ÅRSRAPPORT
2021

NTNU
CCIS – Center for Cyber
and Information Security

Innholdsfortegnelse

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

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. Senteret har som mål å bli et av de fremste akademiske forsknings- og utdanningsmiljøene innen cyber- og informasjonssikker-het i Europa.

NTNU CCIS hadde ved inngangen til 2022 følgende 55 eksterne partnere:
Accenture, Atea, Bouvet, BDO, Buypass, Capgemini, Cisco, Cognite, Cyberforsvaret, Datatilsynet, DNV, Digitaliserings-direktoratet, Eidel, Eidsiva Energi, Forsvarets forsknings-institutt , Forsvarets høgskole, Government of Iceland, Høgskolen i Innlandet, Hewlett-Packhard, IBM, Innlandet fylkeskommune, Innlandet politidistrikt, KINS, Kluge Advokatfirma, Kongsberg Defence & Aerospace, KPMG, Kripos, mnemonic AS, Nasjonalt ID-senter, Nasjonal kom-munikasjonsmyndighet, Nasjonal sikkerhetsmyndighet, NC-Spectrum, Norges domstoler, NORMA Cyber, NorSIS Norsk senter for informasjonssikring, Oslo politidistrikt, Orkla, Palo Alto, Politidirektoratet, Politihøgskolen, Politiets sikkerhetstjeneste, PwC, SANDS Advokatfirma, Skatte-etaten, Sopra Steria, Statkraft, Statnett, Sykehuset Innlandet HF, Thales, Telenor, TietoEVRY, Tussa, Visma, Watchcom Security Group og Økokrim.

2 Årsrapport

2.1. Styrets arbeid og generalforsamling

Styret i NTNU CCIS består etter generalforsamlingen 2021 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 (2018–2022)
- Telenor, ved Hanne Tangen Nilsen (2021–2023)
- Politidirektoratet, ved Olav Skard Jørgensen (2021–2023)
- Politihøgskolen, ved John Ståle Stamnes (2018–2022)
- Statnett, ved Anders Granum (2020–2022)
- NTNU CCIS ansattrepresentant Staal Vinterbo (2018–2022)

I parentes indikeres perioden som medlemmene er valgt for. 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

MÅLSETNING

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 120 forskere har Institutt for informasjonssikkerhet og kommunikasjonssikkerhet (IIK) ved Fakultet for informasjonsteknologi og elektroteknikk (IE) som sitt vertsinstitutt i Norges teknisk-naturvitenskapelige universitet (NTNU). I 2021 har Nils Kalstad, instituttleder for IIK, også fungert som direktør for NTNU CCIS. Senteret har ukentlige møter for koordinatorene i forskningsgruppene. To saksbehandlere har i 2021 administrativt understøttet aktiviteten i NTNU CCIS, i tillegg til at senteret har bred administrativ støtte fra vertsinstitutt og -fakultet. NTNU CCIS sin vitenskapelige aktivitet har blitt utført ved følgende 8 forskningsgrupper:

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

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), EØS-midlene (Innovasjon Norge), 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 Horizon Europe. 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 2021 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) er i drift, med finansiering fra NFR.
For oversikt over alle publikasjoner til personell med tilknytning til CCIS henviser vi til databasen CRIStin (www.cristin.no).

2.4. Utdanning

NTNU CCIS har i tillegg til vertsinstitusjonen NTNU flere utdanningsinstitusjoner i partnerskapet. Cyberingeniørskolen ved Forsvarets 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/sivilingeniør «Kommunikasjonsteknologi og digital sikkerhet»
- 2-årig engelskspråklig masterstudium «Digital Infrastructure and Cyber Security»
- 2-årig masterstudium «Industriell innovasjon og digital sikkerhet»
- 2-årig heltid og 4-årig deltid engelskspråklig masterstudium «Information Security»
- 3-årig deltid erfaringsbasert masterstudium «Information Security»
- 3-årig bachelorstudium i Digital infrastruktur og cybersikkerhet
- 2-årig engelskspråklig Erasmus Mundus masterstudium «Security and Cloud Computing»

Erfaringsbasert mastergrad i informasjonssikkerhet tilbys i samarbeid med Politihøgskolen, Cyberforsvaret og NorSIS. 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.

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. Første halvdel av 2021 har vært fortsettelsen av en spesiell tid preget av Covid-19 og strenge restriksjoner på fysiske møteplasser, som har utfordret denne aktiviteten noe.

I samarbeid med gode partnere har vi likevel klart å opprettholde god aktivitet.

2.5.1. Sønstebyprisen 2021

Her er utdrag fra pressemelding fra Sønstebyfondet:
«I år går prisen til fremtiden: Sivile og militære, private og offentlige cyberforsvarere! Det er helt i tråd med Gunnar Sønstebys visjon om å huske historien, men å arbeide for fremtiden.»

Prismottakere ved siden av NTNU var: Cyberingeniørskolen ved Forsvarets høgskole, Etterretningstjenesten, KRIPOS NC3, Telenor Norge, Næringslivets Sikkerhetsråd, Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet, Norsk senter for informasjonssikring NorSIS, Cyberforsvarets cybersikkerhetssenter og NORMA Cyber.

2.5.2. Partnerkonferanse

NTNU CCIS gjennomførte to årlige Partnerkonferanser. Først 6.mai med ca. 100 deltagere på NTNU Zoom. Blant annet da med innlegg fra en statssekretær fra Forsvarsdepartementet i Singapore som innleder. Han redegjorde for deres policy vedrørende cybersikkerhet, som sjette pilar i deres totalforsvarssystem. Deretter fikk partnerne møte representanter fra våre faggrupper. Den andre Partnerkonferansen ble avholdt 25.11. Møtet var planlagt som et fysisk møte, men grunnet innføring av nye covid-restriksjoner, ble også dette på kort varsel avholdt på NTNU Zoom. Også dette møtet hadde ca. 100 deltagere. Blant foredragene her kan nevnes direktør Audun Solaas ved Kongsberg Defence & Aeropace som hadde et innlegg om Cyber fysiske systemer og tverrfaglighet og assosiert partner Ove Andre Vanebo ved Kluge Advokatfirma om behovet for kunnskapsutvikling knyttet til juridiske aspekter av cybersikkerhet. Deltagerne deltok også på to runder med rundebordsdiskusjoner. Den ene runden ble ledet av faggruppelederne som fasilitator og den andre av våre styremedlemmer.

2.5.3. Cyber 9/12 Challenge

Cybersikkerhetslandslaget "The Norwegian Cyber Chiefs", (bachelor-, master- og phd-studenter), deltok på Cyber 9/12 konkurransen. 3 av våre ansatte deltok som dommere. Arrangementet er i regi av Atlanterhavsrådet og arrangerer vanligvis fysisk ved Geneva Center for Security Policy i Sveits, men denne gangen ble det en digital konkurranse. Målet med konkurransen var å kombinere teknisk-sikkerhets hendelsesadministrasjon med høyt nivå av politisk veiledning.

2.5.4. European Cyber Security Challenge

På oppdrag fra Justis- og beredskapsdepartementet forbereder NTNU CCIS årlig den norske deltakelsen i konkurransen European Cyber Security Challenge.

