ÅRSRAPPORT

2024

Gjøvik, 01.04.2025

NTNU

CCIS – Center for Cyber and Information Security

Center for Cyber and Information Security v/IIK, NTNU, Pb 191, N-2902 Gjøvik, Norway – post@ccis.no – www.ccis.no

Innholdsfortegnelse

Ny direktør ved NTNU CCIS Peggy Sandbekken.

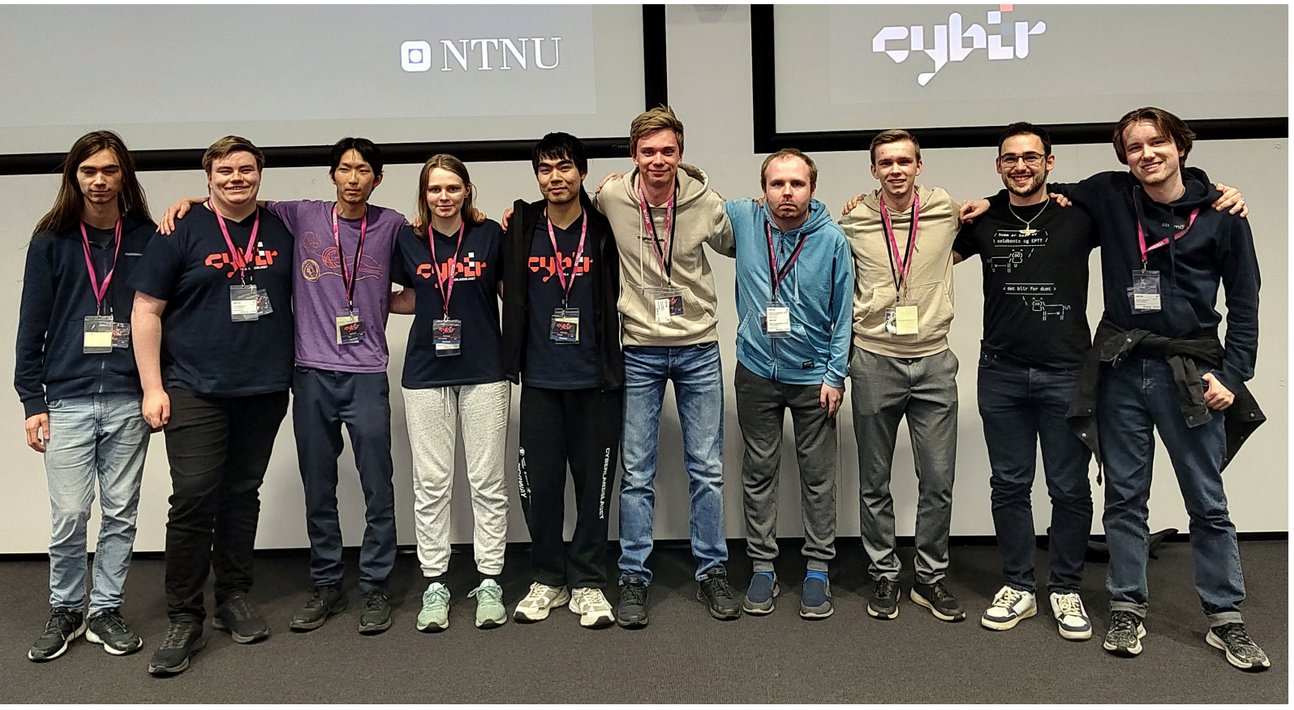
1 Innledning

NTNUs Center for Cyber and Information Security (NTNU CCIS) er et nasjonalt senter for tidsrelevant forskning, utdanning og kompetansebygging innen cyber- og informasjonssikkerhet. Senteret skal bidra til å styrke samfunnets, virksomhetenes og den enkelte borgers evne til å beskytte sine informasjonsaktiva, oppdage relevante trusler, håndtere aktuelle hendelser og hvis nødvendig etterforske kriminelle handlinger i cyberdomenet.

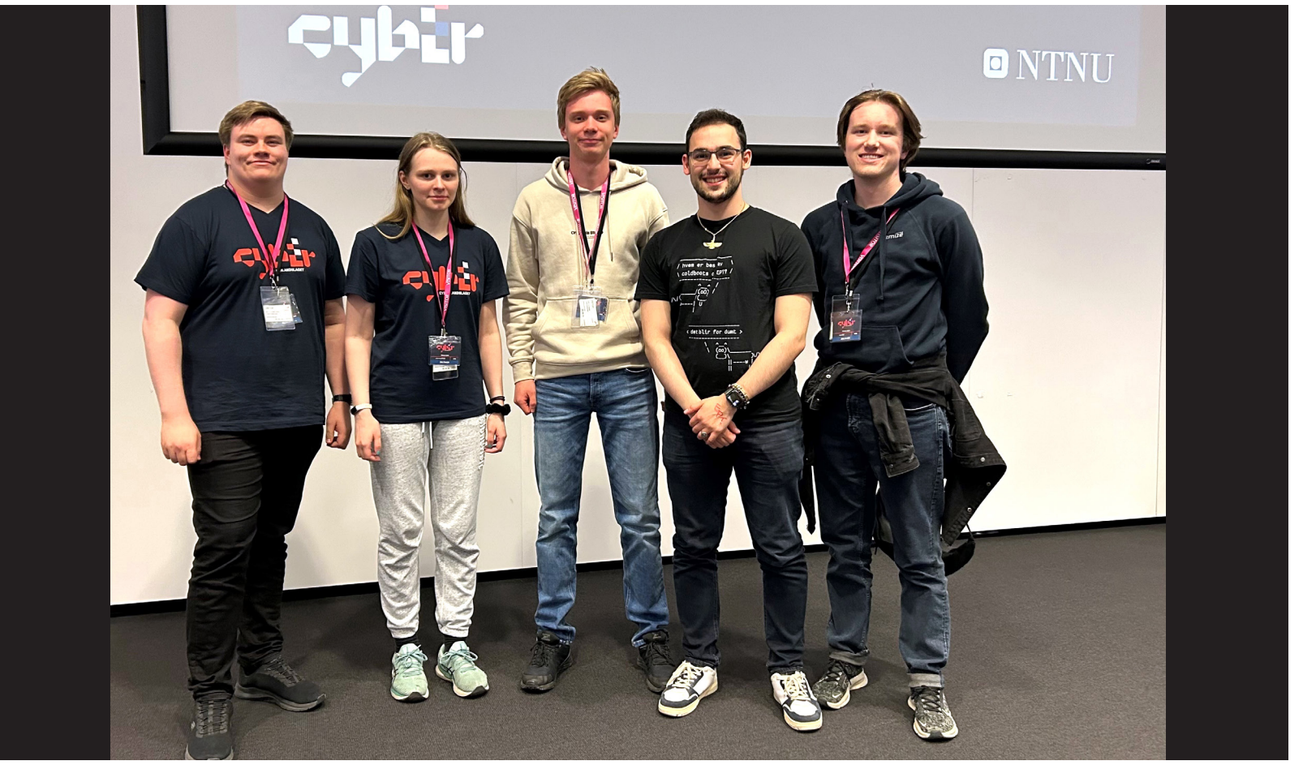
I et komplekst samfunn med stort behov for helhetlig kunnskap om cyber- og informasjonssikkerhet svarer NTNU CCIS på disse behovene på nasjonalt nivå, i samfunnet og hos våre partnere. Kunnskapsutviklingen ved NTNU CCIS har langsiktige perspektiver for utdanning, forskning og formidling. I et dynamisk trusselbilde skal vi bidra til at det ved våre partnerinstitusjoner utdannes relevante kandidater og produseres varig kunnskap.

NTNU CCIS bidrar til effektiv samhandling og utveksling av kunnskap i offentlig og privat sektor ved å forene partnere fra privat og offentlig sektor med akademia.

NTNU CCIS har ved utgangen av 2024 følgende 81 eksterne partnere: ABB, Accenture, Advancia, Aeger Group, Akershus universitetssykehus, BDO, Bouvet, Buypass, Capgemini, CIAM, Cisco, Cognite, Cyberforsvaret, Datatilsynet, Defendable, Digdir, DIPS, Direktoratet for e-helse, DLA Piper, DNV, Eidel, Eidsiva Energi, Fence, FFI Forsvarets forskningsinstitutt, Forsvarets Høgskole, Government of Iceland, Havtil, Helsedirektoratet, HP Hewlett-Packard AS, Høgskolen i Innlandet, Hydro, IBM, IFE, Innlandet Fylkeskommune, Innlandet politidistrikt, KINS, Kluge advokatfirma, KDA Kongsberg Defence & Aerospace, KPMG, Kripos, mnemonic AS, NSM Nasjonal sikkerhetsmyndighet, Nasjonalt ID-senter, NKOM Nasjonal kommunikasjonsmyndighet, NC-Spectrum AS, Norges Bank, NORMA Cyber, Norwegian Cybersecurity Cluster, Norges Domstoler, Norsk Regnesentral, NORSIS Norsk senter for informasjonssikring, Orkla, Omny, Paloalto, Petroleumstilsynet, Politiet Oslo Politidistrikt, POD Politidirektoratet, PHS Politihøgskolen, PST Politiets sikkerhetstjeneste, Posten, PwC, Riskpoint, SANDS Advokatfirma, Schjødt, Siemens Energy, Skatteetaten, Sopra Steria, Sparebankstiftelsen Hedmark, Statkraft, Statnett, Storebrand, Styrmand, Sykehuset Innlandet HF, Telenor Norge AS, Thales Norway, Tietoevry, Tussa Kraft, Visma, Watchcom Security Group, White Label Consultancy og Økokrim.



Cyberlandslaget for 2024 etter finalen i juni. Disse deltar for Norge under ECSC 2024 i Torino, Italia, i oktober.



5 av deltagerne på årets Cyberlandslag er studenter ved NTNU.

2 Årsrapport

2.1. Styrets arbeid og generalforsamling

Styret i NTNU CCIS består etter styremøtet 26.09.2024 (valgperiode i parentes) av:

- Norges teknisk-naturvitenskapelige universitet (NTNU), styreleder ved Ingrid Schjølberg
- Nasjonal sikkerhetsmyndighet, NSM ved Bente Hoff (2023–2025)
- Kripos ved Olav Skard (2023–2025)
- Cyber Forsvaret ved David Henriksen (2023–2025)
- Statnett ved Esben Gudbrandsen (2024–2026)
- DNV ved Anette Roll-Richardsen (2024–2026)
  mnemonic ved Siri Bromander (2024–2026)
- Ansattrepr. ved Staal Vinterbo (2023–2025)

Grunnet arbeid med strukturendringer i 2023 ble det besluttet at alle styremedlemmer sitter til og med general-forsamling 2024. Nytt styre ble derfor konstituert høsten 2024. Det ble i styremøte 19. mars besluttet å endre vedtekter, hvilket medfører at NTNU har sittende styreleder som velges av NTNU.

STRATEGI NTNU CCIS 2021–2026
VISJON
NTNU CCIS – en nasjonal kunnskapsressurs for digital sikkerhet.

NTNU CCIS skal være:

1. En hovedleverandør av tidsrelevant kunnskap og kompetanse for å styrke digital sikkerhet.
2. En synlig samfunnsaktør med nettverksarenaer og møteplasser for offentlig-privat, sivilt- militært og internasjonalt samarbeid.
3. Et nasjonalt og internasjonalt anerkjent forsknings- og kompetansesenter.
4. Et tverrfaglig senter ved NTNU som er sikret god organisering og finansiering.

MANDAT
NTNU CCIS skal styrke samfunnets evne til å forebygge, avdekke, bekjempe og utrede ondsinnede handlinger som skjer ved bruk av informasjons- og kommunikasjons-teknologi. Senteret skal i samarbeid med og gjennom sine partnere gjøre dette ved å:

- Arbeide for å beskrive trender av relevans for digital sikkerhet.
- Videreutvikle forskningsevne og fagmiljøer i inter-nasjonal toppklasse, med tverrfaglige fagdisipliner som er relevante for partnerne og nasjonen. NTNU CCIS skal bidra i internasjonalt samarbeid og bli en kunnskapsnode i Europa.
- Arbeide for å øke rekrutteringen av norske studenter til phd-utdanningene ved å drive opplæring og etablere studieprogrammer av høy kvalitet, og med stor samfunnsrelevans.
- Styrke samarbeid og utveksle tidsrelevant kompetanse mellom sektorer, virksomheter og akademia; likeledes med nasjonale og internasjonale prosjekter, sentre og organisasjoner. NTNU CCIS skal samarbeide med og bidra til organisasjoner som har som oppgave å informere og bevisstgjøre om sikkerhet. I tillegg bidra til aktørenes langsiktige strategier som gjelder kompetanseutvikling og FoU-prosjekter.
- Om nødvendig kunne håndtere sensitiv og/eller gradert informasjon i sin forskning.

Organisering
NTNU CCIS har Institutt for informasjonssikkerhet og kommunikasjonssikkerhet (IIK) ved Fakultet for informa-sjonsteknologi og elektroteknikk (IE) som sitt vertsinstitutt, i Norges teknisk-naturvitenskapelige universitet (NTNU). Senteret ble etablert i 2014.

Senteret ledes daglig av en direktør, med støtte av en koordinator, for å understøtte aktiviteten i senteret. I tillegg har senteret bred tilgang på annen administrativ støtte fra vertsinstitutt og -fakultet.

NTNU CCIS har som mål å bidra til samhandling og utveksling av kunnskap i offentlig og privat sektor, ved å forene partnere fra privat og offentlig sektor med akademia.

Senteret er inndelt i ulike tematiske forskningsgrupper, som har ukentlige koordineringsmøter. Informasjon om disse finnes på NTNU CCIS' nettside.

Partnerskap
NTNU CCIS er åpent for partnerskap både nasjonalt og internasjonalt. Partnere inviteres til å til å bidra til, og delta i aktiviteter i regi av senteret.
En partner som ikke opptrer på en måte som er i tråd med NTNU CCIS sin visjon, kan vurderes ekskludert av direktør i samråd med styret.

