ÅRSRAPPORT
2022

NTNU

CCIS – Center for Cyber
and Information Security

Innholdsfortegnelse

Førsteamanuensis Nils Kalstad er Instituttleder for Institutt for informasjonssikkerhet og kommunikasjons-teknologi og samtidig direktør for Center for Cyber and Information Security, CCIS.

1 Innledning

NTNUs Center for Cyber and Information Security (NTNU CCIS) er et nasjonalt senter for arbeids- og tidsrelevant forskning og utdanning, og kompetanse-bygging innen cyber- og informasjonssikkerhet.

Senteret skal bidra til å styrke samfunnets, virksom-hetenes 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. Kunnskaps-utviklingen 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. Senteret har etablert seg som et av de største akademiske forsknings- og utviklingsmiljøene innen cyber- og informasjons-sikkerhet i Europa mye takket være vår unike partner-profil og sterke partnersamarbeid.

Formelt er senteret, som ble etablert i 2014, et langsiktig prosjekt som eies av Institutt for informasjonssikkerhet og kommunukasjonsteknologi ved NTNU. Senteret har 2/3 av sine ansatte ved Gjøvik og 1/3 av sine ansatte i Trondheim.

Fra Justis- og beredskapsminister Emilie Enger Mehls gjenåpning av Norwegian Cyber Range (NCR).

2 Årsrapport

2.1. Styrets arbeid og generalforsamling

Styret i NTNU CCIS består etter generalforsamlingen 2022 (valgperiode i parentes) av:

- Norges teknisk-naturvitenskapelige universitet (NTNU), styreleder ved Ingrid Schjølberg (2021–2023)
- Nasjonal sikkerhetsmyndighet (NSM), nestleder ved Bente Hoff (2021–2023)
- Cyberforsvaret, ved Roger Samuelsen (2021–2023)
- mnemonic AS, ved Tønnes Ingebrigtsen (2022–2024)
- Telenor, ved Rolv Hauge (2021–2023)
- Politidirektoratet, ved Olav Skard (2021–2023)
- Politihøgskolen, ved Inger Marie Sunde (2022–2024)
- Statnett, ved Anders Granum (2022–2024)
- NTNU CCIS ansattrepresentant Staal Vinterbo (2022–2024)

Styret har i 2021 revidert NTNU CCIS' strategi for 2021–2026, og hovedelementer fra strategien gjengis under.

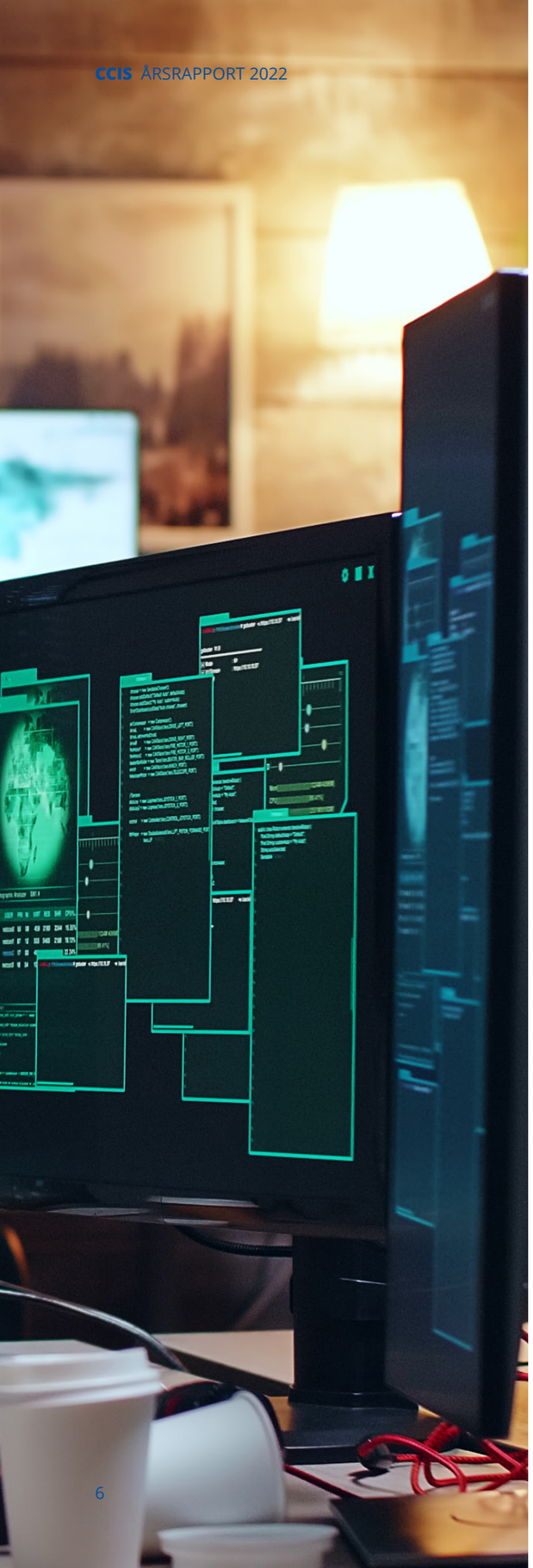
VISJON
NTNU CCIS – en nasjonal kunnskapsressurs for digital sikkerhet

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 internasjonal 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.



2.2. Organisasjon og ledelse

NTNU CCIS med sine 130 vitenskapelige ansatte har Institutt for informasjonssikkerhet og kommunikasjonssikkerhet (IIK) ved Fakultet for informasjonsteknologi og elektroteknikk (IE) som sitt vertsinstitutt i Norges teknisk-naturvitenskapelige universitet (NTNU). I 2022 har Nils Kalstad, instituttleder for IIK, vært direktør for NTNU CCIS. Senteret har ukentlige møter for koordinatorene i tematisk gruppene. 2 saksbehandlere har i 2022 administrativt understøttet aktiviteten i NTNU CCIS, i tillegg til at senteret har bred annen administrativ støtte fra vertsinstitutt og -fakultet.

NTNU CCIS sin aktivitet har i 2022 vært gruppert i følgende 8 tematisk grupper:

- Applied Cryptography
- Critical Infrastructure and Resilience
- Cyber Defence
- E-Health and Welfare Security
- Information Security and Privacy Management
- Biometrics
- Digital Forensics
- System security

Våren 2022 satte Cyberforsvaret i gang prosesser for etablering av en 9. gruppe. Denne har arbeidstittel «organisatorisk kompleksitet, ledelse og cybersikkerhet». Prosessen her er underveis.

NTNU CCIS er fortsatt Nordens største akademiske forsknings og utviklingssenter på fagfeltet.

2.3. Forskning

NTNU CCIS samarbeider med partnerne for å legge til rette for god forskning. Dette er et langsiktig og systematisk arbeid med interne og eksterne grenseflater som spenner fra innspill til forskningsstrategier og -programmer via kapasitets- og konsortiebygging, til søknadsskriving og prosjektgjennomføring. Den løpende kontakten mellom private virksomheter, offentlig virksomhet og forsknings- og utdanningsinstitusjoner gir senteret et bilde av samfunnsmessige utfordringer knyttet til cyber- og informasjonssikkerhet. Dette bruker vi til å gi innspill til tidsrelevante forskningsstrategier og forskningsprogrammer, både nasjonalt og internasjonalt. Norges forskningsråd (NFR), Justis- og beredskapsdepartementet (JD), Helse- og omsorgsdepartementet (HOD), NordForsk (Nordisk ministerråd), Europakommisjonen og National Institute of Technologies and Standards (NIST), er eksempler på organer som er av særlig relevans for NTNU CCIS, våre partnere og våre nettverk. Dette gjøres i form av senterets samarbeide med NTNU om myndighetskontakt gjennom en rekke møter med statsråder, statssekretærer, departementer, andre forvaltningsenheter, og politiske partier. I en annen dimensjon gjøres dette gjennom for eksempel deltagelse i Justisdepartementets forum for digital sikkerhet, Nasjonalt cybersikkerhetssenter (NSM NCSC) sin referansegruppe, Digital Enlightenment Forum, European Cyber Security Organization, North European Cyber Security Cluster og Norges forskningsråds referansegruppe for H2020 Secure Societies. I en tredje dimensjon gjøres dette gjennom ekspertdeltagelse i internasjonale organisasjoner som EUROPOL, INTERPOL, ENISA og NATO, som i tur gir sine innspill til samfunnsutfordringene.