Målet er økt fokus på digital sikkerhet i samfunnet generelt, og økt rekruttering til fagfeltet hos unge spesielt. Årlig samler ECSC 25-30 europeiske land til internasjonal kappestrid i cybersikkerhet, der unge talenter konkurrerer. I 2021 ble ECSC avholdt i Praha, Tsjekkia. Et norsk lag ble forberedt, men grunnet Covid ble de forhindret i å delta fysisk i Praha. De var i stedet samlet på Gjøvik og løste konkurranseoppgavene. For mer informasjon se ECSC 2021 – European Cyber Security Challenge 2021 Prague –
ECSC 2021

CSC'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 2023 – European Cyber Security Challenge (ECSC) – NTNU

2.5.5. Norwegian Cyber Security Challenge

Justis- og beredskapsdepartementet ba NTNU CCIS forberede norsk deltakelse i ECSC 2021 i Praha, Tsjekkia med eget lag. Rekrutteringen til dette landslaget skjer gjennom Norwegian Cyber Security Challenge (NCSC), der målsetning er å finne unge talenter (i aldersgruppen 16 - 25 år) innen cybersikkerhet og motivere disse til å utvikle seg videre. Det har i 2021 blitt arrangert to fysiske samlinger med øvelser og 6 digitale samlinger, før kvalifiseringsrunde i NCSC og uttak til landslaget. I tillegg deltok vi på en Nordisk samling, sammen med Danmark, Island og Estland, som del av forberedelsene til årets ECSC i Praha.

For mer informasjon se https://www.ntnu.no/ncsc.

2.5.6. SFI NORCICS

SFI NORCICS er godt i rute med oppstart og oppbygging av prosjektet.
Partnere er Siemens, Helgeland Kraft, Yara, Lyse Energi, Oslo Politidistrikt, Hydro, Kongsberg, Equinor, Sykehuset Innlandet HF, Elvia, mnemonic, NC-Spectrum, UiA og SINTEF. Senteret vil har 90 millioner i finansiering fra Forskningsrådet, 90 millioner fra partnerne og 40 millioner fra NTNU. Også SFI NORCICS vil ha Institutt for informasjonssikkerhet og kommunikasjonsteknologi som vertsinstitutt i NTNU, og vi ser for oss et stort potensial for samarbeid og synergier mellom NTNU CCIS og SFI NORCICS.

2.5.7. 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 planlegging av deltagelse i Arendalsuka med eget program, cybersikkerhetskonferansen Security Talks, ISF' s høstkonferanse og Totalforsvarets cybersikkerhetskonferanse på Lillehammer. Disse gjennomføres i annet halvår. Vi har også deltatt i planlegging av en rekke andre møter og konferanser om Cybersikkerhet.

Fire kurs a 2,5 studiepoeng i innføring av digital sikkerhet går gjennom året med to kurs i semesteret som bransjeprogram for olje- og gassleverandørindustrien. Første runde med gjennomføring, hadde støtte fra Kompetanse Norge.

2.5.8. Vurdere behovet for utdanningstilbud rettet mot helsesektoren

Med bakgrunn blant annet i strategi for digital sikkerhetskompetanse har Helse- og omsorgsdepartementet bedt oss å utrede etter- og videreutdanningstilbud innen digital sikkerhet for helsesektoren. Utredningen skal danne grunnlag for utvikling av et hensiktsmessig etter- og videreutdanningstilbud i digital sikkerhet innen helsesektoren; primærhelsetjeneste, spesialisthelsetjeneste, forvaltning og leverandørindustri. Dette på ledelsesnivå og teknisk nivå. Rapport ble oversendt Helsedepartementet i første halvår.

2.5.9. 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 pågående pandemi har åpningen av lokalene vært utsatt, men vi planlegger med gjenåpning av NCR i moderne, sterkt utvidet og funksjonelle lokaler våren 2022. Disse lokalene vil by på innbydende mulighet for trening og øving av personell med fokus på både tekniske og organisatoriske ferdigheter.

2.5.10. 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.

Cyber Clever vil bli samkjørt med Cyber Smart, et 3-årig prosjekt vi startet planlegging av i 2020 med sikte på å bidra til å gi barn/unge økt bevissthet og kompetanse på digital sikkerhet. Her vil vi dels arbeide for styrket opplæring på dette området i skolen, samspille med ny læreplan. Dels vil vi arbeide for å fange barn/unges oppmerksomhet på digital sikkerhet også på fritid.
Vi vil bruke en app som nav i prosjektet. Viktig delaktivitet vil være å gi opplæring til lærere, som så skal lære elevene bedre digital sikkerhet. Prosjektet bygger på vellykket forprosjekt over 2 år tidligere. I 2021 har vi fortsatt arbeidet for å finne partnere og sponsorer til prosjektet. Viktige inspirasjonskilder for Cyber Clever og Cyber Smart har vi hentet fra tilsvarende programmer og satsinger i USA (Generation Cyber), UK (Cyber First og Cyber Sprinters), Singapore og Danmark.
https://www.gen-cyber.com/

Se ellers denne hjemmeside:
https://www.ntnu.edu/ccis/cybersmart

2.5.11. Digitale trusler i forsvarssektoren

I samarbeid med Norsk råd for digital etikk (NORDE) har NTNU CCIS levert en utredning «Digitale trusler i forsvarssektoren». Utredingen har fått meget god tilbakemelding fra Forsvarsdepartementet.

2.5.12. Nærings-PhD og offentlig PhD

NTNU CCIS har markedsført ordningen med nærings-PhD og offentlig-PhD for gamle og nye partnere. Følgende virksomheter har kandidater som har startet med finansiering i dette løpet i 2021: NVE, Statnett, Elvia og Siemens.

2.5.13. 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 2021 var det et vellykket arrangement med 200 deltagere og mange gode bidrag på scenen.

2.5.14. 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.

2.5.15. Deltagelse på ulike møteplasser

Ut over de møteplassene hvor NTNU CCIS er med på arrangørsiden så har vi i 2021 også vært til stede på bl.a.

- Arendalsuka: Bidrag på NSMs arrangement og DN's telt:
  I august deltok vi her med eget cybersikkerhetsinnlegg ved vår direktør/instituttleder om bord i M/S Sandnes, samt 30 minutters DN TV-innslag ledet av vår dekan, med deltakelse ellers av tidligere etterretningssjef, vår direktør/instituttleder og digitaliseringsministeren. Dette innslaget fikk bl.a. bred mediedekning i nasjonale aviser og TV. I tillegg ble det bedrevet utstrakt nettverking.
- Norsk-tysk handelskammer:
  Vi deltok på digitalt fagarrangement vedrørende samfunnssikkerhet og digital sikkerhet i november, sammen med bl.a. Norges Geologiske Undersøkelser, tyske og andre internasjonale aktører. God nettverking i tillegg.
- Forsvarsindustrien leverandørforening:
  Som nytt medlem der deltok vi på den årlige, store leverandørmessen på Akershus festning i september. Egen stand og aktiv nettverking.
- Paranoia cybersikkerhetskonferanse:
  I November deltok vi her i Oslo med egen stand og nettverking.
- EHINN; e-Helse I Norge:
  I november deltok vi på eHiN-konferansen i Lillestrøm med egen stand og aktiv nettverking.

Mer om nettverkingen:
Denne aktiviteten har resultert i betydelig markedsføring og i en rekke pågående kontakter.

2.6. Årsregnskap NTNU CCIS 2021

Regnskapsrapporten under viser totaløkonomien for NTNU CCIS. Dette inkluderer bevilgninger, partnerbidrag og NTNU sine bidrag som vertsinstitusjon. Det har i 2021 vært svært lave utgifter til reiser, partneroppfølging og nettverksarbeid. Enkelte av disse udisponerte midlene har vært benyttet til å investere i planlagt, nødvendig infrastruktur og utstyr.

Det er i 2021 også lagt betydelig ressurser i utvikling og leveranse av hybride og heldigitale løsninger for etter- og videreutdanning, møter og konferanser innen våre fagområder.