Administrasjon og styringsorganer
Generalforsamlingen
Generalforsamlingen er åpen for alle partnere i NTNU CCIS. Generalforsamlingen er ikke et besluttende organ. På generalforsamlingen:

- Administrasjonen presenter årsrapport over aktiviteten i senteret

Forskningsgruppeleder på Krypto, Tjerand Silde holder foredrag.

- Administrasjonen gir en oppdatering på relevante forskningsresultater
- Styreleder presenterer plan for fremtidig aktivitet for kommentarer og diskusjoner.

Alle partnere i generalforsamlingen har rett til å foreslå sine kandidater inn i styret. NTNU i samråd med sittende styre oppnevner nytt styre og informerer om dette på generalforsamlingen.

Styret
NTNU CCIS har et rådgivende styre uten beslutningsfullmakt over NTNU CCIS. Styret er sammensatt av arbeidslivsrepresentanter som skal rådgi NTNU CCIS om strategisk retning og ambisjoner, for at virksomheten skal være arbeidslivs- og tidsrelevant.

NTNU CCIS sitt styre består av styreleder fra NTNU, 1 representant valgt blant de ansatte fra IIK NTNU og 7 styremedlemmer fra partnere i senteret. Styret kan tildele observatørstatus til relevante partnere. Det skal etterstrebes en kjønnsbalansert styresammensetning bestående av representanter fra akademia, offentlig sektor og næringsliv. Nye styremedlemmer velges av generalforsamlingen, de velges for to år og kan bli gjenvalgt. Halvparten står på valg hvert år, for å sikre kontinuitet og unngå at hele styret byttes ut samtidig.

Styret skal
- Årlig vurdere innspill og strategi for NTNU CCIS
- Vurdere, gi innspill til og følge opp aktiviteten i NTNU CCIS
- Komme med innspill til og godkjenne årsrapport

Styret møtes minst to ganger i året og NTNU CCIS-administrasjonen er ansvarlig for innkalling og at det føres skriftlige referater.

Direktør, administrasjon og forskningsgruppene
Direktør utnevnes av NTNU. Direktør og administrativt personale er ansatt ved NTNU. Direktør er ansvarlig for daglig drift av NTNU CCIS og skal bidra til å realisere mandatet. Instituttleder ved IIK er nærmeste leder for direktør. Senterets tematiske forskningsgrupper skal årlig gi innspill til direktør på strategiske satsningsområder basert på utvikling og fagekspertise.

Fasiliteter
NTNU CCIS har fysiske lokaler ved NTNU i Gjøvik.

Økonomi
NTNU CCIS er organisert som et prosjekt under NTNU som finansierer administrasjonen i senteret.

Oppdateringer
Vedtektene er oppdatert og godkjent 08.03.2024 og revideres ved behov. Enhver endring vil kreve godkjenning av NTNU.

2.2. Organisasjon og ledelse
NTNU CCIS har Institutt for informasjonssikkerhet og kommunikasjonsteknologi (IIK) ved Fakultet for informasjonsteknologi og elektroteknikk (IE) som sitt vertsinstitutt i Norges teknisk-naturvitenskapelige universitet (NTNU). IIK har 150 årsverk med bred kompetanse innen ulike fagemner tilknyttet informasjonssikkerhet og kommunikasjonsteknologi.

I 2024 har Peggy Lill Sandbekken overtatt som direktør for NTNU CCIS (Senter for Cyber- og informasjonssikkerhet). Denne stillingen kombinerer hun med stillingen som innovasjonsleder ved Institutt for informasjonssikkerhet og kommunikasjonsteknologi (IIK). I begge oppgavene vil hun være døråpner for nye samarbeidsmuligheter mellom ledende kompetansemiljø ved NTNU og ulike næringslivsaktører, blant annet ved å realisere forskningsbasert innovasjon sammen med samarbeidspartnere og å øke synligheten av fagmiljøenes og samarbeidspartnernes aktivitet.

Inge Moen, som i en årrekke har vært tilknyttet CCIS, har gått over i pensjonistenes rekker. Inge har i de senere år vært tilknyttet CCIS som spesialrådgiver og har vært svært delaktig i oppbygging av senteret og vedlikehold av partnerskapet.
Inge har vært primusmotor for to fagturer til IBM Innovation Studio & Think Lab Zürich i Sveits, i 2024. Turer som har gitt verdifull innsikt for deltakerne, med tema innen blant annet kvanteteknologi og cybersikkerhet. Inge ble formelt takket av under partnerkonferansen i november. Vi sender en stor takk til Inge for det bidraget han har gitt over mange år.

Senteret har ukentlige møter for koordinatorene i de tematiske gruppene. To saksbehandlere har i 2024 administrativt understøttet aktiviteten i NTNU CCIS, i tillegg til at senteret har bred administrativ støtte fra vertsinstitutt og -fakultet.

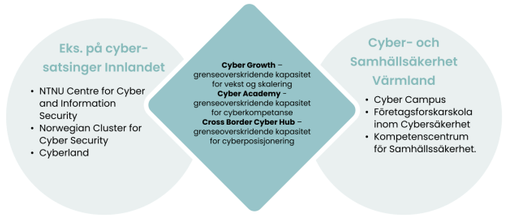
NTNU CCIS' aktivitet var første halvår gruppert i følgende tematisk grupper:
- Applied Cryptography
- Critical Infrastructure and Resilience
- Cyber Defence
- E-Health and Welfare Security
- Information Security and Privacy Management
- Norwegian Biometrics Laboratory
- Digital Forensics Group
- Organizational complexity, management and cybersecurity
- System Security

Siste halvår har det vært noe omorganisering av forskningsgruppene. Organizational complexity, management and cybersecurity har gått over til EVU(kurs). E-Health and Welfare Security og System Security har slått seg sammen og kaller seg nå eHealth and System Security Group (HS2G). Dette for å styrke E-Health and Welfare Security-satsningen.

Forskningsgruppene er nå som følger:
- Applied Cryptography
- Critical Infrastructure and Resilience
- Cyber Defence
- eHealth and System Security
- Information Security and Privacy Management
- Norwegian Biometrics Laboratory
- Digital Forensics Group

2.3. Forskning
NTNU CCIS sine ulike forskningsgrupper og deres arbeid er presentert i kapittel 2.6. i tillegg har NTNU CCIS bidratt i følgende forskningsprosjekter:

Cross Border Cyber Capacity (CBCC) er et interreg-prosjekt hvor Compare er svensk prosjekteier og Digital Innlandet er norsk prosjekteier. Basert på potensialet for grenseoverskridende merverdi er visjonen å utvikle et grenseoverskridende cyberinnovasjonsøkosystem som skaper vekst og verdiskaping gjennom felles kapasitetsbygging og overføring av teknologi og kompetanse.
- NTNU IIK/CCIS deltar i arbeidspakkene og har ledelse for arbeidspakke «Kapasitet for cyberkompetanse – Cyber Academy».
- NTNU IIK og CCIS deltar i styringsgruppen for prosjektet.
- Et gjennomgående sentralt element i CBCC er fokus på å bringe sammen utfyllende kompetanse, infrastruktur og erfaringer for å forsterke kapasitet for innovasjon knyttet til cyber og informasjonssikkerhet. Gjennom Cyber Academy får samfunns- og næringsliv i regionene Innlandet og Värmland et styrket kompetansetilbud, og Cross Border Cyber Hub styrker grenseregionen sin kapasitet for strategisk posisjonering nasjonalt og internasjonalt.



- Forsknings- og utdanningsaktører som deltar er NTNU, HINN, Karlstad Universet, Fagskolen Innlandet, Cyberingeniørskolen og Försvarshögskolan. Prosjektet er inne i sitt andre år.

Nye EU-prosjekter med oppstart i vår:
- **cPAID;** envisions the development of a cloud-based, platform-agnostic defense framework. The project combines AI-based defense methods, security- and privacy-by-design, privacy-preserving, explainable AI, Generative AI, context-awareness as well as risk and vulnerability assessment and threat intelligence of AI systems.
- **CRESCENDO;** the project will develop complementing efforts in the Nordic countries increasing the level of protection and resilience to cyber threats in the energy domain. The project will fund and orchestrate the development of cybersecurity services (existing and developed during its course) at entities (public and private). The services will focus on cyber security testing, risk assessment and real time risk monitoring.
- **TUAI;** Towards an Understanding of Artificial Intelli-

gence via a transparent, open and explainable perspective. The focus will be on the highest quality doctoral training on sustainable AI that is used in smart manufacturing, smart cities, smart healthcare and smart mobility.
- **AMPLIFY;** The aim of this project is to strengthen the competitive capabilities of marginalized but uniquely valuable European CCIs through innovative digital tools and practices by addressing the following objectives:
- Creating novel human-centered artistic experiences that connect people in physical relationships among and between artists and audiences
- Developing an AI-driven audiovisual production tool in a portable box that will enhance the experience of performing and consuming physical live music
- Developing technological XR enablers to create immersive stages for physical engagement and interaction
- Promoting music as a unique, creative, cohesive and inclusive language for society by testing the digital tools in human-centered real-world small-scale pilot trials in four countries
- – Strengthening the sustainability and market position of European CCIs by building their capabilities and use of AMPLIFY's novel technology and formats

BRUA. European Cybersecurity Competence Center and Network – National Coordination Center Norway.

- Norges teknisk-naturvitenskapelige universitet (NTNU), Nasjonal sikkerhetsmyndighet (NSM) og Norges forskningsråd samarbeider for å etablere et nasjonalt koordineringssenter for cybersikkerhet for Norge. Prosjektet kalles BRUA. Senteret vil fungere som et kontaktpunkt på nasjonalt nivå for å støtte den europeiske cybersikkerheten og Industri-, forsknings- og kompetansesenterets (ECCC) formål og mål.

Det vil legge til rette for at industri og andre aktører på nasjonalt nivå kan delta i grenseoverskridende prosjekter og cybersikkerhetstiltak:
- vurdere enheter i Norge til å bli en del av fellesskapet
- etablere synergier med relevante aktiviteter på nasjonalt og regionalt nivå
- identifisere og adressere sektorspesifikke industrielle
- utfordringer innen cybersikkerhet
- gjennomføre konkrete tiltak
- inkludert økonomisk støtte til nasjonale/ lokale økosystemer
- fremme og spre resultatene av arbeidet i Nettverket,
- Fellesskapet og ECCC.

BRUA-prosjektet skal operasjonalisere dette senteret.

- CCIS bidrar blant annet med ledelse av arbeidspakker samt kartlegging og registering av aktuelle utdanninger og virksomheter i Norge som skal være registrert i senteret.

2.4. Utdanning

NTNU CCIS har i tillegg til vertsinstitusjonen NTNU flere utdanningsinstitusjoner i partnerskapet. Forsvarets ingeniørhøgskole, BI, Høgskolen i Innlandet og Politihøgskolen tilbyr alle utdanninger som er relevante for NTNU CCIS sitt arbeid. Den faglige utvekslingen mellom utdanningsinstitusjonene er basert på samarbeid mellom de faglig ansatte, at faglig ansatte ved en institusjon underviser ved en annen institusjon og deltagelse i hverandres interne seminarer. På denne måten er de faglig ansatte brobyggere mellom utdanningsmiljøene.

NTNU er partnerskapets hovedleverandør av studier innen cyber- og informasjonssikkerhet. Utdanninger ved NTNU med særlig fokus på områder av høy relevans for NTNU CCIS er:
- PhD. i informasjonssikkerhet og kommunikasjonsteknologi
- 5-årig masterstudium i teknologi/sivilingeniør i kommunikasjonsteknologi
- 2-årig engelskspråklig masterstudium «Information Security»
- 4-årig deltid engelskspråklig masterstudium «Information Security»
- 2-årig engelskspråklig masterstudium «Digital Infrastructure and Cyber Security»
- 3-årig deltid erfaringsbasert masterstudium «Information Security»
- 3-årig bachelorstudium i Digital infrastruktur og cybersikkerhet
- Partner i Erasmus-program SECCLO «Security and Cloud Computing»

Erfaringsbasert mastergrad i informasjonssikkerhet tilbys i samarbeid med Politihøgskolen og Cyberforsvaret. Noen av masterutdanningene tilbys både på heltid og deltid, og er derfor svært aktuelle tilbud for virksomheter som ønsker å gjennomføre målrettede kompetanseutviklingstiltak for sine ansatte.

2.5. En synlig samfunnsaktør

NTNU CCIS skal være en synlig samfunnsaktør, ved å organisere og være til stede på en rekke møteplasser nasjonalt og internasjonalt. I 2024 gjennomførte/ igangsatte vi følgende aktiviteter:

- **FutureTech 24** En innovasjonskonferanse hvor NTNU CCIS og IIK i fellesskap stod som arrangør sammen med Vaager Innovasjon, Gjøvikregionen utvikling, Byen Vår Gjøvik, NTNU TTO og Innlandet Fylkeskommune. På programmet sto investorforum, offisiell åpning av Cyber City – den nye møteplassen for cyberaktører, lære hvordan IIK har bygget et verdensledende cybersikkerhetsmiljø og mulighet til å høre studenter presentere sine innovative idéer.

- **Techløftet Innlandet** Et samarbeid med Vitensenteret Innlandet. Kompetanseløft som skal gå frem til sommeren 2027, hvor partene skal jobbe samme om å

NTNU IBM Zurich group.

fremme teknologiinteresse og løfte den digitale interessen blant barn og unge i Innlandet. Prosjektet ledes av Vitensenteret Innlandet. Satsningen har et nasjonalt potensial.

- **Fagdag ved IBM Innovation Studio & Think Lab Zürich.** IBM Norge sammen med NTNU CCIS inviterte til en fagdag den 28. mai for lederrepresentanter fra NTNU CCIS sine partnere og IBMs egne partnere. Fokus var orientering på policy nivå om IBMs pågående forskning og utvikling innen kvantedatamaskiner, kvantesikker kryptografi, generativ kunstig intelligens og cybersikkerhet. Senteret i Zürich er ett av IBMs 12 forskningssentra i verden og har ansvar for utviklingen av IBMs produkter innen maskinvare og programvare. Det var 23 påmeldte deltakere.

