NORCICS SFI Norwegian Centre for Cybersecurity in Critical Sectors

Communication and Dissemination management plan 2021

Document Identification	
Due date	**31 March 2021**
Submission date	**31 March 2021**
Version	**1**

Abstract

This document details the communications management plan of the SFI NORCICS. The document defines the narrative, target audiences, channels, and mechanisms to increase awareness on the project activities and disseminate the project results. The SFI-NORCICS communication management plan will be evolving during the project to fit arising needs and adapt to the operational modes.

This document is issued within the SFI-NORCICS. This project has received funding from the Research Council of Norway.

Document Information

Author(s)

Vasileios Gkioulos – NTNU – vasileios.gkioulos@ntnu.no

Contributors

-

Approved by

NORCICS scientific management committee

History

0.1	05/02/2021	Vasileios Gkioulos	Initial draft
0.2	31/03/2021	Vasileios Gkioulos	Draft submitted for review
1	19/04/2021	Vasileios Gkioulos	Final version 1

Contents

List of acronyms

CPS(s)	Cyber-physical system(s)
CrISec	Critical Infrastructure Sectors
NORCICS	Norwegian Center for Cybersecurity In Critical Sectors
SFI	Sentre for forskningsdrevet innovasjon (Centers for research-driven innovation)
WP	Work Package

List of tables

Introduction

Defining the narrative

The main narrative for communication arising from the SFI-NORCICS is founded on the overarching project vision, primary and secondary objectives, as these have been defined within the project proposal.

Vision: To contribute to making Norway the most securely digitized country in the world by improving the cybersecurity and resilience of her critical Infrastructure sectors (CrISec), through research-based innovation.

Primary objective: 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 socio-technical solutions.

Secondary objective-1: To generate new knowledge about interdependencies and dynamics in CrISec; and how CPS especially in CrISec can be attacked;

Secondary objective-2: To design, develop, and test innovative methods and tools for the detection, prevention, and mitigation of cyberattacks against industrial control systems in CrISec, and to validate these in industrially relevant environments;

Secondary objective-3: To demonstrate and validate the efficiency and effectiveness of interlinked cybersecurity measures for control systems in CrISec for selected industrially relevant environments;

Secondary objective-4: To develop novel methods and tools for the improvement of cybersecurity training and awareness, and means for validation of such methods;

Secondary objective-5: To effectively transfer the knowledge created within NORCICS among its user partners, sectoral and industrial clusters, and relevant stakeholders in Norway.

Research and development in the area of security and resilience of CrISec is paramount to enhancing the country's cyber security posture and the business sector's capability to innovate. NORCICS's is the Norwegian centre for research-based Innovation, with the overarching objective to develop innovative cybersecurity solutions at varying technology readiness levels within a dynamically evolving cyber-physical security ecosystem. We achieve this by focusing on long-term research and close alliances between research-intensive enterprises and prominent research groups in academia. In NORCICS, research on cybersecurity technologies is combined with research on human aspects of these technologies, to provide methods and tools, re-usable across different infrastructures, which cover a wide variety of concepts, and are validated in several demonstrators across different CrISec. The primary research areas in focus for NORCICS cover a wide range of cybersecurity domains, enabling technologies, and CrISec. Specifically, the initial application domains are i) Critical Infrastructures; ii) Industrial Control Systems; iii) the Internet of Things; and iv) Smart Environments. Furthermore, the initial sectorial domains are i) Energy; ii) Health; iii) Manufacturing and Supply Chain; iv) Smart Districts, and v) Public Safety. The scientific content and organization of research activities, as well as the research approach and scientific methodology, have been structured in a manner that promotes technology spillovers and transfer of best practices, while reducing duplication of effort. In terms of interdisciplinarity, NORCICS objectives are twofold. Initially, to further the expertise and competence of the involved professional disciplines themselves, through transferring knowledge, and developing common methods and operational knowledge frameworks across them. Additionally, NORCICS aims at research and innovation activities, which are problem focused and address issues of

