TechNet Europe 2017

09 - 11 October · Stockholm · Sweden

"Cyber Capabilities in Hybrid Warfare Scenarios"

An event organised by AFCEA Europe with the cooperation of the AFCEA Stockholm Chapter and under the patronage of the Minister of Defence, Sweden.

Scandic Infra City Hotel, Upplands Väsby, Sweden

SESSION ABSTRACTS

Tuesday, 10 October 2017

Opening Address and Keynote Speech

Naturally, the conference will start with the host nations view presented by Mr. Peter Hultqvist, Minister of Defence, Sweden and General Micael Bydén, Supreme Commander, Swedish Armed Forces, regarding the current political and military situation.

Keynote Speech

The *USA view on cyber issues*, in conjunction with assessing the importance in hybrid warfare from a global perspective will be presented by Dr. John A. Zangardi, Acting DoD CIO.

Keynote panel

In the cyber arena, it all culminates in a *CIO´s responsibility and the role*, self-image and identity she or he has to live up to under the circumstances of hybrid warfare scenarios. This includes the CIOs of the Armed Forces.

The keynote panel consists of:

- Mathias Ekstedt, Professor in Industrial Information and Control Systems, Swedish Royal Institute of Technology (moderator)
- Major General Fredrik Robertsson, Chief Information Officer, Swedish Armed Forces
- Mr. Kristian Vengsgaard, CIO Danish Defence,

- Rear Admiral Maarten Tossings MSc, Principal Director and Information Officer, Ministry of Defense, Principal Directorate of Organisation and Information
- Brigadier General Mikko Heiskanen, CIO Finnish Defence
- Mr. Mats Jonsson, Digital Strategist, Saab

Session 1: "Cyber Operations in Hybrid Warfare Scenarios"

Entering the focus of the conference, todays *Cyber Operations in Hybrid Warfare Scenarios* will be discussed to set the ground for further discussions. In the center of this panel are the findings based on intelligence, the capability to analyze hybrid attacks coming out of the cyber space in time, to ability to categorize them precisely according their origin and threat level. It will be the task to describe mechanisms and effects they may have on the functioning of society and armed forces as well as other security forces in a critical timeframe. Also, existing approaches to gain situational awareness as one of the key elements in hybrid warfare situations are to be assessed. Furthermore, it will be of importance to identify advanced technologies that are in use, including their shortfalls, Finally the implications and demands on strategic planning will have to be highlighted.

Session 2: "Exploring Existing and Future Relationships of all Parties"

In the next part of the conference the panelist will thoroughly be *Exploring Existing and Future Relationships of all Parties*. There are more dependencies than traditional military planning is aware of. A new comprehensive approach is indispensable because more and more common IT tools are used in the military and the private sector. The mounting and employment of forces and their related capabilities (such as logistics, IT support, medical support, recruitment, social media coverage/media support infrastructure) in a time of crisis prior to actual warfighting depend much more on civil/commercial capabilities than in the past. Ways and requirements for a highly integrated, even transnational collaboration, based on technology, will have to be discussed. Ultimately, the question will be, how to build a system of trust.

While exploring common national and trans-national technological dependencies, contingency planning, organizational preparation for hybrid war, and the coordination of governmental and private sector will be assessed. The contribution of the private sector and academia, including the important role of companies in the critical infrastructure sector to a common operational picture in cyber security and cyber defence will play an important part. How advances in IT will be supportive in overcoming existing deficiencies and will enable a time-sensitive cooperation remains also a task of this panel.

Keynote Speech

Thoughts on "The Digital Society and the Challenges of Building a Civil Cyber Defence" will be brought to the audience in a *Keynote* by the highly respected Mr. Nils Svartz, Director General, Swedish Civil Contingencies Agency, with an impressive biography of public service.

Session 3: "Cyber Security in the Future"

When entering the section on *Cyber Security in the Future*, technology isn't the only answer to future threats, but it´s developments will have to be given a look by the experts of that panel.

Increasing no of attacks, increasing conflation of state and non-state actors, criminal intentions, and the proliferation of tools beyond state control add to the threat.

Including effects from the Internet of Things with its exponentially increased vulnerabilities and its military relevance, the foreseeable technological changes call for an improved analysis, deeper situational awareness and for technological support to decision making process. This may contain such features as predictive analytics. multi source intelligence analysis, handling of unstructured data, linguistic analysis. Information assurance and integrity of data will become of high relevance. The respective initiatives under way both in NATO and EU will be discussed.

Session 4 Panel Discussion: "Keeping up with Speed of Development in Cyber – It is a Must!"

Including and beyond technological applications, the organizational, human factor and procedural advantages are to be explored in order to remain dominant in defense against the offensive. This includes procedural improvements, e.g. in the field of rapid procurement and contingency planning, new methods of recruiting the best minds under new paradigms which suit the skills and interests of the millennials (the digital natives with their different set of values and approach to lifestyle). Other demographic factors will also have to be taken into account, as well as enhanced education. Training, both for individuals and teams, will improve inter-actions of multi-disciplinary cyber response teams. With industry being the driving force in a wide range of technology development, the increasing role of the private sector and the ability to transfer and adapt technology for the public sector has to be reflected. A spectrum of measures needs to be developed, and public and private capabilities need to amalgamated in a deeper partnership for the best of a nation's defence. But how to achieve this?

Hackathon Results

During the conference information will be given on progress of the Hackathon which runs in parallel to TechNet Europe. The winners will be presented in this session. The goal of this “capture the flag” style challenge for students and professionals is to demonstrate their hacking abilities in an ethically acceptable environment, to serve as a talent show, to gain the positive experience of serving the public by supporting a nation’s defense, and to offer a different way of thinking, also to the audience of the conference.

Final Keynote Speech

A final *Keynote* from Mr. Mikko Hyppönen with profound practical experience on counter hacking will cross check the findings against reality.