General Micael Bydén

Supreme Commander of the Swedish Armed Forces

Keynote speech on Tuesday 10 October 09:50 – 10:20

Bio can be found here

"Cyber Defence Capabilities from a Military Perspective"

We are living in the most complex and unpredictable security environment since the Second World War. The challenges around Cyber Defence are now a matter for the Armed Forces within a bigger societal context. These challenges can not only be handled from a technology perspective but must also be dealt with by collaborating with trusted partners on a global scale. The Chief of defence will talk about some of the initiatives Sweden is participating in and will introduce the core components of the Swedish Armed Forces Cyber Defence Concept.

Mr. Dylan DeAnda

Senior Director
Federal Team, Tanium

Participant during panel session 1 discussing "Cyber Operations in Hybrid Warfare Scenarios" on Tuesday 10 October 14:05 – 15:40

Bio can be found here

"Dominating Cyber Operations at the Speed of Decision"

Throughout history, our Soldiers, Sailors, Marines, and Airmen have always watched over each other and exercised vigilance in preventing surprise attacks. The cost of losing that vigilance is paid with the lives of those forces, and the security of our nation. It is clear that the hunter versus victim mentality must pervade at every layer of our forces, from the commander, to the overwatch, to the boots on the ground.

Attackers are using hybrid warfare methods to covertly and overtly undermine and destabilize defense forces, by applying both kinetic and cyber attacks to deny operations, disrupt defensive capabilities, and exert their dominance.

In order to dominate the Cyber battlespace, CIOs, Commanders and their forces must employ a construct of constant overwatch, geometry of fires, and unity of command. They must be able to see the entire battlespace, understand their options for effect, coordinate their forces and act with speed. All of these are for not, if the commander cannot make a decision, due to lack of information; at that point, the Commander loses the initiative, the unity of effort, and the speed of action.

Attendees will learn how to employ a progressive approach to dominating Cyber Operations by improving visibility of the battlespace, increasing the reach of their effects, and responding to attacks with unity of command and unity of effort.

Ms. Ida Eklund Lindwall

East Stratcom Task Force
European External Action Service (EEAS)

Participant during panel session 2 discussing "Exploring Existing and Future Relationships of all Parties" on Tuesday 10 October 16:40 – 18:15

Bio can be found here

"Disinformation and the Challenge for Democracies"

The East Stratcom Task Force within the European Union External Action Service was set up after the EU Heads of State and Government stressed the need to challenge Russia's ongoing disinformation campaigns in March 2015. The presentation will be a brief outline of the ongoing Russian disinformation campaign and the challenge it poses to democracies, democratic institutions and the democratic narrative.

Prof. Mathias Ekstedt

Professor in Industrial Information and Control Systems
Swedish Royal Institute of Technology

Moderator during the keynote panel discussing: "CIOs in a Hybrid Warfare Situation – Areas of Responsibility and Future Challenges" on Tuesday 10 October 11:20 – 12:35

Bio can be found here

Anna Granö

Managing Director
HPE Sweden

Participant during panel session 2 discussing "Exploring Existing and Future Relationships of all Parties" on Tuesday 10 October 16:40 – 18:15

Bio can be found here

"Wind of Changes"

Brigadier General **Mikko Heiskanen**

Chief Information and Cyber Defence Officer
Finnish Defence

Participant during the keynote panel discussing: "CIOs in a Hybrid Warfare Situation – Areas of Responsibility and Future Challenges" on Tuesday 10 October 11:20 – 12:35

Bio can be found here

Mr. Julian Meyrick

Vice President
IBM Security Europe

Participant during panel session 3 discussing "Cyber Security in the Future" on Wednesday 11 October 10:35 – 12:10

Bio can be found here

"Cyber Security in the Future - Leveraging Cognitive Security for Better Human Decision-Making"

Security teams face an onslaught of serious challenges as security threats and fraudulent activities continue to grow in sophistication and volume. In order to handle the exponential rise in data volumes and to protect against exponential threats, security leaders on the front line need a whole new approach to threat prevention, recognition and counter measures.