social and technical relevance, involving two or more professional and academic disciplines into the activities of each focus area. The investigated subjects are interdisciplinary by nature, with the cyber security discipline being the prism through which we approach these subjects. Furthermore, the specific tasks across the research areas are primarily driven by the end users, towards directly transferring research results from the laboratory to the real world. Additionally, the research areas are not only relevant from a technical point of view but also to policy making, as NORCICS focuses on critical infrastructures with overlapping requirements and extended interdependencies. In summary, NORCICS focuses on critical national infrastructures, bringing together the expertise of cybersecurity specialists and domain specific specialists, also incorporating the operational experience of end users across the research areas. Such a platform allows the investigation of cybersecurity issues that are central to the research areas, how these interact in order to create cascading failures, and how these interactions can be modified in order to provide implementable, synergetic solutions.

Communications management plan objectives and requirements

The key objectives of communication for the SFI-NORCICS are:

1. Effectively communicate about the past, ongoing and future SFI activities to all relevant stakeholders.
2. Effectively disseminate the SFI-NORCICS results to all relevant stakeholders.
3. Effectively communicate arising opportunities for collaboration to all relevant stakeholders.
4. Enhance the behavior and perceptions of businesses/organizations/citizens to the threats of cyber-attacks and the precautions to be taken against them.

In order to complete these goals, it is vital that this plan:

- has clear and measurable communications objectives with the necessary evaluations to judge their success;
- has a set of activities and a timetable for achieving those activities;
- has several staged review periods to ensure that it is still fit for purpose as the project advances. The plan is a collaborative effort that must be jointly owned by all members of the project;

Assumptions

Communication and dissemination are two separate but interrelated activities. The defining characteristics of each activity are the intended audience and the content of the communication.

• Dissemination of the project results and developed best practices to relevant specialists and stakeholders.

• Communication about the project, its progress and results to a broader audience.

On a practical level, it will be a strategic mixture of the audiences, the communication channels and tailored communication messages that can most effectively be utilized.

Target audiences and stakeholders analysis

The relevant audiences for NORCICS are diverse, each with its own characteristics and associated perspectives and objectives pertaining to cybersecurity.

Table 1: Target audiences and stakeholders

Target audience	Potential users	Technical level	Main focus
Society at large	General public	Understandable by a large number of non-specialists	Economic impact and benefits to society and individuals Challenges addressed within the centre, developed solutions and their (potential) impact
Technical	System developers System operators	Understandable by developers, testers, engineers, and auditors	Technical presentation of project results and objectives
Scientific	Research community International forums	Understandable by the relevant scientific community	Technological and scientific presentations of project results
Business	Industry SMEs Investors	Understandable by decision makers	Business opportunities Potential of technology and societal benefits
Legislators	Public administration Policy makers	Understandable by decision makers	Legislative and social implications Potential background for high-level strategic decisions
Project funding organizations	-	Understandable by decision makers	Project progress, relevant results, and opportunities

Communication and dissemination roles within the project

WP5 is responsible for managing the communication and dissemination activities of the project, under the activities defined within the communication plan. In practice this means.

- Creating content for the project's communication platforms
- Drafting press releases
- Coordinating position papers and statements in reflection to relevant events
- Acting as liaison point for press and media
- Commissioning graphic design and similar work
- Managing the correct usage of the SFI-NORCICS brand

It must be noted that the duty to communicate is a responsibility of all the WP and Task leaders of the project, especially regarding direct communication with the project partners related to coordinating and undertaking the research and innovation activities envisioned within each task description. Furthermore, the individual WP and task leaders are responsible for identifying the target audiences that are relevant to their work, who would be interested to the produced results, and who may be affected by the outcome of their work. The main contact persons and their information for each WP and task are shown in the following table.

Regarding specifically screening of published material for potential intellectual property and classification violations, as well as for the overall quality assurance of published material that are not explicitly described within the communication plan, these are governed by procedures established by WP6 and described within the project handbook.

Table 2: WP and Task leaders and deputies.

