NORCICS

SFI Norwegian Centre for Cybersecurity in Critical Sectors

# Annual Report **2020**

sfi Centre for Research-based Innovation
The Research Council of Norway

NTNU

# Contents

Summary 1

Background 2

NORCICS vision and objectives 3

Our research strategy and plans 4

How NORCICS is organized 5

Scientific activities and results 8

International cooperation 9

Recruitment 10

Communication and dissemination activities 11

Appendices 15

**NORCICS's** vision is to contribute to making Norway the **most securely digitalized country** in the world

# Summary

The Norwegian Centre for Cybersecurity in Critical Sectors (NORCICS) is a research-based innovation centre (SFI) with a 5 – 8 year project period, supported by the Research Council of Norway. The centre is hosted at the Norwegian University of Science and Technology (NTNU) and engages research and industry partners in both public and private sectors.

NORCICS was established in 2020 and officially started operations on October 1st 2020. The first months of operation in 2020 mainly included strategy development and planning for the long-term project, including creating a workplan for 2021.

NORCICS's vision is to contribute to making Norway the most securely digitalized country in the world, by improving the cyber security and resilience of its critical sectors, through supporting research-based innovation. NORCICS contributes to all five strategic goals of the National Cybersecurity Strategy for Norway.

NORCICS follows a holistic, comprehensive and systemic approach addressing people, processes and technology to protect critical sectors throughout the cybersecurity core functions (identify, protect, detect, respond, recover). NORCICS adopts the Open Innovation Model, and the Technology Transfer model for joint industry-research groups research-based innovation, thus allowing its user partners to participate in shaping research and innovation roadmaps. Within NORCICS, the research is organized into three work packages, aiming at improving our understanding of the cybersecurity-related issues in critical sectors; at developing solutions for addressing these issues; and at validating and demonstrating these solutions in a number of critical sectors.

The consortium members have complementary expertise that collectively covers most of the areas of fundamental research, the sectorial domains and the technological applications of cybersecurity. The user partners come from both the public and the private sector and cover all the critical sectors addressed in NORCICS. Additionally, a number of internationally highly reputed centers active in the field of cybersecurity have confirmed their collaboration with NORCICS.

As the centre is in its start-up phase, this first annual report serves more as a public overview of the project rather than a report on completed scientific work.

# Background

## The need

The National Cybersecurity Strategy for Norway acknowledges the need to "address the (cybersecurity) challenges that will inevitably arise in conjunction with the rapid and far-reaching digitalization of Norwegian society". Additionally, in Digital21 -Norway's national strategy on digitalization- cybersecurity is one of the six prioritized areas.

NORCICS contributes to all five strategic goals of the National Cybersecurity Strategy for Norway, which are 1) secure the digitalization of Norwegian companies and protect them against cyber incidents; 2) support critical societal functions with robust and reliable digital infrastructures; 3) improve cyber security competence in line with societal demands; 4) advance the ability to detect and handle cyber-attacks; and 5) strengthen the police in their ability to prevent and combat cybercrime.

NORCICS focuses on the need of organizations within Critical Sectors to engage securely with the digital transformation process. Critical Sectors are those which are critical to the nation and whose incapacity or destruction will have a debilitating impact on national security, economy, public health or safety.

As cybersecurity has not been a design consideration of most Critical Sectors' operational technologies, the latter being traditionally considered secure by virtue of isolation, the integration of the operational technology (OT) with information technology (IT) and their connection to the Internet has resulted in a number of cyber vulnerabilities.

Moreover, the continuous evolution of the Critical Sectors' operating environment, induced by technological advances becoming operational (e.g. the Internet of Things, Industry 4.0) and evolving business practices, introduces new vulnerabilities; and the increased interdependency and interconnection of cyber systems across sectors, jurisdictions, and even national borders introduces new risks.

These risks affect not only the economy and the society, but also the national digital sovereignty and autonomy; accordingly, these risks have to be mitigated for the benefit of both the economy and the society.

On the other hand, cybersecurity is an enabler of digital innovation. It supports business agility, as digital transformation requires strong cybersecurity posture; it facilitates business productivity, by diminishing the disruptive impact of cyberattacks; and it develops customer loyalty, by supporting the development and maintenance of a business's trusted track record.