IBM's research in this area is extensive and has resulted in revolutionary new developments that bring the Watson cognitive era to Cyber Security, enabling every security analyst to become a cognitive analyst, able to gain powerful insights, leverage threat research, and drive better outcomes through a trusted advisor enabling better human decision-making.

Cognitive security will help to bridge the current skills gap, accelerate responses and reduce the cost and complexity of dealing with cybercrime.

Prof. Dr. Udo Helmbrecht

Executive Director
European Union Agency for Network and Information Security (ENISA)

Moderator during panel session 1 discussing "Cyber Operations in Hybrid Warfare Scenarios" on Tuesday 10 October 14:05 – 15:40

"Cyber-Ops in Hybrid Warfare Scenarios"

Internet today looks a lot different that it looked ten or fifteen years ago. Not only the technological advances in speed, portability and reliability but also its deep integration into societies and countries and the dramatic change of how internet is being used today for good and bad, is continuously expanding the scope of cyber security in other domains in order to ensure security for the EU citizens and protection of the EU core values. One of such domains is defence. Today's cyber threat landscape points to a significant increase of incidents aiming military targets and operations originating from non-state and state sponsored actors and capabilities. Hybrid warfare is expanding to include cyber and forces the western societies to consider cyber threats in the context of military operations.

Dr. Åke Holmgren

Office of Cybersecurity and Critical Infrastructure Protection
Swedish Civil Contingencies Agency (MSB)

Participant during panel session 1 discussing "Cyber Operations in Hybrid Warfare Scenarios" on Tuesday 10 October 14:05 – 15:40

Bio can be found here

"Countering Hybrid Threats – Civil Cyber Defence"

The topic Cyber Operations in Hybrid Warfare Scenarios will be discussed from the perspective of societal resilience and the building of a civil cyber defence aimed at safeguarding vital functions and information assets. Particular attention will be given to situational awareness, analysis and assessment of cyber related hybrid threats. The need for public-private cooperation in society and an all hazards approach will be elaborated upon. Further, hybrid threats and the implications for the strategic civil defence planning will be discussed.

Mr. Peter Hultqvist

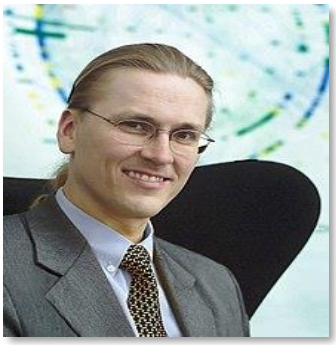
Minister of Defence in Sweden

Opening address on Tuesday 10 October 09:30 – 09:50

Bio can be found here

Mr. Mikko Hyppönen

Chief Research Officer
F-Secure



Final keynote speech on Wednesday 11 October 15:45 – 16:05

Bio can be found here

"The Cyber Arms Race"

We've lived our lives in the middle of a revolution: the internet revolution. During our lifetime all computers started talking to each other over the internet. Technology around us is changing faster than ever. We've already become dependent of our digital devices, and this is just the beginning. As connected devices open new opportunities for imagination, they also open up new opportunities for waging war.

"Where are we today? Where are we going? And how are we ever going to secure ourselves against future threats?"

Martin Indrek Miller

Risk Manager at Cyber Security Branch of the Information System Authority (RIA)
Government of Estonia

Participant during panel session 4 discussing "Keeping up with Speed of Development in Cyber – It is a Must!" on Wednesday 11 October 13:40 – 15:15

Bio can be found here

"Secure Digital Identity, Government Cloud and Cyber Hygiene"

Mr. Mats Jonsson

Digital Strategist
Saab

Participant during the keynote panel discussing: "CIOs in a Hybrid Warfare Situation – Areas of Responsibility and Future Challenges" on Tuesday 10 October 11:20 – 12:35

Harvesting from the vast amounts of stuff clever people around the planet have done. Reading, testing, combining, adding, removing and expanding. Often bending and breaking rules, always challenging conceptions and conventions on a never ending quest to figure out elegant and simple solutions to really hard problems, only to find they often don't need solving. They are the wrong problem.