WP	Task	Leader	Leader (emai)	Deputy leader	Deputy leader (email)
1	-	Ottar Henriksen	ottar.henriksen@ntnu.no	Sokratis Katsikas	sokratis.katsikas@ntnu.no
2	-	Stephen Wolthusen	stephen.wolthusen@ntnu.no	Vasileios Gkioulos	vasileios.gkioulos@ntnu.no
2	1	Stephen Wolthusen	stephen.wolthusen@ntnu.no	Vasileios Gkioulos	vasileios.gkioulos@ntnu.no
2	2	Stephen Wolthusen	stephen.wolthusen@ntnu.no	Vasileios Gkioulos	vasileios.gkioulos@ntnu.no
2	3	Vasileios Gkioulos	vasileios.gkioulos@ntnu.no	Stephen Wolthusen	stephen.wolthusen@ntnu.no
2	4	Halvor Holtskog	halvor.holtskog@ntnu.no	Vasileios Gkioulos	vasileios.gkioulos@ntnu.no
3	-	Bjarne E. Helvik	bjarne@ntnu.no	Vasileios Gkioulos	vasileios.gkioulos@ntnu.no
3	1	Bjarne E. Helvik	bjarne@ntnu.no	Poul E. Heegaard	poul.heegaard@ntnu.no
3	2	Tor Olav Grøtan	tor.o.grotan@sintef.no	Martin Gilje Jaatun	martin.g.jaatun@sintef.no
3	3	Vasileios Gkioulos	vasileios.gkioulos@ntnu.no	Sokratis Katsikas	sokratis.katsikas@ntnu.no
3	4	Katrin Franke	katrin.franke@ntnu.no	Christian WP Omlin	christian.omlin@uia.no
3	5	Danilo Gligoroski	danilo.gligoroski@ntnu.no	Staal Vinterbo	staal.vinterbo@ntnu.no
4	-	Gerd Kjølle	Gerd.Kjolle@sintef.no	Jørn Foros	jorn.foros@sintef.no
4	1	Jørn Foros	jorn.foros@sintef.no	Gerd Kjølle	Gerd.Kjolle@sintef.no
4	2	Halvor Holtskog	halvor.holtskog@ntnu.no	Vasileios Gkioulos	vasileios.gkioulos@ntnu.no
4	3	Bian Yang	bian.yang@ntnu.no		
4	4	Katrin Franke	katrin.franke@ntnu.no	Lasse Øverlier	lasse.overlier@ntnu.no
5	-	Vasileios Gkioulos	vasileios.gkioulos@ntnu.no	Sokratis Katsikas	sokratis.katsikas@ntnu.no
6	-	Sokratis Katsikas	sokratis.katsikas@ntnu.no	Katrin Franke	katrin.franke@ntnu.no

Dissemination mechanisms, channels and practices

Communication tools

Name

The project must at all times and under all circumstances (both for written and oral communications) be addressed and named with one of the following alternatives:

1. Norwegian Center for Cybersecurity in Critical Sectors
2. SFI-NORCICS
3. NORCICS

Logos

The developed logos for the project can be seen below. When used, the three project logos must be used unmodified.

NORCICS

SFI Norwegian Centre for Cybersecurity in Critical Sectors

NORCICS

Website

A permanent project website is currently under development within the NTNU domain (https://www.ntnu.edu/norcics). The chosen template and current structure is presented in the following figures. The website will be continuously updated and expanded to include additional material, such as

1. Description of project results
2. Working groups and team members
3. Social media updates

SFI – Norwegian Center for Cybersecurity in Critical Sectors (SFI-NORCICS)

NORCICS SFI Norwegian Centre for Cybersecurity in Critical Sectors

NTNU

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

Home | Research | Infrastructure | News & Events | Partners | About | Contact

/ NORCICS

Center for Research-based Innovation (SFI)

Norwegian Center for Cybersecurity in Critical Sectors

The protection of critical societal functions and of the individual online becomes increasingly important.

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.

