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

Tallinn (EST) – 19 - 20 June 2018

IT College

Tallinn University of Technology

This Lecture Series is open to citizens

from NATO Nations, Australia, Finland and Sweden

Latest Enrolment Date: 18 June 2018

Enrol on-line at

IST-143 Lecture Series - Tallinn, EST

All presentations and discussions will be held in English.

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 démesuré aux technologies de l'information et de la communication (TIC), ainsi que l'émergence de sciences du Web, sont générés par une large demande commerciale jusqu'à présent insatiable de services informatique, 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 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 dans lequel fonctionnent ces infrastructures et systèmes reposant sur les TIC. 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 comparable aux 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. Une telle série de conférences est manifestement opportune et sera plus que bienvenue.

Lecture Series Director

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

Lecturers

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

Maj. Raul RIKK (EST)
Programme Director of National Cyber Security
e-Governance Academy

Dr. Erika MATSAK (EST)
Associate Professor
IT College
Tallinn University of Technology

Dr. Peeter LORENTS (EST)
Professor
Estonian Business School

Dr. Rain OTTIS (EST)
Associate Professor
Programme Director (Cybersecurity)
School of Information Technologies: Department of Software Science
Tallinn University of Technology

Local Coordinator

Ivar JANSON (EST)
Ministry of Defence
Sakala 1
15094 Tallinn
ivar.janson@kaitseministeerium.ee

LECTURE SERIES PROGRAMME

Tuesday, 19 June, DAY ONE

8:00	Registration
9:00	Opening Ceremony & STO Overview **IT College and STO represented**
9:15	Keynote Address – Maj. **Raul RIKK** How to measure national cyber security capability: The National Cyber Security Index
10:15	Break
10:30	Introduction and Overview – **Col.Dr. Nikolai STOIANOV**
10:45	Cyber Security Models - **Col.Dr. Nikolai STOIANOV**
11:30	Cyber Situation Awareness - **Dr. Margaret VARGA**
12:15	Lunch Break
13:15	Cyber Security Metrics – **Mr. Yavor PAPAZOV**
14:00	From Cyber Risk Management to Operational Risk Management - **Prof. Dr. Wim MEES**
14:45	Group Photo
15:00	Break
15:30	Developing and Measuring a Cyber Security Architecture Course - **Dr. Dennis McCALLAM**
16:15	End of Day 1

Wednesday, 20 June, DAY TWO

8:00	Registration
9:00	Reboot from previous day
09:15	Big-data at the national level and their intelligent exploitation – **Dr. Erika MATSAK**
10:00	Break
10:15	A new method for the identification and numerical assessment of the similarity of situations and developments – **Dr. Peeter LORENTS**
11:00	Security by Design in an Enterprise Architecture Framework - **Prof. Dr. Wim MEES**
11:45	Lessons from the Estonian ID Card Incident of 2017 – **Dr. Rain OTTIS**
12:30	Lunch Break
13:30	The Application of Visual Analytics to Cyber Security – **Dr. Margaret VARGA**
14:15	Social Engineering - Challenges and Prevention – **Mr.Yavor PAPAZOV**
15:00	Break
15:15	A Case Study Analysis of Cyber Reference Architectures-ARMOUR from Different Standpoints - **Dr. Dennis McCALLAM**
16:00	Round Table
16:45	Concluding Remarks – **Col.Dr. Nikolai STOIANOV**
17:00	End

APPLICATION TO ENROLL

LECTURE SERIES IST-143

Tallinn (EST) – 19 - 20 June 2018

IT College

Tallinn University of Technology

Open to citizens from

NATO Nations, Australia, Finland and Sweden.

Enrolment must be made via internet only at

IST-143 Lecture Series - Tallinn, EST

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 enroling.

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: 18 June 2018

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