



# 2015

ÅRSRAPPORT

---

CENTER FOR CYBER AND INFORMATION SECURITY

Gjøvik, 21.03.16

# ØKT KUNNSKAP FOR ET SIKRERE SAMFUNN

CCIS skal styrke samfunnets kompetanse og ferdigheter til å beskytte mot, oppdage, respondere på og etterforske kriminelle handlinger som skjer ved bruk av informasjons- og kommunikasjonsteknologi.

# INNHOOLD

<b>INNLEDNING.....</b>	<b>5</b>
<b>STYRELEDERS OG DIREKTØRS BERETNING .....</b>	<b>6</b>
Oppstartsåret 2015 .....	6
Utvikling av forskning og utdanning innen cyber- og informasjonssikkerhet i Norge .....	6
Faglig utvikling.....	6
Fusjon med NTNU.....	6
Styrets arbeid .....	9
Økonomisk utvikling .....	9
Veien videre.....	9
Regnskapsrapport for 2015 .....	10
Internasjonalt og nasjonalt samarbeid .....	11
Styrking av regional kompetansebygging .....	11
Innovasjon.....	11
Partnere .....	11
Forskning.....	12
Utdanning .....	12
Administrasjon og organisering.....	13
<b>FAGGRUPPE FOR TESTIMON FORENSICS.....</b>	<b>15</b>
Faggruppens visjon .....	15
Samarbeid.....	15
Forskningsprosjekter .....	16
Vitenskapelige publikasjoner .....	17
Viktige møter og aktiviteter.....	18
Faggruppens medlemmer .....	19
<b>FAGGRUPPE FOR SIKKER OG ROBUST KRITISK INFRASTRUKTUR.....</b>	<b>21</b>
Faggruppens visjon .....	21
Partnere .....	21
Videreutvikling av faggruppen.....	21
Strategisk samarbeid.....	21
Forskningsprosjekter .....	21
Vitenskapelige publikasjoner .....	21
Viktige møter og aktiviteter i 2015 .....	22
Faggruppens medlemmer .....	23
<b>FAGGRUPPE FOR CYBERFORSVAR .....</b>	<b>24</b>
Faggruppens visjon .....	24
Forskere.....	25
Videreutvikling av faggruppen.....	25
Strategiske samarbeidspartnere og videre samarbeid .....	25
Forsknings- og utdanningsaktiviteter .....	25
Viktige møter og aktiviteter i 2015 .....	25
<b>FAGGRUPPE FOR BIOMETRI.....</b>	<b>27</b>
Faggruppens visjon .....	27
Videreutvikling av faggruppen.....	27
Strategisk samarbeid.....	27
Forskningsprosjekter .....	27
Samarbeid.....	28
Viktige møter og aktiviteter i 2015 .....	28
Faggruppens medlemmer .....	29
<b>FAGGRUPPE FOR PERSONVERN OG INFORMASJONSSIKKERHETSLEDELSE.....</b>	<b>31</b>
Faggruppens visjon .....	31
Strategisk samarbeid .....	31
Forskningsprosjekter .....	31
Vitenskapelige publikasjoner .....	31
Faggruppens medlemmer .....	31



# INNLEDNING

Center for Cyber and Information Security (CCIS) er et nasjonalt senter for forskning, utdanning og kompetansebygging innen cyber- og informasjonssikkerhet. Senterets mandat er å styrke samfunnets kompetanse og ferdigheter når det gjelder å beskytte mot, oppdage, respondere på og etterforske kriminelle handlinger som skjer ved bruk av teknologi tilknyttet cyber- og informasjonssikkerhet.

I et komplekst samfunn med stort behov for helhetlig kunnskap om cyber- og informasjonssikkerhet svarer CCIS på disse behovene på nasjonalt nivå, i samfunnet og hos våre CCIS-partnere. Kunnskapsutviklingen ved CCIS har langsiktige perspektiver – nasjonalt og globalt – for økt utdanning, forskning og formidling innen feltet cyber- og informasjonssikkerhet. Med et trusselbilde som hurtig forandrer seg, økes og endres behovet for kapasitet og kunnskap fort-

løpende. Samtidig som forskning og utdanning på området har en tidløs dimensjon må den holde tritt med denne utviklingen. CCIS skal bygge en mer effektiv samhandling og utveksling av kunnskap både i offentlig og privat sektor. CCIS møter utfordringene samfunnet står overfor, ved å forene partnere fra privat og offentlig sektor med akademia. CCIS bestod i 2015 av 25 partnere.

CCIS står for en langsiktig kunnskapsutvikling ved å etablere og videreutvikle relevante studier og å bygge miljøer som fokuserer både på grunnforskning og anvendt forskning. Forskningen og utdanningen har et tverrfaglig fokus. CCIS har som mål å bli et av de fremste akademiske forsknings- og utdanningsmiljøene innen cyber- og informasjonssikkerhet i Europa. CCIS er en nasjonal kunnskapsressurs med sterkt internasjonalt samarbeid.

---

Med et trusselbilde som hurtig forandrer seg, økes og endres behovet for kapasitet og kunnskap fortløpende.

---



Bak fra venstre: Rune Fløisbønn, Tor Tanke Holm, Mona Strøm Arnøy, Tønnes Ingebrigtsen, Ingeborg Dårflot og Erik Hjelmås  
Foran fra venstre: Rune Fromreide Sommer, Morten Irgens og Hanne Tangen Nilsen

# STYRELEDERS OG DIREKTØRS BERETNING

Arbeidet ved CCIS har i 2015 vært preget av prosessen frem mot fusjonen med NTNU som trådte i kraft fra 1. januar 2016.

## Oppstartsåret 2015

Center for Cyber and Information Security, CCIS, ble innviet i august 2014 og etablert som et senter med 25 partnere og Høgskolen i Gjøvik som vertsinstitusjon. 2015 var CCIS sitt første hele driftsår, et år med flere viktige milepæler for senterets videre utvikling. Senterets første ordentlige styre tok over ansvaret etter interimstyret og Sofie Nystrøm ble ansatt som direktør. Nystrøm gikk inn i oppgaven med å sikre lang-siktig basisfinansiering for senteret og stake ut den strategiske retningen for CCIS i samarbeid med dets partnere. Hun var i denne perioden også medlem av Det digitale sårbarhetsutvalget<sup>1</sup> som i sin utredning<sup>2</sup> trekker fram CCIS som en viktig nasjonal ressurs. Senteret har fokusert på ansettelse av vitenskapelige ansatte i 2015 i tillegg til å ha fått nye partnere.

CCIS har siden innvielsen gått fra etableringsfasen til en mer operasjonell fase. Organisasjonen har fått finansielle rammer for senterets drift på plass og blitt styrket med viktig nøkkelpersonell både innen ledelse og forskning.

## Utvikling av forskning og utdanning innen cyber- og informasjonssikkerhet i Norge

På flere måter ble regjeringens verktøy for kunnskapsutvikling og kunnskapsformidling tydeligere i året som gikk. Kunnskapsminister Røe Isaksen besøkte Høgskolen i Gjøvik og CCIS to ganger, Forskningsrådet etablerte et tydeligere program for prosjektfinansiering innen informasjonssikkerhet, Norsk senter for informasjonssikring (NorSIS) flyttet inn sammen med CCIS, og Høgskolen i Gjøvik ble overtatt av NTNU hvor et av målene er å koordinere og forsterke informasjonssikkerhetsforskningen.

Nasjonalt har to forskningssentra etablert seg, CCIS og Research Center for Information and

Communication Security (Simula@UiB). Simula@UiB ble etablert høsten 2015 av Universitetet i Bergen og Simula Research og utfører forskning på sikre IKT-systemer, kryptologi og informasjonsteori for nettverk. Sentrene har komplementære forskningsområder og vil dekke de viktigste områdene innen informasjonssikkerhet de nærmeste årene.

## Faglig utvikling

Ved utgangen av 2015 er det 5 forskningsgrupper ved CCIS; 1) Biometri, 2) Cyberforsvar, 3) Kritisk infrastruktur, 4) Personvern og informasjonssikkerhetsledelse og 5) Testimon forensics. CCIS har fått bevilgning på til sammen 47 million kroner gjennom Norges Forskningsråd IKT-Pluss-program til forskningsprosjektene Ars Forensica og SWAN. CCIS har fått tilsagn på en brukerstyrt innovasjonsarena (BIA) søknad og denne koordineres av CCIS sin partner mnemonic. CCIS samarbeider med NISlab om ulike studieprogrammer innen bachelor-, master- og doktorgradsnivå.

## Fusjon med NTNU

Arbeidet ved CCIS har i 2015 vært preget av prosessen frem mot fusjonen med NTNU som trådte i kraft fra 1. januar 2016. NTNU vil gi CCIS flere ressurser, blant annet et meget sterkt internasjonalt nettverk, et kontor i Brussel som vil støtte EUs forskningsprosjekter, og flere forskere innen cyber- og informasjonssikkerhet. I tillegg vil CCIS tilføye NTNU Skandinavias største forsknings- og utdanningsmiljø innen fagområdet. CCIS blir ved fusjonen en betydelig leverandør av kompetanse innen cyber- og informasjonssikkerhet i Europa.