Følgende ansatte er finansiert med midler fra drifts-budsjettet og gjennom partnerfinansiering:

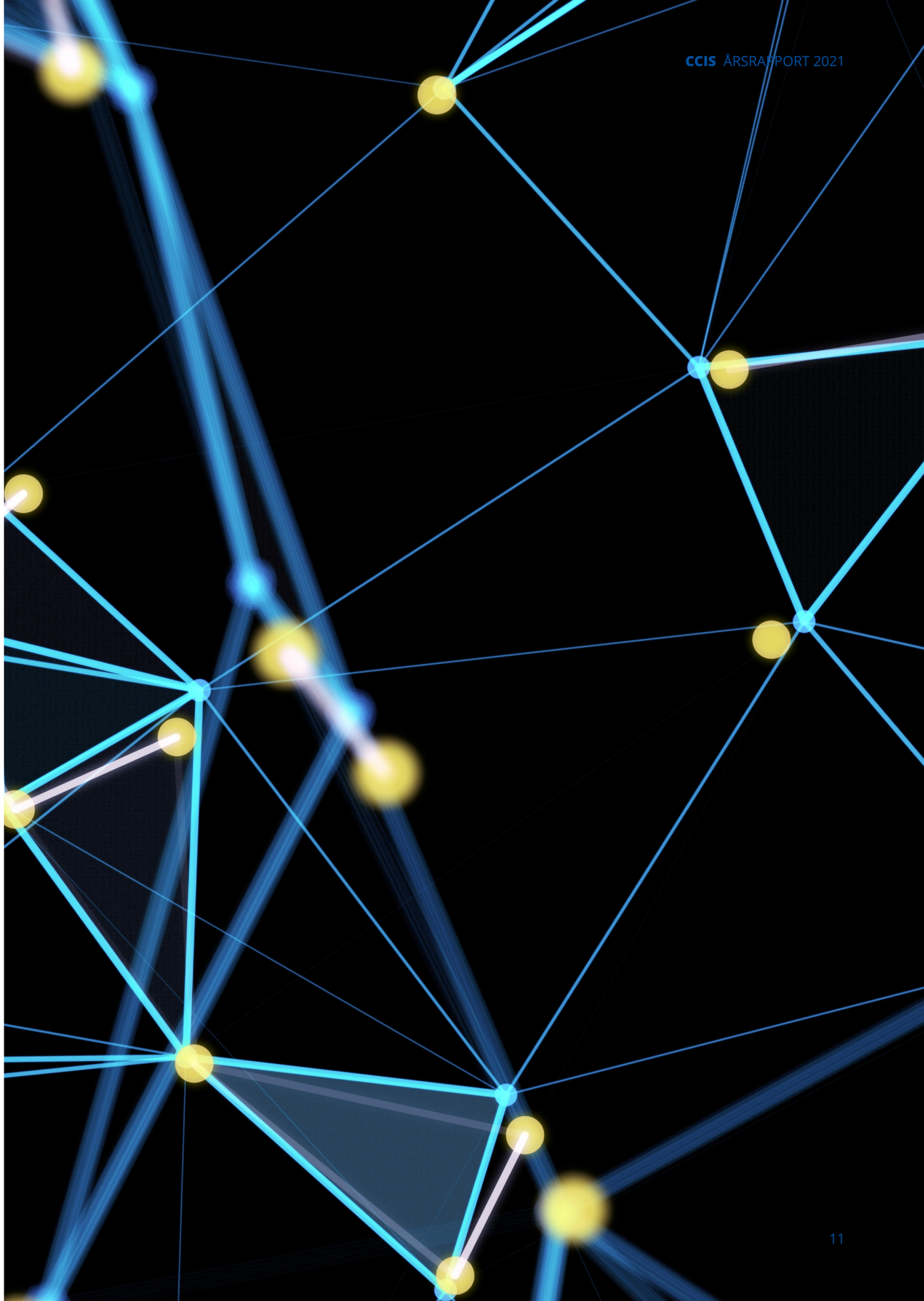
Regnskapsrapport 2021	
Inntekter	
Overføring udisponerte midler 2020	2 589 189
Bevilgning statusbudsjettet – JD	5 000 000
Bevilgning statusbudsjettet – HOD	1 800 000
Bidrag partnere	8 477 502
Bidrag NTNU	**5 927 487**
Totale inntekter 31.12.2021	**23 794 178**
Utgifter	
Administrasjon	
Lønn	2 946 820
Reiser	15 659
Utstyr	2 525
Utvikling	2 589
Teknisk støtte	417 075
Partner- og avtaleoppfølging	871 249
Forskning, utdanning og formidling	
Lønn	13 931 461
Reiser	232 187
Utstyr	787 049
Aktiviteter i forskningsgruppene	93 508
Publikasjoner, trykking, annonser	18 912
Møter og arrangementer	421 486
Formidling og markedsføring	863 663
Utvikling	2 032 915
Totale utgifter 31.12.21	**22 637 098**
Udisponerte midler for 31.12.2021	**1 157 080**

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	Herbert Ziegler	Espen Thorseth
Benjamin Knox	Andrii Shalaginov	Sushma Venkalesh
	Stefan Axelsson	Anne Hilde Nymoen
	Jan William Johnsen	
	Kyle Porter	
	Radina Stoykova	
	Rune Nordvik (PHS)	

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

CCIS ÅRSRAPPORT 2021



Faggruppenes aktivitet i 2021

1. Digital Forensics

Group leader:
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

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

Main research result:
Academic staff
1. Katrin Franke, Professor
2. Lasse Øverlier, Associate Professor
3. Stefan Axelsson, Professor II

Externals and guests
Core members:
1. Geir Olav Dyrkolbotn, Associate Professor, CyFor
2. Jeffery 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. Gunnar Alendal, Kripos
2. Stig Åsmund Andersen, Oslo Police District
3. Merve Bas Seyyar, University of Groningen
4. Jan William Johnson
5. Andre Jung Waltoft-Olsen, Statsnett
6. Jul Fredrik Kaltenborn, Politihøgskolen
7. Martin Karresand, FOI
8. Rune Nordvik, Politihøgskolen
9. Manan Oza
10. Kyle Porter
11. Jens-Petter Skjelvag Sandvik, Kripos
12. Radina Stoykova
13. An Thi Nguyen
14. Michael Ziegler

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

Main research result:
Current research projects
- "ACT"
- "Ars Forensica", Professor Katrin Franke
- "Blockchain Technology", Associate Professor Mariusz Nowostawski
- "Dark Web", Professor Katrin Franke
- "ESSENTIAL", Professor Katrin Franke
- "Forensic Methodology", Professor Katrin Franke
- "Hansken", Senior Researcher, Dr. Carl Stuart Leichter
- "Malware Analytics", Professor Katrin Franke, Associate Professor Geir Olav Dyrkolbotn
- Financial Fraud Forensics and Simulation, Dr. Edgar Lopez-Rojas, Post-doctoral researcher

Journal publications:
- Nordvik, Rune; Stoykova, Radina Raychova; Franke, Katrin; Axelsson, Stefan; Toolan, Fergus. (2021) Reliability validation for file system interpretation. Forensic Science International: Digital Investigation. vol. 37.
- Sandvik, Jens-Petter; Franke, Katrin; Abie, Habtamu; Årnes, Andrè. (2021) Coffee forensics — Reconstructing data in IoT devices running Contiki OS. Forensic Science International: Digital Investigation. vol. 37.