## The expected impact

The expected long term impact of the work within NORCICS and of its results is a safer Norwegian society with improved cybersecurity, reliability and resilience of Critical Sectors, and with enhanced capability to combat cybercrime, which in turn increase the trust of citizens towards digitally transformed services.

The work within NORCICS will result in (a) enhancement of existing and creation of new long-term strategic alliances between industry, government and research institutions; (b) promotion of international collaboration; (c) delivery of research results, as well as development, validation and demonstration of innovative solutions to function as foundations for industry innovation; and (d) training of high-level cybersecurity professionals.

# NORCICS vision and objectives

## Vision

Norway is among the most digitalized countries in the world. NORCICS's vision is to contribute to making Norway the most securely digitalized country in the world by improving the cybersecurity and resilience of its Critical Sectors, through research-based innovation.

## Objectives

NORCICS's primary objective is to enhance the capability of private and public sector stakeholders to respond to the current and future cybersecurity risks by developing, validating, and operationalizing innovative technologies within a cyber-physical security ecosystem that includes highly trained research personnel.

The following secondary objectives will lead to the achievement of the primary objective:

To create new knowledge that will improve our understanding of the dynamics and interdependencies among Critical Sectors; and of cyberattacks against Cyber Physical Systems.

To develop, test and validate in an industrially relevant environment novel, advanced and innovative methods for preventing cyberattacks against industrial control systems in Critical Sectors.

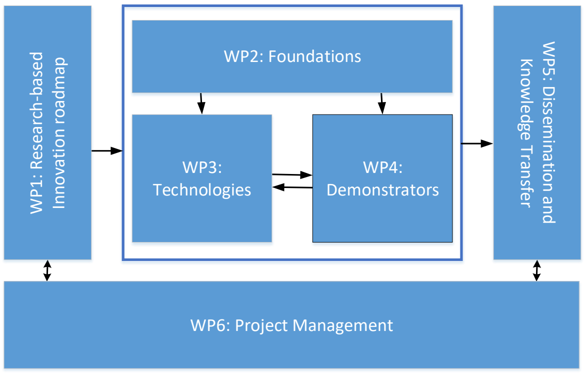
To demonstrate in an industrially relevant environment efficient cybersecurity solutions for industrial control systems in Critical Sectors;

To develop novel methods and tools for cybersecurity training and awareness improvement.

To effectively transfer the knowledge created within NORCICS among its user partners and other Norwegian businesses and stakeholders.

# Our research strategy and plans

The work within NORCICS is organized in 6 work packages, 3 of which are dedicated to research activities. These are:


WP1: Research-based Innovation roadmap
WP2: Foundations
WP3: Technologies
WP4: Demonstrators
WP5: Dissemination and Knowledge Transfer
WP6: Project Management

## Work Package 2
### Foundations

WP2 seeks to identify and address gaps in the state-of-the-art in securing cyber-physical systems and systems in critical sectors through modelling of services and dependencies, enhanced understanding of advanced attacks and both challenges as well as opportunities presented by dynamic cyber-physical environments from industrial systems and critical sectors relying not only on technological aspects but also ensuring that human aspects are given due consideration.

## Work Package 3
### Technologies, applications, and services

WP3 aims at defining and executing research, development and innovation with respect to the next generation of cybersecurity technologies, applications and services. It will provide a selection of horizontal cybersecurity technologies and solutions applicable to a range of Critical Sectors. The provision shall extend the state-of-the-art, enabling innovative systems, mechanisms, and services.

## Work Package 4
### Demonstration environments

The objective of WP4 is to test and demonstrate the solutions developed within WP3 (and foundations from WP2) in laboratory and realistic environments at user partners for validation and verification. We will also define demonstration cases and use cases for identifying the needs for joint research, development and innovation concepts to be developed in WP2 and WP3.

We will test and demonstrate the technologies from WP3 and models from WP2. The work will be split into tasks, each addressing a critical sector. This will give useful knowledge about which cybersecurity technologies and solutions will work for different applications and sectors. The feedback gained through tests will be used to improve the developed technologies (WP3) and models (WP2).