NTNU CCIS har i 2022 hatt svært gode resultater i konkurransebasert forskningsfinansiering med ett nytt EU prosjekter, to NFR- prosjekter, ett RFF-prosjekt, ett oppdragsprosjekt og ett EØS-prosjekt. NTNU CCIS jobber for ytterligere å bedre de vitenskapelige ansattes mulighet til å bli en del av konkurransedyktige søkergrupper, til å ha kapasitet til å skrive gode søknader og til å bidra med ressurser til å kvalitetssikre søknader.

SFI Norwegian Center for Cybersecurity in Critical Sectors (SFI NORCICS) ble etablert i 2021, med finansiering fra NFR. For oversikt over alle publikasjoner til personell med tilknytning til CCIS henviser vi til databasen CRIStin (www.cristin.no).

The Cyber Defence Research Group has been very active through 2022 supporting the NATO Science & Technology Organization to develop understanding and a research pathway (human, technological, societal) concerning Defence & Security against the threat of Cognitive Warfare.

2.4. Utdanning

NTNU CCIS har i tillegg til vertsinstitusjonen NTNU flere utdanningsinstitusjoner i partnerskapet. Cyberingeniørskolen ved Forsvaret høgskole, 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, Forsvarets høgskole 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. Det ble også gjennomført et 15 studiepoengs program «Digital sikkerhet for ledere» i samarbeid mellom BI og NTNU.

I 2022 er det levert 24 bacheloroppgaver på IIK. Det er også levert 40 masteroppgaver ved IIK Gjøvik og 45 masteroppgaver ved IIK Trondheim. Eksempler på titler på noen av disse Masteroppgavene er:

- Effects of Organizational Cyber Security Culture across the Energy Sector Supply Chain
- Cyber Security in the Cellular IoT
- Intelligence of cybercrime prevention
- Cyber security alerts in remote operation centers

2.5. En synlig samfunnsaktør

NTNU CCIS skal være en synlig samfunnsaktør. Dette har vært ved å organisere og være til stede på en rekke møteplasser nasjonalt og internasjonalt. I 2022 har vi kommet godt i gang igjen med fysiske møter etter Covid-19 og i samarbeid med gode partnere er vi i gang igjen med mye aktivitet.

2.6. 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 innenfor 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. NTNU CCIS leverte innholdet og plattformen for 2022-utgaven av konkurransen.

2.7. Videreutdanning i digitalisering for prosessindustrien

Sammen med Eramet, Hydro, Elkem, Jotun, Boliden, Universitetet i Sør-Øst-Norge, Universitetet i Agder og SINTEF bidro NTNU CCIS til etablering av et videreutdanningstilbud i digitalisering for prosessindustrien i Herøya industripark. Prosjektet støttes av Kompetanse Norge og NTNU CCIS bidrar med utdanning i digital sikkerhet for IT/OT systemer.

2.8. EUROCRYPT 2022

NTNU Applied Cryptography Laboratory arrangerte EUROCRYPT 2022, i perioden 30. mai til 3. juni, med professor Colin Boyd som leder av arrangementskomiteen.

Eurocrypt er en av de tre store akademiske møteplassene for kryptologi i verden sammen med Crypto og Asiacrypt. Over seks hundre deltok i Trondheim for presentasjoner, diskusjoner og sosialt samvær. Konferansen ble åpnet av statssekretær i Justis- og beredskapsdepartementet Erik Sandsmark Idsøe.

The Applied Cryptography Group hosted the Eurocrypt conference in May/June 2022 in Trondheim: (https://eurocrypt.iacr.org/2022/program.php).

This is the premier academic cryptography conference in Europe and takes place in a different country every year.

There were 433 physical attendees and an additional 200 online, with 50 countries represented.

2.9. Partnerkonferanser

NTNU CCIS gjennomførte 1.juni årets første Partnerkonferanse, med ca. 100 deltagere til stede på NTNU Gjøvik. En stor del av partnerkonferansen ble gjennomført som en øvelse for å vise partnerne litt av hva forskningen har resultert i ved Norwegian Cyber Rang (NCR). Representanter fra våre faggrupper deltok sammen med partnerne i grupper under øvelsen. Øvelsen ble gjennomført som en policy-øvelse, hvor hensikten var å diskutere hvordan nasjonale reguleringer kan påvirke policyer innenfor informasjonssikkerhet.

Årets andre Partnerkonferanse ble gjennomført den 23. november på Strand Hotel på Gjøvik. Dette var en felles konferanse med NORCICS, NTNU CCIS sin SFI. Her deltok ca. 130 deltagere. Konferansen samlet eksperter fra industri, akademia, regulatoriske og standardiseringsorganer, til et bredt forum for diskusjoner og nettverk.

Konferanseprogrammet inkluderte utvalgte hovedinnlegg fra ulike sektorer, panelsesjoner og muligheter for åpne diskusjoner. Dagen ga verdifull innsikt i trussel-landskapet i utvikling, samt beste praksis og erfaringer fra feltet.

2.10. Norwegian and European Cyber Security Challenge

Justis- og beredskapsdepartementet ba NTNU CCIS forberede norsk deltakelse i ECSC 2022 i Wien, Østerrike med eget lag. Dette ble gjennomført i uke 37, der det norske laget endte på en 18. plass blant ca. 30 deltagerland. Rekrutteringen av disse skjer gjennom Norwegian Cyber Security Challenge (NCSC), som har som målsetning å finne unge talenter (i aldersgruppen 16–25 år) innen cybersikkerhet og motivere disse til å utvikle seg videre. På forhånd ble det i NCSC arrangert en kvalifiseringsrunde.

ECSC's styringsgruppe som er koordinert av ENISA (EU's cybersikkerhetsorgan) har tildelt NTNU CCIS ansvaret for planlegging og gjennomføringen av ESCS 2023 i Norge.

Vi har valgt Vikingskipet på Hamar som arena for dette og har startet planleggingen sammen med dem og en rekke lokale, regionale og nasjonale aktører.

For mer informasjon se https://www.ntnu.no/ncsc og 2023 – European Cyber Security Challenge (ECSC) – NTNU

2.11. 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 selvstendig prosjekt med finansiering fra Norges Forskningsråd. Prosjektet er basert på partnerskapet i NTNU CCIS og det finnes betydelig samarbeid og synergier mellom sentrene. SFI NORCICS har pågående forskningsprosjekter både ekstern (HORIZON Europe, NFR, Kompetanse Norge) og internt (NTNU IE fakultet) -finansierte FoU-prosjekter. Det pågår forskningssamarbeid med internasjonale og nasjonale samarbeidspartnere (akademisk, forskning, industri) og etablering av nye forskningsallianser (f.eks. TalTech i Estland og Aalto universitetet i Finland).

The Critical Infrastructure and Resilience Group has in 2022 a project SDN-µSENSE (SDN – microgrid reSilient Electrical eNergy SystEm).

This is aiming at providing and demonstrating a secure, resilient to cyber-attacks, privacy-enabled, and protected against data breaches solution for decentralised Electrical Power and Energy Systems (EPES).

