Utfordringer innen digital sikkerhet og NTNUs rolle

NTNU
Kunnskap for en bedre verden

Nils Kalstad (nils.kalstad@ntnu.no) Head of Department || Center Host
Department of Information Securitry and Communication Technology || Center for Cyber and Information Security
www.ntnu.no/iik www.ntnu.no/ccis

NTNU Department of Information Security and Communication Technology

Operational ability

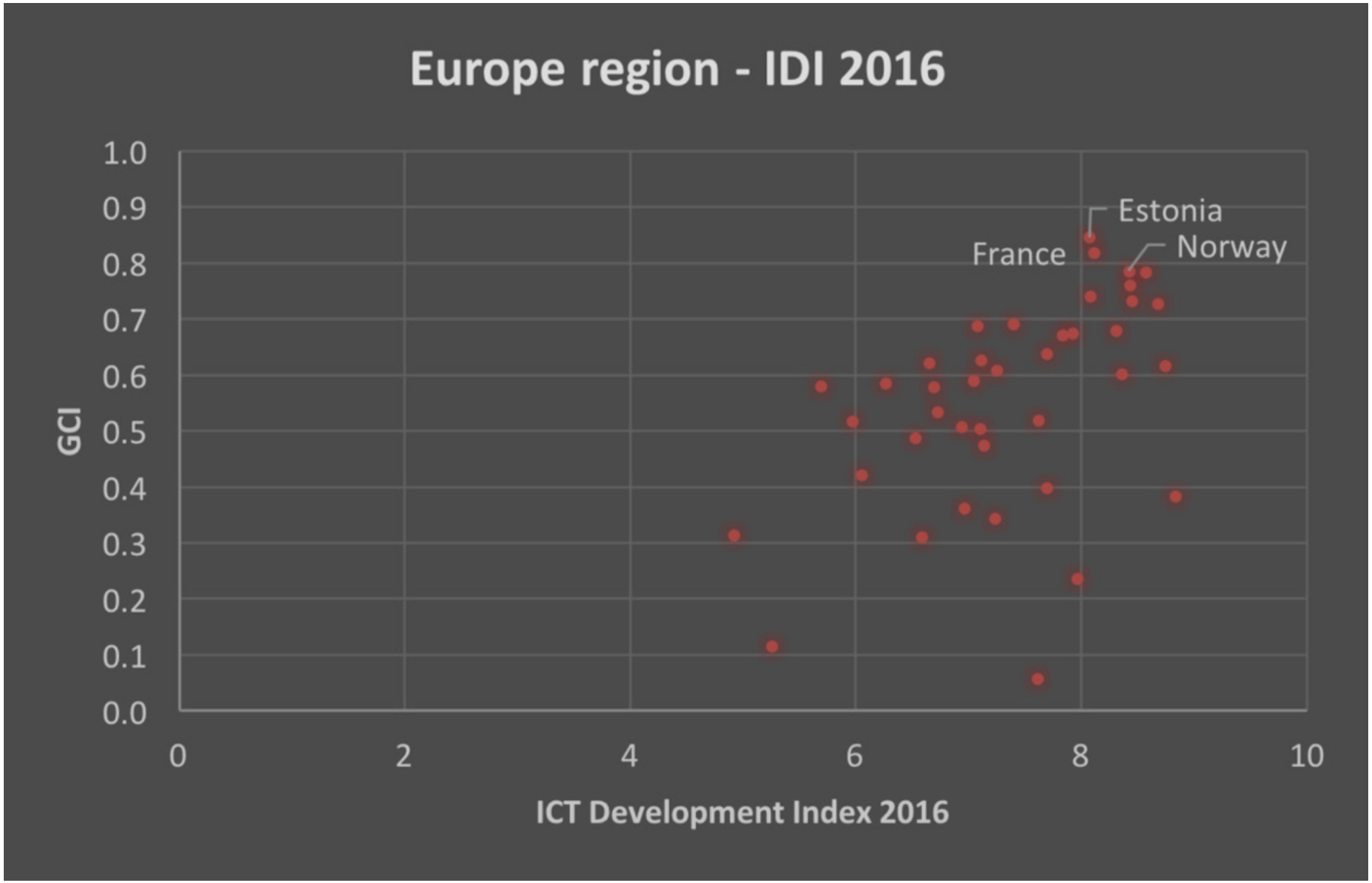
- 10 % increase in digitalization
  0.75% increas of GDP[1)]
- Estimated cost of cyber crime in Norway:
  0.64% fo GDP[2)]

24.000.000.000 NOK/yr

vs

19.000.000.000 NOK/yr

1) World Economic Forum: The Global Information Technology Report 2013 (http://www3.weforum.org/docs/WEF_GITR_Report_2013.pdf)
2) https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf



ITU Global Cyber Security Index 2017: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

Interdisciplinary Content

- **Confidentiality.** Rules that limit access to system information to authorized persons.
- **Integrity.** Assurance that information is accurate and trustworthy.
- **Availability.** Information is accessible.
- **Risk.** Potential for gain or loss.
- **Adversarial Thinking.** A thinking process that considers the potential actions of the opposing force working against the desired result.
- **Systems Thinking.** A thinking process that considers the interplay between social and technical constraints to enable assured operations.

ECS

EUROPEAN CYBER SECURITY ORGANISATION

Contract for Public Private Partnership (cPPP) signed on July 5th 2016.

- The Commission: 450 new million € in H2020
- ECSOs members: 1350 million €

Working groups

1. Standardisation, certification, labeling and supply chain management
2. Market deployment, investments and international collaboration
3. Sectoral demand
4. Support SMEs, coordination with countries and regions
5. Education, awareness, training and exercises
6. Strategic research and innovation agenda

Luigi Rebufi (ECSO) and Gunter Oettinger (Commissioner for Digital Economy and Society)

Norwegian ECSO members are NTNU, SINTEF, Simula@UiB, and the Norwegian Research Council.

Oettinger:«Europe needs high quality, affordable and interoperable cyber security products and services»