Dr. Kai Martius

Chief Technology Officer
secunet Security Networks AG

Participant during panel session 2 discussing "Exploring Existing and Future Relationships of all Parties" on Tuesday 10 October 16:40 – 18:15

"Redefining Secure IT Systems: Achieving Greater Cyber Resilience in Future Multinational Deployments"

Bio can be found here

Major General Earl Matthews USAF (Ret.)

Vice President and General Manager
Enterprise Security Solutions Enterprise Services, U.S. Public Sector
DXC Technology

Participant during panel session 3 discussing "Cyber Security in the Future" on Wednesday 11 October 10:35 – 12:10

Bio can be found here

"The Race to the Swift"

The Race to the Swift is a military necessity for NATO's mission continuity. Transformational thinking changes the mindset from "defense in depth" to "defense in context." Defense in depth results in a war of attrition, where we continually cede the initiative to the opponent. Defense-in-Context leverages all the security-related information available and integrates it to obtain situational awareness and context. This includes information that we have not previously had – e.g. location used to be static; now we're mobile. What is the individual allowed to access? What controls are necessary? Defense-in-Context also encompasses behaviors – is the individual behaving normally on a day-to-day basis? Is that behavior similar to that of peers in the same role?

Defence in Context is built on Cyber Situational Awareness. This includes continuous monitoring of the cyber architecture, fusing that information with threat Intel, and presenting both the situational awareness aspects and the Courses of Action proposals on a single pane of glass. Through this increasing cyber maturity, commanders move from basic data, through risk understanding and visualization, into proactive risk/mission management and cyber resilience.

The electron has become the ultimate precision guided munition, capable of mimicking the effects of a WMD. Cyber supremacy is no longer a given, so the ability to outmaneuver our adversaries in Cyberspace is a strategic imperative. We must build cyber situational awareness, and Cyber resiliency, within acquisition timelines that do not cede the initiative to our adversaries.

Ms. Essye Miller

Deputy Chief Information Officer for Cyber Security
U.S. Department of Defence

Participant during panel 4 session discussing "Keeping up with Speed of Development in Cyber – It is a Must!" on Wednesday 11 October 13:40 – 15:15

Bio can be found here

"Enhancing Departmental Cyber Security for DoD"

Mikael Lindström

Senior Strategic Advisor
National Operations Department
SC^3 - Swedish Cybercrime Centre

Participant during panel session 3 discussing "Cyber Security in the Future" on Wednesday 11 October 10:35 – 12:10

Bio can be found here

"Perspectives from the Swedish National Police and the Recently Established Swedish Cybercrime Centre (SC3)"

Major General Fredrik Robertsson

Chief Information Officer
Swedish Armed Forces

Participant during the keynote panel discussing: "CIOs in a Hybrid Warfare Situation – Areas of Responsibility and Future Challenges" on Tuesday 10 October 11:20 – 12:35

Bio can be found here

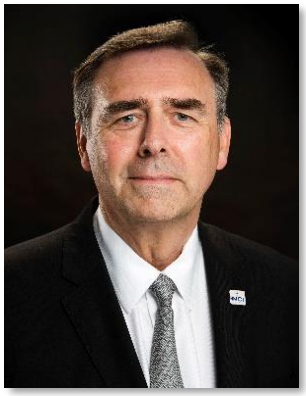
Mr. Matti Saarelainen

Interim Director
European Centre of Excellence for Countering Hybrid Threats

Participant during panel session 1 discussing "Cyber Operations in Hybrid Warfare Scenarios" on Tuesday 10 October 14:05 – 15:40

Bio can be found here

"Hybrid CoE - introduction and intitial activities"



Mr. Kevin Scheid

General Manager
NCI Agency

Moderator during panel session 2 discussing "Exploring Existing and Future Relationships" on Tuesday 10 October 16:40 – 18:15

Bio can be found here

Mr. Shannon Sullivan

Head of Federal
Google Cloud

Keynote speech on Tuesday 10 October 16:10 – 16:40

Bio can be found here

"Innovations in Cloud Computing"

Mr. Chris Smith

Global Public Sector CTO, Vice President
Global Technology Office, AT&T Business Solutions – Global Public Sector

Participant during panel session 2 discussing "Exploring Existing and Future Relationships of all Parties" on Tuesday 10 October 16:40 – 18:15

Bio can be found here

"Situational Awareness and Visualisation for Cyber Threat Sharing"

The speaker, Mr. Chris Smith, will discuss how a multi-faceted technological framework for sharing threat intelligence between organisations, agencies, companies and countries is paramount to the development of a Common Operational Picture (COP) of the Cyber domain. The sharing of cyber threat information between partners with varying degree of trust is difficult. However, methods and technology exist today to share and federate this data. The Speaker will discuss the technology and visualisation components of the COP based on AT&T's commercial capability in the cyber threat domain.