The SDN-µSENSE has now *finished and the final technical review report from the EU states that "the project has fully achieved its objectives and milestones for the period; it has delivered exceptional results with significant immediate or potential impact; and overall the project has delivered and demonstrated excellent results".*

2.12. 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 Cybersec. Cluster) -konferanser. I tillegg til deltagelse i Arendalsuka med eget program, cybersikkerhetskonferansen Security Talks i Arendal, ISF' s Sikkerhetsfestival og Totalforsvarets cybersikkerhetskonferanse på Lillehammer.

Vi har også deltatt i planlegging av en rekke andre møter og konferanser om Cybersikkerhet.

Fire kurs à 2,5 studiepoeng i innføring av digital sikkerhet, ble gjennomført som bransjeprogram for olje- og gassleverandørindustrien. Første runde med gjennomføring, hadde støtte fra Kompetanse Norge.

2.13. Cyber Clever og CyberSmart

Cyber Clever (https://cyberclever.eu/) er et 2-årig-prosjekt med fokus på tilrettelegging for yrkesfag, finansiert av EU sitt Erasmus+ program. Dette bygger på en pilot innen cyber sikkerhet, grunnlagt av norske strategiske partnere, Den amerikanske ambassaden og Godalen videregående skole, Stavanger i 2018. Prosjektet ble startet i 2020. Prosjektets målsetting er å utvikle, gjennomføre og evaluere en opplæringspakke for lærere, for å øke bevissthet og kompetanse omkring cybersikkerhet.

I tillegg har det vært arbeidet med å få i gang CyberSmart. Målsettingen her har vært å få i gang opplæring av lærere og elever i grunn- og videregående skoler, med økt bevissthet og kompetanse innen cybersikkerhet/ digital sikkerhet. Vi har i 2022 ikke lyktes å få rikspolitisk støtte til ideen, men vi har ikke gitt opp.

2.14. Nærings-PhD og offentlig PhD

NTNU CCIS har markedsført ordningen med nærings-PhD og offentlig-PhD for gamle og nye partnere. I 2022 har vi hatt flere ti-talls studenter på disse ordningene.

The Biometrics Group received a Top Rank Position in NIST Face Morphing Detect Competition:

https://pages.nist.gov/frvt/reports/morph/frvt_morph_report.pdf

2.15. Norwegian Cyber Range

Norwegian Cyber Range (NCR) er et tiltak som er nevnt eksplisitt i Nasjonal strategi for digital sikkerhet og som NTNU har ansvar for iverksettelsen av. IKT komponenten i NCR har vært i god utvikling siden 2017, og i 2020 har vi gjort et betydelig løft på den bygningsmessige delen av NCR. Disse ble ferdigstilt i 2020. På grunn av covid-pandemi har åpningen av lokalene vært utsatt, men i august 2022 ble gjenåpning foretatt av Justis- og beredskapsminister Emilie Enger Mehl i moderne, sterkt utvidede og funksjonelle lokaler. Disse lokalene byr på god mulighet for trening og øving av personell med fokus på både tekniske og organisatoriske ferdigheter. Flere virksomheter benyttet seg av muligheten til å holde øvelse i lokalene utover høsten 2022.

2.16. Totalforsvarets cybersikkerhetskonferanse

Cybersikkerhetsuka på Lillehammer har etablert seg som årlig møteplass for den nasjonale kompetansebasen. NTNU CCIS er en sentral aktør gjennom uka og særlig er vi involvert i Totalforsvarets cybersikkerhetskonferanse i samarbeid med CyberLand og andre partnere som Telenor Norge og NSM. I 2022 var det et vellykket arrangement med 200 deltagere og mange gode bidrag på scenen.

2.17. North European Cyber Security Cluster

NTNU er Norsk node i European Cyber Security Cluster (NECC) og er representert i styret. Gjennom NECC gjennomføres flere årlige møteplasser for virksomheter fra deltagende nasjoner. Gjennom dette dannes utgangspunkt for et godt samarbeid.

2.18. Deltagelse på ulike møteplasser

Ut over de møteplassene hvor NTNU CCIS er med på Arrangørsiden, så har vi i 2022 også vært til stede på bl.a.:

- Arendalsuka: Deltok bl.a. på DNs TV-sending. En paneldebatt omkring temaet «Etiske utfordringer ved digitalisering». Vi deltok på andre møter, og drev i tillegg en utstrakt nettverking.
- Norsk-tysk handelskammer: Vi deltok på digitalt fagarrangement vedrørende samfunnssikkerhet og digital sikkerhet, sammen med bl.a. Norges Geologiske Undersøkelser, tyske og andre internasjonale aktører. God nettverking i tillegg.
- Paranoia cybersikkerhetskonferanse: Deltok på konferansen i Oslo med egen stand og nettverking.
- EHINN; e-Helse I Norge: Deltok på EHiNN-konferansen i Lillestrøm med egen stand og aktiv nettverking, som har resultert i betydelig markedsføring og en rekke nye kontakter og samarbeid.
- Sikkerhetsfestivalen på Lillehammer: Deltok her med eget forsknings-spor; et heldagsprogram med foredrag av våre faggruppekoordinatorer sammen med samarbeidspartnere.
- Totalforsvarets cybersikkerhetskonferanse: Deltok i programkomiteen og med stand på konferansen.

The Digital Forensics Group has delivered the SOBI report. The report's primary focus is to describe the development in technology and how it has impacted the possibilities for perpetrators to not only establish contact with children, but also how technology facilitates the access and sharing of Child Sexual Abuse Material (CSAM).

2.19. Kommentarer til Økonomirapporten:

Regnskap NTNU CCIS 2022. Regnskapsrapporten under viser totaløkonomien for NTNU CCIS. Dette inkluderer bevilgninger, partnerbidrag og NTNU sine bidrag som vertsinstitusjon. Det har i 2022 vært svært lave utgifter til reiser. Det har i perioden blitt investert i utstyr/ infrastruktur på kr. 775.000. I 2022 kom vi godt i gang igjen med fysiske møteplasser som partner-konferansene, Eurocrypt og Sikkerhetsfestivalen, men en del av utgiftene til disse ble ikke synlige i regnskapet.

Den totale bevilgningen i 2022 fra HOD er 1 MNOK og fra JD 5 MNOK. Nettoresultat viser et overskudd som inkluderer et mindre overforbruk av rammen fra HOD.

Regnskapsrapport 2022	
Inntekter	
Overføring udisponerte midler 2021	1 157 080
Bevilgning statsbudsjettet – JD	5 000 000
Bevilgning statsbudsjettet – HOD	1 000 000
Bidrag partnere	8 477 502
Bidrag NTNU	5 927 487
Totale inntekter 31.12.2022	**21 562 069**
Utgifter	
Administrasjon	
Lønn	3 641 309
Reiser	28 572
Utstyr	
Utvikling	3 585
Teknisk støtte	326 702
Partner- og avtaleoppfølging	515 796
Forskning, utdanning og formidling	
Lønn	13 883 858
Reiser	275 835
Utstyr	775 000
Aktiviteter i forskningsgruppene	93 508
Publikasjoner, trykking, annonser	18 912
Møter og arrangementer	323 212
Formidling og markedsføring	620 200
Utvikling	832 915
Totale utgifter 31.12.2022	**21 339 404**
Udisponerte midler for 31.12 2022	**222 665**

Følgende ansatte er finansiert med midler fra driftsbudsjettet og gjennom partnerfinansiering:

Fast vitenskapelig ansatte	Midlertidig vitenskapelig ansatte	Administrativt ansatte
Bian Yang	Sushma Venkalesh	Anne Skeidsvoll Granli
Katrin Franke	Alvhild Skjelvik	Inge Moen
Staal Vinterbo	Prosper Yeng	Hilde Bakke
Geir Olav Dyrkolbotn	Michael Herbert Ziegler	Espen Thorseth
Benjamin Knox	Andrii Shalaginov	Sushma Venkalesh
Lasse Øverlier	Stefan Axelsson	Anne Hilde Nymoen
Jan William Johnsen	Radina R. Stoykova	
Kyle Porter	Rune Nordvik (PHS)	

I tillegg til dette kommer en rekke ansatte i partnervirksomhetene som bruker deler av sin arbeidstid inn mot NTNU CCIS.