INDUSTRY 4.0 AND ICS SECTOR REPORT

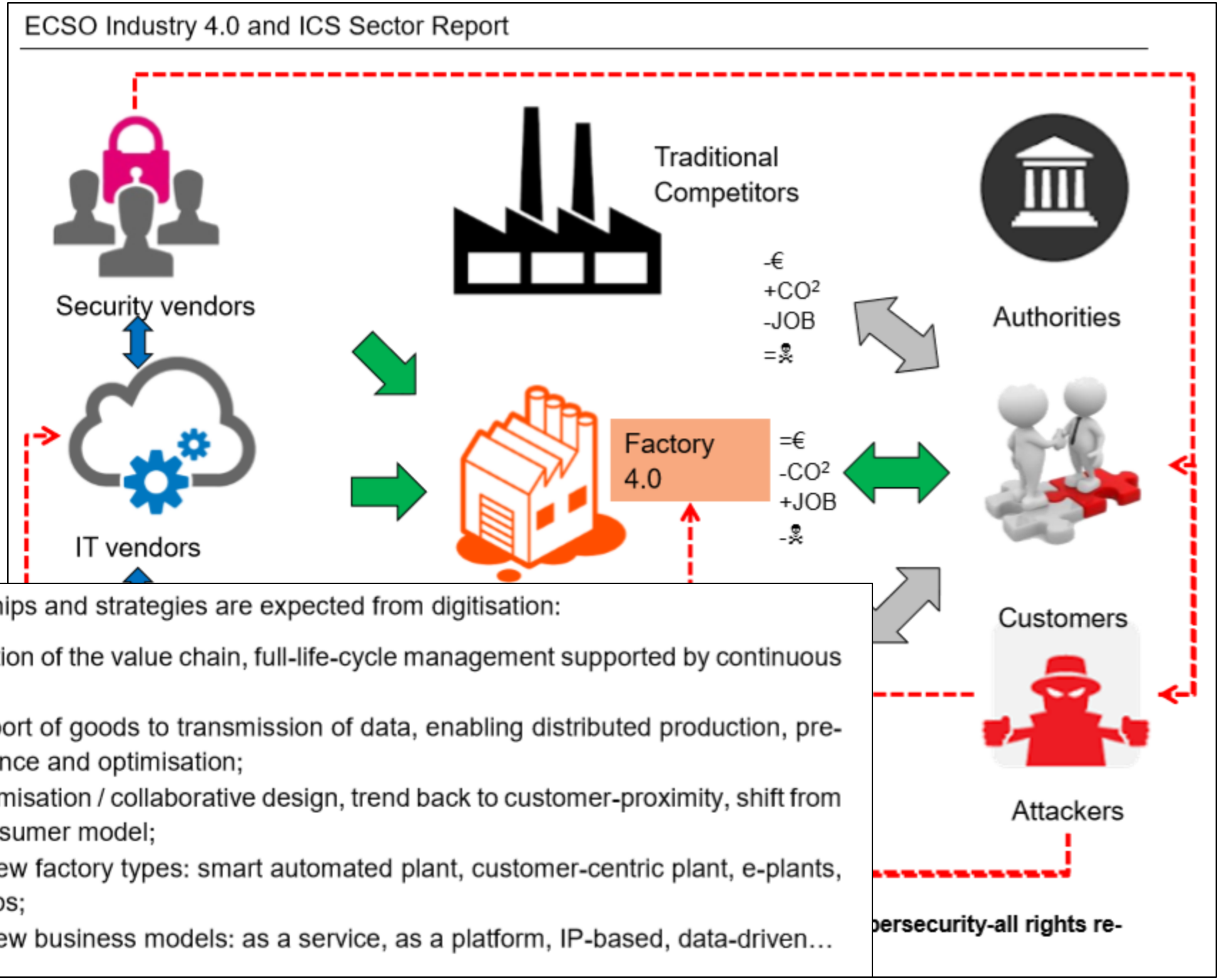
Cyber security for the industry 4.0 and ICS sector

WG3 I Sectoral Demand

MARCH 2018

https://www.ecs-org.eu/documents/publications/5ad7268b92497.pdf

ACCENTURE(Belgium)
AIRBUS Defence & Space - CyberSecurity (France)
aizoOn(Italy)
ALTRAN(France)
APPLUS Laboratories - (Spain)
ATOS Spain (Spain)
BDR – Bundesdruckerei(Germany)
BOSCH(Germany)
Bureau Veritas (France)
CERTSIGN(Romania)
CY4GATE S.r.l. - Elettronica S.p.A. Group (Italy)
DGS S.p.A(Italy)
Engineering Ingegneria Informatica(Italy)
Ericsson(Sweden)
EVERIS Aerospace and Defence (Spain)
Exprivia (Italy)
F-Secure Corporation(Finland)
Giesecke + Devrient Mobile Security GmbH(Germany)
GEMALTO(The Netherlands)
GMV Soluciones Globales Internet (Spain)
Huawei Technologies (Belgium)
HP Inc. - HP Belgium BVBA(Belgium)
IBM (Ireland)
IDEMIA - Idemia Identity & Security France
INDRA(Spain)
Infineon Technologies (Germany)
Intel Corporation (Belgium)
Leonardo - Finmeccanica (Italy)
Microsoft Corporation(Belgium)
NAVAL Group(France)
NEC Laboratories Europe GmbH (Germany)
NOKIA BELL LABS(France)
NXP Semiconductors Netherlands B.V.(The Netherlands)
Rohde & Schwarz Cybersecurity (Germany)
S21SEC - Grupo S21SEC (Spain)
SAP(Germany)
Schneider Electric(France)
SECUNET Security Networks AG(Germany)
SELTA (Italy)
SGS Group(Switzerland)
SIEMENS AG(Germany)
STMicroeletronics International (Switzerland)
STM-Savunma Teknolojileri Mühendislik ve Ticaret (Turkey)
THALES Communications and Security(France)
TID - Texas Instruments Deutschland(Germany)
TÜV SÜD Management Service (Germany)
TÜVIT - TÜV Informationsteknik - (Germany)
UL TS B.V.(The Netherlands)
VITROCISET(Italy)



Some shifts in relationships and strategies are expected from digitisation:

- Growing integration of the value chain, full-life-cycle management supported by continuous data-thread;
- Shift from transport of goods to transmission of data, enabling distributed production, predictive maintenance and optimisation;
- Enhanced customisation / collaborative design, trend back to customer-proximity, shift from consumer to prosumer model;
- Emergence of new factory types: smart automated plant, customer-centric plant, e-plants, mobile workshops;
- Emergence of new business models: as a service, as a platform, IP-based, data-driven…

	New Business models	New use cases
Demand pull	Production optimisation Data-centric Business model Managed security services (MSSP)	Sharing economy Horizontal economy Product personalisation

Industry 4.0

The overall Industry 4.0 market was valued[11] at USD **66.67 billion in 2016** and is expected to reach USD **152.31 billion by 2022**, at a **CAGR of 14.72% between 2017 and 2022**. Increasing adoption of industrial Internet and increased focus on efficiency and cost of production plays a significant role in the growth of the Industry 4.0 market. However, lack of cost–benefit analysis and a shortage of skilled workforce are key factors limiting the growth of this market.

ICS security

The Industrial control systems (ICS) security market size is expected[12] to grow from USD **10.24 Billion in 2017** to USD **13.88 Billion by 2022**, at a **CAGR of 6.3%**. The exponential rise in cyber-attacks and network security threats, huge investments in smart technologies, and support from government organisations for ICS security are some of the factors fueling the growth of the industrial control systems security market across the globe. The base year considered for this study is 2016 and the forecast period considered is 2017–2022.

