vulnerability in this cyber space – regardless of its size – can be exposed and exploited.
There is a worldwide lack of talent with respect to cyber security. This has become an issue facing national governments, and raises the question of how to reduce the shortage of cyber security experts and personnel.
Several NATO member states have issued national cyber security strategies identifying the need to spot and develop cyber defence talent and to boost cyber security education. However, current practice of engineering cyber systems as well as techniques and tools for cyber operations are extremely ad hoc and not guided by a coherent body of knowledge comparable to older fields of engineering.
The main objective of the proposed lecture series is to disseminate knowledge on Cyber Security Science, Cyber Security Architecture and Cyber Security Engineering among researchers and systems engineers in NATO's member states. There are clear indications that such a series of lectures is timely and will be highly welcomed.

Topics to be covered:

• Cyber Security Science
• Identification and elements of Cyber Science that address the volume, velocity, variety and temporal nature of the (big) data
• Steps and processes that define Cyber Security as a science.
• A documented articulation on scope and directions of Cyber Science
• Should Cyber Security Science be considered a System of (complex) Systems?
• Cyber Security (systems) Engineering
• Cyber Security Architecture
• Training specifically for cyber security incident response centre operations.
• Near and long-term academic curricula and certification schemes on cyber security (systems) engineering.

Thème

Le recours systématique et désormais ubiquitaire aux technologies de l'information et de la communication (TIC), ainsi que l'émergence de sciences du Web, sont poussés par une demande commerciale jusqu'à présent insatiable de services informatiques, de télécommunications et multimédias.

Ces évolutions ont eu de profondes répercussions sur les secteurs commerciaux et militaires à tel point que la plupart, si ce n'est l'intégralité, des fonctions, réseaux et systèmes critiques dépendent aujourd'hui des TIC. Le personnel militaire se fie à ces infrastructures comme aux infrastructures et SIC (systèmes d'information et de communication) critiques spécialisés pour la conduite des opérations dans le cadre de capacités réseau-centriques (NEC). Leur point commun, et leur faiblesse, résident en l'espace fonctionnel dans lequel ces infrastructures et systèmes, reposant sur les TIC, sont utilisés. Toute vulnérabilité dans ce cyberespace – indépendamment de sa taille – peut être exposée et exploitée.

Le manque de personnes compétentes en cybersécurité se fait ressentir sur toute la planète. Il constitue désormais un problème pour les gouvernements nationaux, qui se doivent de trouver des solutions pour combler la pénurie en personnel et en spécialistes cybersécurité.

Plusieurs États membres de l'OTAN ont publié des stratégies nationales de cybersécurité faisant état de la nécessité de détecter et développer les talents en matière de cyberdéfense et de stimuler l'éducation à la cybersécurité. Toutefois, les pratiques actuelles d'ingénierie des cybersystèmes et les techniques et outils des cyberopérations sont conçues sur mesure et non guidées par un corpus cohérent de connaissances, comme on en trouve pour des domaines plus anciens de l'ingénierie.

Le principal objectif de la série de conférences proposée est de diffuser les connaissances sur la science, l'architecture et l'ingénierie de la cybersécurité parmi les chercheurs et ingénieurs systèmes des pays membres de l'OTAN.

A ce socle de contenus techniques viennent ici s'ajouter trois sessions couvrant trois thèmes de recherche et de pédagogie traités par l'ENSC et ses partenaires :

- La nature duale (civil/défense) de la cybersécurité,
- L'impact de la cybersécurité sur les questions et les professions du droit et de la justice,
- C2, KX et Cybersécurité.

Le succès rencontré par l'édition précédente (Arlington, VA, avec l'Université Carnegie Mellon) de cette Lecture Series indique qu'une telle série de conférences est manifestement opportune.

Lecture Series Director

Col. Dr. Eng. Nikolai STOIANOV (BGR)
Defence Institute "Prof. Tsvetan Lazarov"
Sofia, Bulgaria
n.stoianov@di.mod.bg

Lecturers

Dr. Paul D. Nielsen (USA)
Carnegie Mellon University, Software Engineering Institute

Prof Dr Wim MEES (BEL)
Royal Military Academy, Brussels, Belgium
wim.mees@rma.ac.be

Dr Margret VARGA (GBR)
Seetru Ltd. and University of Oxford
margaret.varga@oncology.ox.ac.uk

Dr Dennis MCCALLAM (USA)
Northrop Grumman Information Technology Defense
dennis.mccallam@ngc.com