Masters of Cybersecurity
Masters of cybersecurity arrangeres som del av møteplassen The Norwegian Cyber Security Convension – HackCon. Dette er en kunnskapskonkurranse for det norske fagmiljøet i digital sikkerhet hvor alle kan melde seg på. Konkurransen foregår over tre runder. De to første er online og den siste skjer i salen, live under HackCon.

Sikkerhetsfestivalen på Lillehammer

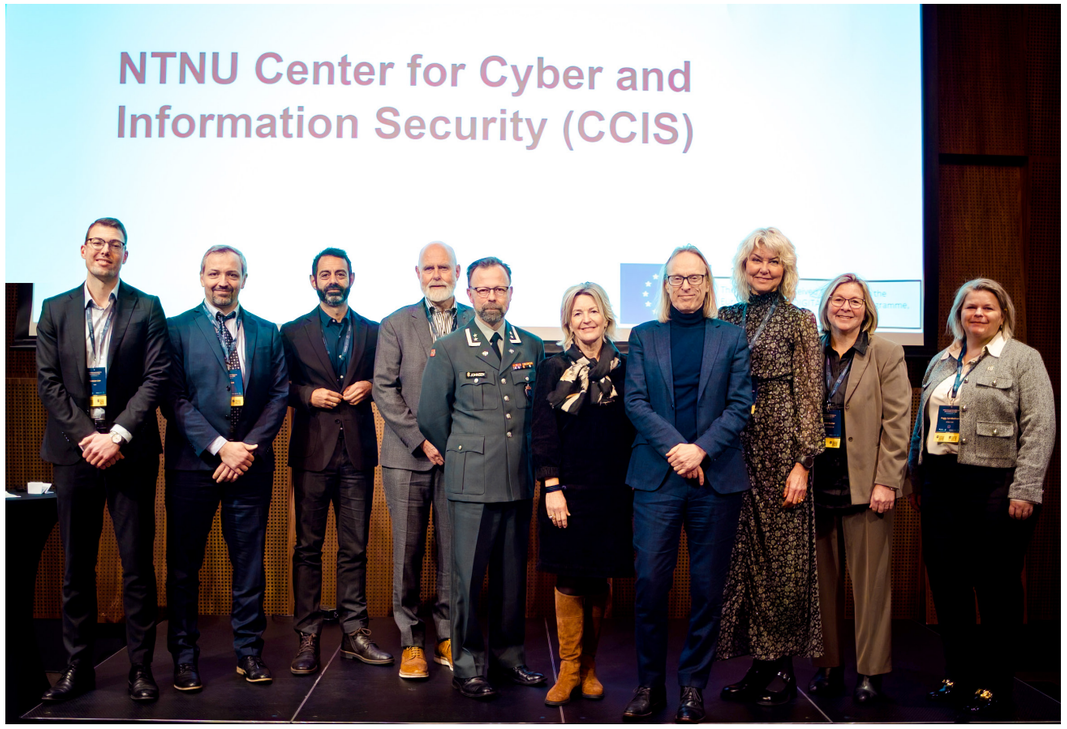
Hvert år deltar NTNU CCIS på Sikkerhetsfestivalen. I år arrangerte vi eget godt besøkt spor onsdag 28.8., med følgende innlegg:

– Strategic Engagement with Cybersecurity Games: A Mini-workshop with Professor Stewart James Kowalski, Professor Aris Kaloudis and Associate Professor Erjon Zoto.

The primary aim of this mini workshop is to provide an overview of how serious games and sandboxing can facilitate a deeper organizational engagement with the complex issues around cybersecurity planning and compliance.

– Oppdag Fremtidens Kryptografi ved NTNU! Presentert av PhD-student Caroline Sandsbråten Kryptografi har tatt et kvantesprang i utdanningen ved NTNU! Særlig for våre engasjerte matematikk- og KomTek-studenter, har kryptografi blitt en uunnværlig del av deres akademiske reise. Snart starter vi med en splitter ny hovedretning: "Kryptografisk Ingeniørvitenskap"!

– Symmetrisk nøkkelutveksling: hva er alternativene for lightweight IoT? Ved Assistant Professor of cryptology Bor de Kock.
Symmetrisk kryptografi som AES er enkel, effektiv og sikker, også i en postkvanteverden, som gjør dem interessant i situasjoner der vi trenger sikker kryptering, men har lite energi og minne tilgjengelig. Tradisjonelt har en ulempe med disse algoritmene vært at nøklene er statiske, som betyr at vi ikke kan oppnå sikkerhetsegenskaper som forward secrecy med mindre vi avtaler en ny nøkkel hver gang.



F.v. Christian Lien NSM, Basel Katt NTNU CCIS/IIK, Pejman Heibø-Bagheri Helse- og omsorgsdepartementet, Inge Moen NTNU CCIS, Roger Johnsen Cyberforsvaret Ingrid Schjølberg NTNU CCIS/IE, Morten Irgens Copenhagen Business School, Hanne Alstrup Velure Innlandet Fylkeskommune, Bente Skattør Oslo Politidistrikt og Peggy Sandbekken NTNU CCIS.

Partnerkonferanser

NTNU CCIS gjennomførte 6. juni sin Generalforsamling. Denne ble holdt digitalt.

NTNU CCIS og SFI NORCICS gjennomførte 20. og 21. november sin kombinerte Partnerkonferanse med i snitt ca. 110 deltagere pr. dag på The Hub i Oslo. NTNU CCIS feiret sitt 10-årsjubileum og dette ble innledet av Morten Irgens som var tidligere styreleder i NTNU CCIS og nå fungerer som Vice Dean Copenhagen Business School. Han ga oss et historisk tilbakeblikk. Deretter sa et knippe av de første partnerne noen ord om NTNU CCIS sin betydning og samarbeidet gjennom 10 år. Christian Lien, representerte Nasjonal sikkerhetsmyndighet, NSM, Pejman Heibø-Bagheri representerte Helse- og omsorgs-departementet, Hanne Alstrup Velure representerte Innlandet Fylkeskommune, Bente Skattør representerte Oslo Politidistrikt og Roger Johnsen var der på vegne av Cyberforsvaret.

Videre ble det holdt korte innlegg som beskrev suksess-historier gjennom 10 år:

– Digital Forensic og samarbeidet med Kriops ved Jan William Johnsen
– Etableringen av SFI NORCICS ved Sokratis Katsikas

Fra Konferansen.

Pejman Heibø-Bagheri ga et historiske tilbakeblikk fra Helse- og omsorgsdepartementet.

– Etableringen Norwegian Cyber Range ved Basel Katt
– Mobai, en oppstartsbedrift ved Brage Strand, CEO Mobai AS
– ENFIELD (EU prosjekt fra Horizon-programmet) ved Georgios Spathoulas
– Samarbeidet med Cyber Defence ved Benjamin Knox
– Cyber Ranges as platforms for Policy Sandboxing of Cyber Security ved Erjon Zoto og Stewart Kowalski.

Siste del av dagen var tematikken «Samarbeid mellom næring og akademia» og en paneldebatt omkring «Digital tillit – en premissgiver for en bærekraftig digital økonomi og et digitalt samfunn?»

Malware Forum på Fornebu, Oslo i oktober.

NTNU Malware Forum

Dette er Norges viktigste nettverksarena for eksperter på analyse og reversering av skadelig programvare. Alle som deltok delte informasjon om «banebrytende» teknikker og avansert skadelig programvare som påvirker Norge. Arrangementet er et samarbeid mellom Norsk Cyberforsvar, NTNU CCIS og NSM, og ble arrangert for åttende gang i år. I år var det nesten 400 påmeldt og mer enn 200 valgte å følge skadevaresporet etter lunsj. Et meget vellykket arrangement og et viktig bidrag til kompetansehevingen i Totalforsvaret, noe som ble understreket i åpningstalen til direktøren for NSM.

Attack24

Attack 2024 var en konferanse arrangert av IKT Norge, som fant sted 5. november 2024 på Oslo Kongressenter. Arrangementet samlet beslutningstakere fra politikk, forsvar, etterretning, globale teknologiselskaper, innovasjonsmiljøer, akademia og næringslivet for å diskutere løsninger på digitale angrep. Temaene inkluderte påvirkningen av det amerikanske valget på geopolitikk, rollen til AI og kvanteberegning i cybersikkerhet, og privatsektorens ansvar for å styrke datasikkerheten. Her deltok NTNU CCIS sin forskningsgruppe Applied Cryptography med et foredrag om Postkvantum Computing, holdt av PhD Hans Heum og en felles stand med Aeger Group og IBM Norge.

Norwegian and European Cyber Security Challenge (ECSC)

Justis- og beredskapsdepartementet har bedt NTNU CCIS forberede norsk deltakelse i ECSC. NTNU CCIS hadde i 2024 ansatt 6 personer fra CTF-miljøet i Norge, med Lasse Lervik i spissen, til å danne et norsk lag. Disse fungerte som landslagstrenere, understøttet administrativt, teknisk og økonomisk fra NTNU CCIS. Rekrutteringen av landslaget skjedde gjennom Norwegian Cyber Security Challenge (NCSC), som har som målsetning å finne unge talenter (i aldersgruppen 16–25 år) innen cybersikkerhet og å motivere disse til å utvikle seg videre. Det har i 2024 blitt arrangert to kvalifiseringsrunder og en finale i NCSC. Se bilder av landslaget side 4.
ENISA (EU's cybersikkerhetsorgan) hadde tildelt Italia og Torino ansvaret for planlegging og gjennomføringen

Det norske landslaget klar for konkurranse.

av ECSC i 2024. Vårt norske lag, bestående av 10 deltagere, reiste dit fra 7.–12. oktober for å konkurrere med omkring 34 andre nasjoner. 5 av årets deltagerne på det norske landslaget er studenter ved NTNU. I kampen mot mange dyktige landslag, endte det norske landslaget på en god 18. plass i den internasjonale konkurransen.

Security Divas konferansen

Mot slutten av 2024 ble det klart at NTNU CCIS i samarbeid med Norwegian Cybersecurity Cluster (administrert av Digital Innlandet) overtar Security Divas-konferansen fra 2025, da NorSIS blir en del av NSM og dermed ikke skal ha denne konferansen i sin portefølje lenger. Security Divas (SD) er et nettverk for kvinner som jobber, studerer eller ønsker å jobbe med informasjonssikkerhet.
Anne Skeidsvoll Granli ved NTNU CCIS har ledet programkomitearbeidet og deltatt i organiseringen av konferansen som skal avholdes på Strand Hotel Gjøvik den 23. og 24. januar 2025.

Security Divas ble første gang arrangert av NorSIS i 2010, med et mål om å få flere kvinner til å velge en karriere innen informasjonssikkerhet og tørre å ta lederroller. Siden har det utviklet seg til å bli et nettverk for kvinner som studerer, jobber eller ønsker å jobbe med digital sikkerhet. Arbeidet med Security Divas er knyttet til FNs bærekraftsmål nummer fem: «Likestilling mellom kjønnene». Security Divas er derfor et viktig tiltak for økt mangfold i en mannsdominert bransje. Det er stor interesse rundt konferansen, og vi har mellom 150–200 deltakere hvert år

Konferansen «Empowering Diversity in Engineering»

NTNU, NTNU CCIS, AAU (Ålborg Universitet i København), DTU, IDA og IDA Connect inviterte til en spennende heldagskonferanse i mangfoldets navn innen ingeniørfaget. Det ultimate målet var å fremme mangfold, rettferdighet og inkludering innen ingeniør- og teknologisektoren på tvers av de nordiske landene ved å dele beste praksis, fremme samarbeid og utvikle handlingsrettede strategier som tiltrekker, beholder og styrker underrepresenterte grupper.

Fra ECSC 2024 sine konkurranselokaler i Torino, Italia

Målet for konferansen er å fremheve eksemplariske praksiser innen utdanning og identifisere vellykkede strategier for mangfold på arbeidsplassen. Disse målene ble utforsket gjennom erfaringsbaserte sesjoner og fremtredende innledere som inspirerte deltakerne til å fremme nye ideer som vil bli brakt til bordet i en interaktiv workshop for alle deltakerne.

Innledere var var bl. a.:
Denmark: Pernille Scholdan Bertelsen, Vice-head of Department of Sustainabilty and Planning, TECH faculty, AAU "How the project Diversity in Tech Education (DITEC) at AAU led to a changed concept for study start."
Norway: Anna Szlavi, Researcher, NTNU
"Gender-inclusive practices in the EUGAIN project and the Women STEM UP project"

Sweden: Simone Fischer-Hübner, Security Divas Sweden
Moderator her var Førsteamanuensis ved NTNU Iwona Maria Windekilde.

Under paneldebatten ble det diskutert hvordan kan vi kan gjøre ingeniørfaget mer mangfoldig og inkluderende på tvers av Norden.

Paneldeltakere var Camilla Hillerup (direktør i Microsoft Danmark), Daniel Askeroth (CTO Norlys) og Maria Fagranes Clemmensen (Nordic Programme Manager at Tech Nordic Advocates I Founder of Sharedrobes). Moderator under paneldebatten var Peggy Sandbekken fra NTNU CCIS.

Security Divas Sverige
7.–8. november markerte den første konferansen i Security Divas Sweden. Denne konferansen oppsto som et resultat av et samarbeid mellom Karlstad Universitet og NTNU i prosjektet Cross Border Cyber Capacity (CBCC). Anne Skeidsvoll Granli ved NTNU CCIS har i flere år vært involvert i den norske utgaven av Security Divas og har også vært involvert i å etablere den svenske utgaven av dette nettverket. Som den norske versjonen er dette også et nettverk for kvinner innen teknologi og informasjonssikkerhet, med mål om å gjøre teknologibransjen mer inkluderende for kvinner og å være en drivkraft i å skape plattformer hvor kvinnelige talenter i feltet blir fremhevet, støttet og inspirert til å være en del av fremtiden innenfor disse fagområdene. Peggy Sandbekken fra NTNU CCIS holdt foredrag om bakgrunnen og historikken omkring Security Divas Norge.