Virtual / Augm. reality
Next generation HMIs

Additive Manuf.
3D printing

Adrien Bécue, Airbus Cyberse-

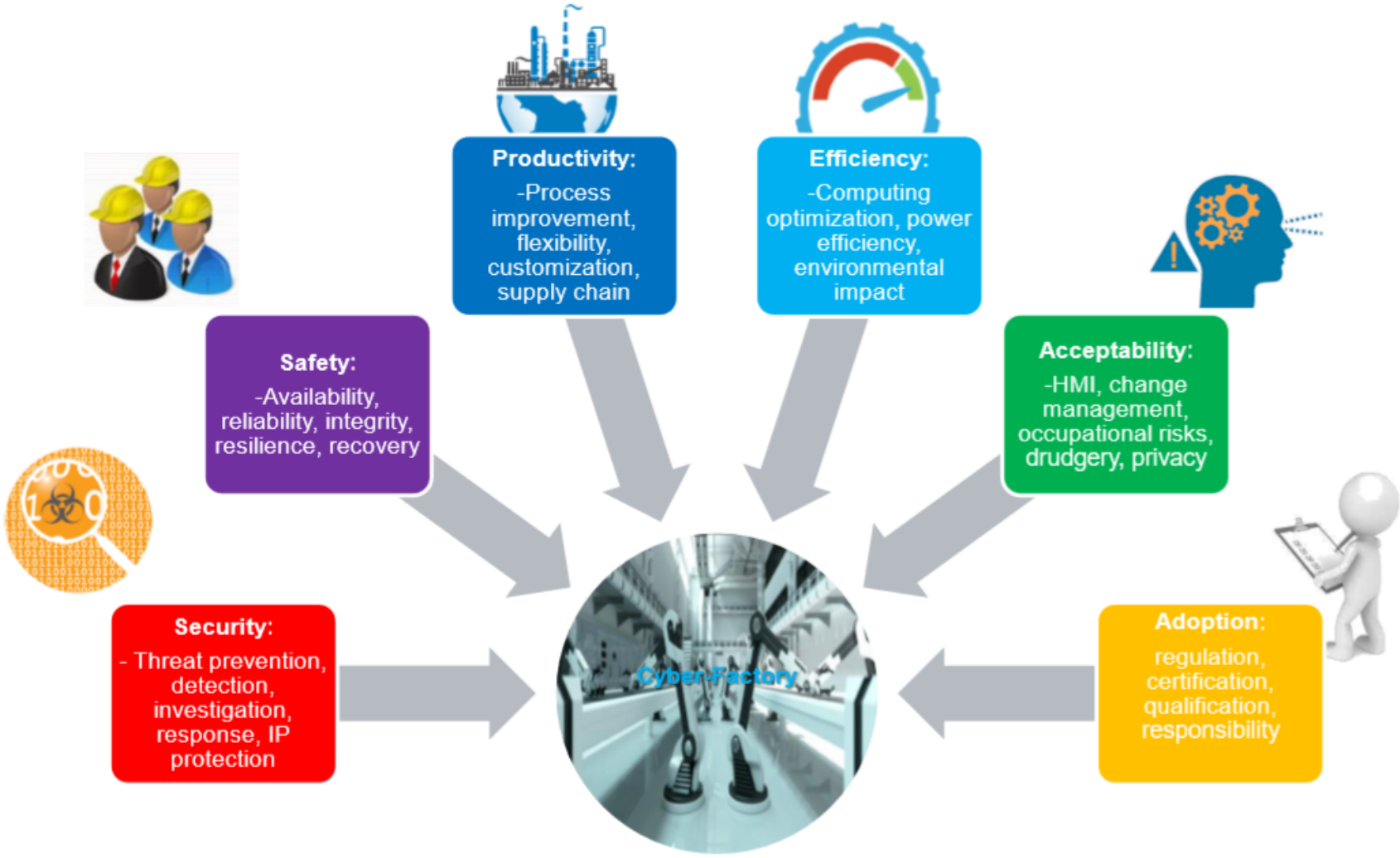


Figure 2 - Industry 4.0 Ecosystem Overview, source: Adrien Bécue, Airbus Cybersecurity-all rights reserved

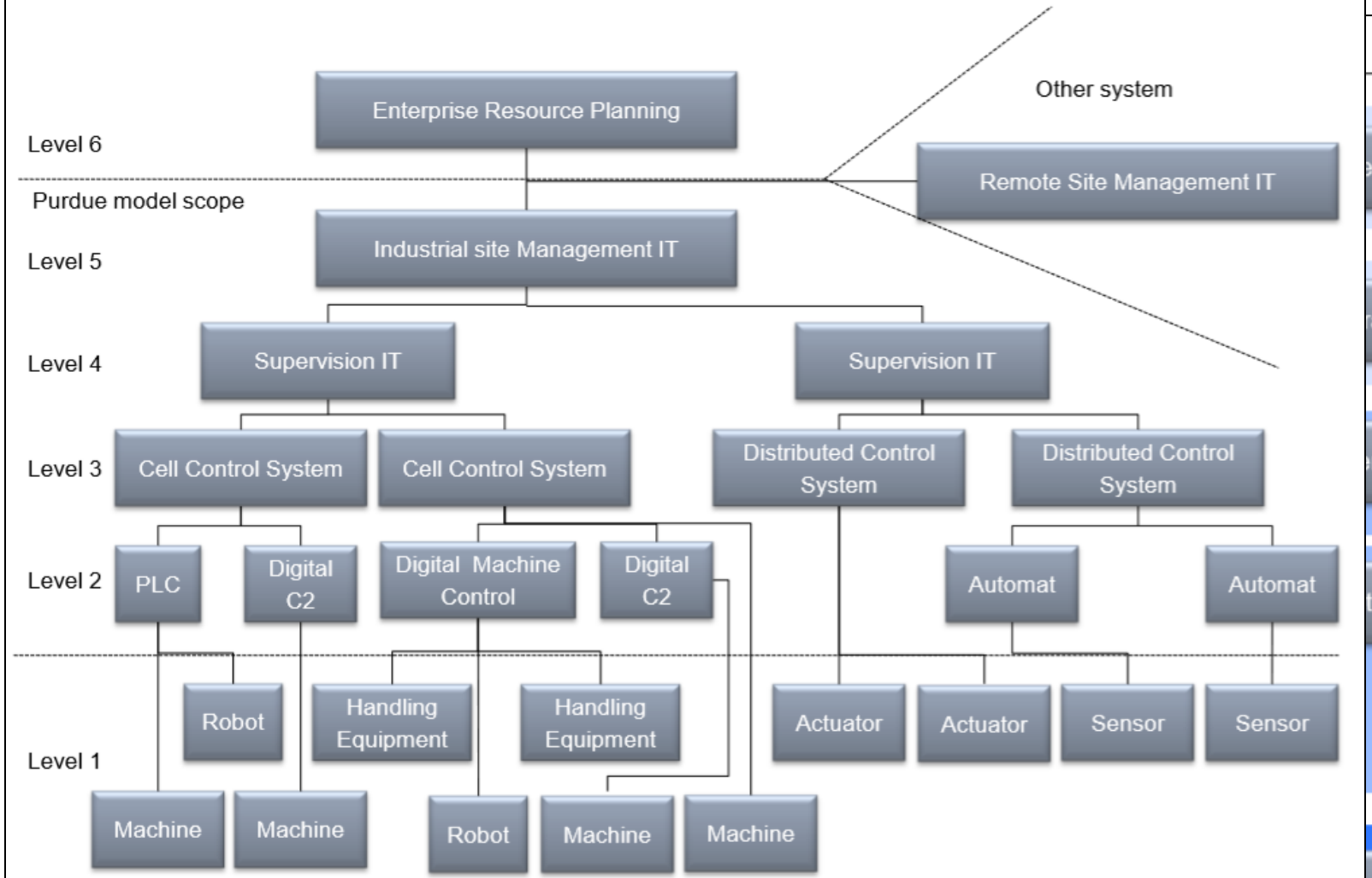


Figure 4 – Supervision tree of industrial control system[3]