Fra European Cyber Security Challenge (ECSC) 2022 i Wien, Østerrike. Norge ved NTNU CCIS stilte med landslag.

Faggruppenes aktivitet i 2022

1. Applied Cryptology Lab (NaCl)

Group coordinator:
Professor Colin Alexander Boyd

NTNU Applied Cryptology Lab is a platform for research activity in cryptology, aiming for mutual scientific inspiration and coordination, interaction with other research groups, international cooperation and projects with industry and other partners.

Our research questions and findings are relevant to the broader context of current and future challenges of the networked information society: Secure telecommunications and networked services with functionality for authenticity, confidentiality, integrity, availability, privacy, and verifiability of communications.

Academic staff
1. Colin Alexander Boyd, Professor
2. Anamaria Costache, Associate Professor
3. Kristian Gjøsteen, Professor
4. Danilo Gligoroski, Professor
5. Stig Frode Mjølsnes, Professor
6. Bor de Kock, Assistant Professor
7. Jiaxin Pan, Associate Professor
8. Slobodan Petrovic, Professor
9. Staal A. Vinterbo, Professor
10. Tjerand Silde, Associate Professor
11. Morten Rotvold Solberg, Assistant Professor

Researchers and Postdoctoral Fellows
1. Tikaram Sanyashi, Postdoctoral Fellow
2. Yao Jiang Galteland, Postdoctoral Fellow
3. Dan Zhang, Postdoctoral Fellow
4. Hans Heum, Researcher / Postdoctoral Fellow
5. Enio Marku, Researcher

PhD students
1. Pia Bauspieß
2. Jonathan Komada Eriksen
3. Sonu Kumar Jha
4. Elsie Staff Mestl
5. Lise Millerjord
6. Kelsey Noel Moran
7. Lea Sibylle Nürnberger
8. Cristian Alonso Baeza Miranda
9. Magnus Ringerud
10. Ole Martin Edstrøm
11. Charlotte Mylog
12. Sahana Sridhar
13. Mattia Veroni
14. Emil August Hovd Olaisen
15. Amir Zarei
16. Caroline Sandsbråten
17. Runzhi Zeng

Collaboration and collaboration partners:
1. Norwegian Defence Research Establishment (FFI), Norway
2. Kongsberg Digital, Norway
3. Thales, Norway
4. University of Wuppertal, Germany
5. University of Luxembourg, Luxembourg
6. Microsoft Research, Redmond, USA
7. Intel, USA
8. Royal Holloway, University of London, UK
9. Australian National University, Australia
10. University of Maryland, College Park, USA
11. Aarhus University, Denmark
12. Technical University of Denmark, Denmark
13. Duality Technologies, USA
14. Université de Lorraine, CNRS, LORIA, France
15. University of Oxford, UK
16. The University of Edinburgh, UK

Main research result:
Ongoing projects:
– Lightweight cryptography for future smart networks
– Post-quantum cryptographic protocols and primitives
– Realistic cryptography for large-scale applications
– "OffPAD" - Optimizing balance between high security and usability
– Quantum-safe IoT

Submitted proposals
– Preparing for SFI application
– 11 Aug 2022 – A one day seminar between IIK Crypto Discipline and 12 Norwegian companies and organizations that work with / use, cryptography in their products or day-to-day routines. Preparation for potential SFI call.
– 26 Aug 2022 – A one day seminar with NSM

Selected publications:
– Jiaxin Pan and Yuyu Wang, Fine-grained NIZK, Eurocrypt 2022
– Kristian Gjøsteen, Mayank Raikwar, and Shuang Wu, " PriBank: Confidential Blockchain Scaling Using Short Commit-and-Proof NIZK Argument", CT-RSA, 2022.
– Kristian Gjøsteen, Practical Mathematical Cryptography, CRC Press, 2022
– Anonymous Tokens with Public Metadata and Applications to Private Contact Tracing, Tjerand Silde, Martin Strand, Proceedings of Financial Cryptography and Data Security 2022
– Differential privacy for symmetric log-concave mechanisms Staal A. Vinterbo, Proceedings of Machine Learning Research, 2022
– Cybersecurity applications of computational intelligence, Álvaro Herrero, Emilio Corchado, Michal Wozniak, Sung Bae-Cho, Slobodan Petrović, Neural Computing and Applications, 43(23), 2022
– PriBank: Confidential Blockchain Scaling Using Short Commit-and-Proof NIZK Argument, Kristian Gjøsteen, Mayank Raikwar, Shuang Wu, Cryptographers' Track at the RSA Conference

Innovation:
– Hasselgren, Anton; Kralevska, Katina; Gligoroski, Danilo; Faxvaag, Arild. VerifyMed for trust and transparency in the healthcare domain

Education:
– Master courses on Applied Cryptography and Network Security, Ethical Hacking, Mobile and Wireless Network Security, Blockchain Technology.

Graduated PhD candidates:
1. Tjerand Silde (graduated August 2022)
2. Shuang Wu (graduated August 2022)
3. Mayank Raikwar (graduated August 2022)
4. Mattia Veroni (thesis submitted)

Supervised MSc theses:
– Securing the boot process of embedded Linux systems, Nahom Aseged Belay (Master thesis, 2022)
– Techniques and tools for cryptocurrency intelligence and blockchain forensics, H Hunshamar, M Frenje (Master thesis, 2022)
– Secure Communication with WireGuard–VPN-as-a-Service in Beyond 5G, SS Kielland (Master thesis, 2022)
– Analysis and improvements of VerifyMed—the blockchain solution for virtualized healthcare trust relations, A Nedaković (Master thesis, 2022)
... and several others)

Dissemination activities:
Organized Events:
– Eurocrypt, Trondheim, May/June 2022
– WAHC 2022 – 10th Workshop on Encrypted Computing & Applied Homomorphic Cryptography, Los Angeles, November 2022

Lifelong learning activities:
Tjerand Silde in relation with NTNU Videre + Microsoft & HP cooperation

Funding:
$100K funding from Intel (Ana Costache) Crypto Discipline received support from IE and NTNU for financing an Onsager Fellowship, a five-year tenure track position at IIK

2. Critical Infrastructures Security and Resilience (CISaR)

Group coordinator:
Professor Sokratis Katsikas

The Critical Infrastructure Security and Resilience (CISaR) research group's mission is to support the private and public sector to prepare for and respond correctly to security incidents involving critical infrastructure in Norway.

We focus on knowledge and capacity building through research, education, and training.

Critical infrastructure is an asset or system which is essential for the maintenance of vital societal functions. In Norway, Communication networks; electric power; water and wastewater; transportation; oil and gas infrastructure; and satellite communications are defined as critical infrastructure.

The security and resilience of national infrastructure has become a part of national security and critical infrastructure security and resilience has emerged*as a field of great interest for research in cyber security.