SFI NORCICS

Senter for forskningsdrevet innovasjon Norwegian Center for Cybersecurity in Critical Sectors (SFI NORCICS) er et viktig og synlig resultat av samarbeidet i NTNU CCIS. SFI NORCICS er et selvstående prosjekt med finansiering fra Norges Forskningsråd. Prosjektet er basert på partnerskapet i NTNU CCIS og det finnes betydelig samarbeid og synergier mellom sentrene. NORCICS visjon er å bidra til å gjøre Norge til det sikreste digitaliserte landet i verden, ved å forbedre cybersikkerheten og robustheten i kritiske sektorer, gjennom å støtte forskningsbasert innovasjon. Mer informasjon finner du på:
https://www.ntnu.edu/ norcics.

Torino pyntet og klar for ECSC 2024.

Etter- og videreutdanning (EVU)

Det foregår løpende markedsføring og gjennomføring av etter- og videreutdanning over hele landet. Vi har også deltatt i planlegging og gjennomføring av NECC (North European Cyber Security Cluster) konferanser i 2024.
- 2 HKdir kurs på videreutdanning

NTNU er partner i Nemonoor, en norsk innovasjonshub for kunstig intelligens og informasjonssikkerhet støttet av EU under Digital Europe programmet. NTNU har hovedansvar i Nemonoor for kompetanse og opplæring, og har som en del av prosjektet etablert moderne plattform for EVU aktivitet til næringsliv og offentlig sektor, inkludert CCIS partnere. Det er gjennomført flere nettbaserte kurs på plattformen i vår og tilbakemeldingene er meget positive. En rekke kurs tilbys våre partnere og andre virksomheter innen kunstig intelligens og informasjonssikkerhet. Beredskapsøvelser på NTNU's Cyber Range er også omfattet av dette tilbudet. NTNU har også fått innvilget statlig støtte til aktivitetene i Nemonoor for SMB virksomheter (inntil 250 ansatte). Med støtteordningene fra EU og Innovasjon Norge vil dette gi svært attraktive og rimelig kompetanseøkning for virksomheter som kvalifiserer for dette. Mer informasjon om de ulike tilbudene kommuniseres i månedlige nyhetsbrev fra CCIS.

Kursene har fått svært gode tilbakemeldinger. Et eksempel her fra evaluering «Introduksjon til Maritim Cybersikkerhet».

Utviklet videreutdanning i digital sikkerhet
NTNU IIK sammen med Universitetet i Innlandet (INN) Institutt for organisasjon, ledelse og styring, vil sammen tilby videreutdanning i digital sikkerhet. Denne er satt opp som tre emner:
- Introduksjon til digital sikkerhet
- Risikostyring, beredskapsplanlegging og øving for digital sikkerhet
- Sikker IKT-drift

Hvert emne er 5 studiepoeng, og tilbys med ett emne per semester der første emne har oppstart høsten 2025.

I Norwegian Cyber Range (NCR) Det har gjennom ØLBIS-prosjektet blitt holdt 4 øvelser for kommuner i Innlandet i NCR. Disse var kommunene Gjøvik, Søndre Land, Nordre Land og Vestre Toten. Øvelsene gikk over to dager hver. Ressurser fra NTNU CCIS deltok som stab under øvelsene.
Det har også vært en sektorøvelse for høgskole- og universitetssektoren med 20 deltagende virksomheter kalt Morris 2024.

Treffpunkt innlandet
Peggy Sandbekken holdt et innlegg på konferansen Treffpunkt Innlandet 19. august, der årets tema var Totalforsvar. Justisminister Emile Enger Mehl åpnet konferansen med å ta for seg Totalforsvaret i en ny tid.

Deretter ble totalforsvaret belyst fra tre ulike sider med forsvars-perspektivet ble belyst av Generalmajor Lars Lervik, landbruks-perspektivet fra fylkesordfører

Thomas Breen og cyber/akademia sin side ble presentert av NTNU CCIS direktør Peggy Sandbekken. Hun vektla det økende kompetansebehovet vi vil møte fremover og viktigheten av samarbeid, samarbeid og samarbeid.

Totalforsvaret sett fra Stortinget ble presentert av Tor Andre Johnsen Justiskomiteen, Bengt Fasteraune Utenriks og -forsvarskomiteen og Rune Støstad Næringskomiteen, med fokus svakheter og på hva innlandet

3 Regnskap

kan bidra med.

2.7. Regnskap NTNU CCIS 2024
Regnskapsrapporten viser totaløkonomien for NTNU CCIS.

Den totale bevilgningen i 2024 var 1 MNOK fra HOD. I tillegg mottok CCIS 100k i sponsorinntekter knyttet til landslaget. Øvrig inntekt er bidrag fra partnere og NTNU.

Sammenlignet med 2023-regnskapet har vi i 2024 hatt lavere inntekt. Dette skyldes i hovedsak at finansieringen på 5 MNOK fra JD er avsluttet. Det ble heller ikke overført ubrukte midler fra 2023.

På bakgrunn av at vi har mistet finansiering fra JD er også aktiviteten i CCIS nedjustert i forhold til dette. Det gjenspeiler seg i de fleste av postene i regnskapet.

I overkant av 90 prosent av kostnadene i 2024 er lønn knyttet til forskning, utdanning og formidling, administrasjon og landslaget.

Det har i 2024 vært høyere kostnader knyttet til reiser sammenlignet med 2023, mens driftskostnadene har vært lavere. Det er også lave kostnader knyttet til møter og arrangementer sammenlignet med fjoråret.

Regnskap 2024	
Inntekter	
Bevilgning statsbudsjettet – HOD	**1 000 000**
Bidrag partnere	**8 048 540**
Bidrag NTNU	**5 867 028**
Totale inntekter	**15 015 568**
Utgifter	
Administrasjon	
Lønn	1 643 498
Partner- og avtaleoppfølging	**207 509**
Forskning, utdanning og formidling	
Lønn	**11 069 695**
Reiser	**309 796**
Aktiviteter i forskningsgruppene	**232 610**
Publikasjoner, trykking, annonser	**30 367**
Møter og arrangementer	**159 037**
Utvikling	**24 011**
Landslaget	
Lønn	**1 028 850**
Reiser	**263 198**
Andre driftskostnader	**80 107**
Totale utgifter	**15 048 678**
Resultat	**33 110**

Faggruppenes aktivitet i 2024

1. Applied Cryptology Lab (NaCl)

Group coordinator:
Associate Professor Tjerand Silde

Research group description:
The NTNU Applied Cryptology Lab (NaCl) is a joint research group between the Department of Information Security and Communication Technology and the Department of Mathematical Sciences at NTNU, focusing on designing and analysing secure cryptographic protocols and systems.

We cooperate with many prominent research groups, both nationally and internationally, as well as with industry and other partners.

Our research interests are the theory and practice of key exchange, digital signatures, homomorphic encryption, verifiable computation, electronic voting, formal verification, symmetric cipher design and analysis, cryptography engineering, and data privacy. We are particularly interested in designing and analysing schemes secure against quantum adversaries.

Members of the group
Academic staff:
1. Tjerand Silde, Associate Professor (Research Group Leader NaCl)
2. Danilo Gligoroski, Professor
3. Colin Alexander Boyd, Professor / Researcher
4. Kristian Gjøsteen, Professor
5. Staal A. Vinterbo, Professor
6. Stig Frode Mjølsnes, Professor
7. Slobodan Petrovic, Professor
8. Jiaxin Pan, Associate Professor
9. Anamaria Costache, Associate Professor
10. Jeongeun Park, Associate Professor
11. Bor de Kock, Associate Professor
12. Morten Rotvold Solberg, Assistant Professor

Researchers and Postdoctoral Fellows
1. Hans Waardal Heum, Postdoctoral Fellow
2. Tikaram Sanyashi, Postdoctoral Fellow
3. Mattia Veroni, Postdoctoral Fellow
4. Dan Zhang, Postdoctoral Fellow

PhD students
1. Cristian Alonso Baeza Miranda
2. Ole Martin Edstrøm
3 Sonu Kumar Jha
4. Lise Millerjord
5. Charlotte Ida Pauline Mylog
6. Lea Sibylle Nürnberger
7. Emil August Hovd Olaisen
8. Caroline Sandsbråten
9. Sahana Sridhar
10. Amir Zarei

Collaboration and collaboration partners:
- Norwegian Defense Research Establishment (FFI), Norway
- Kongsberg Defense & Aerospace, Norway
- Thales Norway, Norway
- University of Wuppertal, Germany
- University of Luxembourg, Luxembourg
- Microsoft Research, Redmond, USA
- Intel, USA
- Royal Holloway, University of London, UK
- Australian National University, Australia
- University of Maryland, College Park, USA
- Aarhus University, Denmark
- Technical University of Denmark, Denmark
- Duality Technologies, USA
- University of Oxford, UK
- University of Edinburgh, UK
- IBM Research Europe - Zurich, Switzerland
- Max Planck Institute for Security and Privacy, Germany
- Ruhr University Bochum, Germany
- Radboud University Nijmegen, The Netherlands
- University of Surrey, UK
- University of Bristol, UK
- University of Lorraine, France
- University of Kassel, Germany
- CISPA Helmholtz Center for Information Security, Germany
- Saarland University, Germany
- IMDEA Software, Spain
- Technology Innovation Institute, UAE
- University of Electronic Science and Technology of China, China
- NXP Semiconductors, Belgium
- Simula UiB, Norway
- Bitdefender, Romania

Main research result:
Overview of ongoing projects:
– "Lightweight cryptography for future smart networks"
– "Realistic cryptography for large-scale applications"
– "OffPAD - Optimizing balance between high security and usability"
– "SOTERIA: Real-world deployment considerations for fully homomorphic encryption"
– "CRYPTO-LAB: theoretical and practical cryptographic research and education"
– "Cryptography and social life"
– NTNU start-up package for Gender Equality and Diversity
– NTNU development stipend for Gender Equality and Diversity

Overview of submitted proposals:
– RCN Centre for Research-based Innovation (advanced to the second round)
– RCN Research School
– RCN AI Centre application on AI Safety and Security
– "SCORE – Secure Computation made real" Horizon doctoral network
– SQUASH – "poSt QUAntum Security with symmetric-key and lattice-based cryptograpHy"

Some selected publications:
– Carlo Brunetta, Hans Heum, and Martijn Stam, "SoK: Public Key Encryption with Openings", IACR Public Key Cryptography 2024
– Jiaxin Pan, Doreen Riepel, and Runzhi Zeng ,"Key Exchange with Tight (Full) Forward Secrecy via Key Confirmation", IACR Eucrocrypt 2024
– Kamil Doruk Gur, Jonathan Katz, and Tjerand Silde, "Two-Round Threshold Lattice-Based Signatures from Threshold Homomorphic Encryption", PQCrypto 2024
– Yuyu Wang, Chuanjie Su, and Jiaxin Pan, "Fine-Grained Non-Interactive Key-Exchange without Idealized Assumptions", IACR Crypto 2024
– Diego F. Aranha, Anamaria Costache, Antonio Guimarães, and Eduardo Soria-Vazquez, "HELIOPOLIS: Verifiable Computation over Homomorphically Encrypted Data from Interactive Oracle Proofs is Practical", IACR Asiacrypt 2024
– Patrick Hough, Caroline Sandsbråten, and Tjerand Silde, "More Efficient Lattice-Based Electronic Voting from NTRU", IACR Communications in Cryptology 2024
– Jeongeun Park, Barry van Leeuwen, and Oliver Zajonc, "FINALLY: A Multi-Key FHE Scheme Based on NTRU and LWE", IACR Communications in Cryptology 2024

Education: Activity:
Teaching the following courses:
– TMA4140 - Discrete Mathematics (B.Sc.)
– TTM4135 - Applied Cryptography and Network Security (B.Sc.)
– TTM4137 - Wireless Network Security (M.Sc.)
– TTM4205 - Secure Cryptographic Implementations (M.Sc.)
– TTM4195 - Blockchain Technologies and Cryptocurrencies (M.Sc.)
– TMA4160 - Cryptography (M.Sc.)
– IMT4124 - Cryptology (M.Sc.)
– TMA4162 - Computational Algebra (M.Sc.)
– TTM4502 - Specialization Project (M.Sc.)
– TTM4905 - Master's Thesis (M.Sc.)
– MA8206 - Advanced Cryptography (Ph.D.)

Overview of graduated PhD candidates:
1. Pia Bauspieß (June 2024)
2. Elsie Margrethe Staff Mestl Fondevik (June 2024)
3. Jonathan Komada Eriksen (August 2024)
4. Runzhi Zeng (September 2024)

Overview of supervised MSc theses:
1. Sondre Rishøi and Jonatan Såstad Østgaard, "Unbiased Distributed Key Generation", supervised by Tjerand Silde
2. Carl Ludvig Digné , "Implementing Quantum Secure Passwordless Authentication", supervised by Tjerand Silde
3. Diderik Kramer, "Service mesh and eBFP security services in cluster net- works", supervised by Danilo Gligoroski
4. Tor Håkon Ingerson Moen and Matija Popovic, "Enhancing Whistleblower Anonymity with ZKPs on the ZkVM SP-1", supervised by Danilo Gligoroski
5. Lukas Neuenschwander, "Intrusion detection in Kubernetes – a comprehensive study of tools and techniques", supervised by Danilo Gligoroski
6. Jørgen Reimers, "Achieving forward secrecy and quantum resistance in TLS pre-shared key mode", supervised by Bor de Kock
7. Jakob Martin Torsvik, "Differentially private named entity recognition model de- velopment", supervised by Staal A. Vinterbo
8. Espen Sund, "Towards Oblivious Transfer in the Quantum Random Oracle Model", supervised by Jiaxin Pan

9. Thomas Fardal Rødland, "A Correct Shuffle Using Product Proofs A Lattice-Based Zero-Knowledge Approach", supervised by Kristian Gjøsteen
10. Sander Støle Hageli, "Constructing Error-Correction Codes using Algebraic Function Fields", supervised by Kristian Gjøsteen
11. Knut Heimdal, "Studying algorithms for solving the Approx-SVP in ideal lattices", supervised by Kristian Gjøsteen
12. Jørgen Eikjeland, "Quantum safe cryptography in a modern peer-to-peer application framework", supervised by Slobodan Petrovic
13. Sindre Williksen, "Anomaly Detection with Machine Learning and Deep Learning in Layer 3 Network Traffic", supervised by Slobodan Petrovic
14. Jan Olaf Storeng, "Developing Long Short-Term Memory Mechanism and Dataset for Intrusion Detection in Critical Infrastructure by Simulation", supervised by Slobodan Petrovic

Hans Heum presenterer artikkel på IACR Public Key Cryptography 2024 i Sydney.