CCIS får ved fusjonen med NTNU tilgang til et stort akademisk nettverk, hvor CCIS i fremtiden kan trekke med seg de mest relevante faglige miljøene inn i aktivitetene i senteret. Det

<sup>1</sup> "Lysneutvalget" etter utvalgets leder, professor Olav Lysne.

<sup>2</sup> NOU 2015:13, «Digital sårbarhet – sikkert samfunn – Beskytte enkeltmennesker og samfunn i en digitalisert verden».



Morten Irgens  
Styreleder CCIS

Foto: Oda Hveem



Sofie Nystrøm  
Direktør CCIS

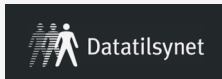
Foto: Oda Hveem



**KRIPOS**



**mnemonic**



**Eidsiva**

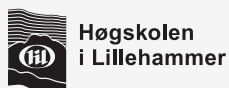
Nasjonalt ID-senter



**FFI** Forsvarets  
forskningsinstitutt  
Norwegian Defence Research Establishment



**Statnett**





foreligger et stort potensiale for uthenting av synergier som vil kunne oppstå i forbindelse med fusjonen.

Fusjonen med NTNU vil også styrke CCIS sitt allerede sterke omdømme, noe som har betydning for fremtidig gjennomslag for finansiering både gjennom nasjonale forskningsordninger ved Norges Forskningsråd og i Horisont 2020 (EUs rammeprogram for forskning).

I 2015 handlet fusjonsprosessen om å sikre stabil drift inn i et krevende overgangsår i 2016, og bygge opp grundig beslutningsfundament til styret i NTNU når det gjelder hvordan administrativ og faglig organisering av NTNU bør være (fakultetsstruktur). NTNU sitt styre besluttet i februar 2016 faglig organisering ned til nivå 2 og neste prosess handler om instituttorganisering (nivå 3), herunder senterstruktur, samt administrativ organisering. CCIS forventer en organisering som vil substansielt styrke og sikre senteret på lang sikt.

## Styrets arbeid

Styret i CCIS ble konstituert i styremøte 19.-20. mars, som var det første av tre styremøter i 2015. Styret har hatt flere saker oppe til drøfting, i tillegg til å initiere, bidra til gjennomføring, og vedta CCIS sin strategi for 2016-2020. Følgende representanter satt i CCIS sitt styre i 2015: Morten Irgens (NTNU) styreleder, Mona Strøm Arnøy (NSM) nestleder, Hanne Tangen Nilsen (Telenor), Rune Fløisbonn (Politidirektoratet), Rune Fromreide Sommer (Cyberforsvaret), Ingeborg Dårflot (Statkraft), Tor Tanke Holm (Politi høgskolen), Tønnes Ingebrigtsen (mnemonic) og Erik Hjelmås (CCIS-tilsatte).

## Økonomisk utvikling

I 2015 mottok mottok 3 millioner kroner fra Politidirektoratet og 1 million kroner fra Oppland Fylkeskommune.

CCIS jobber for å øke finansieringen både til CCIS og til utdanning og forskning innen informasjonssikkerhet generelt i Norge. Siden 2011 har CCIS arbeidet for å sikre basisfinansiering til senteret,

og fikk i april 2015 tilsagn fra Justis- og beredskapsdepartementet på 4 millioner kroner for inneværende år. På slutten av året fikk vi i tillegg den gode nyheten om at CCIS hadde blitt lagt inn i statsbudsjettet for 2016 med øremerkede midler på 5 millioner kroner fra Justis- og beredskapsdepartementet og 2 millioner kroner fra Helse- og omsorgsdepartementet. Styret og ledelsen i CCIS er takknemlige for tilliten og den sterke politisk støtte senteret har fått.

Komplekse og digitaliserte samfunn som Norge trenger solid og kontinuerlig kunnskapsutvikling og kompetanse innen informasjons- og cybersikkerhet. Digitaliseringen har nådd alle samfunnssektorer, og kunnskapsutviklingen må derfor være tverrfaglig og tverrsektoriell. CCIS ønsker derfor å samarbeide med flere departementer for å finne ut hvordan vi best kan møte behovene til kunnskap innenfor departementenes sektorer.

## Veien videre

Fjoråret var preget av stort tempo og utvikling, både når det gjelder økt forskningsaktivitet, nye studieprogrammer og rekrutteringer til senteret. Kommende år vil være preget av etableringsaktiviteter, men med et økt internasjonalt fokus og en vedvarende konsolidering av CCIS sine aktiviteter inn i NTNU.

CCIS vil de neste ti årene substansielt styrke sin leveranse av kunnskap for et sikrere samfunn og styrke sin forankring som et internasjonalt anerkjent forsknings- og kompetansesenter. Senteret vil fortsette å utvikle seg som en hovedleverandør av tverrfaglig kunnskap og kompetanse i cyber- og informasjonssikkerhet i Norge, og det sterkeste instrumentet for offentlig, privat og akademisk samarbeid innen problemområdet. Kilden til CCIS' sterke posisjon og utvikling er den unike støtten fra partnere og myndigheter.

Gjøvik, 7. mars 2016



Morten Irgens  
Styreleder CCIS



Sofie Nystrøm  
Direktør CCIS

## Regnskapsrapport for 2015

Regnskapsrapporten under viser inntektene og utgiftene til de øremerkede midlene til CCIS for regnskapsåret 2015. Oversikten inkluderer ikke noen av prosjektene eller inntektene til NISlab, som er en del av det felles fagmiljøet og som er beskrevet i de faglige delene av rapporten.

Kostnadsprofilen fremstår som noe spesiell i oppstartsåret. Senteret har vært under oppbygging i 2015 og den økonomiske profilen bærer preg av dette. I tillegg påvirker fusjonsprosessen med NTNU økonomisystemet og rutiner.

Finansieringskilde	Total	JD	POD	OFK	NFR
<b>Inntekter 2015</b>					
Overføringer udisponerte midler JD 2014	2 232 918	2 232 918			
Omdisponerte midler Politidirektoratet (POD)	1 800 000		1 800 000		
Bevilgning Justis- og beredskapsdep. ( JD )	4 000 000	4 000 000			
Oppland Fylkeskomm. (tilskudd driftsmidler)	2 000 000			2 000 000	
Statkraft (ressursmidler)	134 928				
Statnett (ressursmidler)	134 928				
NC Spectrum (ressursmidler)	78 000				
Periodiserte Inntekter Forskningsprosj. fra NFR	453 868				453 868
<b>Totale inntekter 2015</b>	<b>10 834 641</b>	<b>6 232 918</b>	<b>1 800 000</b>	<b>2 000 000</b>	<b>453 868</b>
<b>Utgifter 2015</b>					
Lønn strategiarbeid	1 301 233	1 301 233			
Lønn drifts- og forskningsadministrativt arbeid	1 336 663	551 573		785 091	
Lønn ansatte ressursavtaler	779 067		509 212		
Lønn forskningsaktiviteter	2 252 992	1 376 640	375 995		422 356
Konsulent- og juridisk bistand	547 475	547 475			
Seminar, møte og konferanseutgifter	571 240	454 479	11 185	105 576	
Andre driftskostnader	998 852	932 201		35 140	31 512
Investeringer	1 052 955	552 955	500 000		
<b>Totale utgifter 2015</b>	<b>8 840 478</b>	<b>5 716 556</b>	<b>1 396 392</b>	<b>925 807</b>	<b>453 868</b>
<b>Udisponerte midler overført 2016</b>	<b>1 994 163</b>	<b>516 362</b>	<b>403 608</b>	<b>1 074 193</b>	<b>0</b>

## Internasjonalt og nasjonalt samarbeid

CCIS ble i mai 2015 invitert til å bli rådgiver til EUROPOLs EC3 (European Cyber Crime Centre), som CCIS skrev en samarbeidsavtale med i 2014. Høsten 2015 ble CCIS invitert til og deltok ved INTERPOLs Global Complex for Innovation (IGCI) i Singapore. IGCI samler INTERPOLs fagkompetanse i digital etterforskning og datakriminalitet. CCIS sin målsetning er å sikre aktivt samarbeid også med INTERPOL. I tillegg til de som har gått inn som partnere i CCIS, samarbeider CCIS med en rekke nasjonale aktører om forskning, utdanning av PhD-kandidater, forskningsinfrastruktur og publikasjoner.

## Styrking av regional kompetansebygging

Innlandsutvalget leverte høsten 2015 sin rapport til næringsministeren. CCIS ble trukket frem som en av hovedsatsingene som utvalget foreslår for Innlandet: «Utvikle forskning og næringsutvikling innenfor informasjonssikkerhet i tilknytning til de ledende informasjonssikkerhetsmiljøene på Gjøvik og Forsvarets Ingeniørhøgskole på Jørstadmoen». Innlandsutvalgets mandat har vært å beskrive og vurdere relevante forhold for næringslivet i Innlandet, og foreslå tiltak som kan styrke næringsutviklingen, lønnsomme arbeidsplasser og verdiskaping i regionen. Direktør Sofie Nystrøm var til stede og presenterte CCIS da rapporten ble fremlagt.