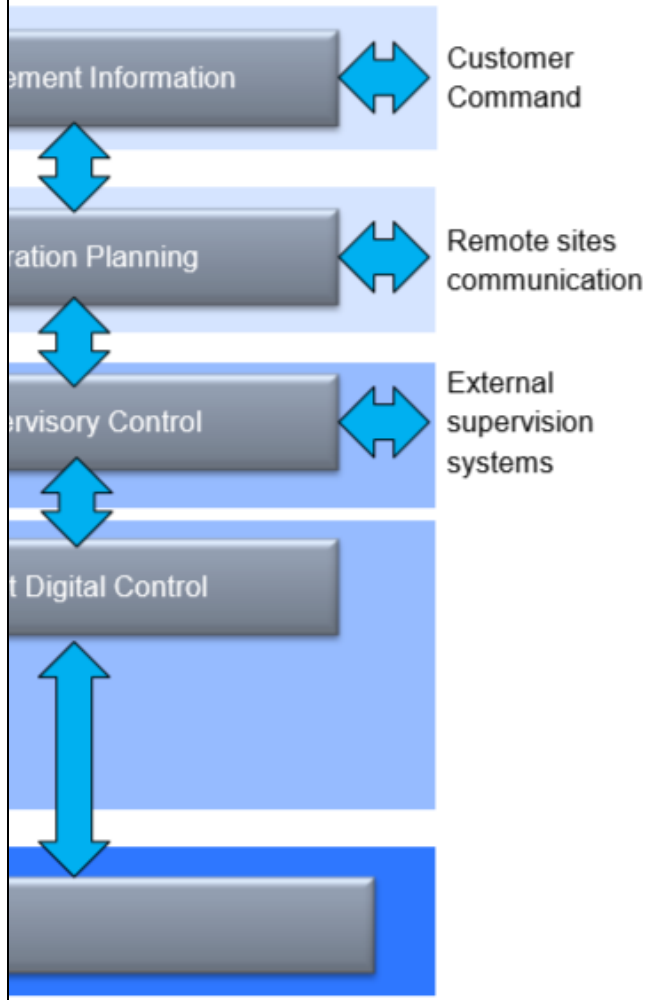
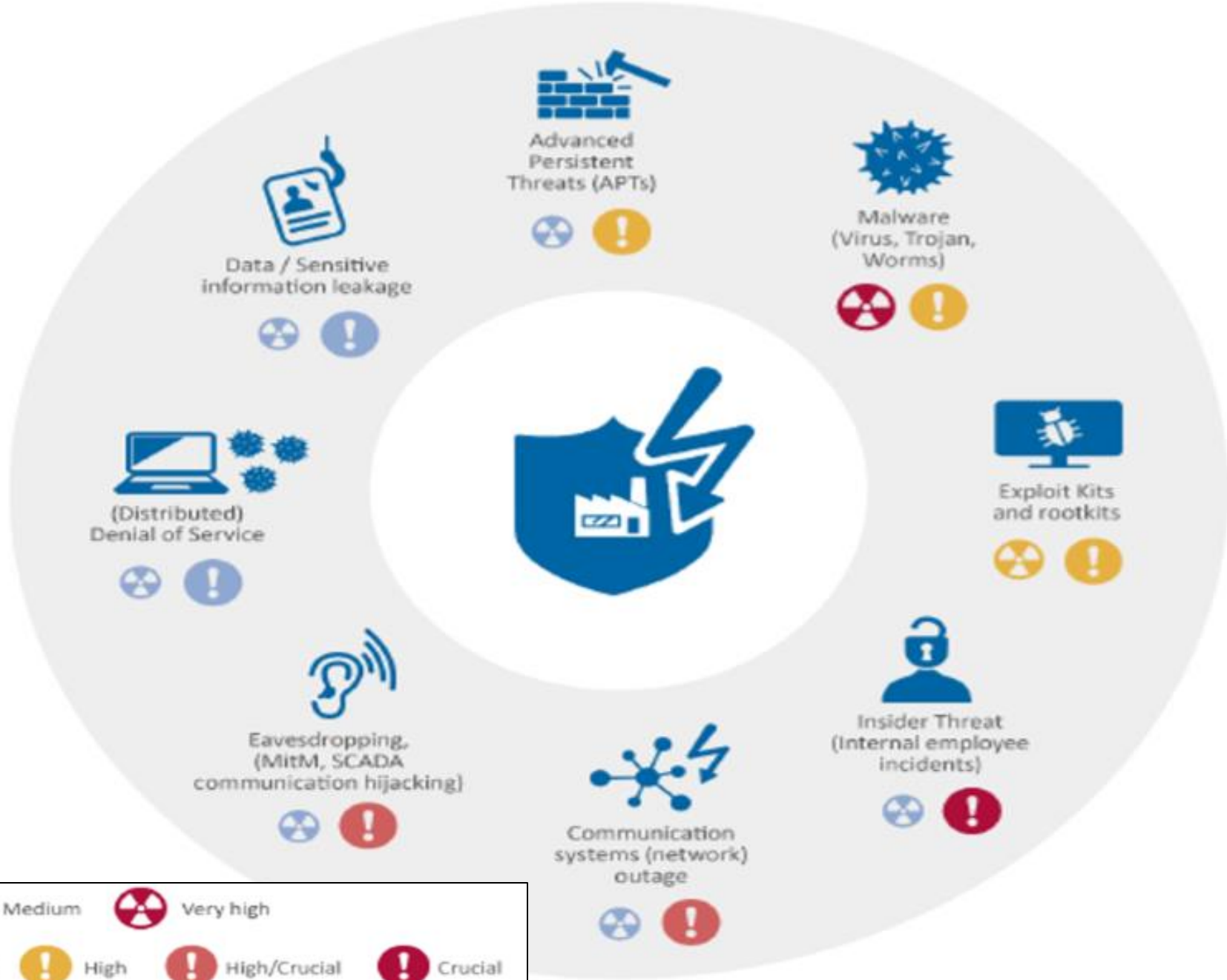


Figure 3 – Reference system architecture for Industrial Control Systems[2]


Advanced Persistent Threats (APTs)
Malware (Virus, Trojan, Worms)
Data / Sensitive information leakage
(Distributed) Denial of Service
Exploit Kits and rootkits
Eavesdropping, (MitM, SCADA communication hijacking)
Insider Threat (Internal employee incidents)
Communication systems (network) outage
Likelihood: Low Medium Very high
Impact: Medium /High High High/Crucial Crucial

Cybersikkerhetsutfordringer

1. Konvergens mellom «safety» og «security»
2. Cybersikkerhet i tingenes industrielle internett (IIoT)
3. Inntrengningsdeteksjon i industrielle kontrollsystemer
4. Forstå det cyber-fysiske trusselbildet
5. Menneskelige og organisatoriske endringer
6. Sikkerhet i verdikjeden

ECSO: The integrated nature of Industry 4.0-driven operations means that cyber-attacks can have devastating effects.

For cyber risk to be adequately addressed in the age of industry 4.0, cyber security strategies should be secure and fully integrated into organisational and information technology strategy from the start. Cyber security should become an integral part of the strategy, design, and operations, considered from the beginning of any new connected, Industry 4.0 driven initiative.

