

Deloitte



3rd edition of Future Cyber Security & Defence Conference

CYBER TRENDS

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 Security
21 OCTOBER 2016

- SIX+ accompanying CYBER WORKSHOPS
- CYBER PAVILION TableTop Presentations

Conference Patronage & Support, Honorary Chairmen:



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



Mr. Milan ČERNÁNEC
Minister of Industry, Czech Republic



Mr. Martin ŠTROPICKÝ
Minister of Defence, Czech Republic



Major-Erich STAUBACHER
Deputy Director of the Bundeswehr Planning Office, Germany



Major-General Prof. Dominik PUTTERA
Rector, Armed Forces Academy of General Milan Rastislav Štefánik, Slovakia



Major-General Prof. Josef PŘIBYL
Rector, University of Defence, Czech Republic



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



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



Assoc. Prof. Ludia Kurlivskaya
Rector, Academy of the Police Forces, Bratislava, Slovakia

Conference is a part of:

FUTURE FORCES FORUM for Trends & Technologies in Defence & Security

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

General Partner



General R&D Partner



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

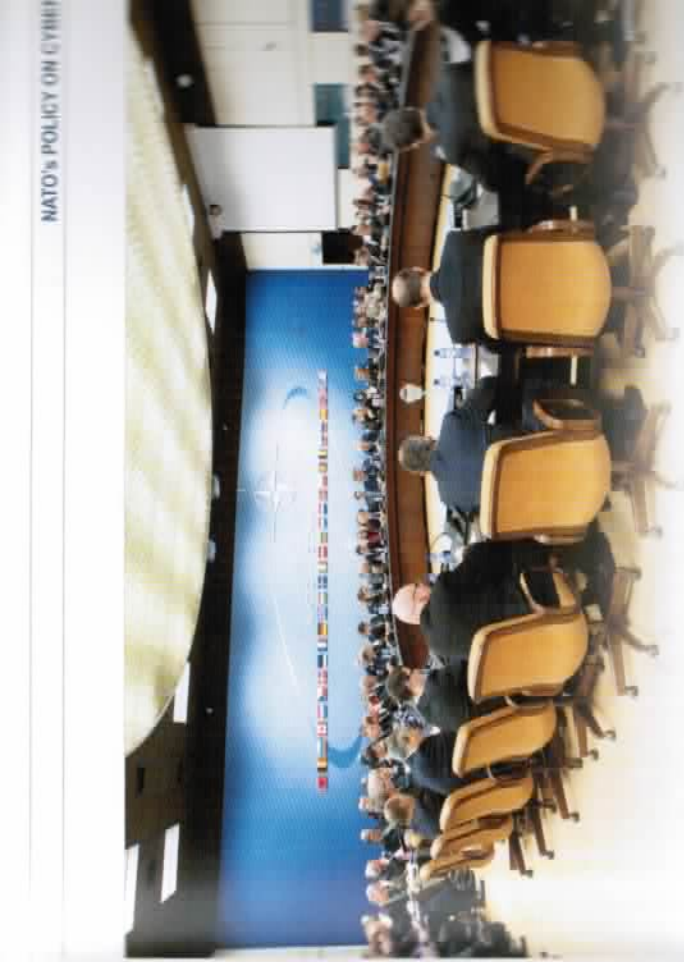


Partner Slot A.17

AEC

Cyber Workshop Pw

NSM C



Meeting of the North Atlantic Council, Jan

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 operate with the growing sophistication of cyber threats while recognizing that cyber defence is not a planning or operations category within a virtual world, but is also increasingly the alliance's ability to function in the traditional land, sea, air and space.

Ten years ago, a meeting of the North Atlantic Council on cyber issues was a rarity and new proposals "zero day vulnerabilities" and "operational readiness" were still comparatively obscure to most NATO officials. Contrastingly, in 2015 NATO defence officials discussed cyber at all of their meetings and Atlantic Council no fewer than 11 times. NATO on its third cyber defence policy since 2008 and policy will no doubt be initiated following the summit in Warsaw in July 2016. These past