## Innovasjon

CCIS har gjennom året hatt løpende drøftelser rundt innrettelsen av sitt innovasjonsarbeid. Senteret har etablert god kontakt med NTNU Technical Transfer Office (TTO) i tillegg til Innovasjon Norge i Oppland og Hedmark. CCIS vil fortsette dette utviklingsarbeidet og samarbeidet med NTNU TTO.

## Partnere

CCIS hadde 25 partnere fra privat og offentlig sektor samt academia, ved utgangen av 2015. Mot slutten av året resulterte samarbeidet med Datatilsynet at også de signerte konsortiumsavtalen og ble partner i CCIS.

### De 25 partnerne er:

Cyberforsvaret med Forsvarets Ingeniørhøgskole  
Datatilsynet  
Eidsiva  
Forsvarets Forskningsinstitutt  
Høgskolen i Gjøvik (nå NTNU)  
Høgskolen i Lillehammer  
IBM  
Kripos  
mnemonic  
Nasjonal Sikkerhetsmyndighet  
Nasjonalt ID-senter  
NC-Spectrum  
NorSIS  
Oppland Fylkeskommune  
Oslo Politidistrikt  
Politidirektoratet  
Politi høgskolen  
PricewaterhouseCoopers  
PST  
Statkraft  
Statnett  
Telenor  
Vestoppland Politidistrikt  
Watchcom Security Group AS  
Økokrim

Senterets sterke samarbeid med partnerne bidrar til utveksling av kompetanse mellom sektorer, virksomheter, academia, sentre og organisasjoner, og med nasjonale og internasjonale prosjekter. CCIS samarbeider med og bidrar også til organisasjoner som har som oppgave å informere og bevisstgjøre om sikkerhet. I tillegg bidrar CCIS til aktørens langsiktige strategier når det gjelder kompetanseutvikling og FoU-prosjekter.



CCIS utvikler  
anvendbar  
og relevant  
kunnskap  
nært knyttet  
til behovene  
og nytte-  
verdien for  
samfunnet.

## Forskning

CCIS samarbeider med og gjennom sine partnere for å videreutvikle forskningsevne og fagmiljøer i internasjonal toppklasse, med fagdisipliner som er relevant for partnerne og nasjonen. CCIS bidrar til internasjonalt samarbeid og er en kunnskap-snode i Europa. CCIS bidrar i tillegg til rekruttering til norske sikkerhetsutdanninger og –miljøer, ved å drive opplæring og etablere studieprogrammer av høy kvalitet og med stor samfunnsrelevans.

CCIS organiserer sin forskning i forskningsgrupper som vist nedenfor. I forskningen legges det stor vekt på den tverrfaglige dimensjonen. CCIS arbeider kontinuerlig med utvikling av sine forskningsgrupper. Detaljert informasjon om dette foreligger i rapportene fra hver enkelt forskningsgruppe.

- Testimon forensics
- Cyberforsvar
- Sikker og robust kritisk infrastruktur (CISR)
- Biometri
- Personvern og informasjonssikkerhetsledelse

## IKTPLUSS-programmet og finansiering fra Norges forskningsråd

CCIS har arbeidet strukturert og kontinuerlig med å skaffe prosjektf finansiering via Norges forskningsråd (Forskningsrådet) sine programmer. Man har fått gode resultater fra dette arbeidet. Fire store IKT-prosjekter er finansiert gjennom Forskningsrådets IKTPLUSS-program, to av dem ledet av CCIS med en bevilgning på henholdsvis 24 millioner kroner og 23 millioner kroner:

- “Large-scale Fraud Detection, Crime Investigation and Prevention - Ars Forensica”, ved CCIS Testimon Digital Forensics Research Group, ledet av HiG/NTNU Professor Katrin Franke.
- “Secure Access Control over Wide Area Network – SWAN”, ved HiG/NTNU Norwegian Biometrics Laboratory, ledet av Professor Christoph Busch.
- «Security in IoT for Smart Grids (IoTSec)», ledet av Universitetet i Oslo med bidrag fra Professor Einar Snekkenes, NTNU
- «Cryptographic Tools for Cloud Security», ledet av NTNU i Trondheim, ved Colin Boyd og Kristian Gjøsteen m.fl.

## Fokus på fremragende forskning ved CCIS

I 2015 søkte CCIS sammen med et konsortium bestående av Norwegian Information Security Laboratory (NISlab), the Norwegian Colour and Imaging Laboratory (Colorlab) fra Høgskolen i Gjøvik, og en rekke prominente representanter fra internasjonale forskningsinstitusjoner om finansiering fra Forskningsrådet for å etablere et Senter for Fremragende Forskning (SFF) i informasjonssikkerhet. Senteret vil, dersom det får finansiering, fokusere på bruk av bildeanalyse for informasjonssikkerhet.

## Forskerskolen COINS

COINS – Research School of Information Security er et samarbeid mellom NTNU i Gjøvik, Universitetet i Tromsø, Universitetet i Stavanger, Universitetet i Oslo, Universitetet i Bergen og Universitetet i Agder. Denne ledes av NTNU Gjøvik.

## Utdanning

Det er et substansielt underskudd i Norge og globalt på kompetanse innen cyber- og informasjonssikkerhet. CCIS utvikler anvendbar og relevant kunnskap nært knyttet til behovene og nytteverdien for samfunnet. Utdanningsprogrammene er under stadig utvikling og evaluering i samarbeid med CCIS sine partnere. Utdanningsprogrammene skal oppleves som relevante og i takt med utviklingen på området. Det er NISlab som leder og drifter studieprogrammene innen fagområdet.



## Studieprogrammer

I 2015 er det følgende studieprogrammer innen cyber- og informasjonssikkerhet:

Studieprogram	
Ph.D. in Information Security	Høgskolen i Gjøvik
M. Sc. in Information Security med studieretninger innen * Cyber Crime Forensics * Information Security Management * Technical Information Security	Høgskolen i Gjøvik
M.Sc. Applied Computer Science	Høgskolen i Gjøvik
Experience-based Master in Digital Forensics and Cybercrime Investigation	Høgskolen i Gjøvik og Politihøgskolen
B.Sc. in IT operations and Information Security	Høgskolen i Gjøvik
B.Sc. Telematics and Military Leadership	Forsvarets ingeniørhøgskole, Høgskolen i Gjøvik
B.Sc. Applied Computer Science	Høgskolen i Gjøvik
B.Sc. Software Engineering	Høgskolen i Gjøvik
B.Sc. Network Administration	Høgskolen i Gjøvik

Ved årsskiftet 2015-2016 var antallet Ph.D.-kandidater 40, hvorav 22 på informasjonssikkerhet og resten på Computer Science. I 2015 ble 5 Ph.D.-kandidater og 19 M.Sc.-kandidater uteksaminert. Av masterkandidatene var 10 innen *technical information security*, 6 innen *cybercrime forensics*, og 3 innen *information security management*.

### Etablering av CCIS Education Advisory Board

CCIS sitt styre besluttet høsten 2015 å etablere CCIS Education Advisory Board med oppstart primo 2016. Utdanningsrådets oppgave blir å komme med råd og innspill fra CCIS sine partnere til utviklingen av studieprogramporteføljen og studieprogrammene. Rådets arbeid skal bidra til å gjøre studieprogrammene hos CCIS' akademiske partnere mer relevante for CCIS sine partnere og samfunnet generelt.

### Administrasjon og organisering

Senteret var i 2015 administrativt bemannet med direktør Sofie Nystrøm og rådgiver Maria Henningsson. I tillegg benyttet CCIS en prosjektleder, Gry Helene Stavseng, som administrativ

støtte og prosjektstøtte. CCIS hadde tilgang til støttefunksjoner innen økonomi, HR og IT ved Høgskolen i Gjøvik. Stilling som seniorrådgiver ved CCIS ble lyst ut i 2015 og Hilmar P. Haraldsson ble tilsatt februar 2016.

CCIS samarbeider med partner Norsk Senter for informasjonssikring (NorSIS). I august 2015 ble NorSIS samlokalisert med CCIS og NISlab på Høgskolen i Gjøvik. Samlokaliseringen skaper et enda sterkere og mer mangfoldig informasjonssikkerhetsmiljø på campus. Et første resultat av det tette samarbeidet var gjennomføringen av den femte årlige konferansen for informasjonssikkerhet, avslutningskonferansen for nasjonal sikkerhetsmåned, SikkertNOK 2015. I tillegg vil dette skape bedre arena for samarbeid rundt Sikkerhetstoppmøtet.

I august 2015 ble NorSIS samlokalisert med CCIS og NISlab på Høgskolen i Gjøvik.