Dissemination activities:
Organized Events, Conferences, and workshops:
– Program Committee members of IACR Eurocrypt, IACR Crypto, IACR Asiacrypt, IACR Communications in Cryptology, ACM CCS, IACR Public Key Cryptography, IACR Real-World Crypto, IACR Journal of Cryptology, and PETS
– Women in Cryptography November seminar series
– ICMS Workshop on Foundations and Applications of Zero-Knowledge Proofs in Edinburgh
– Norsk Kryptoseminar 2024 in Gjøvik
– WAHC 2024 – Workshop on Encrypted Computing & Applied Homomorphic Cryptography in Salt Lake City

The proudest achievements in 2024:
– Publication at major IACR venues Eurocrypt, Crypto and Asiacrypt as well as at Public Key Cryptography and Communications in Cryptology
– The RCN SFI application "Centre for Research-based Innovation in Applied Cryptography" advanced to the final stage. There were 96 applications, 30 advanced, 8 will be funded.

2. Critical Infrastructures and Resilience (CISaR)

Group coordinator:
Professor Sokratis Katsikas

- The CISaR group currently comprises 36 full and part-time members.
- The CISaR group has established collaboration with more than 200 partners (academia, industry, research), mostly in Europe and in Norway, in the context of externally funded R&D programs (HORIZON Europe, NFR etc.)
- Main research result
  - The areas of research interest of the group are: Cyber security of the energy infrastructure; Maritime cyber security and resilience; Cyber security of cyber physical systems; Cyber security of the IoT and of the industrial IoT; Cyber security of digital twins; Security Awareness, Training and Education; Secure, safe, and trustworthy AI.
  - The members of the group are involved in 29 ongoing research projects in the above areas. Details can be found at https://www.ntnu.edu/iik/cisar
  - The members of the group published over 45 publications in journals, books, and conference proceedings in 2024. A (partial) list of the group's publications (retrieved from Cristin) can be found at https://www.ntnu.edu/iik/publications#/view/publications.
- Education
  - Members of the group supervised 6 MSc theses
  - The group provides its members with access to the Infosec Institute Infosec Skills courses. Members of the group have delivered EVU lectures and courses on various occasions.
- Dissemination activities
  - The group leader serves as Editor-in-Chief of the Level-2 "International Journal of Information Security" (Springer) and had been chairing (until September 2023) the steering committee of the ESORICS conferences. Group members serve on the Editorial Board of international journals and on program committees, as chairs or members of the Technical Program Committees, of a large number of international conferences and have organized special issues of international journals. Members of the group have co-organized 5 international workshops.

Members of the group Academic staff:
1. Prof. Sokratis K. Katsikas (Group leader)
2. Prof. Bernhard Hämmerli
3. Prof. Siv Hilde Houmb
4. Prof. Stephen Wolthusen
5. Assoc. Prof. Vasileios Gkioulos
6. Assoc. Prof. Georgios Spathoulas
7. Assoc. Prof. Ernst Gunnar Gran
8. Assoc. Prof. Jia-Chun Lin
9. Assoc. Prof. Marie Haugli-Sandvik
10. Assoc. Prof. Ben Knox – affiliated
11. Assoc. Prof. Katina Kralevska – affiliated

Researchers and Postdoctoral Fellows:
1. Dr Georgios Aggelinos
2. Dr Aida Akbarzadeh
3. Dr Ahmed Amro
4. Dr Alessio Baiocco
5. Dr Nabin Chowdhury
6. Dr Georgios Kavallieratos
7. Dr Chhagan Lal
8. Dr Ming-Chang Lee
9. Dr Pankaj Pandey
10. Dr Øyvind Anders Arntzen Toftegaard
11. Dr Frode van der Laak
12. Dr James Wright

PhD students:
1. Yana Bilous
2. Jessica Barbosa Heluany
3. Gizem Erceylan
4. Konstantinos Kampourakis
5. Vyron Kampourakis
6. Kristian Andreas Kannelønning
7. Arne Roar Nygård
8. Håvard Ofte
9. Samson Ogheneovo Oruma (HiØF)
10. Xhesika Ramaj (HiØF)
11. Safa Zouari

Research assistant
1. Lama Amro
2. Henrik Gjefle

Collaboration and collaboration partners:
Collaboration with more than 200 partners (academia, industry, research), mostly in Europe and in Norway, in the context of externally funded R&D programs (HORIZON Europe etc.)

Main research result:
Overview of ongoing projects (list):
– Areas of research interest for the group: Cyber security of the energy infrastructure; Maritime cyber security and resilience; Cyber security of cyber physical systems; Cyber security of the IoT and of the industrial IoT; Cyber security of digital twins; SDN security; Security Awareness and Education; Cybersecurity risk management for cyber physical systems; Managing cybersecurity in critical sectors; Human and organizational aspects of cyber-security in critical sectors; Applications of blockchain technology.
– The members of the group are involved in 29 ongoing research projects in the above areas:

1. CybAlliance: International Alliance for Strengthening Cybersecurity and Privacy in Healthcare (NFR INTPART)
2. RECYCIN: Reinforcing Competence in Cybersecurity of Critical Infrastructures: A Norway – US Partnership (NFR INTPART)
3. Cyber-Security for Critical Infrastructures Digital Twins (NFR NORCICS)
4. Lowering Cyber Security entry barriers for Industry 4.0 companies (NFR NÆRINGS PHD)
5. Reverse Engineering for verification of security in digital value chains in a critical infrastructure (NFR NÆRINGS PHD)
6. Situation awareness in Virtual Security Operations Centers (NFR NÆRINGS PHD)
7. Towards a user-centred security framework for social robots in public space (NTNU+HiØF)
8. A DevSecOps-enabled framework for risk management of critical infrastructures (NTNU+HiØF)
9. ELECTRON: rEsilient and seLf-healed EleCTRical pOwer Nanogrid (EU H2020)
10. Modelling distributed subversion attacks in cyber physical systems (NFR NORCICS)
11. CIRMAN: Circular Manufacturing research and educational collaboration with India and Japan (NFR INTPART)
12. CRESCENDO: Cyber preparedness and RESilienCe of the Energy sector in the NorDic region (EU DEP)
13. PowerDig: Digitalization of short-term resource allocation in power markets (NFR)
14. Resilient Future Smart Grid Ecosystem – Upcoming Steps in Innovation, Business Cases, its Regulation and Supervision (NFR OFFENTLIG PHD)
15. Operational Technology Resilience in the EU Delegated Act on Cybersecurity for the Power Sector – A Cross Paradigm Analysis of the Policy-Making Process (NVE-RME)
16. Exploring the intersections of digital twins and honeypots (SIEMENS Energy)
17. ENFIELD: European Lighthouse to Manifest Trustworthy and Green AI (EU Horizon Europe)
18. CERTIFAI: Agile conformance assessment for cybersecurity CERTIFication enhanced by Artificial Intelligence (EU Horizon Europe)
19. COMFORTAGE: Prediction, Monitoring and Personalized Recommendations for Prevention and Relief of Dementia and Frailty (EU Horizon Europe)
20. CYBERUNITY: Community for Integrating and Opening Cyber Range Infrastructures that Build an Interoperable Cross-Domain and Cross-Sector Cyber Range Federation (EU DEP)
21. BRUA: National Coordination Centre on Cybersecurity – Norway (EU DEP)
22. ACT: Federated Advanced Cyber physical Test range (EU EDF)
23. NEWSROOM: Adapting Cyber Awareness for Evolving Computing Environments (EU EDF)
24. CYCLE: CYberseCurityLEarning: Master's degree in Cybersecurity (EU ERASMUS+)
25. CORESIM: Context-Based Real-Time OT-IT Systems Integrity Management (NFR KSPKOMPETANSE23)
26. cPAID: Cloud-based Platform-agnostic Adversarial AI Defence Framework (EU Horizon Europe).
27. TUAI: Towards an Understanding of Artificial Intelligence via a transparent, open, and explainable perspective (HORIZON-MSCA-2023-DN-01)
28. Norway-India: Strengthening Institutional Partnerships for Advancing Smart City Security and Resilience through AI-driven Digital Forensic (UTFORSK project)
29. Cybersecurity for Critical Infrastructures (UTFORSK project)

More information can be found at
https://www.ntnu.edu/iik/cisar

Some selected publications:
– More than 45 publications in journals, books, and conference proceedings in 2024. A (partial) list of the group's publications (retrieved from Cristin) can be found at
https://www.ntnu.edu/iik/publications#/view/publications
– Indicative publications:

- Ramaj, Xhesika; Sanchez Gordon, Mary Luz; Gkioulos, Vasileios & Colomo-Palacios, Ricardo (2024). On DevSecOps and Risk Management in Critical Infrastructures: Practitioners´ Insights on Needs and Goals. In 46th International Conference on Software Engineering (ICSE 2024) | EnCyCriS/SVM 2024 | Lisbon, Portugal|April 14-20.
- Oruc, A., Chowdhury, N. & Gkioulos, V. A modular cyber security training programme for the maritime domain. Int. J. Inf. Secur. 23, 1477–1512 (2024). https://doi.org/10.1007/s10207-023-00799-4
- Oruc A., Kavallieratos G., Gkioulos V., Katsikas S.K.: Cyber Risk Assessment for SHips (CRASH). TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation, Vol. 18, No. 1, doi:10.12716/1001.18.01.10, pp. 115-124, 2024
- Toftegaard, Ø., Abraham, D., Shenoi, S., H ämmerli, B. (2024). Smart-Grid-Enabled Business Cases and the Consequences of Cyber Attacks. In: Staggs, J., Shenoi, S. (eds) Critical Infrastructure Protection XVII. ICCIP 2023. IFIP Advances in Information and Communication Technology, vol 686. Springer, Cham. https://doi.org/10.1007/978-3-031-49585-4_2
- Akbarzadeh A, Erdodi L, Houmb SH, Soltvedt TG. Two-stage advanced persistent threat (APT) attack on an IEC 61850 power grid substation. International Journal of Information Security. 2024 May 14:1-20.
- Akbarzadeh, A., Erdodi, L., Houmb, S.H., Soltvedt, T.G. (2024). Decoding the Human Element in APT Attacks: Unveiling Attention Diversion Techniques in Cyber-Physical System Security. In: Moallem, A. (eds) HCI for Cybersecurity, Privacy and Trust. HCII 2024. Lecture Notes in Computer Science, vol 14729. Springer, Cham. https://doi.org/10.1007/978-3-031-61382-1_1
- Akbarzadeh, A. et al. (2024). Workshop on Cybersecurity of Critical Infrastructures. In: Bieker, F., de Conca, S., Gruschka, N., Jensen, M., Schiering, I. (eds) Privacy and Identity Management. Sharing in a Digital World. Privacy and Identity 2023. IFIP Advances in Information and Communication Technology, vol 695. Springer, Cham. https://doi.org/10.1007/978-3-031-57978-3_21
- Pankaj Khatiwada, Bian Yang, Jia-Chun Lin, Bernd Blobel, "Patient-Generated Health Data (PGHD): Understanding, Requirements, Challenges, and Existing Techniques for Data Security and Privacy", Journal of Personalized Medicine 14, no. 3, 2024.
- Pankaj Khatiwada, Bian Yang, Jia-Chun Lin, Godfrey Mugurusi, Stian
- Underbekken, "A Reference Design Model to Manage the Consent in Data Subjects (DS)
- Centered Internet of Things (IoT) Devices," IoT, MDPI, 5(1), pp. 100-122, 2024.
- Ming-Chang Lee, Jia-Chun Lin, Sokratis Katsikas, "GAD: A Real-time Gait Anomaly Detection System with Online Adaptive Learning," accepted by the 39th International Conference on ICT Systems Security and Privacy Protection (IFIP SEC2024)
- Ming-Chang Lee and Jia-Chun Lin, "IoTective: Automated Penetration Testing for Smart Home Environments," accepted by the 9th International Conference on Internet of Things, Big Data and Security (IoTBDS 2024)
- Aafan Ahmad Toor, Jia-Chun Lin, Ernst Gunnar Gran ang Ming-Chang Lee, "UoCAD: An Unsupervised Online Contextual Anomaly Detection Approach for Multivariate Time Series from Smart Homes", accepted by the 9th International Conference on Internet of Things, Big Data and Security (IoTBDS 2024) Best Paper Award
- Ming-Chang Lee and Jia-Chun Lin, "Evaluation of k-means time series clustering based on z-normalization and NP-Free," accepted by the 13th International Conference on Pattern Recognition Applications and Methods (ICPRAM 2024)

Education:
Activity:
– IIK8010, IIK6530, TM8110, IMT4203, IIKG6502, DCSG1001, IIKG1001

Overview of supervised MSc theses:

1. "Implementing Trust Algorithms for securing Spacecraft in Zero-Trust Environment" (Student: Utsash, Masrur Masqub, Supervisors: Georgios Kavallieratos and Sokratis Katsikas)
2. "Threat Modeling in Satellite Communications for Maritime Operations" (Student: Even Kvam Frøseth, Supervisors: Georgios Kavallieratos and Sokratis Katsikas)
3. "Attack Path Analysis of Satellites Connected to Critical Infrastructure" (Student: Fredheim, Jacob Schjøllert, Supervisors: Georgios Kavallieratos and Sokratis Katsikas),
4. "Cybersecurity Evaluation of Maritime Systems" (Student: Abdullah Zafar, Supervisors: Ahmed Amro and Vasileios Gkioulos)
5. "Cloud based Model Predictive Control security – Closing the loop" (Student: Stig Myrland, Supervisors: Vasileios Gkioulos and Aida Akbarzadeh)
6. "Digital Twin for Cybersecurity in the Healthcare Sector" (Student: Rajaram Lakshmanan, Supervisor: Vasileios Gkioulos