These sectors include electricity production and distribution, oil & gas production and distribution, manufacturing, healthcare, industrial production, financial services, transportation, smart districts.

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). The research in NORCICS will result in methods and tools, re-usable across different sectors; these will be validated in demonstrators for different critical sectors.

Learn more about SFI NORCICS.

Research

Research from NORCICS

Infrastructure

Infrastructure at NORCICS

News & Events

News & Events from NORCICS

Partners

Elvia · equinor · Helgeland Kraft · Hydro · Kongsberg · Lyse · mnemonic · NC-Spectrum · NorSIS · NR · NTNU · Politiet · Siemens · SINTEF · Sykehuset Innlandet HF · UiA · Yara (Knowledge grows)

Editoral responsibility | About cookies | Privacy policy

Sign In

SFI – Norwegian Center for Cybersecurity in Critical Sectors (SFI-NORCICS)

NORCICS SFI Norwegian Centre for Cybersecurity in Critical Sectors

NTNU

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

Home | Research | Infrastructure | News & Events | Partners | About | Contact

/ NORCICS / Research

NORCICS

Research & Innovation

NORCICS has the following work packages (WP):

1. Research-based innovation roadmap
2. Foundations
3. Technologies, applications, and services
4. Demonstration environments
5. Dissemination and knowledge transfer
6. Project management

Innovation roadmap

WP1 – Research-based innovation roadmap

Foundations

WP2 – Foundations

Technologies

WP3 – Technologies, applications & services

Demonstration environments

WP4 – Demonstration environments

Dissemination

WP5 – Dissemination and knowledge transfer

Project management

WP6 – Project management

Editoral responsibility | About cookies | Privacy policy

Sign In

SFI – Norwegian Center for Cybersecurity in Critical Sectors (SFI-NORCICS)

NORCICS SFI Norwegian Centre for Cybersecurity in Critical Sectors

NTNU

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

Home Research Infrastructure News & Events Partners About Contact

/ NORCICS / About

NORCICS

About

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

Our 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 socio-technical solutions.

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

1. To generate **new knowledge about interdependencies and dynamics** in Critical Sectors; and how Cyber Physical Systems especially in Critical Sectors can be attacked;
2. To design, develop, and test innovative **methods and tools for the detection, prevention, and mitigation** of cyberattacks against industrial control systems in Critical Sectors, and to validate these in industrially relevant environments;
3. To demonstrate and validate the efficiency and effectiveness of interlinked cybersecurity measures for control systems in Critical Sectors for selected industrially relevant environments;
4. To develop novel methods and tools for the improvement of cybersecurity training and awareness, and means for validation of such methods;
5. To effectively transfer the knowledge created within NORCICS among its user partners, sectoral and industrial clusters, and relevant stakeholders in Norway.