# FAGGRUPPE FOR TESTIMON FORENSICS

## Faggruppens visjon

CCIS Testimon Forensics Group, utviklet seg fra en akademisk forskningsgruppe etablert i september 2010, til et partnerskap og tett samarbeid mellom norske politimyndigheter og akademia ved Norwegian Information Security laboratory, Høgskolen i Gjøvik (HiG)<sup>3</sup>. Hovedaktørene i gruppen er Politidirektoratet (POD), Kripos, ØKOKRIM, Politihøgskolen (PHS), og regionale etater, dvs. Oslo og Innlandet Politidistrikt. En detaljert liste over medlemmene i gruppen er gitt nedenfor.

CCIS Testimon Forensics er et utdannings- og forskningsmiljø, med spesialisering innen digital etterforskning og computational forensics. Gruppen er ansvarlig for en masterspesialisering om digital forensics som en del av MSc i Information Security, som tilbys av Høgskolen i Gjøvik (NTNU)<sup>4</sup>. I tillegg tilbyr CCIS Testimon erfaringsbasert Master i Digital Forensics og Cybercrime Investigation i samarbeid med Politihøgskolen<sup>5</sup>.

## Samarbeid

CCIS Testimon har etablert et langsiktig samarbeid med Netherlands Forensics Institute (NFI) som gjelder Big-data Forensics og Forensics as a Service. NFI og CCIS signerte en samarbeidsavtale i Haag 28. september 2015<sup>6</sup>. Professor Zeno Geradts fra NFI holdt foredraget "Forensic utfordringer i store dataanalyser" som NISlecture hos CCIS i januar 2015<sup>7</sup>. Professor Katrin Franke holdt foredrag om "Digital Investigations Current and Future Needs" ved NFI, Nederland i mars 2015.

CCIS Testimon medvirket også til en avtale om operativt samarbeid og utveksling mellom Vestoppland politidistrikt og CCIS<sup>8</sup>. Medlem

av CCIS Testimon-gruppen, Christoffer V. Hallstensen bidrar med 20% av sin stilling til å utføre operasjonelle aktiviteter ved Vestoppland Politidistrikt, som nå er en del av Innlandet politidistrikt.

Medlem av Testimongruppen, førsteamanuensis Thomas Kemmerich, initierte og støttet samarbeidet om et erfaringsbasert Masterstudie i Digital Forensics and Cybercrime Investigation mellom Polizeiakademie Niedersachsen (PAN), Tyskland, Politihøgskolen i Oslo og Høgskolen i Gjøvik (NTNU). Dette førte til en utvidet samarbeidsavtale mellom PAN og Politihøgskolen i Oslo, inngått 1. september 2015.

CCIS Testimon ved professor Katrin Franke, har institusjonalisert et fruktbart samarbeid med det Dansk Brand- og sikringsteknisk Institut, Danmark (DBI) som innebærer digital etterforskning på "Darkweb". DBI og CCIS inngikk 26. august 2015 en strategisk samarbeidsavtale.

Testimon-medlem, førsteamanuensis Stefan Axelsson samarbeider tett med Blekinge Tekniska Högskola i Karlskrona, Sverige, der hans stilling er delfinansiert av BigData @ BTH-prosjektet<sup>9</sup>. Dette er et stort forskningsmiljøprosjekt finansiert gjennom KK-stiftelsen, med seks års varighet, og inkluderer flere seniorforskere, stipendiater og partnere fra næringslivet. Stefan Axelsson arbeider med partnerne Ericsson og Scorett AB og veileder Edgar Alonso Lopes-Rojas på området "Fraud and money laundering detection".

Professor Katrin Franke er tilknyttet University of Salford i Storbritannia som gjesteprofessor. Her bidrar hun til Marie Curie EU-prosjektet "Privacy-4Forensics" FP7-PEOPLE-2013-IIF (625402) som studerer utvikling av teknikker for beskyttelse av personvern i digital etterforskning.

<sup>3</sup> <https://ccis.no/research-groups/testimon-forensics/>.

<sup>4</sup> <http://tinyurl.com/oeevpwz>

<sup>5</sup> <http://tinyurl.com/ohrjlpz>

<sup>6</sup> <http://tinyurl.com/zbrz6j2>

<sup>7</sup> <http://tinyurl.com/qajtgsh>

<sup>8</sup> <http://tinyurl.com/pb4lauc>

<sup>9</sup> <http://tinyurl.com/zzkb8mc>

Norges Forskningsråd (Forskningsrådet) har gitt 24 millioner kroner til CCIS Testimon gjennom IKTPLUSS-programmet. "Ars Forensica"-prosjektet er knyttet til Testimongruppens forsknings-tema, med fokus på "Big-Data Forensics and Forensics as a Service" i perioden 2015 til 2019. Midlene vil hovedsakelig benyttes til syv PhD-forskere og 40% administrativ støtte. Disse arbeider sammen med medlemmer av CCIS Testimon-gruppen og norsk politi, dvs. POD, KRIPPOS, PHS, Økokrim og Oslo politidistrikt. Prosjektet ledes av Katrin Franke og innbefatter i tillegg et samarbeid med NFI om Hansken, en felles dataplattform<sup>10</sup>. Prosjektet omfatter en rekke internasjonalt anerkjente forskningsorganisasjoner, for eksempel United Nations Interregional Crime and Justice Research Institute i Italia. Mer informasjon om prosjektet nedenfor.

I tillegg er professor Inger Marie Sunde fra PHS involvert i IKTPLUSS-prosjektet "Signal" som ledes av Senter for Rettsinformatikk (SERI) ved Universitetet i Oslo. Inger Marie Sunde planlegger å bygge broer mellom disse to beslektede, ikke-overlappende prosjektene, som vil fremme tekno-juridisk forskning og føre til tettere samarbeid mellom CCIS og SERI i fremtiden.

Forskningsrådet har innvilget 50% finansiering av PhD-forsker Håkon Gunleifsen, gjennom Nærings-PhD-programmet og i samarbeid med CCIS næringsaktør Eidsiva. Gunleifsen veiledes av Thomas Kemmerich og Slobodan Petrovic. I tillegg har CCIS Testimon-gruppen fått en intern stipendiatstilling (KD-stipendiat).

Doktorgradskandidaten har nyansatt professor Stefan Axelsson som medveileder.

## Forskningsprosjekter

CCIS Testimon driver grunnforskning og anvendt forskning på vegne av politiet. Medlemmene i gruppen bidrar med casearbeid innen etterforskning, ekspertvitner og rådgivning i samarbeid med partnere, eksempelvis EC3 - Europol Cyber Crime Centre - AG Internet Security<sup>11</sup> og NRGD - Nederlands Register Gerechtelijk Deskundigen - Ministry of Security and Justice, Nederland<sup>12</sup>. Gruppens medlemmer er også involvert i nett-

verks- og samfunnsbyggende forskningsaktiviteter som konferanser, workshops, opplæring og foredrag. Eksempler på dette er International Workshop on Computational Forensics (IWCF), og the Technical Committee 6 on Computational Forensics, med støtte fra IAPR - International Association of Pattern Recognition<sup>13</sup>.

Forskningsagendaen til faggruppen Testimon Forensics, er i samsvar med politiets strategier, og fokuserer på de tre hovedtemaene:

- 1) Big-data Forensics and Forensic as a Service using secure computing infrastructure,
- 2) Cloud Forensics and Cybercrime Investigation, og
- 3) Mobile & Embedded Device Forensics (IOT, IOE).

Testimongruppen har vært involvert i flere forskningsøknader til nasjonale og europeiske bevilgningsmyndigheter. Fire større søknader har blitt levert:

- Norges forskningsråd, SFF IV – Senter for fremragende forskning - SFF, "Centre for Vision Security: Adaptive Security for ICT and Vision Systems"
- H2020-MSCA-ITN-EJD-2016, ESSENTIAL - Evolving Security Science through Networked Technologies, Information policy And Law"
- H2020-FCT-2015, FCT-01-2015, "FORensic Eco-system Solving National and International Crime (FORENSIC)"
- Norges forskningsråd, BIA - Brukerstyrt innovasjonsarena, "Delautomatisering av trusselinformasjon".

BIA-søknaden som koordineres av CCIS-næringslivspartner mnemonic AS, fikk tilsagn i tidlig 2016 om finansiering av en Postdoc-stilling i to år, og bidrar i tillegg med to seniorforskere sin arbeidstid, hver med 10% stilling.

De andre søknadene er under behandling.

## PhD-avhandlinger

- Sukalpa Chanda: "A Computational Forensic Approach to the Analysis of Questioned Document Fragments", Supervisors: Katrin Franke, Slobodan Petrovic, Umapada Pal<sup>14</sup>. Ytterligere informasjon i Vedlegg 1.

<sup>10</sup> <http://tinyurl.com/nz3a2st>

<sup>11</sup> <https://www.europol.europa.eu/ec3>

<sup>12</sup> <http://english.nrgd.nl>

<sup>13</sup> <http://tinyurl.com/psuwt8p>

<sup>14</sup> <http://tinyurl.com/pd8lx95>



## Pågående PhD-forskning

- Yi-Ching Liao (2013-2016): "Process Tracking for Forensic Readiness", Supervisors: Hanno Langweg, Katrin Franke
  - Andrii Shalaginov (2013-2017): "Application of soft computing for cybercrime investigation: an adaptive approach to big data analysis in agile environments", Supervisors: Katrin Franke, Slobodan Petrovic
  - Ambika Shrestha Chitrakar (2014-2017): "Approximate search techniques for big data analysis", Supervisors: Slobodan Petrovic, Katrin Franke
  - Dmytro Piatkivskiy (2015-2018): "Anonymity of the off-chain transactions in Bitcoin", Supervisors: Mariusz Nowostowski, Stefan Axelsson
- Ytterligere informasjon i Vedlegg 1.