Members of the group:
Academic staff

1. Prof. Bernhard Hämmerli
2. Prof. Siv Hilde Houmb
3. Prof. Sokratis K. Katsikas (Group leader)
4. Prof. Stephen Wolthusen
5. Assoc. Prof. Vasileios Gkioulos
6. Assoc. Prof. Ernst Gunnar Gran
7. Asst. Prof. Jia-Chun Lin
8. Assoc. Prof. Katina Kralevska – affiliated

Researchers and Postdoctoral Fellows

9. Dr Alessio Baiocco
10. Dr Sunil Chaudhary
11. Dr Pallavi Kaliyar
12. Dr Georgios Kavallieratos
13. Dr Ming-Chang Lee
14. Dr Mehari Msgna
15. Dr Pankaj Pandey
16. Dr Georgios Spathoulas
17. Dr James Wright
18. Dr Ben Knox – affiliated
19. Dr Demosthenes Ikonomou – affiliated

PhD students

20. Aida Akbarzadeh
21. Ahmed Amro
22. Nabin Chowdhury
23. Kristian Andreas Kanneløning
24. Livinus Obiora Nweke
25. Arne Roar Nygård
26. Håvard Ofte
27. Aybars Oruc
28. Xhesika Ramaj (HiØF)
29. Øyvind Anders Arntzen Toftegaard
30. Jessica Barbosa Heluany
31. Samson Ogheneovo Oruma
32. Vyron Kambourakis
33. Yana Bilous

Collaboration and collaboration partners:
Collaboration with more than 150 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: Ongoing projects:
Within our collaborative R&D projects and other educational and research activities, the CISaR group maintains partnerships with more than 200 organizations, both nationally and internationally, from academia, government, and industry.

1. SDN-µSENSE: SDN – microgrid resilient Electrical energy System (H2020)
2. ELECTRON: resilient and self-healed Electrical power Nano grid (HORIZON)
3. CPSEC: Cyber-Physical Security in Energy Infrastructure of Smart Cities (NFR INDONOR)
4. CybWin: Cybersecurity Platform for Assessment and Training for Critical Infrastructures – Legacy to Digital Twin (NFR IKTPluss)
5. Reverse Engineering for verification of security in digital value chains in a critical infrastructure (NFR Nærings PhD)
6. Lowering Cyber Security entry barriers for Industry 4.0 companies (NFR Nærings PhD)
7. Situation awareness in Virtual Security Operations Centers (NFR Nærings PhD)
8. Resilient Future Smart Grid Ecosystem – Upcoming Steps in Innovation, Business Cases, its Regulation and Supervision (NFR Offentlig PhD)
9. MarCy: Maritime Cyber Resilience (NFR MAROFF)
10. RECYCIN: Reinforcing Competence in Cybersecurity of Critical Infrastructures (NFR INTPART)
11. CyberSec4Europe: Cyber Security Network ofCompetence Centers for Europe (H2020)
12. LOCARD: Lawful evidence collecting and continuity platform development (H2020)
13. DELTA: Future tamper-proof Demand response framework through selfconfigured, self-optimized and collaborative virtual distributed energy nodes (H2020)
14. CyberClever: Integration of cyber security in initial VET-education (ERASMUS+)
15. ARMOR: Artificial Intelligence driven Cybersecurity trust-worthy platform in connected medical devices environment (NTNU IE Faculty)
16. NORCICS: Norwegian Centre for Cybersecurity in Critical Sectors (NFR SFI)

3. Cyber Defence

Group coordinator:
Adjunct Assoc.
Professor Benjamin J. Knox

The focus of the research group is on strengthening an organization's resilience against and ability to handle cyberattacks. The handling of cyberattacks will aim at reducing the consequences or impact of the attack on individuals, organizations or the society in addition to the underlying incident (e.g. loss of information or downtime of services). This will require research combining deep technical analysis with context information about what are valuable assets for individuals, organizations or society.

Society is going through an increased digitization, which the World Economic Forum has estimated gives a 10 % annual increase in Norway's gross domestic product (GDP). This increase in welfare also has a dark side, namely a sharp increase in cybercrime, cyber espionage and cyber-attacks. One of the consequences is that public and private companies are forced to establish teams to handle attacks, for example. SOC, CERT or CSIRT. A rapid increase in the number of teams provides a large variation in quality and focus. A common method is to focus on the cause of the incident (which malware were infected, the server went down, etc.) and correct the error as soon as possible. Professional teams have long since realized that this is about much more than to prevent, detect and rectify incidents. They focus to a much greater extent on the consequences of the events have for their business-critical values. This could be consequences for individuals (finances, reputation, family), the consequences for the company (sales, stock value, reputation) or social consequences (safety, economic growth, job creation). Research that combines deep technical analysis and context information about what is critical values for the individual, the organization and the community is necessary for society as a whole.

Members of the group:

1. Benjamin Knox, PhD
2. Major Geir Olav Dyrkolbotn, PhD
3. Associate Professor Ricardo Lugo, Post Doc on ACDICOM project.
4. Phd Candidate Torvald Fossen Ask, NFR ACDICOM project.
5. Dr Karen Parish, 20 % position with EEA ADVANCES project.
6. Lt Colonell Roger Johnsen (lecturer)

Collaboration and collaboration partners:

1. Dr Mathew Canham, Beyond Layer 7, UCF.
2. Prof Stefan Sütterlin, HIOF & Albstadt-Sigmaringen University, Germany
3. Totalforsvarets Research Group, FFI
4. NSM
5. Forsvarets Høgskole (FHS)
6. NATO Allied Command Transformation (ACT)
7. NATO Science & Technology Organisation (STO)
8. TalTech, Estonia
9. Telenor, Norge.
10. Crosspoint Labs

Main research result:
Ongoing projects:

- (NFR) ACDICOM project: Advancing Cyber Defence by Improved Communication of Recognized Cyber Threat Situations (ACDICOM). Continuing as per the plan.
- (EEA) ADVANCES project: Advancing Human Performance in Cybersecurity. Continuing as per the plan.
- (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: Finalizing by graduating PhD candidates, closing workshop.
- FFI 'Cyber-Social Influence and Impact' (CSP-I): FD and MoJ funded research project.
- NATO HFM 361 Symposium, Madrid 2023, Mitigating & Responding to Cognitive Warfare, Program and Symposium Chair.

Submitted proposals:

- Application for extension of 'Cyber-Social Influence and Impact' (C-SPI) FFI research project. CYFOR & FFI application submitted in Dec.

Selected publications:

Knox, B. J., Lugo, R.G., Sütterlin, S. (accepted for publication in Handbook of Research on Artificial Intelligence, Innovation and Entrepreneurship.) "Cognitive Agility for Improved Understanding and Self-Governance: A Human-Centric AI Enabler". Awaiting publication.

Pirta-Dreimane, R., Brilingaitė, A., Majore, G., Knox, B.J., Lapin, K., Parish, K., Sütterlin, S. and Lugo, R.G., 2022. Application of intervention mapping in cybersecurity education design. In Frontiers in education (Vol. 7, pp. 1-12). Frontiers Media SA.

Sütterlin, S., Lugo, R.G., Ask, T.F., Veng, K., Eck, J., Fritschi, J., Özmen, M.T., Bärreiter, B. and Knox, B.J., 2022. The Role of IT Background for Metacognitive Accuracy, Confidence and Overestimation of Deep Fake Recognition Skills. In International Conference on Human-Computer Interaction (pp. 103-119). Springer, Cham.

Dyrkolbotn, G.O., Knox, B. J., Johnsen, R., «Defensive cyberoperasjoner som militært virkemiddel i en norsk kontekst», book-chapter in anthology – Cyber-operasjoner på norsk), Awaiting publication – Universitetsforlaget.

Innovation:
Ongoing innovation activities:
Established the Cognitive Security Institute (CSI). The intention is to provide an open online knowledge hub for securing human cognition against adversarial or unintended impacts and effects of modern and dual use technologies. Next step is to establish a Laboratory and additional collaborative initiatives between FFI, CYFOR, NTNU CCIS, HIOF, U.S partners and NATO.
https://www.cognitivesecurity.institute/
https://www.youtube.com/channel/UCcjtBmZGno8co3APMD56fuQ?app=desktop

Education:
Activity:
– IMT4214/IIKG6501 Cyber Intelligence (course responsible)
– Classcoordinator MISEB, year 2
– Military Cyber Operations (pilot course for Defence employees)
– Support to ESDC course (Pilot in 'Implementing behavioural science perspectives for improved cybersecurity awareness education in organisations').
– Supporting Forsvarets Spesial Kommando with cyber operations E&T
– PhD Supervision (Torvald Ask, Håvard Ofte, Martin Karresand, Sergii Banin, Andre Jung Waltoft-Olsen, Freddy Murstad)
– Supporting FHS with malware education
– Malware Forum, Chair

Supervised MSc theses:
– Fanny Sunde
– Mikkel Amundsen
– Henrik Hyndøy

Lifelong learning activities:
IIKG6501Cyber Intel
Special advisor and EXCON support to Telenor Exercise Bukkesprang.