Innovation:
- SFI NORCICS - Norwegian Centre for Cybersecurity in Critical Sectors, https://www.ntnu.edu/norcics
- NTNU CCIS - Center for Cyber and Information Security, https://www.ntnu.edu/ccis
- SOBI - Sektorsamarbeid om forskning på forebygging av seksuelle overgrep mot barn på internett, https://www.ntnu.no/iph/sobi
- Green40 - Center for Green Shift in the Built Environment, https://www.ntnu.edu/green40

Education:
Contributions to study programmes
- MSc in Information Security (full-time / part-time), https://www.ntnu.edu/studies/mis/about-the-programme
- Experience-based master's degree, Information Security, https://www.ntnu.edu/studies/miseb/about-the-programme
- Master Courses
- IMT4114 - Introduction to Digital Forensics, https://www.ntnu.edu/studies/courses/IMT4114#tab=omEmnet
- IMT4130 - Cybercrime Investigation, https://www.ntnu.edu/studies/courses/IMT4130#tab=omEmnet
- IMT4133 - Data Science for Security and Forensics, https://www.ntnu.edu/studies/courses/IMT4133#tab=omEmnet
- IMT4210 - Computational Forensics, https://www.ntnu.edu/studies/courses/IMT4210#tab=omEmnet
- PhD Courses
- IMT6091 - Computational Forensics, https://www.ntnu.edu/studies/courses/IMT6091#tab=omEmnet
- IMT6101 - Computational Intelligence, https://www.ntnu.edu/studies/courses/IMT6101#tab=omEmnet

2. e-Health and Welfare Security

Group leader:
Professor Bian Yang

The e-Health and Welfare Security (e-HWS) research group focuses their research on the **privacy and cyber security challenges related to the fields of eHealth and welfare.**

The group works to create mutual understanding across health and cyber security sectors by identifying key research challenges needing a joint force from both sectors and proposing innovative technical and socio-technical solutions to the identified challenges.

Examples of our current research priorities:
- Secure data management
- Privacy models and privacy enhancing technologies
- System-level security for healthcare applications
- Risk models and risk analysis
- Crypto-biometrics for healthcare uses

Members of the group:

Academic staff
1. Bian Yang, professor
2. Einar Snekkenes, professor
3. Hao Wang, førsteamanuensis
4. Jia-Chun Lin, universitetslektor
5. Stephen Wolthusen, professor

Researchers and Postdoctoral Fellows
1. Adam Szekeres, postdoc.
2. Marius Mølnvik Øye, affiliated
3. Yao Jiang, postdoc.
4. Yuhang Wang, postdoc.

PhD students
1. Ahmad Hassanpour
2. Ahmad Afiouni
3. Alvhild Skjelvik
4. Arnstein Vestad
5. Edlira N. Martiri
6. Egil Utheim
7. Luyi Sun
8. Ming-Chang Lee
9. Muhammad Ali Fauzi
10. Pankaj Khatiwada
11. Prosper Yeng
12. Sarita Sunder

Collaboration and collaboration partners:
1. Ehelse-HAP
2. SI
3. USHT
4. NR
5. HSØ
6. HelseINN
7. Aceso
8. KPMG

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)

Submitted proposals:
- RCN-KSP: SERAPH (homecare AI and security)
- H2020: AVARTHAS (AI and security for post-surgery care at home)

Selected publications:
- 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.
- L.Sun and B.Yang. Your Privacy Preference Matters: A Qualitative Study Envisioned for Homecare. ICTS4eHealth 2021.
- Muhammad Ali Fauzi, Prosper Kandabongee Yeng, Bian Yang, Dita Rachmayani: Examining the Link Between Stress Level and Cybersecurity Practices of Hospital Staff in Indonesia. ARES 2021: 137:1-137:8
- Yuhang Wang, Bian Yang: Reinforcing Health Data Sharing Through Data Democratization. pHealth 2021: 124-129
- Muhammad Ali Fauzi, Bian Yang: Continuous Stress Detection of Hospital Staff Using Smartwatch Sensors and Classifier Ensemble. pHealth 2021: 245-250

Innovation:
- BIOFY on secure biometric and identity management

Education:
- HEALTH DEMOCRATIZATION annual workshop planned in May 2022
- PhD course on human factor methods for information security research fall 2022
- 2022-01-14 Edlira N Martiri defended her thesis on honey biometric template
- Marius Mølnvik Øye 2021-2022 on Automated Contact Tracing – organization aspect
- Ahmad Afiouni 2021-2022 on Privacy-preserving data sharing

Dissemination activities:
- EHiN November 2021
- Co-workshop with Center for Care Research March 2021

3. Applied Cryptology Lab (NaCl)

Group leader:
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.

Members of the group:

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. Ruxandra-Florentina Olimid-Nencioni, Associate Professor
7. Jiaxin Pan, Associate Professor
8. Slobodan Petrovic, Professor
9. Staal A. Vinterbo, Professor

Researchers and Postdoctoral Fellows
1. Enio Marku, Researcher
2. Yao Jiang Galteland, Postdoctoral Fellow
3. Chen Qian, Postdoctoral Fellow

PhD students
1. Pia Bauspieß, PhD student
2. Jonathan Komada Eriksen, PhD Candidate
3. Sonu Kumar Jha, PhD Candidate
4. Elsie Staff Mestl, PhD Candidate
5. Lise Millerjord, PhD Candidate
6. Kelsey Noel Moran, PhD Candidate
7. Lea Sibylle Nürnberger, PhD Candidate
8. Mayank Raikwar, PhD Candidate
9. Magnus Ringerud, PhD Candidate
10. Tjerand Silde, PhD Candidate
11. Morten Rotvold Solberg, PhD Candidate
12. Sahana Sridhar, PhD candidate
13. Mattia Veroni, PhD Candidate
14. Shuang Wu, PhD Candidate
15. Amir Zarei, PhD Candidate
16. Bor de Kock, PhD Candidate

Collaboration and collaboration partners:
1. University of Wuppertal, Germany
2. University of Luxembourg
3. Microsoft Research, Redmond
4. FFI
5. Intel
6. Royal Holloway, University of London

Main research result:

Ongoing projects:
- Lightweight cryptography for future smart networks
- Post-quantum cryptographic protocols and primitives
- Realistic cryptography for large-scale applications
- Blockchain for digital transformation
- Quantum-safe IoT

Selected publications:
- Symmetric key exchange with full forward security and robust synchronization, C Boyd, GT Davies, B Kock, K Gellert, T Jager, L Millerjord, Asiacrypt 2021
- Lattice-based proof of shuffle and applications to electronic voting, DF Aranha, C Baum, K Gjøsteen, T Silde, T Tunge, Cryptographers' Track at the RSA Conference, 2021
- Fine-Grained Secure Attribute-Based Encryption, Y Wang, J Pan, Y Chen, CRYPTO 2021
- Non-Interactive VDF Client Puzzle for DoS Mitigation, M Raikwar, D Gligoroski European Interdisciplinary Cybersecurity Conference, 32-38

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: - Yao Jiang, Cryptographic Tools for Cloud Security, 2021
- Supervised MSc theses:
  WireGuard for Securing Constrained Application Protocol for IoT Devices (CoAP),
  Kazakova, Evgenia (Master thesis, 2021)
  Privacy in the Norwegian Automatic Contact Tracing App Smittestopp, Nes, Hanne Æsøy (Master thesis, 2021)
  Post-Quantum Key Exchange in Telegram's MTProto Protocol, Rognerud, Robert (Master thesis, 2021)
  A Survey of Quantum-safe Digital Signatures and their building blocks, Sridhar, Sahana (Master thesis, 2021)
  Applying Twisted Hessian Curves to Supersingular Isogeny Diffie-Hellman, Eriksen, Jonathan Komada (Master thesis, 2021)

Organized Events:
- Norsk Kryptoseminar, Trondheim, December 2021

4. Critical Infrastructures Security and Resilience (CIRaR)

Group leader:
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

PhD students

19. Aida Akbarzadeh
20. Ahmed Amro
21. Nabin Chowdhury
22. Kristian Andreas Kanneløning
23. Livinus Obiora Nweke
24. Arne Roar Nygård
25. Håvard Ofte
26. Aybars Oruc
27. Xhesika Ramaj (HiØF)
28. Øyvind Anders Arntzen Toftegaard

Collaboration and collaboration partners:

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.