## Avsluttede mastergrader

- Simen Bragen: "Malware Detection Through Opcode Sequence Analysis Using Machine Learning", Supervisor: Katrin Franke
  - Xiongwei Huang: "Understanding of Beaconing for Identifying Targeted Attack by Mining Large-Scale DNS Log Data", Supervisor: Andrii Shalaginov & Katrin Franke
  - Lars Strande Grini: "Feature Extraction and Static Analysis for Large-Scale Detection of Malware Types and Families", Supervisors: Andrii Shalaginov & Katrin Franke
  - Roar Lunde: "Hunting RATs with Differential Forensic Analysis of Memory Snapshot", Supervisor: Katrin Franke
  - Tommy Skaug: "Employing Hadoop Performance to Investigate High Resolution Network Data", Supervisor: Slobodan Petrovic
- Ytterligere informasjon i Vedlegg 1.

## Vitenskapelige publikasjoner

Lopez-Rojas, Edgar Alonso; Axelsson Stefan. *Using the RetSim Fraud Simulation Tool to Set Thresholds for Triage of Retail Fraud, Secure IT Systems*, Vol. 9417 of the series Lecture Notes in Computer Science, Springer, pp 156-171.

Chitrakar, Ambika S.; Petrović, Slobodan. *Approximate search with constraints on indels with application in SPAM filtering, Proceedings of Norwegian Information Security Conference (NISK-2015)*, Ålesund, Norway, November 23-25, 2015, pp. 22-33.

Shalaginov, Andrii; Franke, Katrin. *A New Method for an Optimal SOM Size Determination in Neuro-Fuzzy for the Digital Forensics Applica-*

*tions. I: Advances in Computational Intelligence; 13th International Work-Conference on Artificial Neural Networks, IWANN 2015, Palma de Mallorca, Spain, June 10-12, 2015. Proceedings, Part II.* Springer 2015 ISBN 978-3-319-19222-2. s. 549-563.

Shalaginov, Andrii; Franke, Katrin. *A new method of fuzzy patches construction in Neuro-Fuzzy for malware detection. I: Proceedings of the 2015 Conference of the International Fuzzy Systems Association and the European Society for Fuzzy Logic and Technology, Eusflat-15.* Atlantis Press 2015 ISBN 978-94-62520-77-6. s. 170-177

Shalaginov, Andrii; Franke, Katrin. *Automated generation of fuzzy rules from large-scale network traffic analysis in Digital Forensics Investigations. I: 2015 Seventh Intern. Conference of Soft Computing and Pattern Recognition (SoCPaR 2015).* IEEE Computer Society 2015 ISBN 978-1-4673-9360-7. s. 31-36

Shalaginov, Andrii; Franke, Katrin. *Generation of the human-understandable fuzzy rules from large-scale datasets for Digital Forensics applications using Neuro-Fuzzy.* NordSec; Poster, 2015-10-19 - 2015-10-21

Shalaginov, Andrii; Franke, Katrin. *Towards Improvement of Multinomial Classification Accuracy of Neuro-Fuzzy for Digital Forensics Applications. I: Hybrid Intelligent Systems - proceedings of 15th International Conference HIS 2015 on Hybrid Intelligent Systems.* Springer Publishing Company 2015 ISBN 978-3-319-27220-7. s. 199-210.

Shalaginov, Andrii; Franke, Katrin. *Intelligent generation of fuzzy rules for network firewalls based on the analysis of large-scale network traffic dumps,* International Journal of Hybrid Intelligent Systems, 2016 (ACCEPTED)

Shalaginov, Andrii; Franke, Katrin. *Multinomial classification of web attacks using improved fuzzy rules learning by Neuro-Fuzzy,* International Journal of Hybrid Intelligent Systems, 2016 (ACCEPTED)

Shalaginov, Andrii; Franke, Katrin; Huang, Xiongwei. *Malware Beaconing Detection by Mining Large-scale DNS Logs for Targeted Attack Identification,* 18th International Conference on Computational Intelligence in Security Information Systems, Paris, France, 2016 (ACCEPTED)

Liao, Yi-Ching. *A Survey of Software-Based String Matching Algorithms for Forensic Analysis*. Proceedings of the Conference on Digital Forensics, Security and Law 2015 p. 77-86.

Liao, Yi-Ching; Langweg, Hanno. *Developing Metrics for Surveillance Impact Assessment*. I: 39th IEEE Annual Computer Software and Applications Conference. IEEE Computer Society 2015 ISBN 978-1-4673-6564-2. p. 297-302.

Liao, Yi-Ching; Langweg, Hanno. *Events and causal factors charting of kernel traces for root cause analysis*. I: 20th IEEE Symposium on Computers and Communications (ISCC). IEEE Conference Proceedings 2015 ISBN 978-1-4673-7194-0. p. 245-250.

Himmel, Julia; Siebler, Nikolas; Laegeler, Felix; Grupe, Marco; Langweg, Hanno. *Privacy Points as a Method to Support Privacy Impact Assessments*. I: Proceedings of the 1st International Workshop on Technical and Legal Aspects of Data Privacy and Security (TELERISE 2015). IEEE Computer Society 2015 ISBN 978-1-4673-7097-4. p. 50-53.

Thomas Kemmerich, Vivek Agrawal, Carsten Momsen, *Secure Migration to Cloud – In and Out*, The Cloud Security Ecosystem, Elsevier 2015, ISBN 978-0-128-01595-7.

## Viktige møter og aktiviteter

- INTERPOL Cybercrime Expert Group meeting, Singapore, 31. november - 1. desember 2015, Katrin Franke deltok.
- Bitcoin Blockchain - A Dublin Hackathon Event, 6. - 9. november 2015, førsteamanuensis Mariusz Nowostawski og PhD-forsker Dmytro Piatkivskiy deltok på tredagersarrangementet, og opprettet en proof of concept-prototype som bruker Bitcoin blockchain-teknologi. De vant prisen for beste innovative ide i FinTech award av Fidelity Investments<sup>15</sup>.
- Francesca Bosco, United Nations Interregional Crime and Justice Research Institute (UNICRI), er gjesteforsker i ArsForensica-prosjektet og

deltok på avslutningskonferansen for nasjonal sikkerhetsmåned SikkertNOK, 29. oktober 2015<sup>16</sup>. Dagen etter ble det avholdt møte med ArsForensica teamet hos Kripos, der Inger Marie Sunde (PHS), Steffen Thorkildsen, Eirik Trønnes Hansen, Jens-Petter Sandvik (alle Kripos), Stefan Axelsson og Katrin Franke (CCIS) deltok<sup>17</sup>

- Europol-Interpol-konferanse, Haag i Nederland, 30. september til 1. oktober 2015, Katrin Franke deltok<sup>18</sup>
- Norges Forskningsråd-IKTPLUS-prosjektet - Ars Forensica: Kick-off møte 24. september 2015<sup>19,20</sup>
- COINS PhD-seminar, 18.-19. oktober, Andrii Shalaginov og Ambika Shrestha Chitrakar deltok
- 3rd National Workshop on Data Science (SweDS), 30. september - 1. oktober 2015, deltagere var Slobodan Petrovic, Stefan Axelsson, Andrii Shalaginov og Ambika Shrestha Chitrakar
- Norsk Crypto Seminar, 8. september 2015 i Trondheim, Slobodan Petrovic deltok
- Kick-off EU ICT4COP-prosjekt, Community-Based Policing and Post-Conflict Police Reform, Oscarsborg, 31. august - 2. september 2015, med Stefan Axelsson som deltager<sup>21</sup>
- Annual Big Data Value Association summit, Madrid, 17. - 19. juni 2015, med Slobodan Petrovic som deltager
- EUROPOL EC3 Advisory group møte, Katrin Franke deltok.
- Justis – og beredskapsdepartementet Forskningsstrategi - Bekjempelse av IKT-kriminalitet, Tiltak 11 – arbeidsgruppemøte, ledet av Inger Marie Sunde (PHS), og med Stefan Axelson og Katrin Franke (CCIS) som deltagere
- CCIS Testimon masterseminar hos Kripos, 10. juni 2015. Vertskap: Steffen Thorkildsen, Kripos.
- Månedlige Testimon-seminarer (siste torsdagen i hver måned), med deltagelse av CCIS Testimon sine vitenskapelige ansatte, PhD-forskere, masterstudenter innen digital etterforskning (første- og andre-året) og representanter fra norsk politi.