Mr. Christopher Stace

Head of Unit Information Superiority
European Defence Agency (EDA)

Participant during panel session 4 discussing "Keeping up with Speed of Development in Cyber – It is a Must!" on Wednesday 11 October 13:40 – 15:15

Bio can be found here

"How to Increase the Pace of Collaborative Cyber Defence?"
- Review of current policy and programmatic instruments
- Successes and failures
- New opportunities

Mr. Nils Svartz

Director General
Swedish Civil Contingencies Agency

Keynote speech on Wednesday 11 October 09:45 – 10:05

Bio can be found here

"The Digital Society and the Challenges of Building a Civil Cyber Defence"

The security environment in Europe and in Sweden's vicinity has changed. At the same time we are seeing a rapid digitalisation of our society. This poses increasing challenges on governments to protect their populations and maintain the continuity of critical infrastructures and services. A key component in strengthening societal resilience is the building of a robust civil cyber defence aimed at safeguarding vital functions and information assets.

Rear Admiral Maarten Tossings

Principal Director and Chief Information Officer
Dutch Ministry of Defense

Participant during the keynote panel discussing: "CIOs in a Hybrid Warfare Situation – Areas of Responsibility and Future Challenges" on Tuesday 10 October 11:20 – 12:35

Bio can be found here

Mr. Kristian Vengsgaard

Chief Information Officer
Danish Defence

Participant during the keynote panel discussing: "CIOs in a Hybrid Warfare Situation – Areas of Responsibility and Future Challenges" on Tuesday 10 October 11:20 – 12:35

Bio can be found here

Mr. Johan Wiktorin

Director Intelligence
PWC

Participant during panel session 4 discussing "Keeping up with Speed of Development in Cyber – It is a Must!" on Wednesday 11 October 13:40 – 15:15

Bio can be found here

"Threat Intelligence Challenges for the Future Struggle"

Looking into the future, the cyber conflicts will be messier, more fluent and a competition for raising sustainable capabilities. Which challenges does the Intel side have in dealing with old opponents and emerging ruthless new adversaries?

To answer this, we need to start with a common understanding of the field and its surroundings, the special characteristics and peculiarities of the cyberspace in the ongoing cyber struggle.
The presentation will touch upon this including the strengths and weaknesses of generic threats.
Different intelligence challenges in personal, organisation, the interdependence between technology, tactics and law as well as TTP:s and leadership will then be explored.
How can the public and private sector forge a strategic partnership in cyber intelligence in order to enhance the defense of our tangible and intangible assets?

Air Cdre Bruce Wynn OBE FBCS CITP RAF (retd)

Freelance Cyber Consultant and Advisor
Member of AFCEA's International Cyber Committee

Moderator during panel session 3 discussing "Exploring Existing and Future Relationships" on Tuesday 10 October 16:40 – 18:15

Bio can be found here

Dr. John A. Zangardi

Acting Department of Defence Chief Information Officer
United States of America Government

Keynote speech on Tuesday 10 October 10:50 – 11:20

Bio can be found here

“DoD CIO Perspective - Innovation to Combat an Increasingly Sophisticated Cyber Threat”

In todays' cyber threat environment, thinking differently about capabilities and challenges - also called innovation - is the only way to accomplish the cyber mission. Acting Department of Defence Chief Information Officer, Dr. John Zangardi, will discuss how DoD is thinking differently about information technology and cybersecurity for the mission. Information technology is integral to the mission, and the efficiency, effectiveness, reliability, and last - but certainly not least - security of every single one of the Department's systems is of unparalleled importance.