Dissemination activities:
Organized Events, Conferences and workshops:
– Program Committee Totalforsvarets Cybersikkerhets Conference.
– NATO ACT Cognitive Warfare Concept Development: Expert advisor.
– NATO Tide Sprint, Norfolk (Virginia), Speaker, Medicine Track.
– NATO Industry Advisory Group, Quick Reaction Team, Cognitive Warfare Concept development, Madrid.
– NATO HFM S&T 356 Cognitive Warfare: Specialist team.
– Human Computer Interaction International (HCII), Board member and session chair.
– NATO IST 195 Symposium, Stockholm, Societal Challenges for Operations in the Information Environment, speaker.
– NATO STB Cognitive Warfare Workshop, Norway, Speaker and Moderator
– NTNU Malware Forum – Chair

4. Digital Forensics Group

Group coordinator:
Professor Katrin Franke

Focus Topics
- Research in the area of large-scale investigations; automatic search through terabytes of electronic data storage within closed systems and the Internet,
- Research and development for the rapid acquisition, correlation, and analysis of Internet-related evidence,
- Technologies for cross-media search and data integration to access diverse sources of information, in particular data enrichment from Internet sources,
- Algorithms for the analysis of encrypted evidence and cryptographic credentials,
- Design of advanced computing technologies to achieve more objective evidence analysis and final decision making by implementing computational intelligence,
- Develop of methods and tools for digital penetrator attribution and profiling, visualization of serious criminal relationships and associations, and geographical mapping of digital and physical evidence.

Computational-intelligent Methods used
- Machine Learning and Pattern Recognition: Abstract measurements are classified as belonging to one or more classes, e.g., whether a sample belongs to a known/abnormal class and with what probability, a mathematical model is learnt from examples.
- Data Mining: large volumes of data are processed to discover nuggets of information, e.g., presence of associations, number of clusters, outliers, etc.
- Computer Graphics / Data Visualization: Two-dimensional images or three-dimensional scenes are synthesized from multi-dimensional data for better human understanding,
- Signal / Image Processing: One-dimensional signals and two-dimensional images are transformed for better human or machine processing,
- Computer Vision: Images are automatically recognized to identify objects
- Robotics: human movements are replicated by a machine.

Members of the group:
Academic staff:
1. Katrin Franke, Professor
2. Lasse Øverlier, Associate Professor
3. Stefan Axelsson, Professor II
4. Kyle Porter, Researcher
5. Jan William Johnsen, Researcher
6. Arvind Sharma, Associate

Collaboration and collaboration partners:
Affiliated IIK staff:
1. Andrii Shalaginov, Professor II
2. Slobodan Petrovic, Professor

Externals and guests:
Core members:
1. Geir Olav Dyrkolbotn, Associate Professor, CyFor
2. J effery Hamm, Assistance Professor, DCSO
3. Mariusz Nowostawski, Associate Professor, NTNU IDI
4. Bente Skattør, PhD, Oslo Police District
5. Thomas Walmann, Associate Professor, Økokrim
6. Andre Årnes, Professor, Telenor Group

Affiliated members:
1. Inger Marie Sunde, Professor, Politihøgskolen
2. Siv Hilde Houmb, Statnett

PhD researchers:
1. Odin Heitmann, Kripos
2. Stig Åsmund Andersen, Oslo Police District
3. Merve Bas Seyyar, University of Groningen
4. Raymond Andre Hagen, Digdir
5. Andre Jung Waltoft-Olsen, Statnett
6. Jul Fredrik Kaltenborn, Politihøgskolen
7. Martin Karresand, FOI, Sverige
8. Rune Nordvik, Politihøgskolen
9. Jens-Petter Skjelvag Sandvik, Kripos
10. An Thi Nguyen
11. Michael Ziegler

Alterations in 2022:
In the past year, five PhD candidates have graduated in the Digital Forensics group, and there are probably two more PhD candidates who will complete their assignments by the end of 2023.

The group has received two new participants who are employed at NTNU in Research positions: Jan-William Johnsen and Kyle Porter. In addition, we collaborate extensively with the new Associate Professor position in hardware reverse engineering at NORCICS, Arvind Sharma.

The NTNU Digital Forensics group has already secured support for two new projects and is in the process of attracting several new PhD candidates.

Collaboration and collaboration partners:
External stakeholders (selection)
- UNICRI - United Nations Interregional Crime and Justice Research Institute, Centre for AI and Robotics, The Hague and Organized Crime, Illegal Trafficking and Illicit Financial Flows, Turin, http://www.unicri.it
- NFI – Netherlands Forensic Institute, https://www.forensicinstitute.nl
- NPAI – Politielab AI, https://nationaal-politielab.sites.uu.nl
- MET – Metropolitan police, https://www.met.police.uk/
- SWP – South Wales Police & UK CCTV Group, https://www.south-wales.police.uk

- Hessen Polizei - https://www.polizei.hessen.de/
- POD – Politidirektoratet, https://www.politiet.no/
- KRIPOS incl. NC3 - The National Criminal Investigation Service incl. Nasjonalt cyberkrimsenter, https://www.politiet.no/kripos
- PHS – Politihøgskolen, https://www.politihogskolen.no
- ØKOKRIM – National Authority for Investigation and Prosecution of Economic and Environmental Crime, https://www.okokrim.no
- PIT – Politiets IKT-tjenester, https://www.politiet.no/om/organisasjonen/andre/pit/
- Politidistriktene - https://www.politiet.no/om/organisasjonen/
- OPD – Oslo Politidistrikt
- TPD – Trøndelag Politidistrikt
- IDP – Innlandet Politidistrikt
- ØPD – Øst Politidistrikt
- NSM – Nasjonal Sikkerhets¬myndighet, https://www.nsm.stat.no
- Oslo Kommune Beredskap – https://www.oslo.kommune.no/etater-foretak og ombud/beredskapsetaten
- BaneNOR
- Mnemonic - IT security service providers, https://www.mnemonic.no
- RedRock – Digitisation and integrated operations, https://www.redrock.no/
- Nordic Edge – Smart City Innovation Cluster, https://nordicedge.org/smart-city-innovation-cluster/
- BI - Norwegian Business school, https://www.bi.no
- RUG.STeP – University of Groningen, Law department, – https://www.rug.nl/rechten/onderzoek/expertisecentra/step-research-group/
- UIA.CAIR - University of Agder, Artificial Intelligence Research Centre, https://cair.uia.no
- ESSENTIAL Project partners, https://www.essentialresearch.eu/consortium/
- THESEUS Project partners, https://project-theseus.eu/the-consortium/
- SFI NORCICS Project partners, https://www.ntnu.edu/norcics/partners
- CCIS Partners, https://www.ntnu.edu/ccis/center-for-cyber-and-information-security

5. e-Health and Welfare Security

Group coordinator:
Assoc. Professor
Bian Yang

Members of the group:
1. Aafan Ahmad Toor
2. Adam Szekeres
3. Ahmad Hassanpour
4. Ahmad Afiouni
5. Alvhild Skjelvik
6. Arnstein Vestad
7. Bian Yang
8. Egil Utheim
9. Einar Snekkenes
10. Elena Serkova
11. Hao Wang
12. Jia-Chun Lin
13. Luyi Sun
14. Marius Mølnvik Øye
15. Ming-Chang Lee
16. Muhammad Ali Fauzi
17. Pankaj Khatiwada
18. Prosper Yeng
19. Sarita Sunder
20. Stephen Wolthusen
21. Yao Jiang