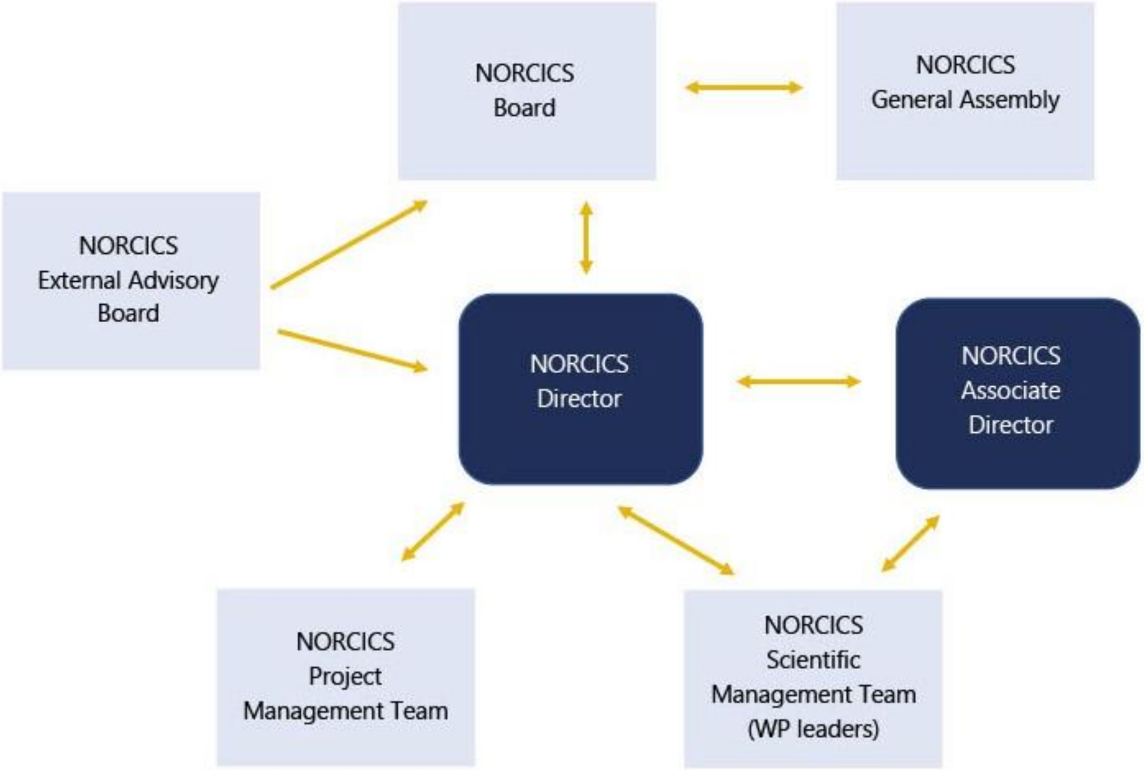
As of 2020 we have identified four critical sectors to focus our initial efforts on, i.e. Secure cyber-physical electricity system, Secure Industry 4.0, Secure Distributed Healthcare, and Secure smart districts. Over the course of the NORCICS lifespan these sectors can be extended based on partner needs and contributions.

The results from the demonstration and test activities will be the basis for finding the "best practice" for cybersecurity solutions. In addition to the horizontal technologies applicable to several sectors, these may need to be adapted and adjusted to the practicalities in the specific sectors.

The combination of testing and demonstration of the horizontal technologies, together with specific sector adjustments, will allow us to formulate guidelines and make recommendations for cybersecurity solutions in a variety of sectors. The first part of the activity in this WP will be to develop use cases describing the tests and demonstrators at the user partners within each task.

# How NORCICS is organized

NORCICS is hosted by the Norwegian University of Science and Technology (NTNU), under the department of Information Security and Communication Technology. The centre's work is closely connected to the department's Center for Cybersecurity and Information Security – a public-private and civilian-military cooperation with 32 partners. NORCICS builds upon these relationships to provide a centre focused on innovation driven research in cybersecurity of the critical sectors.


NORCICS Board
NORCICS General Assembly
NORCICS External Advisory Board
NORCICS Director
NORCICS Associate Director
NORCICS Project Management Team
NORCICS Scientific Management Team (WP leaders)

## General Assembly

The General Assembly consists of one delegate from each partner. The General Assembly is responsible for setting the strategic directions of the centre; for approving the plans to implement the strategy; and for assessing the results. It meets once a year.