CCIS Centre for Cyber and Information Security

Information Security and Privacy Management

Cyber Defence

Critical Infrastructure Security and Resilience

e-Health and Welfare Security

System Security

Norwegian Biometrics Laboratory

Applied Cryptography

NTNU Digital Forensics Group

NTNU

Norges teknisk-naturvitenskapelige universitet

Statkraft

IBM

KRIPOS

FORSVARET

Datatilsynet

telenor

NorSIS

mnemonic

POLITIET OSLO POLITIDISTRIKT

FFI

Sykehuset Innlandet HF

Statnett

ØKOKRIM

Nasjonalt ID-senter

NC-Spectrum

NASJONAL SIKKERHETSMYNDIGHET

POLITIET

KPMG

pwc

Eidsiva

OPPLAND fylkeskommune

WATCHCOM

HØGSKOLEN I INNLANDET

POLITIHØGSKOLEN

PST

www.ccis.no

North European Cybersecurity Cluster (NECC)

FISC
Finnish Information Security Cluster

BLUE SCIENCE PARK
KARLSKRONA

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

EISA

ERICSSON

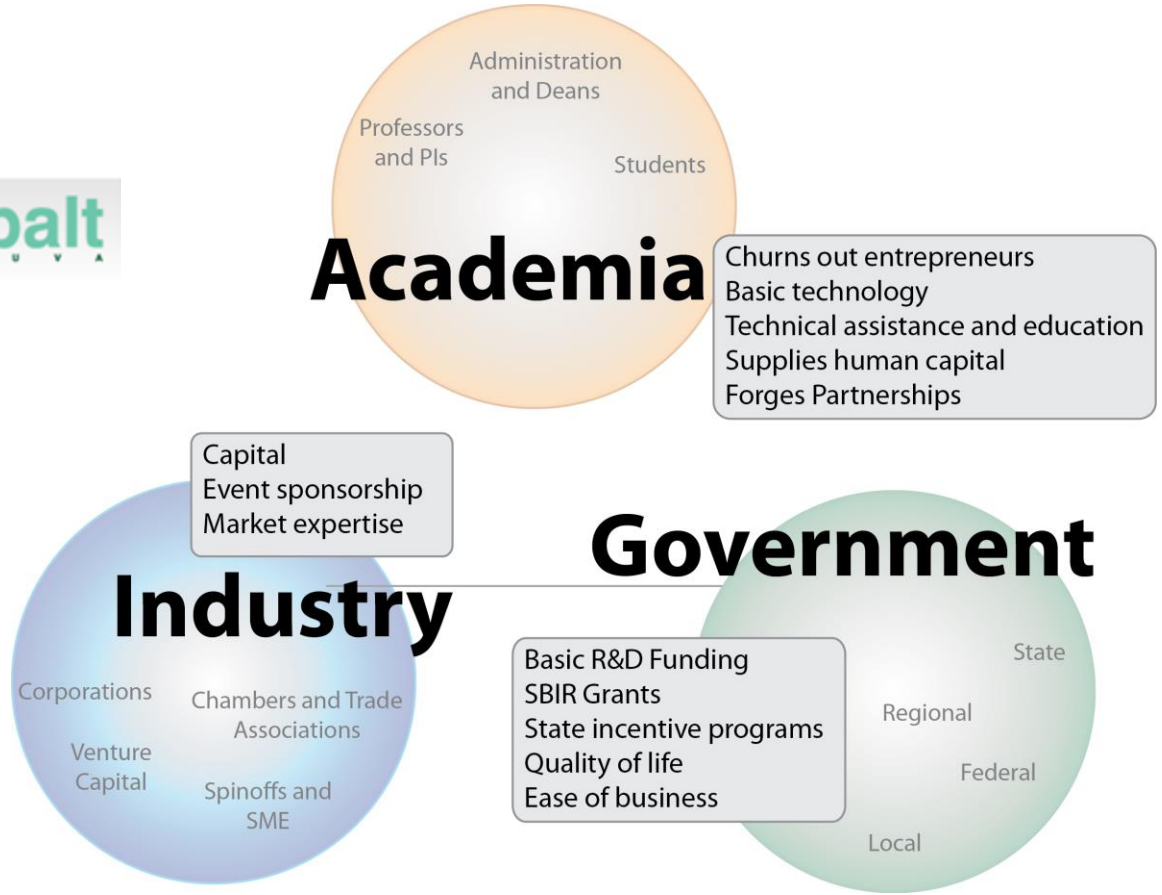
infobalt

CenSec
CENTER FOR DEFENCE, SPACE & SECURITY

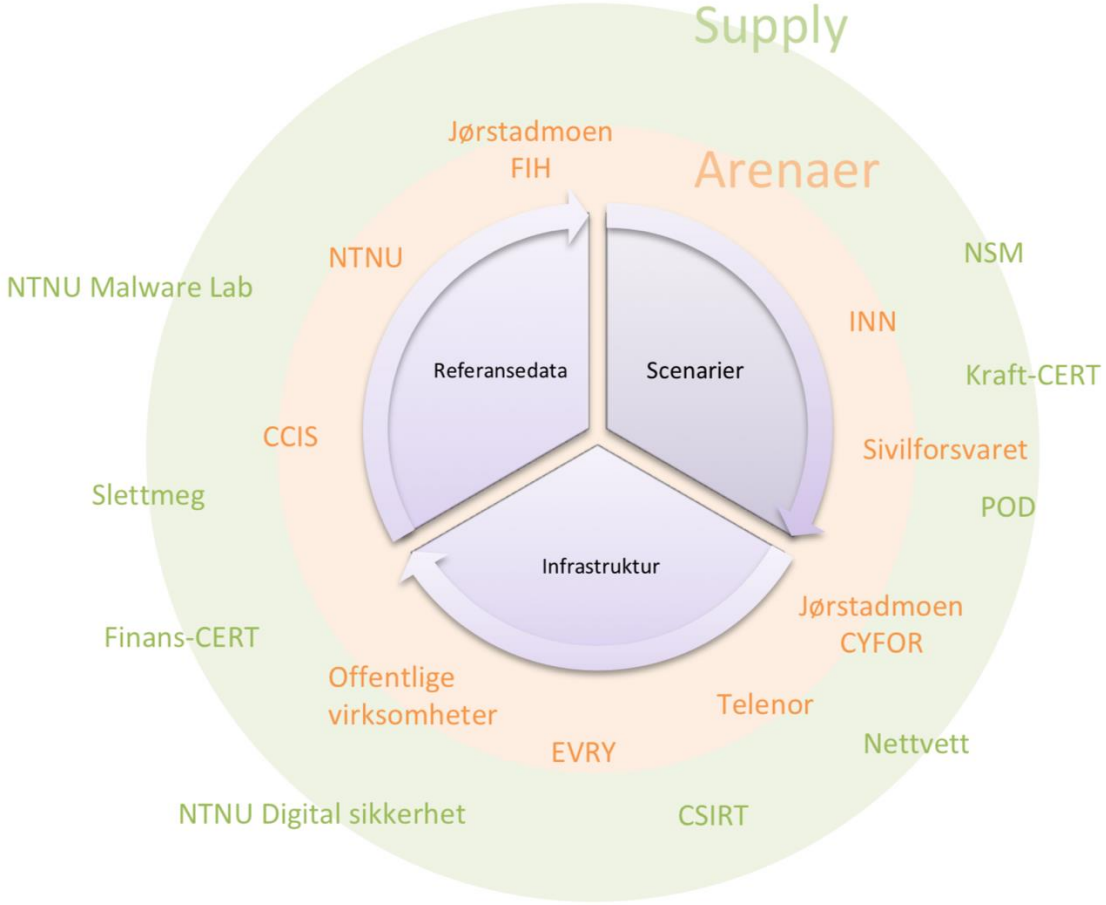
VTT

NTNU CCIS
Center for Cyber and Information Security

LIKTA
Latvijas Informācijas un komunikācijas tehnoloģijas asociācija



- Engage North European Industries in cybersecurity
- Position Nordics and North of Europe us in Europe
- Define a Nordic speciality in the field