Dissemination activities:
Organized Events, Conferences, and workshops:
– Editorship of journal special issues:

- Special Issue "Cybersecurity and Privacy Issues in Cyber-Physical Systems and Industrial Control Systems", Electronics (Guest Editors: Georgios Kavallieratos, Georgios Spathoulas)
- Special Issue "Techniques and Frameworks to Detect and Mitigate Insider Attacks", Information (Guest Editors: Santosh Aditham, Sokratis Katsikas)
- Special Issue "Cybersecurity and Artificial Intelligence: Advances, Challenges, Opportunities, Threats", Frontiers in Big Data – Cybersecurity and Privacy, (Guest Editors: Sokratis Katsikas, Nikos Pitropakis, Pavlos Papadopoulos)
- Special Issue "Security Mechanisms for Wireless Sensor Networks in Cyber-Physical Systems", Future Internet (Guest Editors: Georgios Kavallieratos, Georgios Spathoulas)
- Special Issue "Cybersecurity, Blockchain, and Privacy-Preserving Technologies: Innovations, Trends, Challenges, Opportunities", Electronic Research Archive, (Guest Editors: Sokratis Katsikas, Nikos Pitropakis, Pavlos Papadopoulos)
- Special Issue "Advances in Sensor-Based Lightweight and Adaptive Time Series Anomaly Detection", sensors (Guest Editors: Jia-Chun Lin and Ming-Chang Lee)

– The group leader serves as Editor-in-Chief of the Level-2 "International Journal of Information Security" (Springer)
– Group members serve on the Editorial Board of international journals

– Group members chair or serve on program committees of a large number of international conferences
– Members of the group have organized the following workshops:
- CyberICPS 2024 (ESORICS workshop)
- TrustBus 2024 (ARES workshop)
- SecIndustry 2024 (ARES workshop)
- EpesSEC 2024 (ARES workshop)
- SecHealth 2024 (ARES Workshop)
- SUNRISE 2024 (NIKT Workshop)
- CWEURP 2024 (IoTBDS Workshop)

Lifelong learning activities:
– The group provides its members with access to the Infosec Institute Infosec Skills courses.
– Several ad hoc EVU lectures.

Organization
– Current sources of funding for the group are:
- European Commission HORIZON Europe
- European Commission ERASMUS+
- NFR
- NTNU
- Kompetanse Norge
- EU Digital Europe Programme
- European Defense Fund
- HKDir

The proudest achievements in 2024:
– Largest Research Group in CCIS and IIK
– Extensive publication portfolio
– Extensive externally funded – both nationally and internationally- research portfolio

3. Cyber Defence

Group coordinator:
Adjunct Assoc.
Professor Benjamin J. Knox

Members of the group Academic staff:
1. Dr Benjamin J. Knox
2. Maj Dr Geir Olav Dyrkolbotn

Researchers and Postdoctoral Fellows:
3. Lt Col Roger Johnsen
4. Torvald Fossen Ask
5. Dr Øyvind Jøsok

PhD students:
6. Torvald Fossen Ask
7. Håvard Ofte (co-supervise)
8. Elizabeth Noble (PhD through HiØ)
9. Andre Jung Waltoft-Olsen (co-supervise)
10. Rune Nordvik (co-supervise) – defended 11. April 2024 (se below)

Collaboration and collaboration partners:
- FFI
- NSM
- Norwegian Ministry of Defence
- Telenor
- Forsvarets Høgskole
- NATO STO
- NATO ACT
- Østfold University College (HiØ)
- Albstadt-Sigmaringen University, Germany
- TalTech, Estonia
- Beyond Layer 7, U.S
- Crosspoint Labs
- Reykjavik University & University of Iceland
- IBM
- Virtual Rangers

Main research result:
Overview of ongoing projects (list):
– (NORCCIS) Norwegian Center for Critical Infrastructures Cyber Security: Subject matter expert research project: T3.3. Reverse Engineering Lab
– (ArsFornesica) Computational Forensics for Large-scale Fraud Detection, Crime Investigation & Prevention (FFI).
– Cyber-Social Influence and Propaganda (CSP-I II): FD and MoJ funded research project (FFI).
– AInception (EDF project) (AI Framework for Improving Cyber Defence Operations) - Member of the External Expert Advisory Board (EEAB) and project member through NDRE (FFI)
– EDF Project FACT. CYFOR is “Bruker Ansvar”.

Overview of submitted proposals:
– Forging Cyber-Physical Security Alliances for Sustainable Arctic Development, NordForsk, This pre-proposal is being submitted for the “Sustainable Development of the Arctic” call.

Some selected publications:
Rehman, M., Bahsi, H., Bukauskas, L., and Knox, B. J., (2024) ‘Exploring Trainees’ Behaviour in Hands-on Cyber-security Exercises Through Data Mining’, [being presented in June at ECCWS].

Zehnder, E., et al. (2024), ‘Digital Twins and Extended Reality for tailoring better adapted cybersecurity trainings in Critical Infrastructures’, [being presented in July at HCII].
Dyrkolbotn, G. O., Knox, B. J., og Johnsen, R., (2024) ‘Defensive cyberoperasjoner som militært virkemiddel i en norsk kontekst’ in Cybermakt. En tverrfaglig innføring, 2024, Berrefjord and Lund (red.), Universitetsforelaget, Ch. 5.

Ask, T. F., Knox, B. J., Lugo, R. G., Sütterlin, S. (2024) ‘Mental motstanskraft’ in Cybermakt. En tverrfaglig innføring, 2024, Berrefjord and Lund (red.), Universitetsforelaget, Ch. 16.
Knox & Jahl (2024) ‘Norge driver med symbolpolitikk når det gjelder kunstig intelligens’, Digi.no (https://www.digi.no/artikler/debatt-norge-driver-med-symbolpolitikk-nar-det-gjelder-kunstig-intelligens/540241).
Andre Waltoft-Olsen, Phillip Johnson2, Lasse Øverlier and Geir Olav Dyrkolbotn, “Exploring a Low-Cost Hardware Reverse Engineering Approach: A Use Case Experiment”, IFIP SEC 2024.

Brilingaitė, A., Bukauskas, L., Domarkienė, I., Rančelis, T., Ambrozaitytė, L., Pirta-Dreimane, R., Lugo, R.G. and Knox, B.J., 2024. Towards projection of the individualised risk assessment for the cybersecurity workforce. Computer Standards & Interfaces, p.103962.

André Waltoft-Olsen, Lasse Øverlier and Geir Olav Dyrkolbotn. Evaluating End-User Feasible Methods for Ensuring Trojan-Free FPGA Hardware, ESREL & SRA-E 2025.

Innovation:
Status on ongoing innovation activities:
– Cognitive Security Institute (CSI) https://cognitivesecurity.institute/

Education:
Activity:
Courses:
– IMT4214 Cyber Tactics (NTNU IIK) – 30 students
– IMT4116 Reverse Engineering and Malware Analysis (NTNU IIK) – 120 students
– Course: IMT4214 Cyber Intel (NTNU IIK) – 15 students
– Course: Military Cyber Operations (internal for Forsvaret)
– Course: Malware Analysis and Reversing (internal for Forsvaret)
– Committee: PhD committee: Gazmend Huskaj, Offensive Cyber Operations, Swe

PhD candidates:
– Rune Nordvik successfully defended on April 11th, "Interpretation of File System Metadata in a Criminal Investigation Context "
– Torvald Fossen Ask successfully defended his thesis on June 24th titled: "Neuroergonomic Approaches to Understanding and Improving Communication of Recognized Cyber Threat Situations".

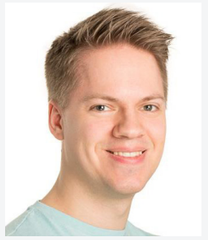
Overview of supervised MSc theses:
– Ola Joachim Åse: "Small languages and big models"
– Jacob Hofgaard: "Static control flow graph analysis for inlined function detection and identification"
– Erlend Frankrig: «Automated Binary Differential Analysis and Behavior Identification for Closed-Source Software Supply Chain Attack Detection
– Gaute Dvergsdal: "Long-context LLMs: how Extended Context length is Utilized, and its potential for Refining Decompiled code"
– Martin Holst Vaaden: "Using Large Language Models for Binary Decompilation"
– Jonas Gundersen: AI vs AI: Exploring Synthetic Text Detection of Large Language Models in a Low-Resource Language

Dissemination activities:
Organized Events, Conferences, and workshops:
– [Collaboration] Workshop University of Reykjavik, May.
– [Keynote] NFCERT Annual Conference, Reykjavik, May.
– [Keynote] HV01 Annual Conference, Rygge, Jan.
– [Keynote] Samhandlingsforum, Sarpsborg
– [Collaboration] ConnectCon, NIST&CSI, Las Vegas, August
– [Keynote] Digital Security, Jyväskylä, Finland, December
– [Keynote] Norges Bank, Oslo, October
– [Symposium] Co-chair, NATO STO, Meaningful Human Control, Amsterdam, Nov
– [Workshop] Multinational Capability Development Campaign, Integrating Cyber into Multinational Operations, Lillehammer, Sep
– [Workshop] NATO STO HFM, Chair, Cognitive Security Exploratory Team, Prague, Aug
– [Conference] HCII, session chair, 'Investigating and Strengthening the Human Factor in IT-Security'
– [Symposium & working group] EU & U.K Foreign Information Manipulation & Influence (FIMI) forum, invited guest, London, Oct
– NTNU Malware Forum

Funding (other than NTNU CCIS):
– Project ATHENA. This Digital Europe (DIGITAL) funded project aims to boost cyber resilience of critical infrastructure in the water sector through innovative and co-created competence building. EUR 3.42 Mil, 3yrs. Partners from Norway, Netherlands, Estonia, Luxemburg, Germany and Belgium.

The proudest achievements in 2024:
– Feedback on courses, quote from survey about IMT4116, "It's probably the best course I've had at NTNU."
– Feedback from Keynote for NFCERT in Reykjavik: "Mind-blowing"
– NTNU Malware Forum
This is Norway's most important networking arena for experts in malware analysis and reversing. Everyone who attended shared information about "cutting edge" techniques and advanced malware that affects Norway. The event is a collaboration between the Norwegian Cyber Defence, NTNU CCIS and NSM, and was held for the eighth time this year. This year, there were almost 400 registered and more than 200 chose to follow the malware trail after lunch. A very successful event and an important contribution to the competence enhancement of the Total Defence, which was emphasized in the opening speech by the director of NSM.

4. Digital Forensics Group



Group coordinator:
Researcher Jan William Johnsen

The research group leader is researcher Jan William Johnsen.
The group currently consists of 7 full time and part time members and 11 PhD students.

The group currently consists of 7 full time and part time members and 11 PhD students.

Members of the group
Academic staff:
1. Lasse Øverlier, Associate Professor
2. Arvind Sharma, Associate Professor

Researchers and Postdoctoral Fellows:
1. Kyle Porter, Researcher
2. Jan William Johnsen, Researcher

PhD students:
1. Odin Heitmann, Kripos
2. Raymond Andre Hagen, Digdir
3. Andre Jung Waltoft-Olsen, Statnett
4. An Thi Nguyen, NTNU
5. Michael Ziegler, NTNU
6. Mads Skipanes, Kripos
7. Freddy Murstad, NFCERT
8. Merve Bas Seyyar, University of Groningen

Collaboration and collaboration partners:
Affiliated IIK staff:
1. Stefan Axelsson, Profesor II
2. Andrii Shalaginov, Professor II
3. Slobodan Petrovic, Professor
Externals and guests:
4. Geir Olav Dyrkolbotn, Associate Professor, CyFor
5. Jeffery Hamm, Assistant Professor, DCSO
6. Mariusz Nowostawski, Associate Professor, NTNU IDI
7. Bente Skattør, PhD, Oslo Police District
8. Thomas Walmann, Associate Professor, Økokrim
9. Andre Årnes, Professor, White Label Consultancy
Affiliated members:
10. Inger Marie Sunde, Professor, Politihøgskolen
11. Siv Hilde Houmb, Professor II, NTNU

Main research result:
Overview of ongoing projects (list):
– AI4Citizens research, coordination, and management.
– I4Interviews research, coordination, and management.
– SafeHaven research, coordination, and management.
– Development of the Hardware Reverse Engineering Laboratory through Task 3.7 in NORCICS.
– Norway-India: Strengthening Institutional Partnerships for Advancing Smart City Security and Resilience through AI-driven Digital Forensic

Overview of submitted proposals:
– FAIR – Fast and Accurate Investigation and Response is a proposal sent to NFR. This project uses LLMs to extract and investigate information obtained from investigative interviews. Project partners include Davidhorn, University of Agder's Center for Artificial Intelligence Research and Center for Integrated Emergency Management, IIK NTNU, and the Institute of Population Health at the University of Liverpool.
– FORTICHAIN-Proactive Security by Design for Resilient Software and Hardware Supply Chains submitted to HORIZON-EUROPE.

Some selected publications:
– Raymond Andre Hagen. "Indicators of compromise". EVCSS 2024, Finland.
– Resubmitting "The AI Act and Automatic Speech Recognition for Transcribing Investigative Interviews". Radina Stoykova, Kyle Porter, and Thomas Beka.
– Submiting "Tool Induced Biases: Misleading data presentation as a biasing source in digital forensic
– analysis", Daniel Bing Andersen, Nina Sunde, and Kyle Porter this month to FSI Digital Investigation Special Issue.
– Andre Waltoft-Olsen, Phillip Johnson, Lasse Øverlier, and Geir Olav Dyrkolbotn. "Exploring a Low-Cost Hardware Reverse Engineering Approach: A Use Case Experiment". IFIPSEC 2024 12-14 June 2024.
– Arne Roar Nygård, Arvind Sharma, and Sokratis Katsikas. "Hardware Reverse Engineering for Secure Smart Grids" chapter in the book The Role of Cybersecurity in the Industry 5.0 Era, IntechOpen-2024.
– Stoykova, Radina, Kyle Porter, and Thomas Beka. "The AI Act in a law enforcement context: The case of automatic speech recognition for transcribing investigative interviews." Forensic Science International: Synergy 9 (2024): 100563.