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.

Main research result:

Ongoing projects:

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 of Competence Centers for Europe (H2020)
12. LOCARD: Lawful evidence collecting and continuity platform development (H2020)
13. DELTA: Future tamper-proof Demand response framework through self-configured, 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 trustworthy platform in connected medical devices environment (NTNU IE Faculty)
16. NORCICS: Norwegian Centre for Cybersecurity in Critical Sectors (NFR SFI)
17. +CityxChange: Positive City ExChange (H2020)
18. DIGIPRO – Digitalisering av prosessindustrien (Kompetanse Norge)
19. CIRMAN: Circular Manufacturing research and educational collaboration with India and Japan (NFR INTPART)
20. PowerDig: Digitalization of short-term resource allocation in power markets (NFR ENERGIX)
21. Cybersikkerhet og Industri 4.0 (Norsk Industri)

Submitted proposals:

1. ARGUS: Advanced Research for Guarding Unconnected cybersecurity domains in ports environments (EUROSTARS)
2. ASSURANCE: AI assisted business continuity and Resilience relying on Augmented Cybersecurity mEchanisms (HORIZON)
3. D2Gov: Digitalization 2.0 – new mechanisms of domain data modelling for smart governance in the built environment (NFR)
4. HoliCyber: The smart and vulnerable society – holistic cyber security management in smart cities and regions (NFR IKTPluss)
5. INSPIRE: A citizens privacy enabling framework towards a fairer and more sustainable world wide web (HORIZON)
6. SecuGrid: Securing the power grid against cyber-physical failures and attacks (NFR KSPKOMPETANSE21)
7. NorCare: Modeling Cybersecurity and Safety for SDN-enabled Norwegian Homecare Services (NFR Forskerprosjekt 2021)
8. Development of cybersecurity training and exercise scenarios for the oil and gas sector (PTIL)
9. RESISTANT: Cyber Resilience framework for Smart manufacturing infrastructures (HORIZON)
10. SYSTEMIC: A Systemic Approach to Collaborative Regulatory Risk Management in a Cross-Sector and Cross-Border Context (HORIZON)
11. THEMIS: A European Lighthouse Community for Safe and Secure AI (HORIZON)
12. TrustId: Trust empowered framework for our digital identities, striving for a transparent and privacy preserving Internet (HORIZON)

Selected publications:

- Joseph K. Liu, Sokratis Katsikas, Weizhi Meng, Willy Susilo, Rolly Intan (Eds.), Information Security, Proceedings of the 24th International Security Conference (ISC), Virtual event, Springer Publishing Company, 2021.
- G. Spathoulas, L. Negka, P. Pandey, S. Katsikas, "Can Blockchain Technology Enhance Security and Privacy in the Internet of Things?", in Tsihrintzis G., Virvou M. (eds), Advances in Core Computer Science-Based Technologies. Learning and Analytics in Intelligent Systems, vol 14. Springer, Cham, pp. 199-228, 2021.
- P. Pandey, S. Katsikas, "The Future of Money: Central Bank Issued Electronic Money", in Tsihrintzis G., Virvou M. (eds), Advances in Core Computer Science-Based Technologies. Learning and Analytics in Intelligent Systems, vol 14. Springer, Cham, pp. 229-259, 2021.
- A.N. Yannacopoulos, S.K. Katsikas, "Cyber Insurance and Security Investment Strategy", in: Jajodia S., Samarati P., Yung M. (eds) Encyclopedia of Cryptography, Security and Privacy, Springer, Berlin, Heidelberg, 2021.
- S. Katsikas, "Security Risk Assessment for Cyber Physical Systems", in: Jajodia S., Samarati P., Yung M. (eds) Encyclopedia of Cryptography, Security and Privacy, Springer, Berlin, Heidelberg, 2021.
- S. Katsikas, G. Kavallieratos, "Cybersecurity of the unmanned ship", in V. Maglaras and I. Kantzavelou (Eds.), Cybersecurity Issues in Emerging Technologies, pp. 21-42, CRC Press, 2021.
- A. Goudosis, S. Katsikas, "ARIBC: Online reporting based on Identity Based Cryptography", Future Internet Vol. 13, article no. 53, https://doi.org/10.3390/fi13020053r, 2021.
- G. Kavallieratos, G. Spathoulas, S. Katsikas, "Cyber risk propagation and optimal selection of cybersecurity controls for complex cyberphysical systems", Sensors, Vol. 21, no. 1691, https://doi.org/10.3390/s21051691, 2021.
- A. Akbarzadeh, S. Katsikas, "Identifying and analyzing dependencies in and among complex Cyber Physical Systems", Sensors, Vol. 21, no. 5, art. No. 1685, https://doi.org/10.3390/s21051685, 2021.
- S. Pirbhulal, V. Gkioulos, S. Katsikas, "A Systematic Literature Review on RAMS Analysis for Critical Infrastructures Protection", International Journal of Critical Infrastructure Protection, Vol. 33, https://doi.org/10.1016/j.ijcip.2021.100427, 2021.
- A. Amro, V. Gkioulos, S. Katsikas, "Communication architecture for autonomous passenger ship", Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, March 2021. https://doi.org/10.1177/1748006X211002546, 2021.
- Grammatikis, P.R.; Sarigiannidis, P.; Dalamagkas, C.; Spyridis, Y.; Lagkas, T.; Efstathopoulos, G.; Sesis, A.; Pavon, I.L.; Burgos, R.T.; Diaz, R.; Sarigiannidis, A.; Papamartzivanos, D.; Menesidou, S.A.; Ledakis, G.; Pasias, A.; Kotsiopoulos, T.; Drosou, A.; Mavropoulos, O.; Subirachs, A.C.; Sola, P.P.; Domínguez-García, J.L.; Escalante, M.; Alberto, M.M.; Caracuel, B.; Ramos, F.; Gkioulos, V.; Katsikas, S.; Bolstad, H.C.; Archer, D.-E.; Paunovic, N.; Gallart, R.; Rokkas, T.; Arce, A. SDN-Based Resilient Smart Grid: The SDN-microSENSE Architecture. Digital, 1, 173-187. https://doi.org/10.3390/digital1040013, 2021.
- S. Pirbhulal, V. Gkioulos, S. Katsikas, "Towards Integration of Security and Safety Measures for Critical Infrastructures based on Bayesian Networks and Graph Theory: A Systematic Literature Review", Signals, 2, 771-802. https://doi.org/10.3390/signals2040045, 2021.
- M. Msgna, S. Katsikas, and V. Gkioulos, "WYK: Mobile Device Authentication Using the User's Address Book", in Proceedings, 4th International Workshop on Emerging Technologies for Authorization and Authentication, Darmstadt, Germany, 2021.
- G. Kavallieratos, G. Spathoulas, S. Katsikas and A. Baiocco, "Attack path analysis and cost-efficient selection of cybersecurity controls for complex cyberphysical systems", in Proceedings, 7th Workshop on the Security of Industrial Control Systems & of Cyber-Physical Systems (CyberICPS 2021), Darmstadt, Germany, 2021.