SOCIETY

- Strategic, policy and regulation level

DIGITAL VALUE CHAINS

- Operational and tactical decision level

CYBER INFRASTRUCTURE

- Technical and design decision level

Departementene

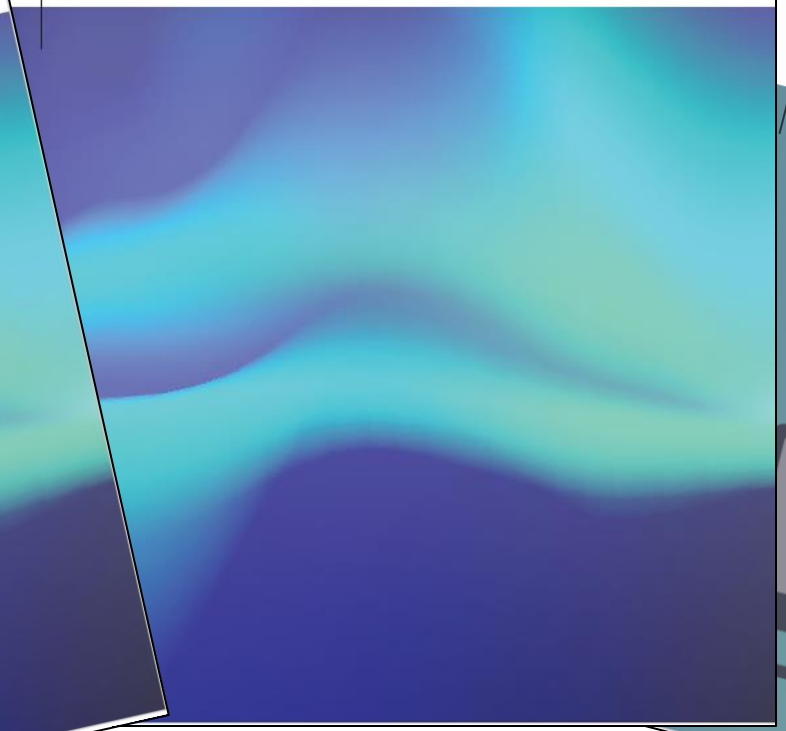
Strategi

Nasjonal strategi for digital sikkerhet

Departementene

Tiltaksoversikt

Tiltaksoversikt til nasjonal strategi for digital sikkerhet



Departementene

Strategi

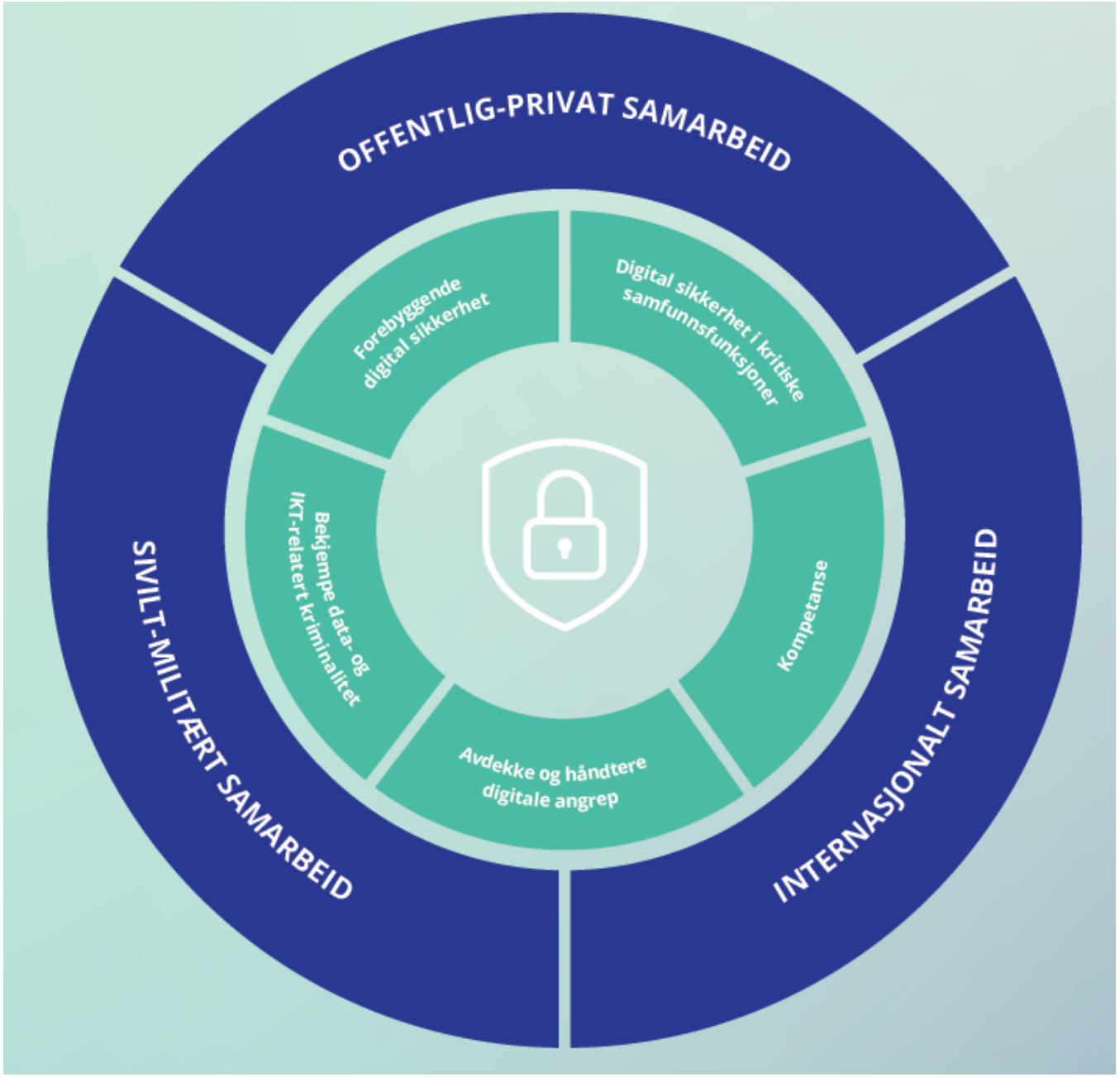
Nasjonal strategi for digital sikkerhetskompetanse

NTNU sin rolle

Nasjonal hovedleverandør av forskning, utdanning og kompetanse relevant for fokusområdene i strategien

Strategiens 5 satsningsområder sammenfaller med aktiviteter i NTNU

NTNU fokuserer på offentlig privat, sivil-militært og internasjonalt samarbeid både gjennom våre partnerskap (CCIS og NCR) og øvrige prosjekter



Eksplisitte referanser til NTNU

Tiltak 27: Norwegian Cyber Range (NCR)

Norwegian Cyber Range (NCR) er den første nasjonale test- og øvingsarenaen for cyber- og informasjonssikkerhet på tvers av alle samfunnssektorer. NCR skal både være en akademisk og kommersiell øvingsarena, og på sikt også tilby kommersielle tjenester mot ulike markedssegmenter både privat og offentlig.

