CYBER SECURITY –

HVILKE MULIGHETER FINNES PÅ DEN EUROPEISKE FORSKNINGSAGENDAEN?

Marie Moe, Research Manager Cyber Security, SINTEF Digital
@MarieGMoe @SINTEF_Infosec

Referansenettverk for digital sikkerhet

Et referansenettverk for digital sikkerhet gjør at norske organisasjoner kan samarbeide med å dekke deltagelse i de relevante EU-fora, dele informasjon og støtte hverandre ved avstemminger, valg og gi koordinerte innspill til EUs forskningsagenda.

WORKING GROUPS & TASK FORCES

ECS
EUROPEAN CYBER SECURITY ORGANISATION

WG 1
Standardisation Certification, Labelling, Supply Chain Management

WG 2
Market development, Investments, and International collaboration

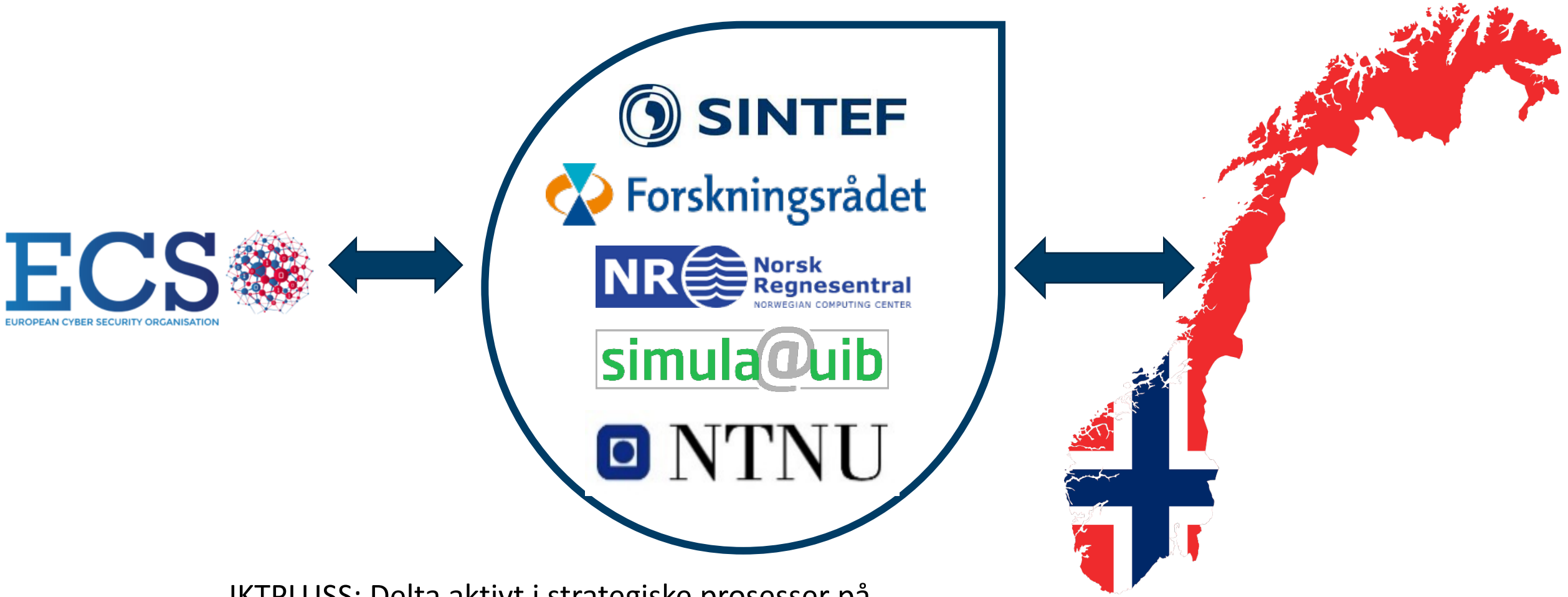
WG 3
Sectoral demand (vertical market applications)

WG 4
Support SME, coordination with countries (in particular East EU) and regions

WG 5
Education, training, awareness, cyber ranges

WG 6
Strategic research and innovation agenda (SRIA)

SINTEF



IKTPLUSS: Delta aktivt i strategiske prosesser på den europeiske forskningsarenaen

Kontaktpersoner i nettverket

Samarbeidspartnere	Kontaktpersoner
SINTEF	Marie Moe Per Håkon Meland Aida Omerovic
NTNU/CCIS	Nils Karlstad Svensen Laura Georg Sokratis Katsikas Basel Katt Katrin Franke
UiO	Audun Jøsang Nils Gruschka
Simula@UiB	Kjell Jørgen Hole Øyvind Ytrehus
Norsk Regnesentral	Åsmund Skomedal Habtamu Abie

Målgruppe

- Forskningsmiljøer innen informasjonssikkerhet ved UoH- og instituttsektoren.
- Norske bedrifter og offentlige organer med informasjonssikkerhetsinteresser/-ansvar.