Education:

Activity:

- Delivery of MSc course IMT4203 Critical Infrastructure Security
- Supervision of 11 PhD candidates of the CISaR group
- Co-supervision of several PhD candidates of other groups/NTNU Departments

Graduated PhD candidates:

- Georgios Kavallieratos, "Security of the Cyber Enabled Ship"
- Supervised MSc theses:
- Chen Hsin-Yi, "Domain-specific Threat Modeling for Mobile Communication Systems"
- Daniel del Riego San Martin, "Cybersecurity control evaluation and validation platforms for medical devices"
- Bjørnar Fidje Liberg, "Risk Perception of Influence Operations in Social Media".
- Weronica Nilsen,, "Security Culture in the Norwegian Health Care Domain".
- Salman Ayyaz Khan, "Public Risk Perceptions When Participating in Debate on Digital Platforms".
- Gard Hoel Grøttan, "Security Awareness of Students at NTNU".
- MSc Student (Thesis) Eivind Jørgen Gilje Dybvik, "Public Risk Perception in Norwegians When Participating in Online Debates".
- Ulrik Johansen Ruud, "Cyber Threats and Vulnerabilities in the Integrated Navigation System".

- Susanne Barkhald Sandberg, "Effects of organizational cyber securityculture across the energy sector supply chain"
- Ivar Olav Moen, "Improving Cyber Security Awareness of Seafarers"
- Audun Landøy Solli, "A Testbed for Evaluating Cyber Security in the Maritime Sector"
- Sander Løken Berntsen, "Ontological Event Analysis in Industrial Control Systems"

Dissemination activities:

Organized Events, Conferences and workshops:

- CyberICPS 2021: 7th Workshop On The Security Of Industrial Control Systems & Of Cyber-Physical Systems
- Chairing of/membership in TPCs/steering committees of more than 60 international conferences
- Cybersikkerhetsuka – Industri 4.0

Funding:

- European Commission
- Research Council of Norway
- Norsk Industri

5. Biometrics

Group leader:
Professor
Raghavendra Ramachandra

The biometric research group at NTNU focuses on various biological and behavioral biometrics including 2D- and 3D-face recognition, fingerprint recognition, finger vein recognition, ear recognition, signature recognition, gait recognition, keystroke recognition, gesture recognition and mouse dynamics.

Norwegian Biometrics Laboratory is more than just a physical room at the campus. It is a discussion forum to brainstorm, to generate new ideas and projects and to present intermediate results. Thus it is an essential part of the Department of Information Security and Communication at the Norwegian University of Science and Technology (NTNU) and represents an active focus point with many international research projects.

Further, it is the intention of the laboratory to increase the awareness of biometrics in Norway via the Norwegian Biometric Forum and its potential involvement in the Norwegian legislation and to contribute to the international standardization in the field.

Furthermore, we focus on:

- privacy enhancing technologies, such as biometric template protection
- presentation attack detection
- face morphing attack detection

Members of the group:

1. Patrick Bours, professor
2. Christoph Busch, professor
3. Kiran Raja, førsteamanuensis
4. Guoqiang Li, forsker
5. Raghavendra Ramachandra, professor
6. Patrick Schuch, afilliated
7. Raymond Velduis, professor
8. Mudasir Wani, foreleser
9. Bian Yang, professor
10. Pia Bauspiess
11. Parisa Borj
12. Cristian Botezatu
13. Marcel Grimmer
14. Alexander Kirfel
15. Raghavendar Mudgal-Dundurai
16. Jag Mohan Singh
17. Martin Stokkenes
18. Sushma Venkatesh
19. Haoyu Zhang

Collaboration and collaboration partners:

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

Main research result:

Ongoing projects:

– eu-LISA (Synthetic Face Images)
– iMARS (Morphing Attack Detection / Face Image Quality)
– SALT (Face Image quality/Presentation Attack Detection)
– AiBA (Author input Behavioral Analysis)

Submitted proposals:

– LETITBE
– FairFace
– VasCoDe
– TRANS

Selected publications:

– M. Grimmer, H. Zhang, R. Raghavendra, K. Raja, C. Busch: "Generation of Non-Deterministic Synthetic Face Datasets Guided by Identity Priors", in Proceedings Norwegian Information Security Conference (NISK), Trondheim, NO, November 29 to December 1, (2021), https://arxiv.org/pdf/2110.03464.pdf
– E. Tabassi, M. Olsen, O. Bausinger, C. Busch, A. Figlarz, G. Fiumara, O. Henniger, J. Merkle, T. Ruhland, C. Schiel, M. Scwaiger: "NFIQ 2 - NIST Fingerprint Image Quality", NISTIR 8382, (2021)
– C. Rathgeb, R. Tolosana, R. Vera-Rodriguez, C. Busch: "Handbook of Digital Face Manipulation and Detection", Springer, (2021)
– N. Agarwal, T. Ünlü, M.A. Wani, and P. Bours, "Predatory Conversation Detection Using Transfer Learning Approach", International Conference on Machine Learning, Optimization, and Data Science, 2021

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 2022: https://eab.org/events/program/246

Graduated PhD candidates:

– Hailin Li: "Face Age Progression with Realness-Distribution GANs" July 2021
– Audun Einangen: "Go Phish! – Educating Users Not to Bite on Phising", Spring 2021
– Octavian Stoian: "Passwords habits, the attacker perspective", Spring 2021
– Marit Sylstad: "Chat Room safety", Spring 2021.
– Nakul Pathak: "Building Effective Interactions", Spring 2021.
– Duy Thomas Do: "Offline Signature Verification using GED on Labelled Graphs", Spring 2021
– Reidar Johannessen Strømme: "Early gender detection using keystroke dynamics and stylometry", Spring 2021
– Tobias Moe: "I still know who you are! – Soft Biometric Keystroke Dynamics performance with distorted timing data", Spring 2021
– Riccardo Matteini Palmerini: "Graph theoretical approach to sexual predator detection", Spring 2021.
– Emiil Kløvik: "Determining the age and gender of an individual based on text classification - Comparing a two binary classification approach with a 4-class classification approach", Fall 2021
– Joakim Granli Antonsen: "Cyber Grooming Detection: Human or Machine? Or Hybrid?", Fall 2021.
– Mats Johan Pedersen: "Detection of Text Copying", Fall 2021
– Karl-Sverre Knutsen: "Signature Authentication using graph edge labelling", Fall 2021.

Lifelong learning activities:

– NBF in May 2021: https://eab.org/events/program/230
– NBF in October 2021: https://eab.org/events/program/257

Dissemination activities:

Organized Events, Conferences and workshops:

– Artfiicial Intelligence Workshop in November 2021: https://eab.org/events/program/277
– NIST face image quality workshop in November 2021 with 670 registered experts: https://eab.org/events/program/261

6. Cyber Defence

Group leader:
Phd Benjamin 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. Oberst Lt Roger Johnsen (foreleser)

Collaboration and collaboration partners:

1. Cyber Forsvaret
2. FFI
3. Forsvarets Høgskole
4. HiOF
5. NSM
6. Albstadt-Sigmaringen University, Germany
7. Tal Tech, Estonia
8. Beyond Layer 7, USA
9. Telenor Norge AS
10. Norton LifeLock

Main research result:

Ongoing projects:

- BK: Research Council of Norway (NFR); NOK 10.060.000. 4 years, Advancing Cyber Defense by Improved Communication of Recognized Cyber Threat Situations (ACDICOM), CO-Principal Investigator.
- BK: European Economic Area (EEA); EUR 999.132, 3 years, Advancing Human Performance in Cybersecurity (ADVANCES). Management Committee and work-package lead. (EEA; # LT08-2-LMT-K-01-051)
- BK: NATO HFM S&T 356 Cognitive Warfare: Specialist team.
- BK: FFI project: Cyber-Social Influence. Management board
- BK: Editorial Board. Anthology: Cyber Operations. Norwegian Defense University College.

Submitted proposals:

- BK: Under review: Twinning (HORIZON-WIDERA-2021-ACCESS-03), Twin4AI, EUR 1.4 MIL, 36 months, Strengthening Research & Innovation on Artificial Intelligence at TUIASI. WP collaborating partner.