## Board

The Board is the formal decision body of NORCICS. The Board is chaired by the Dean of the NTNU Faculty of Information Technology and Electrical Engineering Professor Ingrid Schjølberg.

Representatives of the following partners, selected according to their extent of participation to the project and on sector representativeness, make up the Board: Elvia AS, Norsk Hydro ASA, Equinor ASA, Mnemonic AS, Oslo Police District, NTNU, SINTEF Energi. In February 2021, the Board was enlarged to include a representative of Kongsberg Gruppen ASA. The Board is responsible for the overall management of the project. Board members are delegated the necessary authority to make decisions binding the partner they represent.

The Board meets every four months to monitor and direct the progress of the project.

### The tasks of the Board include:

1) Ensure that the progress is maintained according to the project plan;
2) Review and approve financial status;
3) Review and approve the regular project risk assessment;
4) Approve and follow up the Quality Assurance Plan;
5) Approve and follow up the effective Innovation Management Plan;
6) Review the project technical results; and
7) Provide guidance related to a) Innovation and Exploitation potential, b) Intellectual property management, c) Dissemination and communication activities, d) Resolve potential and actual disputes between participants which cannot be resolved at lower decision levels, e) Reallocate budgets if necessary, and f) Assess ethical issues.

## Centre director

The centre director, Professor Sokratis Katsikas, is responsible for the overall project coordination and management. He reports to the EB; he has overall responsibility for the project; is responsible for implementing the decisions of the EB; is implementing the technical directions and strategies of the project; and is the contact point of the project with the Research Council of Norway. In his duties he is assisted by the Associate Director, Prof. Katrin Franke.

## External Advisory Board

The research and development work in the project is supported by an international External Advisory Board (EAB), consisting of leading scientists in the fields of interest to the project, representatives of the Norwegian industry, and policy makers. The EAB provides external quality assurance to NORCICS; it convenes once every year, during the annual NORCICS workshop.

## Scientific Management Team

The coordination, planning, and monitoring of the research and development work in the project is performed by the NORCICS Scientific Management Team, which includes the WP leaders and is chaired by the Director. The Scientific Management Team meets weekly. The responsibility for the planning, execution, and monitoring of the work within the research activities lies with the WP Leaders.

## NORCICS partners

The NORCICS consortium has been put together following a number of criteria, including: skills balance; complementarity of expertise; manageability; and sector coverage. It comprises academic and research partners; organizations that can act as multipliers; industrial stakeholders and end users. Its composition has been carefully designed so that the combination of the individual skills of its members will enable NORCICS to achieve its objectives.

The consortium members have complementary expertise that collectively covers the areas of fundamental research, The NORCICS user partners can broadly be classified in three groups:

- A group of businesses/organizations with activity in diverse critical sectors - Group 1 (Elvia, Norsk Hydro, Kongsberg Gruppen, Yara International, Sykehuset Innlandet HF, Equinor, Lyse Elnett, Helgeland Kraft, NCSpectrum)
- A group of cybersecurity and/or operational technology providers – Group 2 (Mnemonic, Siemens)

- A group of organizations dedicated to striving towards a safer society, to rising awareness and to providing advice to Norwegian citizens and enterprises concerning cyber threats, vulnerabilities and information security – Group 3 (Oslo Police District, NorSIS).

## Cooperation between the centre's partners

NORCICS enables involvement from the user partners through working groups, expert groups, workshops, participation in research tasks, in particular through the demo/pilot testing as described in WP4.

The demonstration of the common technologies ensures a close cooperation between researchers and the industry, contributing to involvement, exchange of ideas and mutual learning for user partners in different sectors.

In addition, the SFI aims for visiting and exchange of PhD students, Post docs and researchers with the industrial partners.

The SFI also plans for visits to individual industry partners by groups of researchers and other partners in order to discuss relevant use cases and thereby ensure knowledge transfer and involvement by the users.

On the task level, NORCICS establishes expert groups with participation from both research and industrial partners for discussion and involvement in the work at an early stage. The industrial partners are also expected to provide labs and R&D facilities when this form of contribution is envisaged, to participate in decisions about the directions of research, and in curricula and training courses development, and are also encouraged to have their staff engaged with the centre to spend time at the research partners.