Mr Yavor PAPAZOV (BGR)
CyResLab, ESI CEE, Sofia, Bulgaria
yavor@esicenter.bg

Speakers

Prof. Bernard CLAVERIE (FRA), ENSC
François du CLUZEL (NATO ACT Innovation Hub)
Gal. Gilles DESCLAUX (FRA), RACAM
Eloïs DIVOL (EU), European External Action Service
Sylvain HOURLIER (FRA), THALES
Claude KIRCHNER (FRA), INRIA
Hervé LE GUYADER (FRA), ENSC
Yves LEON (FRA), Judicial Expert
Thierry MATUSIAK (FRA), IBM
Gal. Denis MERCIER (NATO SACT) (video message)
Laurent OUDOT (FRA), TEHTRI
Bernard POULIQUEN (FRA), Conseil Régional Bretagne
Myriam QUEMENER (FRA), Ministry of Interior
Thierry WICKERS (FRA), EXEME, Law Firm

Local Coordinator

Mr Hervé LE GUYADER, ENSC
Tel: +33 6 5292 8173
herve.le-guyader@ensc.fr

LECTURE SERIES PROGRAMME

Monday, 13 March, DAY ONE

08:00	Registration
09:00	Opening Ceremony & STO overview ENSC, CRNA and STO represented
09:30	Keynote Address – **Paul D. NIELSEN**
10:15	**Break**
10:30	Introduction and Overview – **Nikolaï STOIANOV**
10:45	Cyber Security Models – **Nikolaï STOIANOV**
11:30	Cyber situation awareness – **Margret VARGA**
12:15	Cyber Security Metrics – **Yavor PAPAZOV**
13:00	**Lunch Break**
14:00	From Cyber risk management to operational risk management – **Win MEES**
14:45	The dual nature of Cyber Security Moderator – **Hervé LE GUYADER** **Speakers: Bernard POULIQUEN – Eloïs DIVOL – Thierry MATUSIAK – Laurent OUDOT**
16:15	Group Photo
16:30	**Break**
16:45	A Case Study Analysis of Cyber Reference Architectures – ARMOUR from different standpoints – **Dennis McCALLAM**
17:30	End of Day 1

Tuesday, 14 March, DAY TWO

08:00	Registration
09:00	Reboot from previous day
09:15	Developing and Measuring a Cyber Security Architecture Course – **Dennis Mc CALLAM**
10:00	**Break**
10:15	Cybersecurity: Impact on legal matters and professions" Moderator: **Hervé LE GUYADER** **Speakers: Myriam QUEMENER – Thierry WICKERS – Yves LEON**
11:30	FR Research on Cybersecurity, a cartography – **Claude KIRCHNER**
12:00	Security by design in an enterprise architecture framework – **Win MEES**
12:45	**Lunch Break**
14:00	Human considerations in C2, KX and Cybersecurity Moderator: **François du CLUZEL** **Speakers: Bernard CLAVERIE – Gilles DESCLAUX – Gal MERCIER (video message)**
15:00	The application of visual analytics to cyber security – **Margret VARGA**
15:45	**Break**
16:00	Social Engineering – challenges and prevention – **Yavor PAPAZOV**
16:45	Round Table
17:30	Concluding Remarks - **Nikolaï STOIANOV**
17:45	End of Conference

APPLICATION TO ENROLL

LECTURE SERIES IST-143

Talence (FRA) – 13-14 March 2017

Ecole Nationale Supérieure de Cognitique

109 Avenue Roul, 33400 Talence, FRANCE

Open to citizens from

NATO Nations, Australia, Finland and Sweden.

Enrolment must be made via internet only at:
https://events.sto.nato.int/index.php/upcoming-events/event-list/event/0/19-lecture-series/18-ist-143-cyber-security-science-and-engineering-bordeaux-talence-fra

STO Events Website:
https://events.sto.nato.int/index.php/event-summary

Note: the NATO CSO is currently using a new enrolment system. Each participant has to create an account prior to enrolling.

General Information Package with information on travel, accommodation and local arrangements will be placed on the enrolment site. Participants are to make their own travel arrangements.

If you are unable to enrol via the internet, please contact the CSO enrolment coordinator:
lectureseries@cso.nato.int

Latest Enrolment Date: 28 February 2017

Contact/Enrolment Coordinator

NATO Collaboration Support Office (CSO)

Anne Reboul
+33 (0)1 55 61 22 67 (phone)
+33 (0)1 55 61 96 28 (fax)
lectureseries@cso.nato.int