Selected publications:

- Knox, B. J., Lugo, R.G., Sütterlin, S. (accepted for publication in Handbook of Research on Artificial Iintelligence, Innovation and Entrepreneurship.) "Cognitive Agility for Improved Understanding and Self-Governance: A Human-Centric AI Enabler"
- Matthew Canham, Stefan Sütterlin, Torvald F. Ask, Benjamin J. Knox, Lauren Glenister, and Ricardo G. Lugo (accepted for publication at the Journal of Information Warfare) "Ambiguous Self-Induced Disinformation (ASID) Attacks: Weaponizing a Cognitive Deficiency".
- Sütterlin, Stefan; Knox, Benjamin James; Maennel, Kaie; Canham, Matthew & Lugo, Ricardo Gregorio (2021). On the Relationship Between Health Sectors Digitalization and Sustainable Health Goals: A Cyber Security Perspective. I Flahault, Antoine (Red.), Transitioning to Good Health and Well-Being. MDPI. ISSN 978-3-03897-864-0.
- Ask T.F., Lugo R.G., Knox B.J., Sütterlin S. (2021) Human-Human Communication in Cyber Threat Situations: A Systematic Review. In: Stephanidis C. et al. (eds) HCI International 2021 - Late Breaking Papers: Cognition, Inclusion, Learning, and Culture. HCII 2021. Lecture Notes in Computer Science, vol 13096. Springer, Cham. https://doi.org/10.1007/978-3-030-90328-2_2
- Alendal, Gunnar; Axelsson, Stefan; Dyrkolbotn, Geir Olav. (2021) Chip chop — smashing the mobile phone secure chip for fun and digital forensics. Forensic Science International: Digital Investigation. vol. 37.
- Alendal, Gunnar; Axelsson, Stefan; Dyrkolbotn, Geir Olav. (2021) Leveraging The USB Power Delivery Implementation For Digital Forensic Acquisition.IFIP Advances in Information and Communication Technology. vol. 612.
- Alendal, Gunnar; Dyrkolbotn, Geir Olav; Axelsson, Stefan. (2021) Digital Forensic Acquisition Kill Chain – Analysis and Demonstration. IFIP Advances in Information and Communication Technology. vol. 612.

Education:

- 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:

- GOD: Cyber Tactics
- GOD: Cyber Intel
- GOD: Reverse Engineering
- BK & GOD: Support to Forsvarets Høgskole
- BK: Summer Course Supervisor. University of California Berkeley (UC Berkeley). Haas School of Business & Jacobs Institute for Design Innovation Summer Course "Design and Cybersecurity"

Graduated PhD candidates (& under supervision):

- Torvald Fossen Ask. PhD finansiert av NFR ACDICOM project: 2021-2024. Hovedveileder. «Cognitive engineering approaches to improving human-human communication in cyber threat situations».
- Håvard Ofte. Nærings PhD NC-Spectrum, NORCIS: 2022-2025. Medveileder. «Situation awareness in Virtual Security Operations Centers»
- Sergii Banin (2016–2020), "Applying low-level features for malware dissection and detection", hovedveileder Geir Olav Dyrkolbotn, medveileder Katrin Franke. Stillingen er finansiert av CCIS (JBD). Submitting Q2 2022
- Gunnar Alendal (2016-2020), "Security vulnerability research for use in digital forensics", hovedveileder Geir Olav Dyrkolbotn, medveiledere Stefan Axelsson, Lasse Øverlier og Katrin Franke. Stillingen er finansiert gjennom forskningsrådets ArsForensica 248094/O70, ledet av Katrin Franke. Defence March 25th 2022
- Martin Karresand (2017–2019), "Utnytte iboende data strukturer for digital etterforskning ", hovedveileder Geir Olav Dyrkolbotn, medveileder Stefan Axelsson, Stillingen er finansiert av CCIS (JBD). Submitting Q1 2022
- Rune Nordviken (2018–2024, "File system metadata as an investigative approach", Hovedveilder Stefan Axelsson, medveileder Fergus Toolan og Geir Olav Dyrkolbotn. Stillingen er finansiert av PHS.
- André Jung Waltoft-Olsen (2021-2024, «Revealing Hardware Trojans in the Power Supply System», Hovedveileder Lasse Øverlier, medveildeder Geir Olav Dyrkolbotn. Nærings PhD StatNett

Graduated supervised MSc theses (& under supervision):

- Under supervision:
  Tiril Tinde (Experienced based Master > blir ferdig I 2022): BK
  Fanny Sunde (Experienced based Master > blir ferdig I 2022): BK & GOD
  Mikkel Amundsen (Experienced based Master > blir ferdig I 2022): BK & GOD
  Kristian Kastet (Experienced based Master > blir ferdig I 2022): BK
  Kristian Wrali (Experienced based Master > blir ferdig I 2022): BK
  Aleksander Bjørkhaug, «Finding Educationally friendly malware»
  Tormod Lien, "Hunting malicious scripts using machine learning"
  Alexander Daniel Forfot, "Exploring the PE header and the Rich header for effective Malware Classification and Triage"
  Robin Berg Jønsson, "Detecting packed and encrypted malware samples using Static Malware-as-Image Network Analysis (STAMINA)"
  Mats Authen, "Detecting PowerShell obfuscation using machine learning"

Lifelong learning activities:

- Cyber Tactics
- Cyber Intel

Dissemination activities:

Organized Events, Conferences and workshops:

- GOD: Malware Forum (Nov 2021): Chair
- BK: Board Member/Session Chair: Human Computer Interaction International, HCII (Augmented Cognition), (July 2021).
- BK: Exploiting Human Psychological Vulnerabilities Through Cyberspace, Forsvarets Cyber Power Conference, Norway. (Sept, 2021)
- BK: The Human Factors, Norwegian Information Security Forum (ISF). (Sept, 2021).

Interdisciplinarity:

- Utredning på oppdrag fra Forsvarsdepartementet, L. Onarheim Bergsj., G. Dyrkolbotn, M. Thorseth, S., Wolthusen (Ed.), L. Øverlier, L. Berg, C. Bendiksen «DIGITALETISKE TRUSLER I FORSVARSEKTOREN En trussel mot demokratiet»

7. Information Security Management and Privacy management

Group leader:
Professor
Professor Stewart Kowalski

The activities of Information Security and Privacy Management group provide theoretical, empirical and clinical research results to modeling, measurement and management of information security. This knowledge is applicable to the community by answering questions on the site and come up with solutions to problems.

The group has a special responsibility towards NTNU´s course of study at Masters level in the field. The research by the group helps with a wide range of results on socio-technical system security, covering the social, psychological, legal, ethical, cultural, political and rhetorical education aspect. The group also covers the technical aspect of cyber and information security management.

Research in the group centers along 3 major themes: modeling, measuring, and managing. Theoretical and empirical research is carried out on information security management problems and solutions. Research work is also carried out in the area of security and privacy metrics which also included governance and compliance issues. Action and applied research is performed in the group to describe and understand the management practice used today and to make suggestion how they can be improved through evidence based measures.

Members of the group:

1. Stewart Kowalski
2. Erjon Zoto
3. Grethe Østby
4. Mazaher Kianpour
5. Gaute Wangen

Associate Members

1. Richard Mcevoy

Collaboration and collaboration partners:

1. Innlandet Hospital Trust
2. Southern and Eastern Norway Regional Health
3. Direktoratet for Samfunnsikkerhet og Beredskap
4. Norwegian Digitalization Agency
5. NSM (National Security Authority)
6. NorSIS
7. (Deloitte AS) Non-CCIS
8. Østre Toten municipality
9. Gjøvik municipality
10. 1Lier municipality

Main research result:

Ongoing projects:

Ovelse.no

– Plattformen ovelse.no eies av Direktoratet for samfunnssikkerhet og beredskap (DSB), og driftes av Norwegian Cyber Range ved Norges teknisk-naturvitenskapelige universitet (NTNU). Øvelser for bedre digital sikkerhet omfatter alle scenarioene på denne plattformen, og disse er utviklet i et samarbeid mellom DSB, NTNU, NorSIS, Digitaliseringsdirektoratet og Nasjonal sikkerhetsmyndighet (NSM).