Collaboration and collaboration partners:
1. Ehelse-HAP
2. SI
3. USHT
4. NR
5. HSØ
6. HelseINN
7. Aceso
8. KPMG
9. PraksisNett (Norwegian Center for eHealth Research)

Main research result:
Ongoing projects:
– PriMa (privacy model and preserving methods)
– Health Democratization (health data sharing mechanism)
– IoMT (welfare technology for homecare)
– DigiRemote (welfare technology for homecare)
– Qubit High (qualifying biometrics for eIDAS HIGH)

Submitted proposals:
– RCN-KSP: SERAPH (homecare AI and security)
– RCN-IKTPLUSS: PIAD (privacy inference attack and defense)
– RCN-IKTPLUSS: medical device security
– H2020: AVARTHAS (AI and security for post-surgery care at home)

Some selected publications:
– Ahmad Hassanpour, Majid Moradikia, Bian Yang, Ahmed Abdelhadi, Christoph Busch, Julian Fiérrez: Differential Privacy Preservation in Robust Continual Learning. IEEE Access 10: 24273-24287 (2022)

– Ahmad Hassanpour, Amir Etefaghi Daryani, Mahdieh Mirmahdi, Kiran B. Raja, Bian Yang, Christoph Busch, Julian Fiérrez: E2F-GAN: Eyes-to-Face Inpainting via Edge-Aware Coarse-to-Fine GANs. IEEE Access 10: 32406-32417 (2022)
– Prosper Kandabongee Yeng, Muhammad Ali Fauzi, Bian Yang: A Comprehensive Assessment of Human Factors in Cyber Security Compliance toward Enhancing the Security Practice of Healthcare Staff in Paperless Hospitals. Inf. 13(7): 335 (2022)

– Prosper Kandabongee Yeng, Muhammad Ali Fauzi, Bian Yang, Peter Nimbe: Investigation into Phishing Risk Behaviour among Healthcare Staff. Inf. 13(8): 392 (2022)
– P.Yeng, M. Fauzi, L.Sun, B.Yang. A scoping review of Legal Aspect of Information Security Requirement in healthcare: A Benchmark for Assessing the Security Practice in hospitals. JMIR Human Factors 2022
– L.Sun, B.Yang, E.Uthei, H.Luo. Privacy Predictive Models for Homecare Patient Sensing. Nature Springer 2022

Innovation:
– BIOFY on secure biometric and identity management, with NTNU involved in the RCN-FORNY project Qubit HIGH

Education:
Activity:
– HEALTH DEMOCRATIZATION annual workshop planned in May 2022
– PhD course on human factor methods for information security research fall 2022

Graduated PhD candidates:
– 2022-01-14 Edlira N Martiri defended her thesis on honey biometric template

Supervised MSc theses:
– Marius Mølnvik Øye 2021-2023 on Automated Contact Tracing – organization aspect
– Ahmad Afiouni 2021-2023 on Privacy-preserving data sharing
– Elena Serkova 2022-2023 on medical device security

Lifelong learning activities:
– eHWS group internal training in November 2023

Dissemination activities:
Organized Events, Conferences and workshops:
– Paranoia March 2022 (stand)
– EHiN November 2022 (stand)
– pHealth November 2022 (host)
– SIET November 2022 (keynote speech)

Funding:
– RCN event support to pHealth 2022
– HOD

6. Information Security and Privacy Management

Group coordinator:
Assist. Professor
Erjon Zoto

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

Associate Members:
1. Richard Mcevoy
2. Einar Arthur Snekkenes
3. Aristidis Kaloudis (IØT)

Collaboration and collaboration partners:
1. Innlandet Hospital Trust
2. Southern and Eastern Norway Regional Health
3. Direktoratet for Samfunnssikkerhet og Beredskap
4. Norwegian Digitalisation Agency
5. NSM (National Security Authority)
6. Norsis
7. Deloitte AS
8. Østre Toten municipality
9. Gjøvik municipality
10. Lier municipality
11. Megagame Oslo

Main research result:
– Ovelse.no
The platform ovelse.no is owned by Direktoratet for samfunnssikkerhet og beredskap (DSB), and run by Norwegian Cyber Range ved Norges teknisk-naturvitenskapelige universitet (NTNU). Exercises for better digital security cover all the scenarios on this platform, and these are developed in collaboration between DSB, NTNU, NorSIS, Digitaliseringsdirektoratet og Nasjonal sikkerhetsmyndighet (NSM).

– Serious games

– Agreement with Akershus universitetssykehus on developing and conducting cyber crisis practice research on the 11th og 12th of October in the NCR.

– Meetings with KTH Centre for Cyber Defence and Information Security in Sweden on potential joint Nordic projects.

– ECSC 2023

Members of the research group are part of the organizing committee for ECSC 2023. Focus of the activities will be towards side events before, during, and after the main event.

Selected publications:

- Zoto, Erjon; Shaikh, Sarang; Yildirim Yayilgan, Sule; Abomhara, Mohamed. Designing an innovative toolkit for assessing user acceptance of border control technologies. International Conference "Rebound, Rebuild, and Reinvent for a Sustainable and Equitable Development (3R4SED).
- Shaikh, Sarang; Yildirim Yayilgan, Sule; Zoto, Erjon; Abomhara, Mohamed. A survey of artificial intelligence techniques for user perceptions' extraction from social media data.. Lecture Notes in Networks and Systems.
- Shaikh, Sarang; Yildirim Yayilgan, Sule; Zoto, Erjon; Abomhara, Mohamed. Towards Understanding of User Perceptions for Smart Border Control Technologies using a Fine-Tuned Transformer Approach. Proceedings of the Northern Lights Deep Learning Workshop. volum 3.
- Kowalski, Stewart James; Østby, Grethe. (2022) A Socio-Technical Regime Transitions Model for Gerontechnology Service Design: Privacy, Information Security and Cyber Security in Focus. Studies in Health Technology and Informatics. volum 299.
- Østby, Grethe; Kowalski, Stewart James. (2022) Introducing Serious Games as a Master Course in Information Security Management Programs: Moving Towards Socio-Technical Incident Response Learning. Handbook of Research on Cross-Disciplinary Uses of Gamification in Organizations.
- Østby, Grethe; Kowalski, Stewart James. (2022) ORGANIZATIONAL LEARNING WITH CRISES. EDULEARN22 Proceedings.
- Kianpour, Mazaher, Stewart James Kowalski, and Harald Øverby. "Advancing the concept of cybersecurity as a public good." Simulation Modelling Practice and Theory 116 (2022): 102493.
- Wangen, Gaute Bjørklund. «Det blir ingen varige arbeidsplasser av kryptoutvinning». Fjuken.
- Wangen, Gaute Bjørklund. «Lat oss berre avkrefte at det blir mange arbeidsplassar av datasentre». Fjuken.