Kanaler

- Åpne informasjonsmøter
- Tematiske workshops
- Epost-liste med informasjon fra EU-fora (meld på til marie.moe@sintef.no)
- Nyhetsbrev
- Bloggposter (https://infosec.sintef.no) og andre sosiale medier

AKTUELLE UTLYSNINGER INNEN DIGITAL SIKKERHET

SU-ICT-02-2020: Building blocks for Resilience in Evolving ICT systems

Frist: 19. November 2019

- Cybersecurity/privacy audit, certification and standardisation
- Trusted supply chains of ICT systems
- Designing and developing privacy-friendly and secure software and hardware

(SINTEF Digital proposal: http://pr.fessor.eu)

SINTEF

SU-DS02-2020: Intelligent Security and Privacy management

Frist: 27. August 2020

- Dynamic governance, risk management and compliance
- Cyber-threat information sharing and analytics
- Advanced security and privacy solutions for end users or software developers
- Distributed trust management and digital identity solutions

SU-DS02-2020: Expected impact (short term)

- Reduced number and impact of cybersecurity incidents;
- Efficient and low-cost implementation of the NIS Directive and General Data Protection Regulation;
- Effective and timely co-operation and information sharing between and within organisations as well as self-recovery;
- Availability of comprehensive, resource-efficient, and flexible security analytics and threat intelligence, keeping pace with new vulnerabilities and threats;
- Availability of advanced tools and services to the CERTs/CSIRTs and networks of CERTs/CSIRTs;
- An EU industry better prepared for the threats to IoT, ICS (Industrial Control Systems), AI and other systems;
- Self–recovering, interoperable, scalable, dynamic privacy-respecting identity management schemes.

SU-DS02-2020: Expected impact (medium and long term)

- Availability of better standardisation and automated assessment frameworks for secure networks and systems, allowing better-informed investment decisions related to security and privacy;
- Availability and widespread adoption of distributed, enhanced trust management schemes including people and smart objects;
- Availability of user-friendly and trustworthy on-line products, services and business;
- Better preparedness against attacks on AI-based products and systems;
- A stronger, more innovative and more competitive EU cybersecurity industry, thus reducing dependence on technology imports;
- A more competitive offering of secure products and services by European providers in the Digital Single Market.

SU-DS03-2019-2020: Digital Security and Privacy for Citizens and Small and Medium Enterprises and Micro Enterprises

Frist: 27. August 2020

- Protecting citizens' security, privacy and personal data
- Small and Medium-sized Enterprises and Micro Enterprises (SMEs&MEs): defenders of security, privacy and personal data protection

SU-DS03-2019-2020: Expected impact

- Citizens and SMEs&MEs are better protected and become active players in the Digital Single Market, including implementation of the NIS directive and the application of the General Data Protection Regulation.
- Security, privacy and personal data protection are strengthened as shared responsibility along all layers in the digital economy, including citizens and SMEs&MEs.
- Reduced economic damage caused by harmful cyber-attacks and privacy incidents and data (including personal data) protection breaches.
- Pave the way for a trustworthy EU digital environment benefitting all economic and social actors.

SU-DS04-2018-2020: Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches

Frist: 27. August 2020

- Cybersecurity of SCADA and ICS in Energy
- SIEM, logging, information sharing with CERTs
- Recommendations on standardisation, certification, exchange of communication
- Pilot at large scale, TSO/DSO encouraged as partner

SU-DS04-2018-2020: Expected impact

- Built/increased resilience against different levels of cyber and privacy attacks and data breaches (including personal data breaches) in the energy sector.
- Ensured continuity of the critical business energy operations and resilience against cyberattacks, including large scale, demonstrating effective solutions to a) the real-time constraints of an electric system, b) barriers to the cascading effect and c) the adaptation of legacy equipment or their coexistence with state of the art technology.
- The energy sector is better enabled to easily implement the NIS directive.
- A set of standards and rules for certification of cybersecurity components, systems and processes in the energy sector will be made available.
- Cyber protection policy design and uptake at all levels from management to operational personnel, in the energy sector.
- Manufacturers providing more accountability and transparency, enabling third parties monitoring and auditing the privacy, data protection and security of their energy devices and systems.

SU-INFRA01-2018-2019-2020: Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe

Frist: 27. August 2020

- Forecast, assessment of physical and cyber risks, prevention, detection, response, mitigation of consequences and fast recovery after incidents
- Interrelations between different types of critical infrastructure
- *NB! Energy (Gas networks), Transport (Airports), Sensitive industrial sites and plants have already got funding* (oil&offshore, ports/railways/multimodal, water systems, space, health, e-commerce and postal, financial more likely in last round)

SU-INFRA01-2018-2019-2020: Expected impact (short term)

- State-of-the-art analysis of physical/cyber detection technologies and risk scenarios, in the context of a specific critical infrastructure.
- Analysis of both physical and cyber vulnerabilities of a specific critical infrastructure, including the combination of both real situation awareness and cyber situation awareness within the environment of the infrastructure.
- In situ demonstrations of efficient and cost-effective solutions to the largest audience, beyond the project participants.

SU-INFRA01-2018-2019-2020: Expected impact (medium term)

- Innovative (novel or improved), integrated, and incremental solutions to prevent, detect, respond and mitigate physical and cyber threats to a specific Critical Infrastructure.
- Innovative approaches to monitoring the environment, to protecting and communicating with the inhabitants in the vicinity of the critical infrastructure.
- Security risk management plans integrating systemic and both physical and cyber aspects.
- Tools, concepts, and technologies for combatting both physical and cyber threats to a specific critical infrastructure.
- Where relevant, test beds for industrial automation and control system for critical infrastructure in Europe, to measure the performance of critical infrastructure systems, when equipped with cyber and physical security protective measures, against prevailing standards and guidelines.
- Test results and validation of models for the protection of a specific critical infrastructure against physical and cyber threats.
- Establishment and dissemination throughout the relevant user communities of specific models for information sharing on incidents, threats and vulnerabilities with respect to both physical and cyber threats.

SU-INFRA01-2018-2019-2020: Expected impact (long term)

- Convergence of safety and security standards, and the pre-establishment of certification mechanisms.
- Secure, interoperable interfaces among different critical infrastructures to prevent from cascading effects.
- Contributions to relevant sectorial frameworks or regulatory initiatives.

Brainstorming session

Analysis of impact of the calls:

- Expected impact
- Innovation
- Societal
- Barriers

SINTEF

Teknologi for et bedre samfunn