DIGSAM-project

– https://ehealthresearch.no/en/projects/digsam-digital-sikkerhet-i-helse-og-sosialfag
– Hovedmålet med prosjektet er å sørge for at alle Norges kandidater i helse- og sosialfaglige utdanninger, gjennom et samstemt og kvalitetssikkert undervisningsopplegg, tilegner seg kompetanse og oppnår læringsutbyttet i digital sikkerhet, og at alle undervisere i helse- og sosialfaglige utdanninger skal ha mulighet til å tilegne seg kompetanse i digital sikkerhet.

Multi-university Team 9/12 Challenge Geneva
https://www.gcsp.ch/events/cyber-912-strategy-challenge-2021
Mazaher Kianpour lead a Multi-University Team University of Oslo, Lund University in Sweden and to the second round in the annual RISE Sweden, and NTNU competed in the Cyber 9/12
Full-Stack Exercises (Cyber Ranges Exercise)

- Preparation for exercises
- Crisis management analysis'
- Scenario building based on historical events
- Execution of exercises - EXCON-build
- Information sharing (escalation and deescalation of information in infosec crisis)

Selected publications:

– Østby, Grethe; Kowalski, Stewart James. (2021) A case study of a municipality phishing attack measures - towards a socio-technical incident **management** framework. CEUR Workshop Proceedings. vol. 3016.
– Kianpour, Mazaher, Stewart J. Kowalski, and Harald Øverby. "Systematically Understanding Cybersecurity Economics: A Survey." Sustainability 13, no. 24 (2021): 13677.
– Richard McEvoy, Stewart Kowalski: **Consulting the Oracle at Delphi - Combining Risk I and Risk in cyber security.** STPIS 2021: 22–31.

Innovation:

Ongoing innovation activities: (Pre-Cyber Range Training and Educational Assessment and Training Gap analysis (TTO – Disclosure of Innovation/ Invention).

Education:

IMT4115 – Introduction to Information Security Management
DCSG1002 – Cyber security and teamwork
DCST2004 – Digital service management
IIKG1001 – Cyber security and computer networks
IMT4128 – Socio-technical Systems Enabled Crime
CSG2005 – Risk Management
IMT4016 – Experts in Teamwork – Digital Communities and Welfare

Activity:

– 9/12 Challenge
– Full Stack Exercise
– Evaluation ovelse.no
– Evaluation cyber-attack Østre Toten municipality
– New collaboration with Ahus hospital in regards to escalation maturity modeling and cyber range activities.

Graduated PhD candidates:
Grethe Østby

– June 2021 – Midterm reviewed approved, planned defense Spring 2023

Mazaher Kianour

– current in last term working on summary chapter, planned thesis defense in June 2022

Supervised MSc theses:

– Rune Schumann - The Norwegian Infection-Tracing App analyzed from a Socio-Techincal Perspective.

Lifelong learning activities:
– Lectures at BI
– NTNU Videre Lectures

Dissemination activities:

Organized Events, Conferences and workshops:
– "Later in the Bar" A Zero Day Critical Infrastructure Multiplayer Online Game at the end of the NORDICS Dec 8th Conference was held with 10 participants from Norway, Sweden, England.

Interdisciplinarity:

NTNU departments/disciplines that we have worked together with to apply for funding over the year 2021.
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)

8. System Security

Group leader:
Professor Christian Johansen

The mission of the System Security research group (S2G) is to ensure that systems in our society are resilient against cyber-attacks and fulfill essential security and privacy requirements. The Systems we focus our research on go beyond the classic ICT perspective and include societal, economical, and human factors.

Research objectives

Develop models, methods, techniques and tools that can be used for:

- building secure systems
- evaluating and assessing the security level of systems
- enhancing the security of systems
- training and educating users and organization to understand and apply systems and adversarial thinking

The research activities of our group are application oriented in nature and are conducted in different areas including secure software development lifecycle, security assurance and maturity modeling, socio-technical systems analysis, vulnerability, threat and risk analysis, DevOps security, model-driven security, and information security economics.

Members of the group:

1. Christian Johansen (**new** head of group)
2. Laszlo Erdodi (**new** member as Assoc.Prof.)
3. Erik Hjelmås, førsteamanuensis
4. Basel Katt (**new** Leader of the IS discipline this year)
5. Mazaher Kianpour
6. Stewart James Kowalski
7. Hanno Langweg
8. Eigil Obrestad
9. Ankur Shukla
10. Gabriel Andy Szalkowski (**new** PhD student)
11. Muhammad Mudassar Yamin
12. Erjon Zoto
13. Grethe Østby
14. Harald Øverby

Collaboration and collaboration partners:

1. Multiple new collaborations with industry initiated through the NCR activities.
2. New research collaboration with Luxembourg Uni. who are strong, e.g., in security for space satellites.
3. Strengthened collaborations with Forsvarets etterretningsskole.

Main research result:

Ongoing projects:

– Participate strong in managing the events held i the Norwegian Cyber Range
– Participate in the new project Open Cyber Range (financed by EEA)
– Participate in the new project AI-Based Scenario Management for Cyber Range Training (financed by NFR)

Submitted proposals:

– Several applications were made by different group members, but we did not keep track of them. Selected publications:
– The group has published multiple journal articles, besides contributions to conferences and workshops. Most prestigious are:
– Paper published in NSD level 2 Formal Methods in System Design journal from Springer in collaboration with SINTEF, UiO, and Chalmers University (https://doi.org/10.1007/s10703-021-00368-2)
– 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 (https://doi.org/10.1016/j.cose.2021.102450)
– Paper published in Elsevier's Journal of Information Security and Applications which is the top journal in applications of security in Google Scholar (https://doi.org/10.1016/j.jisa.2020.102722)
– Paper published in Springer's journal AI & Society in collaboration with UiO and Forsvarets etterretningsskole (https://doi.org/10.1007/s00146-021-01328-4)

Innovation:

– One new startup is in the process of being establishing together with NTNU-TTO (with Basel as main contact point)

Education:

Activity:

– Started the S2G Playground with CTF ethical hacking bi-weekly events for all NTNU students in both Gjøvik and Trondheim campuses.
– Teaching many courses at all levels, for example on Software Security; Cyber security and computer networks; Operating systems; or Information Security Management.

Lifelong learning activities:

– Involved in one large project proposal focused on Lifelong learning in security.
– Introduced topics on Sustainability in several courses.
– Involved in (re-)training security to professionals coming from industry

Dissemination activities:

Organized Events, Conferences and workshops:

– Organized a Seminar on Cyber Ranges with international invited speakers.
– Organized bi-weekly CFT events part of the S2G Playground every semester, sometimes also collaborating with the student organization.
– Involved in the organization of Hackcon - The Norwegian Cyber Security Convention (which attracts 400+ participants from all sectors).

Interdisciplinarity:
The group has continued to focus on Cyber Ranges but takes a broader view, including not only technologies for use in a Cyber Range but also adds methodological and human aspects.

The research publications show the breadth of research output, e.g., within AI and Society, AI and cybersecurity, formal methods for security, or verification of critical systems, besides traditional security topics where we have always been active.

NTNU CCIS sine 59 partnere pr 1. mars 2022 (Forsvaret høgskole, Cyberingeniørskolen er en partner):