Editoral responsibility | About cookies | Privacy policy

Sign In

NORCICS SFI Norwegian Centre for Cybersecurity in Critical Sectors

NTNU

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

Home Research Infrastructure News & Events Partners About Contact

/ NORCICS / Contact

NORCICS

Contact us

Work package leaders

Vasileios Gkioulos
WP5 - Dissemination and Knowledge Transfer

Bjarne Emil Helvik
WP3 - Technologies, applications, and services

Ottar Henriksen
WP1 – Research-based innovation roadmap

Sokratis Katsikas
WP6 - Project Management

Stephen Dirk Bjørn Wolthusen
WP2 – Foundations

Gerd Kjølle
WP4 - Demonstration environments

Centre board

Ingrid Schjølberg
NTNU

Substitute members

Nils Kalstad
NTNU

Contact us

Sokratis Katsikas
Center Director

Katrin Franke
Associate Director

Hanne Mari Solhaug Djupdal
Coordinator

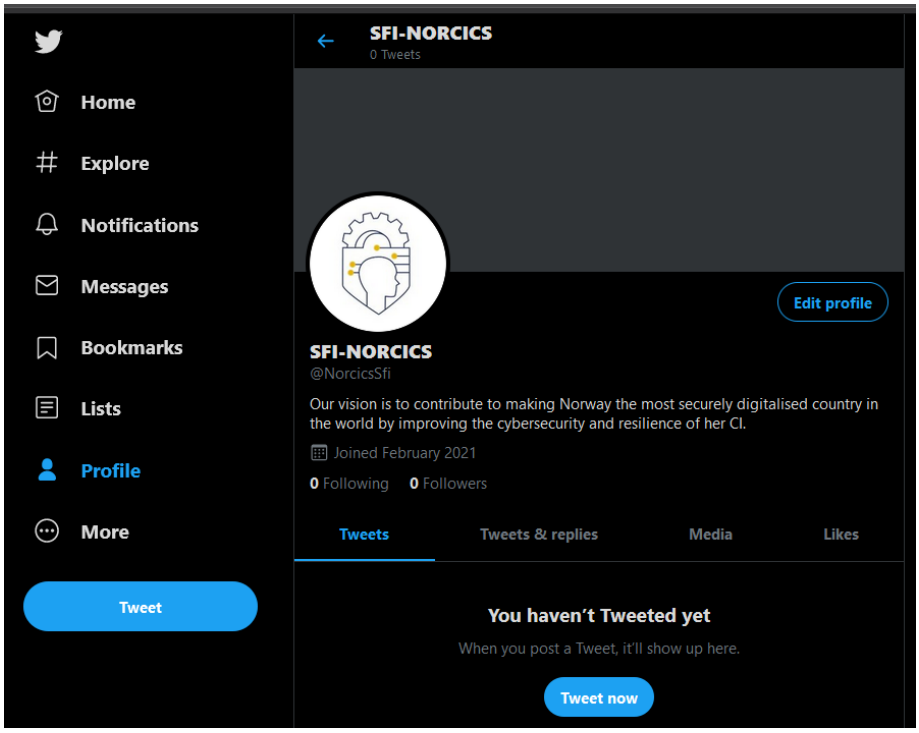
Editoral responsibility | About cookies | Privacy policy