Testing, trening og øving er virkemidler for å eksponere virksomheter og mennesker for hendelser i realistiske, men trygge omgivelser. NCR sikrer effektiv og virkelighetsnær kompetansebygging, og kobler sammen samfunnsmodeller, digitale verdikjeder og digital infrastruktur i ett eller flere definerte miljøer. I tillegg vil man ut fra en slik øvingsarena kunne legge til rette for målrettet etter- og videreutdanningstilbud innenfor nasjonal IKT-sikkerhet.

NTNU har fått støtte fra fylkeskommunen i Oppland på 20 mill. kroner fordelt over tre år til å bygge opp NCR. Dette gjøres som en del av et samarbeid med Cyberforsvaret, Sivilforsvaret, Telenor Norge, EVRY, NorSIS, NSM og mnemonic gjennom NTNUs Center for Cyber and Information Security (NTNU CCIS).

Samarbeidet inkluderer også et felles prosjekt med Estland. Denne delen av prosjektet kalles «Open Cyber Range». Estland og Norge har fått 32 mill. kroner av EØS-midlene for å bli bedre til å bekjempe cyberkriminalitet. Prosjektet ledes av Estlands forsvars-departement, med deltagelse fra Teknologiuniversitet i Tallinn og NTNU sitt Institutt for informasjonssikkerhet og kommunikasjonsteknologi.

Ansvarlig virksomhet: NTNU
Gjennomføres: Lansert 2018

Styrke kjernemiljøene ved en kryptologisatsing fra 2018

Basisbevilgningen fra JD til NTNU CCIS (fra 2016) er på 5 mill. kroner årlig til områder som personvern, digital etterfors-kning og biometri. HOD bidrar til grunnbevilgningen med 2

En pilot om opplæring av barn og ungdom i regi av NSM, NVE, NorSIS, NTNU, UiO og Abelia i Oppegård, Ski og Rogaland.

Piloten er finansiert gjennom et spleiselag fra norske myndig-

CyberSec4Europe – et pilotprosjekt som del av den fremtidige etableringen av et felles europeisk kompetansenettverk for digital sikkerhet:

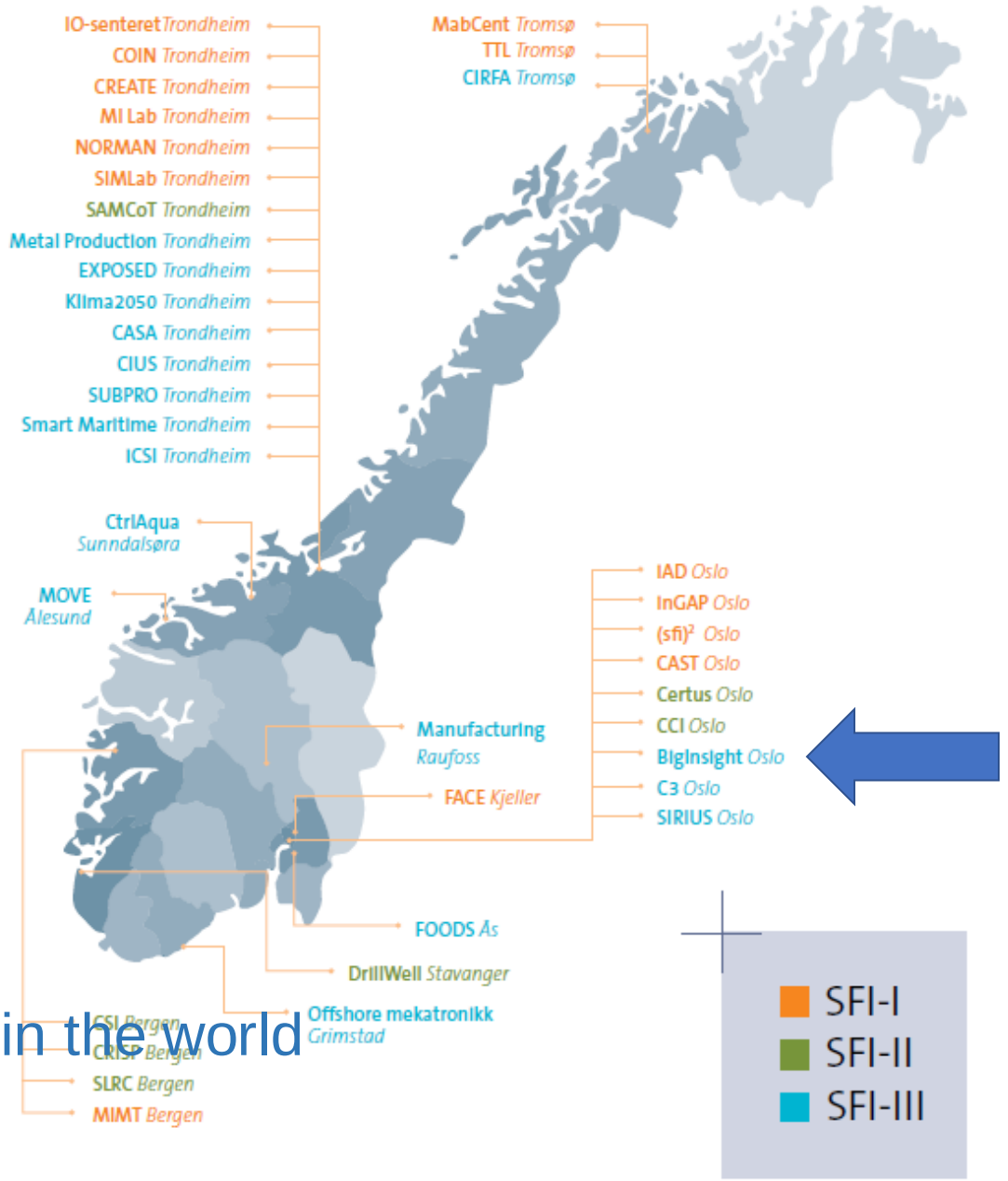
Pilotprosjektet startet ved årsskiftet 2018/2019. Formålet med

European Cyber Security Challenge i regi av ENISA

Dette er en nasjonal og internasjonal konkurranse for å synliggjøre unge talenter. En juniorgruppe 16-20 år og en seniorgruppe 21-25 år. NTNU CCIS står for den norske kon-kurransen. Slike tiltak kan bidra til å skape blest og medie-oppmerksomhet om kompetanse på digital sikkerhet blant ungdom og unge voksne.

Norske sentre for forsknings-drevet innovasjon (SFI)