<sup>15</sup> <http://tinyurl.com/hmbb9at>

<sup>16</sup> <http://tinyurl.com/z7b55al>

<sup>17</sup> <https://ccis.no/interview-francesca-bosco/>

<sup>18</sup> <http://tinyurl.com/h2dpx8c>

<sup>19</sup> <http://tinyurl.com/h57k3yo>

<sup>20</sup> <http://tinyurl.com/gnceeka>

<sup>21</sup> <http://tinyurl.com/zpqd6ot>

## Faggruppens medlemmer

### Akademisk ansatte, fulltid

Stefan Axelsson, PhD, førsteamanuensis (POD/  
Politihøgskolen Professor)  
Katrín Franke, PhD, professor (POD/Økokrim  
Professor)  
Thomas Kemmerich, PhD, førsteamanuensis  
Carl Leichter, PhD (POD/Økokrim PostDoc)  
Slobodan Petrovic, PhD, Professor  
Utlyst stilling som Professor eller første-  
amanuensis i Digital Forensics / Computer,  
Mobile & Embedded Device Forensic (POD/Kripos  
Professor)

### Akademisk ansatte, deltid 20%

Christoffer V. Hallstensen, sikkerhetskonsulent –  
HiG (NTNU)  
Jeffery D. Hamm, Lecturer – Mandiant / FireEye  
Hanno Langweg, PhD, førsteamanuensis –  
Hochschule Konstanz, Germany  
Thomas Walmann, PhD, førsteamanuensis –  
Økokrim  
Andre Årnes, PhD, førsteamanuensis – Telenor

### Tilknyttede akademiske ressurser

Hallstein Hansen, PhD, Oslo Politidistrikt  
Basel Katt, PhD, førsteamanuensis  
Mariusz Nowostawski, PhD, førsteamanuensis  
Inger Marie Sunde, Professor, Politihøgskolen

### PhD-kandidater

Håkon Gunleifsen, Eidsiva  
Yi-Ching Liao  
Andrii Shalaginov  
Ambika Shrestha Chitrakar  
Dmytro Piatkivskyi  
Takashi Watanabe, Hitachi Central Research  
Laboratory, Tokyo, Japan  
7 x NN – Forskningsrådet - IKTPLUSS finansiering

### Administrativ støtte

Urszula Nowostawska, PhD, – 40% Forsknings-  
rådet -IKTPLUSS-finansiering + 20% POD-  
finansiering.

### Studenter

Ca 15 studenter per år velger spesialisering i  
'Digital Forensics' i Master-programmet.  
Ca 8 studenter per år velger spesialisering i etter-  
forskning i Master-programmet (startet 2014).





# FAGGRUPPE FOR SIKKER OG ROBUST KRITISK INFRASTRUKTUR

## Faggruppens visjon

I Norge regnes følgende som kritisk infrastruktur: Elkraft, kommunikasjonsnett, vann og avløps-systemer, transportsystemer, olje- og gassinfrastruktur og satellittkommunikasjon.

Faggruppens misjon er å støtte beredskapsakti-viteter og håndtering av sikkerhetshendelser hos aktører innen kritisk infrastruktur, både i privat og statlig/kommunal sektor.

Faggruppen vil fokusere på opplysning, undervisning, forskning og trening innen disse infrastrukturene. For tiden er elkraft vårt primære fokusområde.

## Partnere

Statkraft, Statnett, NC Spectrum, Telenor og Eidsiva.

## Videreutvikling av faggruppen

Faggruppens mål er å bli et av de ledende miljøene i Europa. Faggruppen jobber med å starte opp strategisk samarbeid med viktige aktører innenfor vårt felt, primært gjennom felles forskningsprosjekter. For å utvide gruppens forskningsarbeid på andre områder, ser man på muligheter til å utvide gruppen med flere forskere.

## Strategisk samarbeid

Faggruppen har startet opp strategisk samarbeid med Statkraft og Statnett (begge er partnere i CCIS).

## Forskningsprosjekter

### Finansiering og støtte

Norges Forskningsråd og South African Research Foundation støttet SmartPowerNet prosjekt (2014-2016) ved å finansiere tre doktorgrads-studenter som er ledet av Dr. Anne Kayem (University of Cape Town) og Prof. Stephen Wolthusen (NTNU). Doktorgradsstudentene er

Pacome Ambassa, Aderonke Sapere og Anesu Marufu samt masterstudent Heinrich Strauss i Cape Town. I tillegg er doktorgradsstudent Mr. Goitom Weldehawaryat involvert i faggruppens arbeid.

## Søknader forskningsprosjekter

Vision Security, SFF prosjektsøknad.

## Pågående forskning

Goitom Weldehawaryat arbeidet i 2015 på sitt forskningsområde og publiserte "Secure Distributed Demand Projection in Micro-Grids" på 2015 Global Information Infrastructure and Networking Symposium (IEEE GIIS 2015, Mexico City, Mexico) samt "Modelling Interdependencies over Incomplete Join Structures of Power Law Networks" (Proceedings of the 11th International Conference on Design of Reliable Communication Networks, IEEE DRCN 2015, Kansas City, MO, USA). Begge publikasjonene er en fortsettelse av hans arbeid på strukturanalyse og effektive distribuerte algoritmer i nettverkinfrastruktur.

I 2015 har Dimitra Anastasopoulou påbegynt sin doktorgradsstudier under støtte av KD etter at hun forsvarte sin masteroppgave innen informasjonssikkerhet hos Royal Holloway, University of London. Hun forsker på sikkerhet med spesielt fokus på deteksjon og håndtering av angrep på intelligente energisystemer som kombinerer kraft- og varmegenerasjon. Veiledere: Første-amanuensis Sule Yildirim-Yayilgan (information security), Professor Alemayehu Gebremedhin (electrical engineering) og Professor Stephen Wolthusen.

## Vitenskapelige publikasjoner

P. L. Ambassa, A.V.D.M. Kayem, S. Wolthusen, C. Meinel: "Privacy Violations in Constrained Micro-Grids". Proceedings of the 30th IEEE International Conference on Advanced Information Networking and Applications (AINA-2015, Crans-Montana, Switzerland)

A.V.D.M. Kayem, H. Strauss, S. Wolthusen, C. Meinel: "Key Management for Secure Demand

Data Communication in Constrained Micro-Grids”. Proceedings of the 30th IEEE International Conference on Advanced Information Networking and Applications (AINA-2015, Crans-Montana, Switzerland)

B. Schneidhofer, S. Wolthusen: ”Multi-Graph Critical Infrastructure Model and Vulnerability Analysis”. Proc. Tenth Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection (Arlington, VA, USA, 2016) – *accepted for publication*.

A. Baiocco, S. Wolthusen: ”Delay and Jitter Attacks on Hierarchical State Estimation”. In Proc. 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm 2015, Miami, FL, USA, Nov. 2015).

Pacome L. Ambassa, Stephen D. Wolthusen, Anne V.D.M. Kayem, Christoph Meinel, ”Robust Snapshot Algorithm for Power Consumption Monitoring in Computationally Constrained Micro-Grids”, in Proceedings of IEEE PES Innovative Smart Grid Technologies Asia Conference 2015.

Goitom K. Weldehawaryat, Stephen D. Wolthusen, ”Secure Distributed Demand Projection in Micro-Grids”, in Proceedings of Global Information Infrastructure and Networking Symposium 2015.

Anesu Marufu, Anne Kayem and Stephen Wolthusen, ”A Distributed Continuous Double Auction Framework for Resource Constrained Microgrids”, in Proceedings of the 10th International Conference on Critical Information Infrastructures Security (CRITIS 2015).

Pacome L. Ambassa, Anne V. D. M. Kayem, Stephen D. Wolthusen, Christoph Meinel, ”Secure and Reliable Power Consumption Monitoring in Untrustworthy Micro-Grids”, in Proceedings of the International Conference on Future Network Systems and Security 2015.

György Kálmán, Security Implications of Software Defined Networking in Industrial Control Systems, in Proceedings of the 10th International Multi-Conference on Computing in the Global Information Technology 2015.

S. K. Katsikas and A.B. Sideridis (Eds.), ”E-Democracy – Citizen Rights in the World of the New Computing Paradigms”, Communications in Computer and Information Science, Springer, 2015.

N. Pitropakis, S. Katsikas and C. Lambrinouidakis, ”Cloud Security, Privacy and Trust Baselines”, in J. Vacca (Ed.), Cloud Computing Security: Foundations and Challenges, Morgan Kaufmann, 2015.

A. Michota, S. Katsikas, ”Compliance of the LinkedIn privacy policy with the principles of the ISO 29100:2011 standard”, in B. Boualem et al. (Eds.), Web Information Systems Engineering – WISE 2014 Workshops, 15th International Workshops IWCSN 2014, Org2 2014, PCS 2014, and QUAT 2014, Thessaloniki, Greece, October 12-14, 2014, Revised Selected Papers, Org2 Workshop - Towards Organization 2.0: Advancements in Enterprise Social Networks, pp. 1–12, 2015.

V. Anastopoulos and S. Katsikas, ”A Methodology for Building a Log Management Infrastructure”, in Proceedings, IEEE International Symposium on Signal Processing and Information Technology (ISSPIT 2014), pp. 000301-000306, DOI: 10.1109/ISSPIT.2014.7300604, 2015.