– Accepted paper: Mads Skipanes, Tollef Emil Jørgensen, Kyle Porter, Gianluca Demartini and Sule Yildirim Yayilgan. "Enhancing Criminal Investigation Analysis with Summarization and Memory-based Retrieval-Augmented Generation: A Comprehensive Evaluation of Real Case Data". COLING 2025.
– A. Sharma and S. -F. Wen, "A Quantitative Framework for Assessing and Enhancing Hardware Security Resilience," 2024 IEEE Physical Assurance and Inspection of Electronics (PAINE), Huntsville, AL, USA, 2024, pp. 1–7, doi: 10.1109/PAINE62042.2024.10792846.

Innovation:
Status on ongoing innovation activities:
–Sharma,Arvind; develop an experiment setup to perform a Side-Channel Analysis.

Education:
Activity:
_Teaching and managing courses: i) IMT4114 Introduction to Digital Forensics, ii) IMT4130 Cybercrime Investigation, iii) IMT4133 Data Science for Security and Forensics, iv) IMT4210 Computational Forensics, v) IMT4905 MISEB Master's Thesis, and vi) IMT6091 Computational Forensics.
– The course Hardware Security in Embedded Systems (7.5 ECTS) started in autumn 2024. Developed the first course on hardware security in Norway, collaborating with other departments. The course targets master students from the IIK and IES in Gjøvik and Trondheim.
– Supervision of (at least) 11 Ph.D. students.
– Supervision of (at least) 8 master students.
– Supervision of (at least) 7 bachelor students.

Overview of graduated PhD candidates:
– Rune Nordvik, Politihøgskolen, defended his doctoral thesis "Interpretation of File System Metadata in a Criminal Investigation Context" on 11. June 2024. Supervisors: Stefan Axelsson, Geir Olav Dyrkolbotn and Fergus Thomas Toolan.
– Jens-Petter Skjelvåg Sandvik, defended his doctoral thesis "Forensic triage of digital evidence from the Internet of Things" on 2. September 2024. Supervisors: Professor Katrin Franke and professor André Årnes.

Overview of supervised MSc theses:
– Supervision of (at least) 8 master students. Some topics that were delivered this summer: Supervised topics include i) advancements in audio analysis for security applications, ii) speech recognition under noise, iii) overlay networks, iv) digital forensics of secure messaging, v) disinformation detection using AI, and vi) cybersecurity in embedded systems.

Dissemination activities:
Organized Events, Conferences, and workshops:
– AI4Interviews webinar, focusing on enhancing interrogation efficiency through AI, attracted an online audience of over 200 participants.
– A second AI4Interviews webinar, also centered on AI in interrogation, drew around 160 participants.
– Presentation for the accepted paper Mads Skipanes et al. "Enhancing Criminal Investigation Analysis with Summarization and Memory-based Retrieval-Augmented Generation: A Comprehensive Evaluation of Real Case Data".
– On 24. January, the AI4citizens workshop was held at the University of Agder (UiA).
– On 24. February, the AI4citizens workshop took place online.
– Kyle Porter joined the Advisory Board for Forensic Science International: Digital Investigation and served on the Technical Committee for DFRWS EU 2025.
– Kyle Porter, Zeno Geradts, and Bente Skattør were interviewed by Rise-World about "AI in Forensic Sciences," a book featuring contributions from multiple authors in our group and associates. This notable collaboration was highlighted in the previous year's CCIS report. The interview is published in Polizeiliche Datenverarbeitung.
– On 3. September, Arvind presented Hardware Reverse Engineering Lab research activities at the SFI-NORCICS Workshop organised by Elvia, at Scandic Hotel Hamar.
– On 19.-20. March, Arvind participated in and chaired a session focused on "Imaging & Image Segmentation." Hardware Reverse Engineering Workshop (HARRIS 2024).
– at Ruhr University Bochum (RUB) in collaboration with the Max Planck Institute for Security and Privacy (MPI-SP) in Bochum, Germany.

Organization:
– MISEB (and MIS) study program restructuring process.
– Lasse Øverlier has been granted a one-year sabbatical to study "spontaneous self-configuring overlay networks," commencing this autumn.

Funding (other than NTNU CCIS):
– AI4Interviews. Project number: 331893. Funded by: NRC.
– AI4citizens. Project number: 320783. Funded by: NRC.
– Arvind Sharma seeks funding for a technical assistant in the hardware reverse engineering lab, while Jan William Johnsen seeks funding for a scientific programmer to integrate research methods into Hansken for law enforcement benefits.

The proudest achievements in 2024:
The Digital Forensics Group's proudest achievements include the successful coordination and management of our AI4Interviews, AI4Citizens and SafeHaven projects, the development of a pioneering hardware reverse engineering laboratory, and the significant contribution to education through the introduction of Norway's first course on hardware security. Additionally, the group has overseen the supervision of numerous Ph.D. and master's students, with notable publications in international conferences and workshops, and secured substantial funding for innovative research impacting national and international law enforcement. Lasse Øverlier's one-year sabbatical to study overlay networks marks a significant personal academic advancement within the group.

5. e-Health and Welfare Security

Group coordinator:
Assoc. Professor Bian Yang

Professor Bian Yang is the group leader. The eHWS group currently comprises 18 full and part-time members, 2 researchers and Postdoctoral Fellows and 7 PhD students.

Members of the group Academic staff:
1. Arne Helme
2. Arvind Sharma
3. Aud Obstfelder
4. Bian Yang
5. Egil Utheim
6. Einar Snekkenes
7. Hao Wang
8. Inge Moen
9. Jacky Mallet
10. Jia-Chun Lin
11. Johan Gustav Bellika
12. Kassaye Yigsaw
13. Katina Kralevska
14. Katrien De Moor
15. Sandeep Pirbhulal
16. Sigurd Eskeland
17. Stephen Wolthusen
18. Svetlana Boudko

Researchers and Postdoctoral Fellows:
1. Ahmad Hassanpour
2. Sona Alex
3. Ahmed Baig

PhD students:
1. Aafan Ahmad Toor
2. Alvhild Skjelvik
3. Arnstein Vestad
4. Luyi Sun
5. Pankaj Khatiwada

Collaboration and collaboration partners:
- Norsk Helsenett
- Norwegian Center for E-health Research
- Sykehuset Innlandet
- Utviklingssenter for sykehjem og hjemmetjenester
- Norsk Regnesentral
- SINTEF
- University of Oslo
- University of Stavanger
- Helse Sør Øst
- HelseINN
- Biofy AS
- Cognuse Inc
- University of Genoa
- Chinese Academy of Science
- Universitas Brawijaya

Main research result:
Overview of ongoing projects (list):
– Horizon Europe DN Towards an Understanding of Artificial Intelligence via a transparent, open, and explainable perspective (TUAI)
– RCN-SFI-NORCICS T4.3 Secure Distributed Care Services
– H2020-ITN PriMa (privacy model and preserving methods)
– RCN-IKTPLUSS Health Democratization (health data sharing mechanism)
– RFF IoMT (welfare technology for homecare)
– RCN-IKTPLUSS DigiRemote (welfare technology for homecare)
– RCN-FORNY IncluDe (Leveraging Cryptographic Multi-Factor Authentication Solutions for Inclusive eID and Access Management Services)
– NTNU-TSO JOIN (Joining perspectives and forces at NTNU Gjøvik for research excellence in value-based healthcare services)

Overview of submitted proposals:
– NTNU-TSO JOIN (Joining perspectives and forces at NTNU Gjøvik for research excellence in value-based healthcare services)
– THCS Advancing GEriatric Medication SAFEty: Optimising Prevention of Adverse Events
– Estonian Programme for applied research: CoNurse Patient Safety Model

Some selected publications:
– Baig, A.F.; Eskeland, S.; Yang, B. Novel and Efficient Privacy-Preserving Continuous Authentication. Cryptography 2024, 8, 3.
– Ahmad Hassanpour, Fatemeh Jamalbafrani, Bian Yang, Kiran Bylappa Raja, Raymond Nicolaas Johan Veldhuis, Julian Fierrez. E2F-Net: Eyes-to-face inpainting via StyleGAN latent space. Pattern Recognition. Volume 152, August 2024, 110442
– Sun L, Yang B, Kindt E, Chu J. Privacy Barriers in Health Monitoring: Scoping Review. JMIR Nursing 2024;7:e53592
– Khatiwada, P.; Yang, B.; Lin, J.-C.; Blobel, B. Patient-Generated Health Data (PGHD): Understanding, Requirements, Challenges, and Existing Techniques for Data Security and Privacy. J. Pers. Med. 2024, 14, 282.
– Aafan Ahmad Toor, Jia-Chun Lin, Ernst Gunnar Gran ang Ming-Chang Lee, "UoCAD: An Unsupervised Online Contextual Anomaly Detection Approach for Multivariate Time Series from Smart Homes", accepted by the 9th International Conference on Internet of Things, Big Data and Security (IoTBDS 2024)
– Vestad, A., Yang, B. (2024). Adoption of Cybersecurity Innovations—A Systematic Literature Review. In: Onwubiko, C., et al. Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media. CYBER SCIENCE 2023. Springer Proceedings in Complexity. Springer, Singapore.

Innovation:
Status on ongoing innovation activities:
– NTNU-IIK-CII innovation: A Clinical Communication Network (2023–2024)
– NTNU-TTO: Privacy-preserving remote diagnosis protocols
– NTNU-IIK-CII innovation: Edge Camera System for Privacy-Preserving Patient Care (2024–2025)

Education:
Activity:
– PhD course on human factor methods for information security research fall 2024

Overview of graduated PhD candidates:
– Ahmad Hassanpour
– Luyi Sun
– Alvhild Skjelvik

Overview of supervised MSc theses:
– Helene Fagkom Bjørnsen and Eva Vartdal Kvalø: Security, privacy, and usability analysis of HelseID

Dissemination activities:
Organized Events, Conferences, and workshops:
– EHiN 2024
– IoTBDS 2024
– CWEURP 2024 (IoTBDS Workshop)
– April 26th, 2024 Health Democratization project Demo workshop

Funding (other than NTNU CCIS):
– Horizon Europe DN Towards an Understanding of Artificial Intelligence via a transparent, open, and explainable perspective (TUAI)
– RCN-FORNY IncluDe (Leveraging Cryptographic Multi-Factor Authentication Solutions for Inclusive eID and Access Management Services)
– NTNU-TSO JOIN (Joining perspectives and forces at NTNU Gjøvik for research excellence in value-based healthcare services)

6. Information Security and Privacy Management

Group coordinator:
Assoc. Professor
Erjon Zoto

Associated Professor Erjon Zoto is the group leader. The group currently comprises 6 full and part-time members and 4 PhD students.

Members of the group
Academic staff:
1. Erjon Zoto
2. Stewart Kowalski
3. Aristidis Kaloudis
4. Grethe Østby
5. Gaute Wangen
6. Bernhard Markus Hämmerli
7. Laura Georg

Associate Members:
Richard Mcevoy
Einar Arthur Snekkenes
Marie Haugli-Sandvik
Halvor Holtskog (IØT)
Eirik Bådsvik Hamre Korsen (IØT)

PhD students:
1. Øyvind Anders Arntzen Toftegaard
2. Daria Kovalevskaya
3. Tone Vold
4. Benjamin Vigdel

Associated PhDs:
5. Raymond Hagen
6. Sarang Shaikh
7. Guro Bråten Olsborg

Collaboration and collaboration partners:
- Digitaliseringdirektoratet (Digdir)
- Innlandet Hospital Trust
- Southern and Eastern Norway Regional Health
- Direktoratet for Samfunnsikkerhet og Beredskap
- Norwegian Digitalisation Agency
- Norwegian Cybersecurity Cluster (Cyberklynga)
- NSM (National Security Authority)
- NKOM
- Datatilsynet
- Politiet
- Økokrim
- Norges bank
- Nordic Finance CERT
- Deloitte AS
- KPMG
- Østre Toten municipality
- Gjøvik municipality
- Lier municipality
- Megagame Oslo
- Lund University, Sweden
- Linnaeus University, Sweden
- RISE Sweden
- George Washington University
- The Karlstad University
- The Copenhagen University
- Hochschule Luzern (HSLU), Switzerland
- University of Tirana (UT), Albania
- Birmingham City University (BCU), United Kingdom

Potential partners:
- *PwC*
- *NVE*
- *NCCC*
- *KRIPOS*
- *Styrmand*

Main research result:
Ongoing projects
EU-funded
– Interreg-project CBCC (2023–2026) – project in collaboration with Digital Innlandet, COMPACT (SE) and University of Karlstad (SE)
– BRUA (2024-2027) - Kick off meeting 29th May. Collaboration with the ECCC, NSM and Research Council of Norway.
– Erasmus Global Mobility Project (2024-2027) – An exchange project in collaboration with the University of Tirana, including staff & students mobility
– CRESCENDO (2024-2028) – Kick-off meeting November 4th

National projects
– CyberSecurity Cluster (Cyberklynget) – Collaboration with Digital Innlandet, where 2 members of the group are representing IIK in the ongoing activities

Finished projects
– METICOS (2020–2023) – A platform for Monitoring and Prediction of Social Impact and Acceptability of Modern Border Control Technology

Overview of submitted proposals:
– AVIT
Members of the research group were actively involved in submitting a proposal on "Hybrid Cyber Range decision

making research infrastructure, (HCRDM)". The proposal involved other colleagues from different research groups at IIK, even from other Faculties at NTNU

– BIFROST

A Digital Europe Programme proposal, a continuation of BRUA for strengthening and targeting activities at the NCC-NO with the contributions of the NTNU (work package leader).

