CYBER ATTACK
How to Immunize Government

A joint event organised by AFCEA Europe and eSRT

20 February 2018, NH Collection Grand Sablon, Brussels, Belgium

Ms. Despina Spanou

Director for Digital Society, Trust and Cybersecurity
European Commission

Keynote Speech from 09:15 – 09:30 during Part A – "This is what we are facing", Cyber Societal Aspects

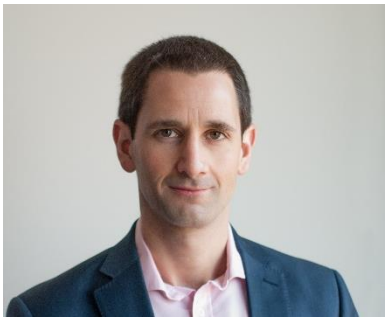
"Policy Efforts for Addressing Cyber Security Societal Challenges"

Mr. Ian West

Chief of Cyber Security
NCI Agency

Keynote Speech from 09:30 – 09:45 during Part A – "This is what we are facing", Cyber Physical Aspects

Bio can be found here



Mr. Mark Sparshott

Senior Director, Strategy
Tanium UK Ltd.

Keynote Speech from 10:00 – 10:20 during part B – "New tools on their way"

Bio can be found here

"New Tools on their Way - Limitless Endpoint Visibility and Control"

Mr. Ken Ducatel

Acting Head of CERT-EU

Moderator of the Panel Session from 10:50 – 12:15 during part B – "New tools on their way"

Bio can be found here

Mr. Dirk Schrader

CMO
Greenbone Networks GmBH

Panelist during the Panel Session from 10:50 – 12:15 during part B – "New tools on their way"

Bio can be found here

From fail-safe to safe-to-fail, why our IT security paradigm has to change from Fortification to Resilience. Billions of dollars have been spent to secure IT infrastructures, its assets and the data contained in them. Still, stories of massive data breaches are making headlines frequently not only in our industry specific news channels but in main-stream media. Looking at the foundational paradigms of IT security, their evolution so far, and where they should be in future is the topic of this brief session.

Mr. Markku Korkiakoski

Director, Sales & Business Development
Bittium

Panelist during the Panel Session from 10:50 – 12:15 during part B – "New tools on their way"

Bio can be found here

"Cyber Resilience –Device aspect"

The role of devices is changing and will continue to change. They are becoming a more essential part and a more integrated part of the E2E solution and thus are tightly connected to overall IT infrastructures. The certification policy is a critical aspect as is how all of these devices will comply.

Mr. Mika Hållfast

Global Cyber Defense Practice Leader
CGI

Panelist during the Panel Session from 10:50 – 12:15 during part B – "New tools on their way"

"Resiliency and Detective Capabilities, Preparing for Future ICT Environments"

Dr. Jamie Shea

Deputy ASG for Emerging Security Challenges
NATO HQ

Keynote Speech from 12:15 – 12:30 during part B – "New tools on their way"

Bio can be found here

"NATO Facing up to the Cyber Challenge"

In his keynote, Dr. Jamie Shea will focus on how. NATO's cyber defences are adapting to the challenge of full spectrum cyber threats and operations. He will give a preview of what we can expect from NATO in 2018 in terms of the Alliance implementing its Cyber Defence Pledge to improve the cyber capabilities of individual Allies and the new structures and strategies that the Alliance will build to be able to use cyberspace as a domain of operations; for instance, the planning for a Cyber Operations Centre as part of its new, revamped military command structure. The keynote will also highlight the prospects for greater NATO-EU interaction in the cyber domain, particularly in addressing the various scenarios of hybrid warfare, and comment finally on how the NATO Summit next July will be a milestone in taking all these efforts forward.

Ms. Ana Gomes

Member of the European Parliament

Keynote Speech from 14:15 – 14:30 during part C – "More needs to be done"

Bio can be found here

"We are just as strong as our weakest link: Are our Members States at similar and reasonable level of awareness and preparedness in Cyber Resilience?"

Mr. Olivier Onidi

Deputy Director General for Security, DG Migration and Home Affairs
European Commission

Keynote Speech from 14:30 – 14:45 during part C – "More needs to be done"

Bio can be found here

Mr. Gordon Lawson

SVP, Global Sales
PhishMe

Participant during the government and industry perspectives session from 15:00 – 15:20 during part C – "More needs to be done"

Bio can be found here

"Enabling Human Phishing Defence"

Enterprises and Governments rely on technology to defend against the cybersecurity threat. While technology is essential, there is another layer of defense in depth that people in your organization can provide. When conditioned and harnessed properly, people can report potentially malicious activity more quickly and make organizations more resilient.

Dr. George Sharkov

Adviser on Cyber Defence
Ministry of Defence Bulgaria

Midterm Review of Bulgaria's EU Presidency from 15:20 – 15:40 during part C – "More needs to be done"

Bio can be found here

"Midterm review of EU Council Presidency"

Cyber Resilience beyond technology - other factors, training, education. Industry's involvement in new ways of civil cyber protection and collective defense. Approaches for improving the collaborative resilience - at national and EU level.

Dr. Sandro Gaycken

Founder and Director
Digital Society Institute ESMT

Closing Keynote from 15:40 – 16:10 during part C – "More needs to be done"

Bio can be found here

"High Assurance Solutions for Military Cyber Defence"

Military and governmental systems will have to confront the most capable hackers and the most devastating tactics in hacking. To date, none of these systems can be considered anywhere near sufficiently secure. High assurance systems can turn this game around.