Sign In

Social media accounts

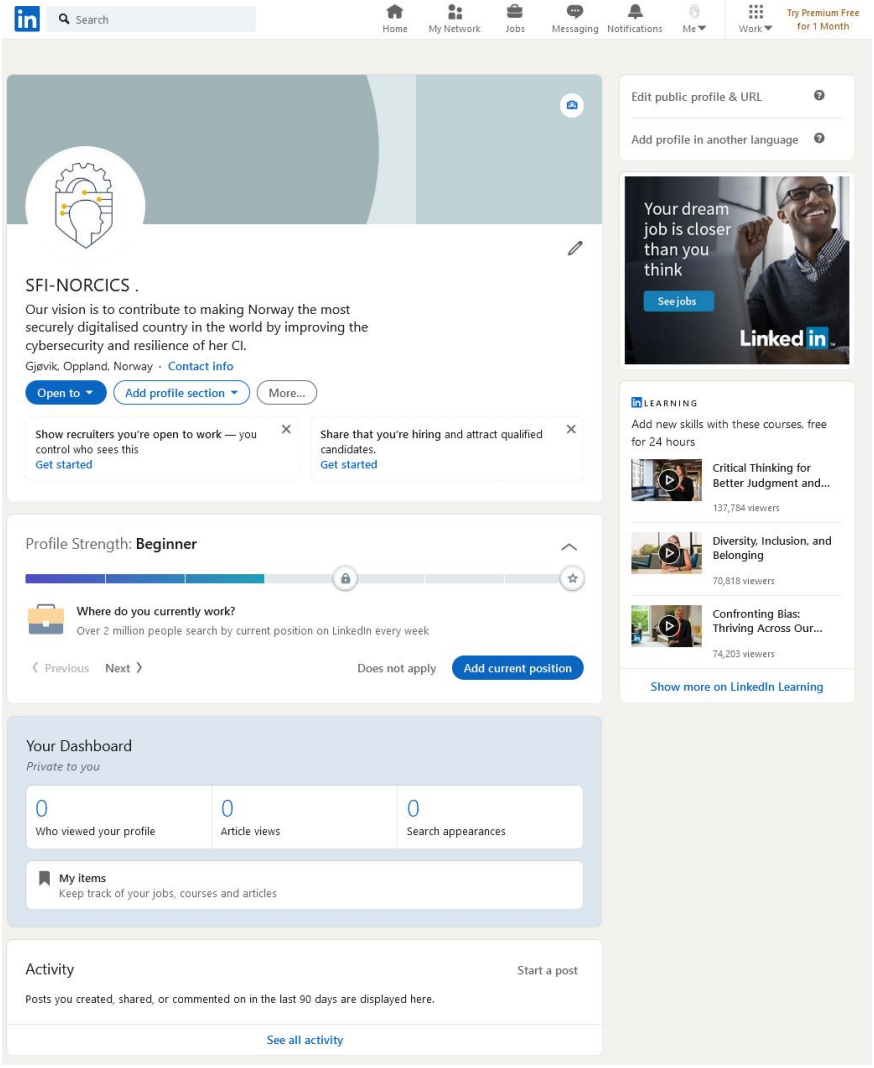
Twitter account

We have recently created a Twitter account for NORCICS, to be used for widespread communication about the project, its activities, and results.



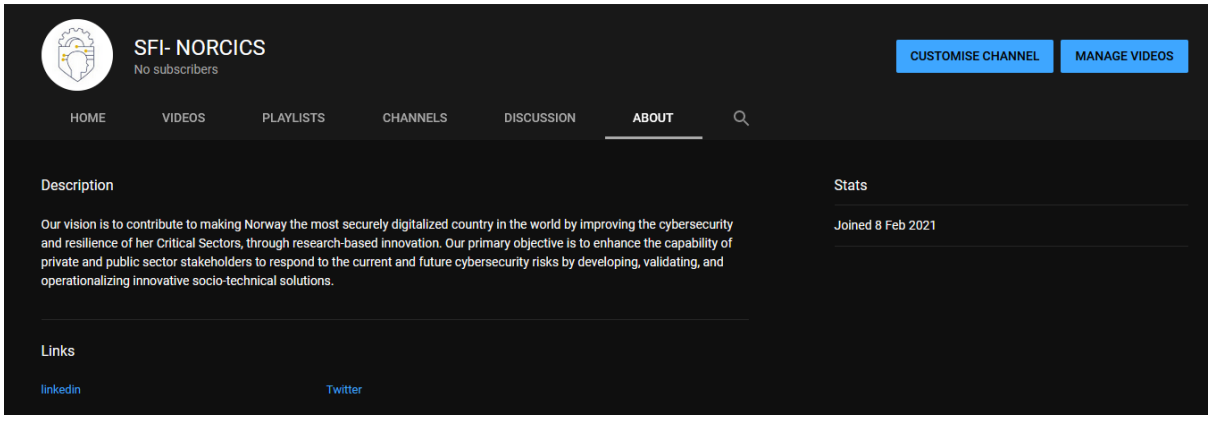
LinkedIn account

We have recently created a LinkedIn account for NORCICS, to be used for widespread communication about the project, its activities, and results. The account is also to be used for recruiting.



YouTube channel

We have recently created a YouTube account for NORCICS, to be used for widespread communication about the project, its activities, and results.



Templates

Word template

A word template has been created for the project. All written reports should be compiled using this template, which is available at the project repository.

Powerpoint template

We have created a Powerpoint template for the project. All presentations should be compiled using this template, which is available at the project repository.

Promotional material

Continuous presentation

A continuously updated presentation on the objectives and status of the project has been developed and will be used as a comprehensive mechanism for updating and informing on the project.

Mailing lists

We have defined the following mailing list for the communication between the project participants. The mailing lists are indirectly managed by the project administration and the WP5 leader, while they are directly managed by the corresponding responsible administrator as described below.