– Samfunnsikkerhet (TSO)

Members of the research group have been involved from the start with the activities of the TSO, led from Nils Kalstad. The group has been part of the discussions around creating a working group for "Liberal resilience narratives", which included submitting a proposal for its establishment and potential future funded activities

– Proposal for center on AI & Security

The group members have been involved with the proposal for a new research center focusing on AI & Security, as part of the NFR Initiative, where we are collaborating with other research groups at IIK, and further with Simula & Sintef.

Submitted January 15th 2025.

– NORDFORSK Call for pre-proposals: Sustainable Development of the Arctic

Members from the research group have contributed to a draft document shared, as part of the activities related to the NORDFORSK Call in question. The Call invites for collaboration with other entities from Nordic countries, as well as Canada and USA.

Some selected publications:

– Smart-Grid-Enabled Business Cases and the Consequences of Cyber Attacks

Øyvind Anders Arntzen Toftegaard, Doney Abraham, Sujeet Shenoi, Bernhard Markus Hämmerli

IFIP Advances in Information and Communication Technology

– Consequence Verification During Risk Assessments of Smart Grids

Doney Abraham, Øyvind Anders Arntzen Toftegaard, Alemayehu Gebremedhin, Sule Yayilgan

IFIP Advances in Information and Communication Technology

– Addressing Agents' Strategies in a Cyberwar Game – CyberAIMs 2.0

Erjon Zoto, Stewart Kowalski

International Conference on Economy, Business, Innovation and Technology

– Iran's Cyberattack on Albania: A Socio-Technical Root Cause Analysis

Fatjon Thomai, Stewart Kowalski, Erjon Zoto

International Conference on Economy, Business, Innovation and Technology

Innovation:

Status on ongoing innovation activities:

– CyberAIMs

The tool now includes a mapping of the NIST CSF strategies for the defense side, and the Unified Kill Chain approach for the attack side. An optimal allocation can be defined from the user/player given the different combinations and final outcome

– Megagames

The game now can be migrated to a digital environment, built to host the different files needed to progress in each round, as well as additional modules specific for each user group/team involved.

– Security card games

A card game is being promoted with students in Norway and beyond, aiming to improve its design and game mechanics further, with the main goal of increasing the target groups' (players) awareness around security issues related to the use of AI models and tools

– Rector's office, NTNU

Aristidis has been in close cooperation with the Rector's office and Head of Innovation, while participating in internal projects and leading others within the area of innovation policies and practices

– Nemonoor

The group has participated in several activities that support main objectives of Nemonoor, as related to NTNU participation towards helping the local industry increase their awareness and preparation around cyber incidents

Education:

Activity:

Study programs:

- Digital infrastruktur og cybersikkerhet (bachelor)
- Bachelor i programmering (Bachelor)
- Industriell innovasjon og digital sikkerhet (master)
- Information Security (full-time master)
- Information Security (Experience based master)
- PhD Information Security (PhD Program)

Main courses:

- DCSG1002 – Cyber security and teamwork
- IIKG1001 – Cyber security and computer networks
- IMT4115 – Introduction to Information Security Management
- IMT4128 – Socio-technical Systems Enabled Crime
- IIK5000 – Digital Law and Business
- IDS4000 – Research methods
- IØ8303 – Forecasting models in Economics and Finance
- IMT4127 – Information Security Metrics
- DCSG2005 – Risk Management
- TS501822 – Maritime Cyber Security

Management:

- Study program responsible, MISEB – Erjon Zoto

Overview of graduated PhD candidates:

– Øyvind Anders Arntzen Toftegaard

Thesis: "Regulatory Strategies for a Resilient Smart Grid: Cybersecurity Compliance in the Electric Energy Sector».

PhD defense: October 10th 2024

– Daria Kovalevskaya

Thesis: "Exploring Business Triads in the Context of Lean Management". PhD defence: December 18th 2024.

Overview of supervised MSc theses:

Selected theses:

– Measuring the effectiveness of the gamification of security awareness training

Farhaz Hamid Ismail (MIS)

– Cyber risk management for modern SMEs

Simen Ramberg (MIS)

– Measuring Risk Appetite Statement and Gamification

Trym Richardson Oterholm (MISD)

– Cyber Threat Intelligence Distributions using Games

Morten Lyngås (MISD)

– Use of cyber intelligence reports in the banking sector

Bilal Letsjievitsj Israilov (MIIDS)

– Academic Digital Entrepreneurship in NTNU.

Marte Lien Johnsen (MTKOM)

–NIS2 and the generation of actionable intelligence – a socio-technical analysis of Norway

Kjæraas, Morten L. (MISEB)

Dissemination activities:

Organized Events, Conferences, and workshops:

– Workshop

Title: C.S. Technopoly Megagame – LOGIN

Authors/Hosts: Stewart Kowalski, Erjon Zoto

Partners: LOGIN student organization

Venue: Topas-bygget, NTNU Gjøvik, April 2024

– Tutorial

Title: Interactive Strategies: Employing Serious Games for Secure and Sustainable Socio-technical Cybersecurity Systems Design

Authors/Hosts: Stewart Kowalski, Aristidis Kaloudis, Erjon Zoto

Venue: AHFE 2024 (International Conference on Applied Human Factors and Ergonomics), Nice, France, July 2024

– Conference

Attendees: Stewart Kowalski, Aristidis Kaloudis

Venue: International Conference on Socio-Technical Perspectives in Information Systems (STPIS 2024), Jöngköping, Sweden, August 2024

– Workshop

Title: Strategic Engagement with Cybersecurity Games : A Mini-workshop

Authors/Hosts: Stewart Kowalski, Aristidis Kaloudis, Erjon Zoto

Partners: ISF Norge, Nemonoor

Venue: Sikkerhetsfestivalen, Lillehammer, August 2024

– Workshop

Title: Cybersecurity Megagame

Authors/Hosts: Stewart Kowalski

Partners: CEER (Council of European Energy Regulators)

Venue: CEER Secretariat, Brussels, Belgium, September 2024

– Workshop

Title: Cyberøvelse (Industridagene)

Authors/Hosts: Stewart Kowalski, Erjon Zoto. Aristidis Kaloudis, Espen Torseth

Partners: Norwegian Cyber Range, Krudtverket

Venue: NCR, NTNU Gjøvik, October 2024

– Workshop

Title: Elevation of MLSec

Authors/Hosts: Elias Brattli Sørensen, Erjon Zoto

Partners: Kantega

Venue: Helvin-bygget, NTNU Gjøvik, November 2024

– Conference

Chair: Stewart Kowalski

Venue: International Conference on Economy, Business, Innovation and Technology (ICEBIT 2024), December 2024

– Workshop

Title: Cybersecurity Investment game

Authors/Hosts: Erjon Zoto

Venue: University of Tirana, December 2024

– Workshop

Title: Elevation of MLSec

Authors/Hosts: Elias Brattli Sørensen, Erjon Zoto

Partners: Kantega

Venue: University of Tirana, December 2024

Lifelong learning activities:

– TS501822 – Maritime Cyber Security

– IIKG6503 – Introduction to Information Security Management

Organization

– European Cybersecurity Organization (ECSO)

Stewart Kowalski is recently elected as Chair of the Education workstream

– RISE Sweden, Working Group on Education & Cyber Ranges

Stewart Kowalski is leading the working group at RISE

– Teknologirådet

Aristidis has been appointed as a member of the Norwegian Technology Assessment Office

Funding (other than NTNU CCIS):

– CBCC

– BRUA

– CRESCENDO

– Samfunnssikkerhet

7. Norwegian Biometrics Laboratory (NBL):

Group coordinator:
Professor
Raghavendra Ramachandra

Professor Raghavendra Ramachandra is the group leader at the NBL research group.

Members of the group
Academic staff:
Permanent group members:
1. Christoph Busch

Affiliated Members:
2. Bian Yang
3. Marta Gomez-Barrero
4. Patrick Schuch

Researchers and Postdoctoral Fellows:
Guoqiang Li

PhD students:
5. Bhanu Shrestha
6. Frøy Løvåsdal
7. Hailin Li
8. Haoyu Zhang
9. Marcel Grimmer
10. Raghavendra Mudgal-Gundurao
11. Tabita Lumban Tobing
12. Wassim Kabbani

Collaboration and collaboration partners:
13. AIBA AS
14. Politiet
15. BSI
16. BKA
17. eu-LISA
18. ISO/IEC
19. University of Twente
20. Hochschule Darmstadt
21. Universität der Bundeswehr

Main research result:
– iMARS
– EINSTEIN
– PopEye
– IAMI
Overview of submitted proposals:
– nAIss
– CIRCULATE

Some selected publications:
– I. Joshi, M. Grimmer, C. Rathgeb, C. Busch, F. Bremond, A. Dantcheva: "Synthetic Data in Human Analysis: A Survey", in IEEE Transactions on Transactions on Pattern Analysis and Machine Intelligence (PAMI), (2024)
– M. Ibsen, R. Nichols, C. Rathgeb, D. Robertson, J. Davis, F. Løvåsdal, K. Raja, R. Jenkins, C. Busch: "Conditional Face Image Manipulation Detection: Combining Algorithm and Human Examiner Decisions", in Proceedings of 12th Workshop on Information Hiding and Multimedia Security (ACM IH&MMSEC 2024), Balona, ES, June 24-25, (2024)
– P. Chandaliya, K. Raja, R. Raghavendra, Z. Akhtar, C. Busch: "Towards Inclusive Face Recognition Through Synthetic Ethnicity Alteration", in Proceedings of 1th International Workshop on Synthetic Data for Face and Gesture Analysis (SDFGA 2024), Istanbul, TK, May 27-31, (2024)
– T. Arican, R. Veldhuis, L. Spreeuwers, L. Bergeron, C. Busch. E. Jalilan, C. Kauba, S. Kirchgasser, S. Marcel, B. Prommegger, K. Raja, R. Raghavendra, A. Uhl: "A Comparative Study of Cross-Device Finger Vein Recognition using Classical and Deep Learning Approaches", in IET Biometrics, (2024)
– M. Grimmer, R. Veldhuis, C. Busch: "Efficient Expression Neutrality Estimation with Application to Face Recognition Utility Prediction", in Proceedings of 12th International Workshop on Biometrics and Forensics (IWBF 2024), Enschede, NL, April 11-12, (2024)

Innovation:
Status on ongoing innovation activities:
– AIBA AS (Author Input Behavioural Analysis): growing to 10 staff member, signing contract with Police, signing first paying customer.

Overview of graduated PhD candidates:
22. Jag Mohan Singh (May 2024): "Robust Algorithms for 2D and 3D Face Morphing Attacks"

Overview of supervised MSc theses:
– Katrine Bay and Gabriella Kierulff "Enhancing Face Recognition Models with Synthetic Child Data"; June 2024
– Iris Björk "Age manipulation with Latent Diffusion Models", March 2024
– Yujing Gu, "LandmarkAgnostic Face Image Quality Assessment", January 2024
– Teakosheen Joulak "LandmarkAgnostic Face Image Quality Assessment", January 2024

Dissemination activities:
Organized Events, Conferences, and workshops:
– NBLAW in March 2024
https://eab.org/events/program/331
– EAB workshop on standards 2024
https://eab.org/events/program/345

8. System Security

Group coordinator:
Professor Christian Johansen

Professor Christian Johansen is the group Leader at the S2G research group.

The group currently consists of 3 full-time and part-time members, 3 researchers and Postdoctoral Fellows and 2 PhD students.

Members of the group
Academic staff:
1. Christian Johansen
2. Basel Katt
3. Muhammad Mudassar Yamin (new Associate Professor)

Researchers and Postdoctoral Fellows:
4. Shao-Fang Wen (new Post-doc)
5. Eigil Obrestad
6. Hanno Langweg
7. Gabriel Andy Szalkowski
8. Safa Zouari

Collaboration and collaboration partners:
1. Maintained most of previous collaborations with, e.g.: Luxembourg (space security), Strathclyde (security modelling), Estonia (cyber security training), Etterretningstjenesten (human in security), Chalmers (system security), etc.
2. Multiple collaborations with industry through the NCR activities and through CCIS
3. Regional collaborations, e.g. new Interreg project on Cross Border Cyber Capacity

Main research result:
– Open Cyber Range (financed by EEA)
– ASCERT AI-Based Scenario Management for Cyber Range Training (financed by NFR)
– DREAM ("norDic-baltic cybeR summEr cAMp", Joint training of ESTONIA, Norway and Denmark cyber security national teams)
CyberUnity project (Integrating Cyber security training facilities across Europe)

Overview of submitted proposals:
– Multiple applications were made by different group members.

Some selected publications:
– The group has published multiple journal articles, besides contributions to conferences and workshops. Most prestigious are:
– Article in Elsevier's Science of Computer Programming, a top journal of level 2 up to last year, titled: "XACML2mCRL2: Automatic transformation of XACML policies into mCRL2 specifications" in collaboration with Oslo, UK, and Netherlands (https://doi.org/10.1016/j.scico.2023.103046)
– Article in Elsevier's journal Expert Systems with Applications titled: "All flags are not created equal: A deep look into CTF Scoring Algorithms" with results from our work in the NCR (https://doi.org/10.1016/j.eswa.2024.124436)

Innovation:
– Continuing work on establishing a startups on security assurance one on security management in DevSecOps

Education:
Activity:
– The S2G Playground CTF ethical hacking bi-weekly events for students has expanded outside the campus Gjøvik to Trondheim. The number of participants in the autumn semester has exploded, from ca.50 to ca. 200–250, courses using this and now other institutions asking to be allowed in.
– Teaching many courses at all levels, for example on Software Security; Systems Security; Cyber security and computer networks; Operating systems; or Information Security Management.

Overview of supervised MSc theses:
– A considerable number of MSc students (ca. 5+ finished and many ongoing) on a varied range of topics, such as Cyber range Federation, Cyber crisis management, Artificial Intelligence used for cyber security exercises generation.

Organization:
– One major aspect this first half of year is that Basel Katt has applied to become full time Head of Department.
– Another is plans to merge S2G with the eHealth group of Bian.

NTNU CCIS sine 81 partnere pr. 1.3.2025

Layout/trykk: NTNU Grafisk senter