E. Darra, C. Skouloudi and S.K. Katsikas, ”A Simulation Platform for Evaluating DoS Attacks in Wireless Sensor Networks”, in Proceedings, 19th Panhellenic Conference on Informatics (PCI 2015), doi:10.1145/2801948.2801949, 2015.

A. Michota and S.K. Katsikas, ”Designing a Seamless Privacy Policy for Social Networks”, in Proceedings, 19th Panhellenic Conference on Informatics (PCI 2015), doi: 10.1145/2801948.2801998, 2015.

A. Michota and S.K. Katsikas, ”Tagged Data Breaches in Online Social Networks”, in Proceedings, 6th International Conference on e-Democracy (e-Democracy 2015), Athens, Greece, pp. 95-106, 2015.

## Viktige møter og aktiviteter i 2015

Innenfor SmartPowerNet-prosjektet (ledet av Professor Wolthusen), har Professor Anne Kayem fra University of Cape Town vært gjesteforsker hos CCIS i september og oktober 2014. Dr. Wolthusen hadde et tilsvarende opphold hos University of Cape Town i desember 2014. Han var også bi-veileder av masterstudenter Anesu Marufu og Pacome Landry Ambassa i løpet av april og mai i 2015.

Professor Katsikas var co-chair på den første workshopen for Security of Cyber Physical Systems (WOS-CPS 2015) i Wien, Østerrike i

september 2015, og også 10th International Conference on Risks and Security of Internet and Systems i Mytilene, Hellas, samt 6th International Conference on e-Democracy (e-Democracy 2015), Aten. Han er medlem av styringskomiteen til konferanseserien ESORICS og International conference on cryptography and information security in Balkan (BalkanCryptSec).

Professor Wolthusen har vært programkomité co-chair (sammen med E. Rome fra Fraunhofer IAIS, Tyskland og Marianthi Theocharidou fra European Commission Joint Research Centre, Italia) av CRITIS 2015, og han er også medlem av styringskomiteen til konferanseserien.

Gruppemedlemmer er også synlige som programkomitémedlemmer på forskjellige konferanser og også som medlemmer av forskjellige rådgivende miljøer.

## **Faggruppens medlemmer**

### **Akademisk ansatte, fulltid**

Professor Sokratis K. Katsikas  
Professor Stephen Wolthusen

### **Akademisk ansatte, deltid**

Førsteamanuensis. Siv Hilde Houmb;  
Professor Bernhard Hämmerli  
Dr. Richard McEvoy

### **Postdocs**

Dr. György Kálmán

### **PhD-kandidater**

Goitom Weldehawaryat  
Dimitra Anastasopoulou

### **Administrativ støtte**

Faggruppen har administrativ støtte fra CCIS sin ledelse og generelle administrasjonsstab.





# FAGGRUPPE FOR CYBERFORSVAR

## Faggruppens visjon

Samfunnet går gjennom en økt digitalisering, noe World Economic Forum har anslått gir en 10% årlig økning i Norges brutto nasjonalprodukt (BNP). Denne velferdsøkningen har også en bakside, nemlig en kraftig økning i cyberkriminalitet, cyberspionasje og cyberangrep.

En av konsekvensene er at offentlige og private bedrifter ser seg nødt til å etablere team for å håndtere angrepene, f.eks. SOC, CERT eller CSIRT. En rask økning i antall team gir stor variasjon i kvalitet og fokus. En vanlig fremgangsmåte er å fokusere på årsaken til hendelsen (hvilken malware ble vi infisert av, hvilken server gikk ned etc.) og rette feilen hurtigst mulig.

Profesjonelle team har for lengst innsett at dette handler om mye mer enn å forebygge, detektere og ordne opp i hendelser. De fokuserer i mye større grad på hvilke konsekvenser hendelsene har for bedriftens kritiske verdier. Dette kan være konsekvenser for enkeltpersoner (økonomi, omdømme, familie), konsekvenser for bedriften (salg, aksjeverdi, omdømme) eller konsekvenser for samfunnet (trygghet, økonomisk vekst, arbeidsplasser). Forskning som kombinerer dyp teknisk analyse og kontekstinformasjon om hva som er kritiske verdier for individet, organisasjonen og samfunnet er nødvendig for samfunnet i sin helhet.

Et velfungerende team (e.g. SOC, CSIRT) fokuserer på å kontrollere cyberdomenet til det beste for bedriften. Dette krever mye kompetanse, på tvers av flere fagområder. Personellet må beherske avansert teknisk analyse som «malware analyse», «computer forensics», «network forensics» og «penetration testing». Samtidig må de ha kunnskap om hvordan teamets ressurser best kan organiseres og utnyttes for å opprette og beholde kontroll over cyberdomenet. Dette for at virksomheten eller samfunnet kan fortsette å fungere og utvikle seg på tross av pågående cyberkriminalitet og cyberangrep. Dette kan vi kalle cybertaktikk og cyberoperasjoner.



## Forskere

Førsteamanuensis Geir Olav Dyrkolbotn  
Førsteamanuensis Basel Katt  
Førsteamanuensis Mass Soldal Lund  
(gjesteforsker)

## Videreutvikling av faggruppen

CCIS sin forskningsgruppe for cyberforsvar er under oppbygging, og inkluderer per dags dato Førsteamanuensis Geir Olav Dyrkolbotn, Førsteamanuensis Basel Katt og tilknyttede ressurser (representanter fra Cyberforsvaret, Nasjonal sikkerhetsmyndighet, Forsvaret forskningsinstitutt og NISLab).

## Strategiske samarbeidspartnere og videre samarbeid

Cyberforsvaret (CYFOR), herunder Forsvarets ingeniørhøgskole (FIH), Nasjonal sikkerhetsmyndighet (NSM), Forsvarets forskningsinstitutt (FFI). Faggruppen ser på mulig samarbeid med Telenor.

## Forsknings- og utdanningsaktiviteter

CCIS og faggruppen for cyberforsvar har i 2015 hatt to hovedaktiviteter. En ny studiespesialisering innen cyber sikkerhet, under allerede eksisterende erfaringsbasert master i informasjonssikkerhet, er under etablering med oppstart allerede høsten 2016. Studieretningen kalles for «Cyber operations» og innebærer emnene: «Introduction Cyber and Information Security Technology», «System Security», «Malware Analysis and Reverse Engineering», «Intrusion Detection in Physical and Virtual Networks», «Cyber Tactics» og «Cyber Intelligence». I tillegg er det startet et prosjekt for å etablere en digital øvingsarena - Cyber Range - ved senteret. Dette innebærer at CCIS ved NTNU fra høsten 2016 tilbyr en Cyber Range inn i sine studieprogrammer. Videre vil CCIS sammen

med Cyberforsvaret etablere Cyber Range som et nasjonalt virtuelt øvingsfelt for forskning og utdanning på både beskyttelse og angrep på systemer og nettverk (NOU 2015:13).

Et prosjekt for etablering av en digital øvingsarena - en nasjonal cyber range (The Norwegian Cyber Range) ble startet ved Høgskolen i Gjøvik høsten 2015. Prosjektet er delt inn i to faser. Fase 1 vil etablere en Cyber Range til bruk i undervisning ved NTNU campus Gjøvik og fase 2 har som ambisjon å etablere en cyber range som en nasjonal kapasitet.

En nasjonal cyber range (The Norwegian Cyber Range) vil tilby et virtuelt miljø hvor Norges cyberforsvarsaktører kan møtes for å trene operatører, utvikle cybertaktikk, teknikker og prosedyrer. En Cyber Range er en digital trenings- og øvelsesarena for studenter, forskere, private og offentlige organisasjoner. Gjennom tett samarbeid med partnerne i CCIS kan cyber rangen raskt tilpasses ny teknologi, forskning og trusler og dermed speile behovet hos bedriftene og samfunnet. Samarbeid med partnerne vil også gi mulighet for å basere undervisning og trening på reelle problemstillinger, i motsetning til rene akademiske problemstillinger med mindre forankring i den virkelige verden. Cyber range kan også benyttes til å kjøre nasjonale eller internasjonale øvelser, hvor samhandling og informasjonsutveksling står i fokus.

## Viktige møter og aktiviteter i 2015

- Ansettelser i ledige stillinger
- Forstudie Cyber Range
- Planlegging av 3 nye emner



# FAGGRUPPE FOR BIOMETRI

## Faggruppens visjon

Faggruppen for biometri er samlet i Norwegian Biometrics Laboratory (NBL). NBL har for tiden tre internasjonale forskningsprosjekter, se Forskning nedenfor.

Fokuset ved laboratoriet å øke bevisstheten om biometri i Norge via Norwegian Biometrics Forum. Norwegian Biometrics Forum har, i sin kapasitet som spydspiss i Norge innen biometriske sikkerhetsløsninger, mulighet for å bistå i utforming av norsk lovgivning, og til å bidra til internasjonal standardisering i feltet.