Education:
Activity:

- IMT4115 - Introduction to Information Security Management
- DCSG1002 - Cyber security and teamwork
- IIKG1001 - Cyber security and computer networks IMT4128 - Socio-technical Systems Enabled Crime DCSG2005 - Risk Management
- IMT4016 - Experts in Teamwork - Digital Communities and Welfare
- IMT4127 – Information Security Metrics

Graduated PhD candidates:

- In November, Mazaher Kianpour defended his doctoral thesis entitled "Cybersecurity Economics: A Multi-paradigmatic Inquiry into Theory and Practice". Following a transdisciplinary research strategy, this thesis explores the theoretical and practical challenges of research on cybersecurity economics. The solutions to overcome these challenges are also outlined in this thesis.
- Grethe Østby is close to her final defense. Planned: April 2023

Supervised MSc theses:

- Student: Eivind Nes Fossum, Former Investigator NC3,
- Title: Intelligence for cybercrime prevention: A study of stakeholders' needs for actionable intelligence
- Student: Henrik Larsen, Kongsberg Maritime
- Title: Cyber security alerts in remote operation center

Lifelong learning activities:

- NTNU Videre

Dissemination activities:
Organized Events, Conferences and workshops:

- Online presentasjon for Purdue University's Purdue Systems Thinkers (PurSysT) on CyberSecurity Management Education & Serious games, April 2022
- Atlantic council 9/12 cyber-security challenge
- Policy-exercise with CCIS-partners, with EXCON and administration help from FFI, The Norwegian Army's Cyber Defense, NTNU/NCR, NTNU Media and the Innlandet county governor
- Full-scaled exercise with Ahus and Sykehuspartner, EXCON team from NTNU/NCR, Ahus, Sykehuspartner, NTNU Media
- Information sharing exercise with SIKT (exercise Morris)
- Crisis management exercise with management group in Kripos, EXCON-support from Innlandet police district, justiceCERT, IT-group in Kripos, and NorSIS
- Wangen, Gaute Bjørklund. (2022) How to create value from data? IE day NTNU IE Faculty; Trondheim, Clarion Hotel. 2022-06-15 - 2022-06-15
- Cybercation Education Forum October
- CS-Technopoly Cybersecurity Megagame, Sikkerhetsfestivalen, Lillehammer, August 22
- Megagame, National Security Month, Reykjavik, Iceland, October 22
- P-Health

Interdisciplinarity:
Collaboration with departments in Gjøvik & Trondheim:

- Department of Computer Science (IDI/IE)
- Department of health sciences Gjøvik (HIG/MH)
- Department of Interdisciplinary Studies of Culture (KULT/HF)
- Department of Industrial Economics and Technology
- Management (IØT-G/ØK)

7. Norwegian Biometrics Laboratory

Group coordinator:
Professor
Raghavendra Ramachandra

Members of the group:

1. Christoph Busch
2. Partick Bours
3. Raghavendra Ramachandra
4. Raymond Velduis

Collaboration and collaboration partners:

1. Politiet
2. BSI
3. BKA
4. eu-LISA
5. ISO/IEC
6. MovieStarPlanet
7. Sulake

Submitted proposals:

– TRUESEC

Innovation:

- Top Rank Position in NIST Face Morphing Detect Competition: https://pages.nist.gov/frvt/reports/morph/frvt_morph_report.pdf
- Innovation activities with TTO on face morphing detection and presentation attack detection.
- Innovation activities with TTO on sexual predator detection

Education:
Activity:

- NBLAW in March 2023

Lifelong learning activities:

- NBF in May 2023
- NBF in October 2023

Dissemination activities:
Organized Events, Conferences and workshops:

- WACV 2023 workshops
- IJCB 2022 Special Session

Main research result:
Ongoing projects:

- iMARS
- SALT
- TRANS
- AiBA

8. Organizational Complexity, Leadership and Cybersecurity

Group coordinator:
Professor Stig Ole Johannessen

The group is established as part of a collaboration between CCIS and The Norwegian Armed Forces Cyber Defence - aiming at exploring and creating new knowledge on organizational and leadership challenges related to security issues in cyber and crisis contexts. This includes strategic coordination in and between organizations with different critical roles in public security and crises.

The group takes a broad understanding of cyber security as an organizational and societal theme, including dynamic and emerging strategies and strategic leadership in organizations where cyber security is of critical importance; organizational dynamics and complexity in security crises contexts; organizational practices/cultures and leadership competences in and between various groups in cyber integrated organizations.

9. System Security

Group coordinator:
Professor Christian Johansen

Members of the group:

1. Christian Johansen
2. Laszlo Erdodi
3. Erik Hjelmås
4. Basel Katt
5. Hanno Langweg
6. Eigil Obrestad
7. Gabriel Andy Szalkowski
8. Safa Zouari (new PhD student)
9. Muhammad Mudassar Yamin (new post-Doc)
10. Grethe Østby

Collaboration and collaboration partners:

1. Strengthened the collaboration with Luxembourg University (who are strong, e.g., in security for space satellites) through 3+ articles co-authored and published in prominent venues and with Forsvarets etterretningsskole.
2. Multiple new collaborations with industry are being initiated through the NCR activities and through CCIS.
3. Active participation in the new life-long-learning course suite offered by the department together with HP and Microsoft.

Main research result:
Ongoing projects:
- Active participation in managing the events held in the Norwegian Cyber Range (NCR)
- Active participation in Open Cyber Range (financed by EEA)
- Active participation in ASCERT AI-Based Scenario Management for Cyber Range Training (financed by NFR)

Submitted proposals:
- Several applications were made by different group members.

Selected publications:
The group has published multiple journal articles, besides contributions to conferences and workshops. Most prestigious are:

- Paper published at top conference in the field of theoretical computer science CONCUR, titled: "Diamonds for Security: A Non-Interleaving Operational Semantics for the Applied Pi-Calculus" (https://doi.org/10.4230/LIPIcs.CONCUR.2022.30)
- Paper that received the Best Artifact Award at this year's confederated conferences DisCoTech, titled: "Process Algebra Can Save Lives: Static Analysis of XACML Access Control Policies Using mCRL2" (https://doi.org/10.1007/978-3-031-08679-3_2)
- Paper published in Elsevier's journal Computers & Security which is ranked by Google Scholar as the second most cited journal in the field of security, titled: "Modeling and executing cyber security exercise scenarios in cyber ranges" (https://doi.org/10.1016/j.cose.2022.102635)
- Second paper in Computers & Security, titled: "Use of cyber-attack and defense agents in cyber ranges: A case study" (https://doi.org/10.1016/j.cose.2022.102892)

Innovation:
Ongoing innovation activities:
- Continuing work on establishing the startup started last year (with Basel as main contact point).
- One new startup idea is in the process of evaluation together with NTNU-TTO (with Christian as main contact point).

Education:
Activity:
- Strengthened and popularized the S2G Playground CTF ethical hacking bi-weekly events with a constant participation of 30-50 students mostly in the campus Gjøvik but also online.
- Teaching many courses at all levels, for example on Software Security; Systems Security; Cyber security and computer networks; Operating systems; or Information Security Management.

Graduated PhD candidates:
- Muhammad Mudassar Yamin (in summer, and now hired as post-doc).

Supervised MSc theses:
- Rather many on a varied range of topics, but no good overview was kept (ca. 10+ students finished and many ongoing).

Lifelong learning activities:
- Established the large project with Microsoft and HP focused on Lifelong learning in security (interactions started last year).
- Routinely teaching a Sustainability Lab in several courses.
- Involved in (re-)training security to professionals coming from industry in the NCR exercises.

Dissemination activities:
Organized Events, Conferences and workshops:
- Main organizers of the International Workshop on System Security Assurance (SecAssure)
- Co-located with the 27th European Symposium on Research in Computer Security (ESORICS) in Copenhagen, Denmark - 26-30, September 2022
- Organized bi-weekly CFT events part of the S2G Playground every semester, always collaborating with the student organization
- Involved in the organization of Sikkerhetsfestivalen in Lillehammer with at least on megagame and one panel.

Interdisciplinarity:
- Our publications show breadth of research output, e.g., within Concurrency community or Formal tools for security, besides traditional security topics where we have always been active.
- The group has continued to focus on Cyber Ranges taking a broad view, including technologies and frameworks for Cyber Ranges as well as methodological and human aspects.

Organization:
- One major change this year in the S2G group's organizational structure was that several important members have left the group, without new members replacing them.

NTNU CCIS sine 72 partnere pr 31. desmber 2022 (Forsvaret høgskole, Cyberingeniørskolen er en partner):

Layout/trykk: NTNU Grafisk senter