# Scientific activities and results

NORCICS became operational on October 1, 2020. In the three months of operation in 2020 work within NORCICS focused on planning and preparation.

The Annual Workplan for 2021 was created and agreed, which included the preparation of tasks within each work package. An overview of these tasks follows:

| Task/WP# | Title | Start - End |
|---|---|---|
| **WP1** | Research-based innovation roadmap | 01.2021 – 09.2028 |
| **WP2 - T2.2** | Modelling distributed subversion attacks in cyber physical systems | 07.2021 – 06.2024 |
| **WP2 - T2.3** | Digital Twin Security Models and Mechanisms | 07.2021 – 06.2024 |
| **WP2 - T2.4** | Human side of secure Industry 4.0 | 01.2021 - 12.2023 |
| **WP3 – T3.1.1** | Assessing 5G and beyond as an element of critical services | 04.2021 – 03.2024 |
| **WP3 - T3.1.2** | Autonomous Adaptive Security for 5G-enabled IoT | 01.2021 – 12.2023 |
| **WP3 - T3.3.2** | Reverse engineering lab | 01.2021 – 12.2022 |
| **WP3 – T3.4** | Humanised deep Learning & Big-data Analytics | 01.2021 – 12.2023 |
| **WP3 - T3.5.1** | Codes for sub-millisecond latencies in 5G and beyond | 01.2021 – 12.2024 |
| **WP3 - T3.5.2** | Secure broadcasting in wireless critical systems | 01.2021 – 12.2023 |
| **WP4 – T4.1** | Secure cyber-physical electricity system | 01.2021 – 09.2028 |
| **WP4 – T4.2** | Secure industry 4.0 | 01.2021 – 09.2028 |
| **WP4 - T4.3** | Cybersecurity models for remote medical and care services delivery | 01.2021 – 09.2028 |
| **WP4 - T4.4** | Secure smart districts | 01.2021 – 09.2028 |
| **WP5** | Dissemination and knowledge transfer | 01.2021 – 09.2028 |
| **WP6** | Project management | 01.2021 – 09.2028 |

# International cooperation

A number of internationally highly reputed centers active in the field of cybersecurity collaborate with NORCICS. The selection of international collaborators has been made on the basis of the complementarity of expertise; of geographical coverage; of the strategic importance of a long-lasting alliance and of existing strong collaboration relationship with NORCICS partners.

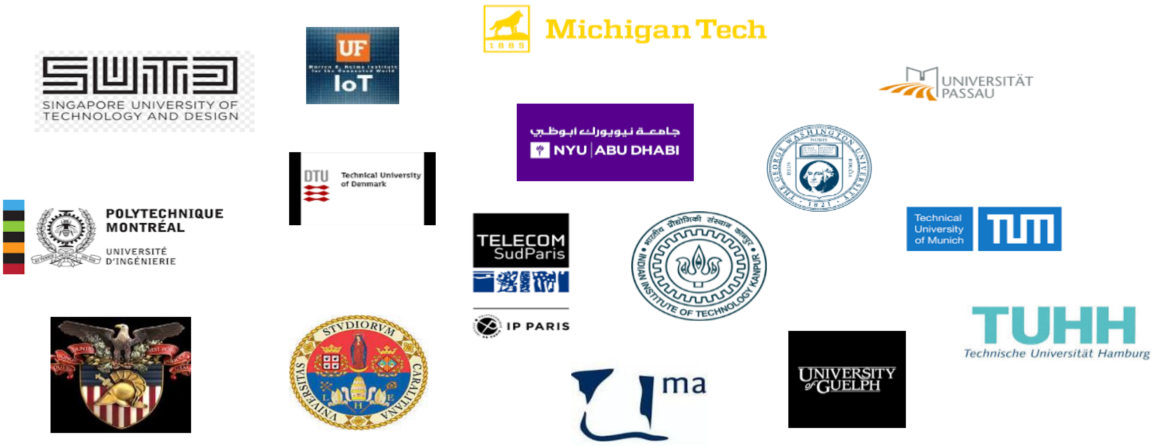
International collaboration is important to ensure that Norwegian partners are up-to-date with international developments in the field, and to multiply the spread of new knowledge and innovation. It is also expected to play an important role in the innovation process by allowing Norwegian industry to gain access to a broader pool of resources and knowledge.

