Deloitte.

Executive Guarantor

In cooperation with

NCBI ČIMIB

CYBER TRENDS

3rd edition of Future Cyber Security & Defence Conference

Conference Partners

Microsoft

Topic Sponsors

secunet

Partner Slot & T

AEC

Cyber Workshop Pa

NSM G

20 – 21 OCTOBER 2016

PVA EXPO PRAGUE, Czech Republic

Cyber Threats & Trends 20 OCTOBER 2016

CIIP and Cyber Education 20 OCTOBER 2016

Cyber/Hybrid Warfare 21 OCTOBER 2016

Cloud Securit 21 OCTOBER 201

and

- SIX+ accompanying CYBER WORKSHOPS
- CYBER PAVILION TableTop Presentations

Conference Patronage & Support, Honorary Chairmen:

Mr. Dušan NAVRÁTIL, Director, National Security Authority, Czech Republic

Mr. Milan CHOVANEC, Minister of Interior, Czech Republic

Mr. Martin STROPNICKÝ, Minister of Defence, Czech Republic

MGen. Erich STAUDACHER Deputy Director of the Bundeswehr Planning Office, Germany

BGen. Prof. Bohuslav PŘIKRYL Rector, University of Defence, Czech Republic

Assoc. Prof. Jozef PUTTERA Rector, Armed Forces Academy of General Milan Rastislav Štefánik, Slovakia

Assoc. Prof. Josef SALAČ Rector, Police Academy Prague, Czech Republic

Mr. Petr JIRÁSEK Chairman, AFCEA Czech Cyber Security Working Group, Czech Republic

Assoc. Prof. Lucia Kurilovská Rector, Academy of the Police Force Bratislava, Slova

Conference is a part of:

FUTURE FORCES FORUM International Platform for Trends & Technologies in Defence & Security

POLICY - DIPLOMACY - DEFENCE - SECURITY - R&D - ACADEMIA - INDUSTRY

General Partner

LOM PRAHA

General R&D Partner

CZECH TECHNICAL UNIVERSITY IN PRAGUE

Partner

VOP

Future Forces Exhibition, 19 – 21 October 2016
World CBRN & Medical Congress, 19 – 21 October 2016
Future Soldier Systems Conference, 20 – 21 October 2016
Military Advanced Robotic Systems Conference, 20 – 21 October 2016
Geospatial, Hydro meteorological and GNSS Workshop, 19 – 21 October 2016
Logistics Capability Workshop, 19 – 21 October 2016
CBRN Workshop, 19 – 21 October 2016
Medical Workshop, 19 – 21 October 2016

Meeting of the North Atlantic Council, Ja

NATO's POLICY ON CYBER DEFENCE – TODAY AND TOMORROW

By Dr. Jamie Shea, Deputy Assistant Secretary General, Emerging Security Challenges, NA

As an international organization with 28 (and soon to be 29) members and employing the rule of consensus, NATO can at times be slow in recognizing new threats. However, once allies have identified major and lasting shifts in the security environment, they ensure that NATO rapidly responds. New policies lead to the creation of new structures that in turn generate more expertise, original thinking and faster policy upgrades.

This has certainly been the case with NATO's policy on cyber defence. This issue was first highlighted roughly a decade ago as a threat primarily to the commercial world and as a new form of organized crime. However, as we have seen, 'cyber' issues have also moved into the world of state-to-state relations and hybrid warfare, with cyber attacks inflicting lasting damage to key national infrastructures and command and control systems. As such, NATO has had to ensure that its own defences are able to k with the growing sophistication of cyber thre to be able to operate across the entire cyber while recognizing that cyber defence is not a planning or operations category within a virtual world, but is also increasingly the k alliance's ability to function in the traditional land, sea, air and space.

Ten years ago, a meeting of the North Atlan on cyber issues was a rarity and new jargo "zero day vulnerabilities" and "spear phishin was still comparatively obscure to most NA officials. Contrastingly, in 2015 NATO defence discussed cyber at all of their meetings and Atlantic Council no fewer than 11 times. NA on its third cyber defence policy since 2006 policy will no doubt be initiated following the summit in Warsaw in July 2016. These polic