None on information or cyber security



Norway is the most digitalized country in the world

Sønadsfrist 25. september

NTNU CCIS

Center for Cyber and Information Security

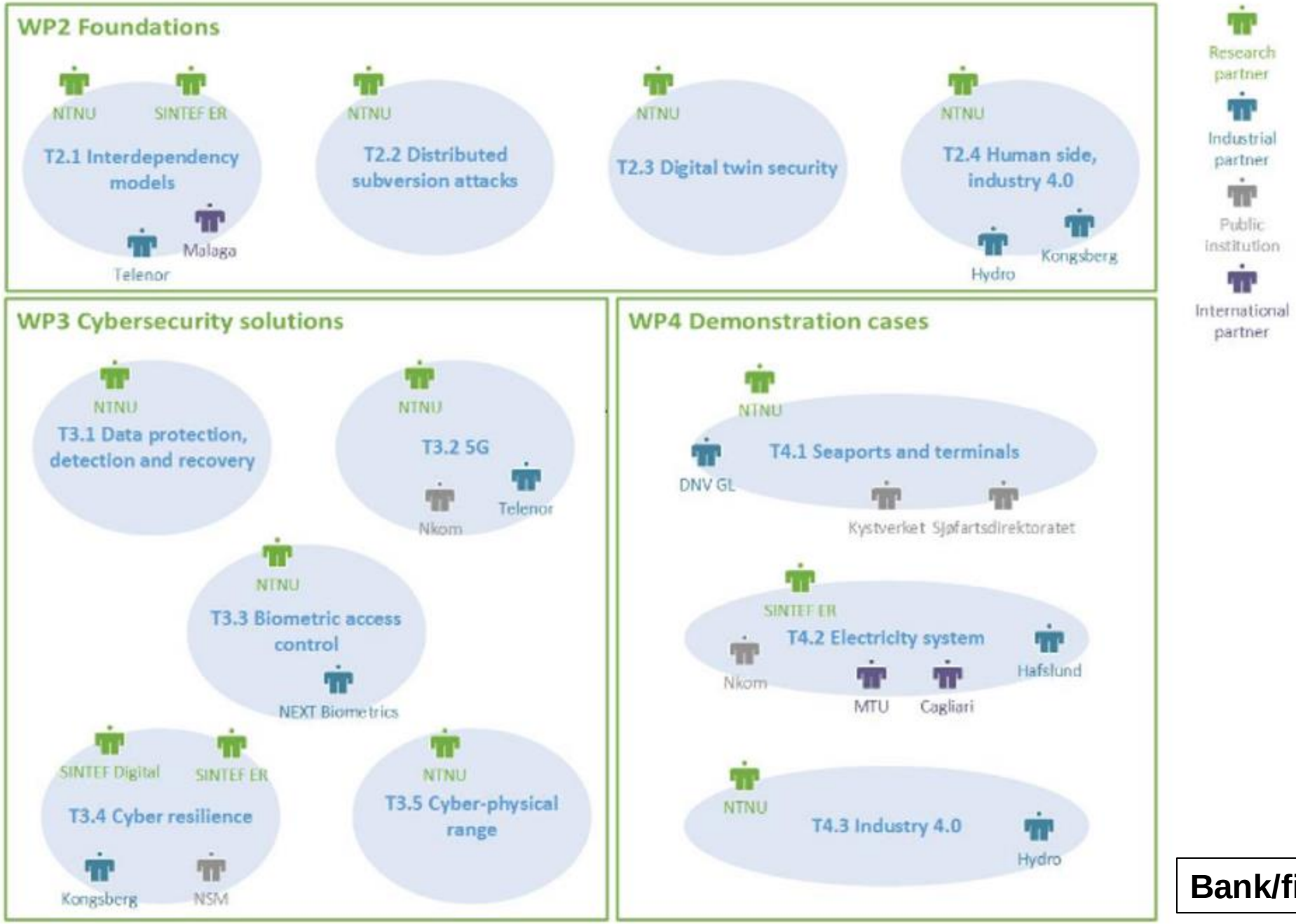
Senter for forskningsdrevet innovasjon

Norges forskningsråd

Norwegian Center of Excellence for Critical Infrastructure Cyber-Physical Security (NORCICS)

Sokratis K. Katsikas
Center for Cyber & Information Security
Dept. of Information Security & Communication Technology
Norwegian University of Science & Technology
sokratis.katsikas@ntnu.no

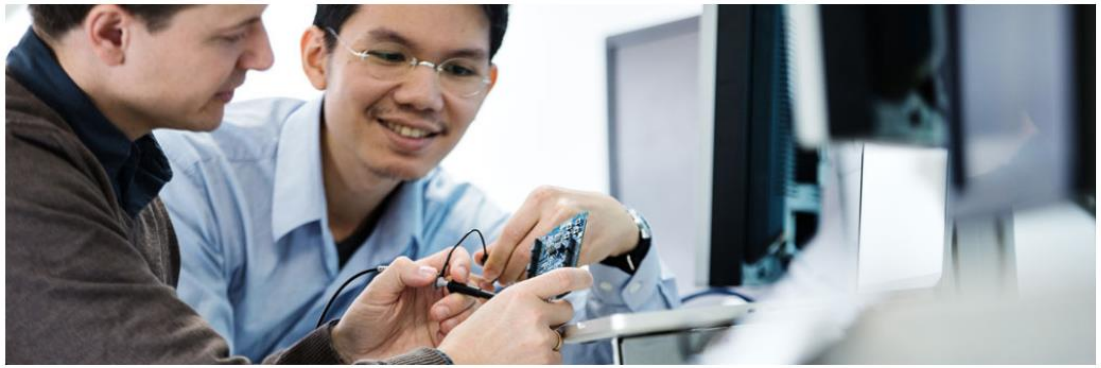
Research tasks



Bank/finans?

FAKULTET FOR INFORMASJONSTEKNOLOGI OG ELEKTROTEKNIKK

Institutt for informasjonssikkerhet og kommunikasjonsteknologi



Ved Institutt for informasjonssikkerhet og kommunikasjonsteknologi (IIK) utøves forskning innen cybersikkerhet, informasjonssikkerhet, kommunikasjonsnettverk og nettverkstjenester. Instituttet betjener studieprogrammer på doktor-, master-, og bachelorgradsnivå innen informasjonssikkerhet og kommunikasjonsteknologi. IIK er også vert for Center for Cyber and Information Security (CCIS) og Norges nasjonale forskerskole innen data og informasjonssikkerhet (COINS). IIK er et av åtte institutter ved Fakultet for informasjonsteknologi og elektroteknikk.

Kontakt

- Instituttleder: Nils K. Svendsen
- Ansatte ved instituttet
- 61 13 54 00 (Gjøvik)
- 73 59 45 33 (Trondheim)
- kontakt@iik.ntnu.no

- Kontakt oss
- Om oss
- Ledige stillinger – Trondheim
- Ledige stillinger – Gjøvik

Forskning

Forskning ved Institutt for informasjonssikkerhet og kommunikasjonsteknologi (på engelsk)

Studier

Studier ved Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Nyheter

Tweets by @IIK_NTNU

IIK_NTNU @IIK_NTNU

Flott artikkel som profilerer IIKs Frank Kraemer og David Palma. «IoT har ennå ikke hatt sitt iPhone øyeblikk» gemini.no/2018/03/tingen…

Tingenes internett nærmer seg

Veier varsler fra når de er glatte. Søppeldunker når de bør tømmes.

gemini.no

Mar 6, 2018

IIK_NTNU Retweeted

The Department of Information Security and Communication Technology

- 80 employees in Gjøvik and Trondheim
- Research in areas of biometrics, cyber defence, critical infrastructure protection, cryptography, digital forensics, e-health and well being, intelligent transportation systems, internet of things, information security management, malware, quantitative modelling of dependability and performance
- 1 bachelor (90), 2 master (100 + 25), 5 yrs master (45) and PhD (2) educations
  Offer flexible and part time study programs
- Forskningsprosjekter: EU H2020 (5), EU FP7 (4), EU Cost (1), EDA (1), IARPA Odin Thor (1), NFR FME (1), NFR IKT+ (4), NFR ENERGIX (1), NFR BIA (2), NFR Forskerskole (1), NFR NæringsPhD (1), RFF (4)
  Totally 40 MNOK in 2017 (45% of the department budget)
- Public private partnership: NTNU Center for Cyber and Information Security
- Innovation platform: Norwegian Cyber Range