International cooperation also provides opportunities for exchange of visiting researchers and PhD candidates; for joint supervision of PhD theses, following the model of the ITN (Innovative Training Networks) of the Marie Curie Actions for collaborative PhD education; and for adjunct professorships to international faculty.

NORCICS actively pursues the enlargement of the initial pool of international collaborators, including through its initiation of and participation in consortia to apply for projects funded by the European Commission.

The following universities are collaborating with NORCICS:

- Michigan Technological University, USA
- George Washington University, USA
- University of Florida, Nelms Institute for the Connected World, USA
- US Military Academy, USA
- University of Guelph, Canada
- Polytechnique Montréal, Canada
- New York University Abu Dhabi, UAE
- Technische Universität München, Germany
- Universität Passau, Germany
- Technische Universität Hamburg, Germany
- Danmarks Tekniske Universitet, Denmark
- Singapore University of Technology and Design, Singapore
- Telecom SudParis, France
- Università degli Studi di Cagliari, Italy
- Universidad de Málaga, Spain
- Indian Institute of Technology Kanpur, India


Michigan Tech
UF IoT
SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
UNIVERSITÄT PASSAU
NYU ABU DHABI
DTU Technical University of Denmark
POLYTECHNIQUE MONTRÉAL UNIVERSITÉ D'INGÉNIERIE
TELECOM SudParis
IP PARIS
Technical University of Munich
TUM
TUHH Technische Universität Hamburg
UNIVERSITY of GUELPH
ma

# Recruitment

Following the announcement of the establishment of NORCICS, in June 2020, the process for hiring the Project Manager (administrative coordinator) of NORCICS started. The process was concluded in August 2021 and resulted in the hiring of Hanne Mari Solhaug Djupdal. Hanne Mari joined NORCICS on February 1, 2022.

Several of the tasks in the Annual Workplan for 2021 include also hiring of PhD-candidates or Postdoc positions. The positions planned to be filled in 2021 were announced in December 2020, with deadline on January 31st 2021.

An overview of the announced positions follows:

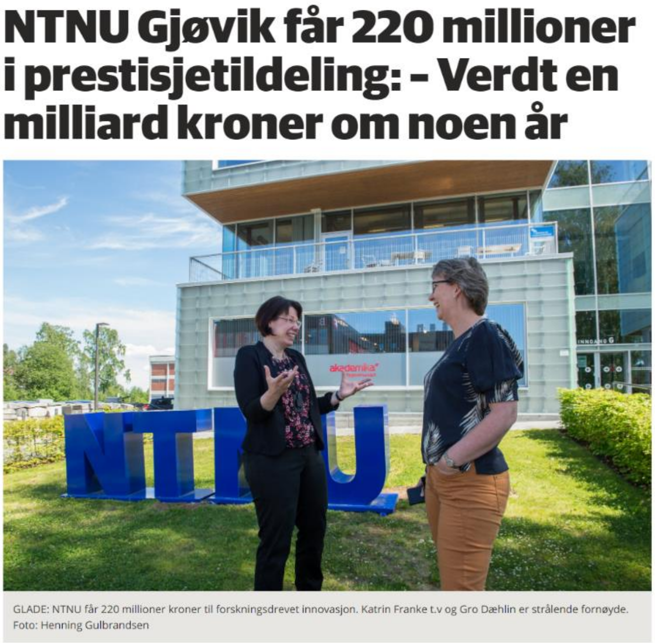
| WP | Task | Title | Main supervisor | PhD | Postdoc |
|---|---|---|---|---|---|
| **2** | **2.2** | Modelling distributed subversion attacks in cyber physical systems | Stephen Wolthusen (NTNU IIK) | | 1 |
| | **2.3** | Digital Twin Security Models and Mechanisms | Vasileios Gkioulos (NTNU IIK) | 1 | |
| | **2.4** | Human side of secure Industry 4.0 | Halvor Holtskog (NTNU IØT) | 1 | |
| **3** | **3.1** | 5G and beyond as an element of critical services | Bjarne Helvik (NTNU IIK) | 1 | |
| | **3.3** | Reverse engineering lab | Geir Olav Dyrkolbotn (NTNU IIK) | | 1 |
| | **3.4** | Humanised deep Learning & Big-data Analytics | Christian Omlin (UiA) | 1 | |
| | **3.5** | Sub-millisecond control layer codes for 5G and beyond | Danilo Gligoroski (NTNU IIK) | 1 | |
| **4** | **4.3** | Cybersecurity models for remote medical and care services delivery | Bian Yang (NTNU IIK) | 1 | |