Table 3: Mailing lists.

Mailing list	**Participants**	**Example of purposes**	**Administrator**
NORCICS Partners partners@norcics.ntnu.no	All partner contacts (technical)	General assembly	SFI administrator
NORCICS Board board@norcics.ntnu.no	Board members	Board meetings	SFI administrator
NORCICS activity leaders activitylead@norcics.ntnu.no	All task leaders All work package leaders	Project internal communication for research coordination	SFI administrator
One for administrative/financial contacts of all partners administration@norcics.ntnu.no	Contact point at partner for administrative/financial matter (e.g. reporting)	In-kind reporting to the NFR, invoicing, distribution of funds	SFI administrator
One for everybody involved in the SFI sfinternal@norcics.ntnu.no	All partner contacts + all internal personnel	Broad project internal communication	SFI administrator, WP5 leader
One for each WP wpx@norcics.ntnu.no	WP leader, task leaders within that WP (all relevant personnel in that WP)	WP internal communication	SFI administrator, WP leader
One for each task wpxty@norcics.ntnu.no	Task leader + all relevant personnel in that task + corresponding WP leader	Task internal communication	SFI administrator, Task leader

One for WP leaders wplead@norcics.ntnu.no	WP leader team	Scientific management committee communication	SFI administrator
One for management/administration team admintnu@norcics.ntnu.no	Management/admin team, including those at NTNU-IIK associated with NORCICS	Administrative personnel communication	SFI administrator
One open list sfi@norcics.ntnu.no **(Restricted list – posting only by the administrators)**	All who wants to be, upon registration	Mailing list available on the website, where anyone can subscribe to a newsletter and other communication	SFI administrator, WP5 leader

Online publishing

Newsletters

A quarterly newsletter will be established, which will be distributed at the public mailing list. The newsletter will include a brief status report and updates on the project achievements for each period.

Blogs

A monthly blog post will be established focusing on selected topic across the project focus areas, or alternatively on recent incidents. We will publish the blog posts on the project's social media and for the first months they will focus on communicating the project objectives. The initial blog posts are as follows.

Date	**Topic**	**Author**
4/2021	Project narrative	WP5 leader + director
4/2021	WP1 perspectives	WP1 leader
5/2021	WP2 perspectives	WP2 leader
6/2021	WP3 perspectives	WP3 leader
7/2021	WP4 perspectives	WP4 leader
8/2021	WP5 perspectives	WP5 leader

Press releases

When deemed necessary by the scientific committee or the board, or upon request by the funding organization, the project may proceed to press releases, with the objective of providing an expert opinion on recent incidents and occurring developments with significant impact on cybersecurity. We may alternatively integrate such press releases into the project's newsletter. Under all circumstances, a press release bearing the logo and/ or name of the project, or claiming to originate from the project, must first obtain approval by the scientific committee and the board.

Posters

A series of posters will be created for:

1. The overall project
2. Each WP
3. Each Task
4. Each research activity (i.e. within the tasks)

A common template will be created for this purpose, and this material will be continuously updated in order to reflect current developments. The material we will use this material as an integral part of the continuously updated presentation, and for dissemination/ communication purposes across the aforementioned channels.

Videos

A series of videos will be created for:

1. The overall project
2. Each WP
3. Each Task
4. Each research activity (i.e. within the tasks)

A common template will be created for this purpose, and this material will be used for dissemination/ communication purposes across the aforementioned channels.

Annual Workshop

Each year we will organize an open workshop to present and demonstrate the project's results and enable discussion with government and industry. Industrial and governmental organizations and project partners will be invited to contribute with presentations and demonstrations. We will combine this yearly workshop with a project review.

Acknowledging funding

Any form of work that is produced within the SFI-NORCICS and does not follow the defined template, must acknowledge the project and the funding authority by integrating the following acknowledgment when published.

“This work was partially or fully conducted within the SFI-NORCICS (https://www.ntnu.edu/norcics). This project has received funding from the Research Counsil of Norway.”