# Communication and dissemination activities

The announcement of NORCICS being established at the Department of Information Security and Communication Technology of NTNU was made in June 2020. Following the announcement, NORCICS was the subject of numerous dissemination activities until the end of the year. The assignment of an SFI to the Department of Information Security and Communication Technology at NTNU was highly regarded, and also noticed specifically in Innlandet Fylke, as the majority of the SFI activity will be taking place at NTNU Campus Gjøvik.

NORCICS was presented at several occasions in the local newspaper:

- Gjøvik, NTNU | NTNU Gjøvik får 220 millioner i prestisjetildeling: – Verdt en milliard kroner om noen år (oa.no)
- Debatt, NTNU i Gjøvik | Om 20 år kan NTNU ha 12.000 studenter og 1200–1300 ansatte: – En eventyrlig utvikling (oa.no)



**NTNU Gjøvik får 220 millioner i prestisjetildeling: - Verdt en milliard kroner om noen år**

GLADE: NTNU får 220 millioner kroner til forskningsdrevet innovasjon. Katrin Franke t.v og Gro Dæhlin er strålende fornøyde.
Foto: Henning Gulbrandsen

NTNU's own internal news outlet, Innsida, has also presented NORCICS on several occasions:

- Start - innsida.ntnu.no
- Start - innsida.ntnu.no

The latter was in relation to the **NORCICS Kickoff meeting** and official opening that was held on October 20th 2020, after the official start date of NORCICS on October 1st. All NORCICS partners and involved personnel was invited to join the kickoff, where some were physically present at NTNU Gjøvik, while most joined digitally through Microsoft Teams.

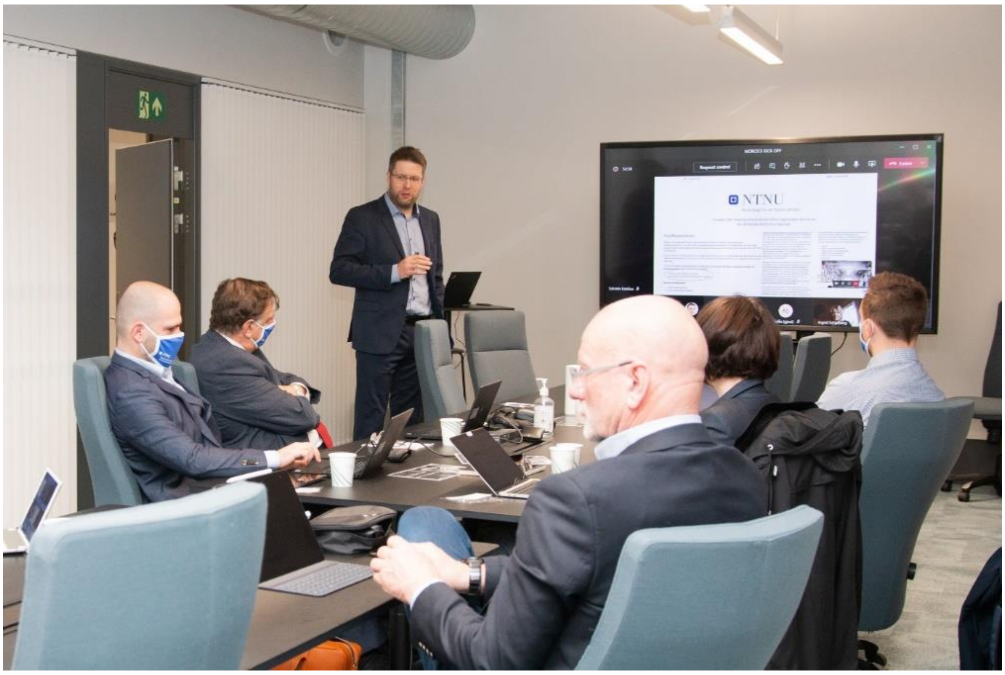
Key personnel associated with NORCICS has also presented the centre in various forums:

The Dean of the NTNU Faculty of Information Technology and Electrical Engineering, **Ingrid Schjølberg**, who is also the head of the Board at NORCICS, expressed her thoughts on the announcement in a NTNU blogpost:

https://www.ntnu.no/blogger/ingrid-schjolberg-ie/2020/10/20/opening-day-for-norwegian-centre-for-cyber-security-in-critical-sectors/

The head of the department, **Nils Kalstad**, also had the chance to present NORCICS on several occasions in 2020, including at the:

- Helse- og omsorgsdepartementet, Innlandet fylkeskommune
- Totalforsvarets cybersikkerhetskonferanse 2020
- GCE Blue Maritime, Security Talks 2020 (GCE Node)
- Næringslivets sikkerhetsråd, CCIS – board meeting
- Cisco
- Eidsiva
- Sparebankstiftelsen
- Telenor
- CapGemeni
- Uniconsult



**The Centre director Sokratis Katsikas** was interviewed by the media outlet Media Planet in the fall of 2020, which led to a physical magazine article, as well as publishments online: Setter Norge på kartet som verdensledende på digitalisering og digital sikkerhet - Alt om samfunnssikkerhet. He also gave two keynote lectures, one at the 3rd International Conference on Intelligent Technologies and Applications (INTAP 2020), Gjøvik, Norway; and the other at the 4th Cyber Security in Networking Conference (CSnet 2020), Lausanne, Switzerland.

Another important feature of the plan for NORCICS' communication is **the centre's website:** Norwegian Centre for Cybersecurity in Critical Sectors (NORCICS) - NTNU. This was set up at the end of 2020, as a first version with the most crucial information about the centre and its research. This will continue to be updated as the project develops.

# Appendices

## A1. Personnel

### NORCICS Key Researchers:

| Name | Institution | Main research area |
|---|---|---|
| Sokratis Katsikas | NTNU | Critical Infrastructure Security and Resilience |
| Katrin Franke | NTNU | Digital Forensics; Computational Intelligence; AI in Forensics |
| Vasileios Gkioulos | NTNU | Critical Infrastructure Security and Resilience |
| Stephen Wolthusen | NTNU | Critical Infrastructure Security and Resilience |
| Bjarne Emil Helvik | NTNU | Dependability of ICT services |
| Ottar Henriksen | NTNU | Industrial economics and technology management |
| Gerd Kjølle | SINTEF Energi | Security of electricity supply |
| Christian Omlin | UiA | Artificial Intelligence and Machine learning |
| Bian Yang | NTNU | Health informatics and security; Privacy enhancing technologies and biometrics |
| Halvor Holtskog | NTNU | Industrial economics and technology management |
| Habtamu Abie | Norsk Regnesentral | Adaptive Security, Trust, Privacy, Risk Management, Distributed Object Computing |
| Thor Kristoffersen | Norsk Regnesentral | Visual systems, Distribution systems |
| Danilo Gligoroski | NTNU | Information Security and Cryptography |
| Geir Olav Dyrkolbotn | NTNU | Cyber Intelligence, Cyber tactics, and Reverse engineering |
| Sigurd Eskeland | Norsk Regnesentral | Information security and Cryptographic protocols |
| Jørn Foros | SINTEF Energi | Security of electricity supply |
| Lasse Øverlier | NTNU | Information security and privacy, Content-based multimedia analytics |

## A2. Statements of Accounts

### Financial reporting 2020:

| Funding (1000 NOK) | Amount |
|---|---|
| Research Council | 420 |
| Host institution NTNU | 387 |
| Research Partners* | |
| User Partners** | 242 |
| **Total** | **1049** |

| Costs (1000 NOK) | Amount |
|---|---|
| Host institution NTNU | 625 |
| Research Partners* | 382 |
| User Partners** | 42 |
| Equipment | 0 |
| **Total** | **1049** |

* Sintef Digital, Norsk Regnesentral

** Lyse Elnett, Helgeland Kraft, NC-Spectrum, NorSIS