NBL er et diskusjonsforum for brainstorming, for å generere nye ideer og prosjekter, og for å presentere foreløpige forskningsfunn og -resultater. Dermed er det en viktig del av CCIS og Norwegian Information Security Laboratory (NISlab), og representerer et aktivt fokuspunkt.

NBL sin biometriske forskning dekker ulike fysiologiske og atferdsmessige biometri, inkludert 2D- og 3D-ansiktsgjenkjenning, fingeravtrykk anerkjennelse, blodåregjenkjenning, tannbiometri, øregjenkjenning, i tillegg til signaturgjenkjenning, ganglagsgjenkjenning, tastetrykk-gjenkjenning, bevegelsesgjenkjenning og musdynamikk.

Videre har NBL fokus på via personvern å styrke teknologier som biometrisk malbeskyttelse og integrasjon i fysisk og logisk tilgangskontroll. NBL fungerer også som uavhengig testingsinstitusjon for biometriske ytelseevalueringer, basert på våre in-house biometriske databaser.

NBL er et aktivt medlem i European Association for Biometrics og medarrangør av den internasjonale konferansen BIOSIG samt the Biometric Session IEEE IHH-MSP.

## Videreutvikling av faggruppen

Faggruppen er godt etablert både på nasjonalt og internasjonalt nivå.

## Strategisk samarbeid

NBL samarbeider med privat næringsliv når det gjelder bilaterale forskningsaktiviteter og har også etablert et prosjektforhold til Nasjonalt ID-senter (NID). NBL sin forskning og testing understøtter fremtidige beslutninger som privat næringsliv må ta. På nasjonalt nivå ble NBL nylig tildelt SWAN-prosjektet, som blir finansiert av Norges Forskningsråd under IKTPLUS-programmet.

## Forskningsprosjekter

NBL har for tiden fire pågående EU-forskningsprosjekter under FP7 rammeprogrammet. Prosjektene er FIDELITY, INGRESS, ORIGINS og PIDaaS og dreier seg om biometri og identitets-håndtering. I tillegg er to prosjektforslag under evaluering.

## Søknader forskningsprosjekter

To prosjektforslag er under evaluering per februar 2016.

## Pågående forskning

Informasjon om hvert av forskningsprosjektene foreligger på nislab.no.

- SWAN<sup>22</sup>
- PIDaaS<sup>23</sup>
- Smartphone Based Eye Biometrics<sup>24</sup>
- FIDELITY<sup>25</sup>
- BEST Network<sup>26</sup>
- TURBINE<sup>27</sup>
- Hitachi<sup>28</sup>
- IDEX<sup>29</sup>
- National Institute of Standards and Technology NIST<sup>30</sup>

## Samarbeid

- 3D-GAA S.A<sup>31</sup>, Greece
- ARTTIC<sup>32</sup>, France
- BehavioSec<sup>33</sup>, Sweden
- Cryptolog<sup>34</sup>, France
- Hitachi<sup>35</sup>, Japan
- IDEX<sup>36</sup>, Norway
- ITS-Norway<sup>37</sup>, Norway
- K.U.Leuven<sup>38</sup> (ICRI, COSIC), Belgium
- National Institute of Standards and Technology (NIST)<sup>39</sup>, USA
- Philips Research Europe<sup>40</sup>, The Netherlands
- Precise Biometrics AB<sup>41</sup>, Sweden
- priv-ID<sup>42</sup>, The Netherlands
- Sagem Orga<sup>43</sup>, Germany
- Sagem Sécurité<sup>44</sup>, France
- University of Twente<sup>45</sup>, The Netherlands

## Viktige møter og aktiviteter i 2015

2. mars 2015 organiserte The Norwegian Biometrics Laboratory sitt femte årlige seminar på Høgskolen i Gjøvik, Norge. NBLAW-2015 fokuserte på temaet Presentation Attack Detection innen biometri. Dagen, med internasjonale foredragsholdere fra ulike europeiske land, illustrerte løste og uløste utfordringer. Spesielt av interesse er Presentation Attacks (falske angrep) på biometriske sensorer (for eksempel fingeravtrykksensorer), som er utformet for å få uautorisert tilgang til sikre biometriske systemer, ved å presentere et biometrisk artefakt hentet fra en replika av et legitimt individ.

Målet med NBLAW 2015 var å sette fokus på alle aspekter av eksisterende forskningsspørsmål som etter hvert vil etablere robuste presentation attack detection-metoder for biometriske systemer. Dette inkluderte diskusjonen om ulike utfordringer og løsninger som er oppnådd på Presentation Attack Detection for ulike modaliteter inkludert ansikt, iris, fingeravtrykk, og tale biometri.

NBL representerer også Norge i COST ACTION IC1106 og organiserte i denne rollen den 3rd International Workshop on Biometrics and Forensics (IWBF'15), som fant sted i Gjøvik, 3. til 4. mars 2015. Mer enn 70 deltakere fra 30 forskjellige land deltok på IEEE seminaret.

<sup>22</sup> [http://nislab.no/biometrics\\_lab/swan](http://nislab.no/biometrics_lab/swan)

<sup>23</sup> <http://www.pidaas.eu/cms/>

<sup>24</sup> [http://www.nislab.no/research/projects/smartphone\\_based\\_eye\\_biometrics](http://www.nislab.no/research/projects/smartphone_based_eye_biometrics)

<sup>25</sup> <http://www.nislab.no/research/projects/fidelity>

<sup>26</sup> [http://www.nislab.no/research/projects/best\\_nw](http://www.nislab.no/research/projects/best_nw)

<sup>27</sup> <http://www.nislab.no/research/projects/turbine>

<sup>28</sup> <http://www.nislab.no/research/projects/Hitachi>

<sup>29</sup> <http://www.nislab.no/research/projects/Idex>

<sup>30</sup> <http://www.nislab.no/research/projects/NIST>

<sup>31</sup> <http://www.3dsa.gr/>

<sup>32</sup> <http://www.arttic.eu/>

<sup>33</sup> <http://www.behaviosec.com/>

<sup>34</sup> <http://web.cryptolog.com/>

<sup>35</sup> <http://www.hitachi-omron-ts.com/>

<sup>36</sup> <http://www.idex.no>

<sup>37</sup> <http://www.its-norge.no/>

<sup>38</sup> <http://www.kuleuven.be/>

<sup>39</sup> <http://www.nist.gov/>

<sup>40</sup> <http://www.research.philips.com/>

<sup>41</sup> <http://www.precisebiometrics.com/>

<sup>42</sup> <http://www.priv-id.com/>

<sup>43</sup> <http://www.morpho.com/e-documents>

<sup>44</sup> <http://www.morpho.com/>

<sup>45</sup> <http://www.sas.el.utwente.nl/>

Den 16. april 2015 organiserte Norwegian Biometrics Forum sitt vårmøte ved Nasjonalt ID-senter i Oslo, og høstutgaven av Norwegian Biometrics Forum ble arrangert 19. november 2015 samme sted. På møtene var deltakere fra flere offentlige etater, industri og forskningsorganisasjoner fra Norge, Sverige, Danmark, Island og andre ikke-skandinaviske land representert. Møtene ble arrangert i samarbeid med European Association for Biometrics. Norsk Biometriforum er en uformell møteplass for presentasjoner og diskusjon om bruken av biometri.

### **Faggruppens medlemmer**

#### **Akademisk ansatte, fulltid**

Christoph Busch  
Patrick Bours  
Bian Yang  
Raghavendra Ramachandra  
Sule Yildirim Yayilgan  
Erik Hjelmås

#### **Tilknyttede vitenskapelig ansatte**

Katrin Franke  
Ivar Farup

#### **PhD-kandidater**

Guoqiang Li  
Danish Mairaj  
Ctirad Sousedik  
Martin Stokkenes  
Nabeel Al-Bahbooh  
Edlira Martiri  
Kiran Bylappa Raja  
Patrick Schuch  
Pankaj Wasnik  
Daniel Hartung  
Mohammed Derawi  
Aniks Pflug  
Martin Olsen  
Soumik Mondal

#### **Administrativ støtte**

Faggruppen har administrativ støtte fra CCIS sin ledelse og generelle administrasjonsstab.





# FAGGRUPPE FOR PERSONVERN OG INFORMASJONSSIKKERHETSLEDELSE

## Faggruppens visjon

Faggruppen for personvern og informasjonssikkerhetsledelse sine aktiviteter gir teoretiske, empiriske og kliniske forskningsresultater til modellering, måling og administrasjon av informasjonssikkerhet. Denne kunnskapen kommer til anvendelse for samfunnet ved å besvare spørsmål på området, og komme opp med løsninger på problemer.

Gruppen har et særskilt ansvar for NTNU i Gjøvik sine studieløp på masternivå innen fagområdet. Forskningen ved gruppen bidrar med et bredt spekter av resultater på sosio-teknisk system-sikkerhet, som dekker det sosiale, psykologiske, juridiske, etiske, kulturelle, politiske og retoriske utdanningsaspektet. Gruppen dekker i tillegg det tekniske aspektet av cyber- og informasjonssikkerhetsledelse.

## Strategisk samarbeid

Gruppen benytter sin faglige forskning på den nasjonale arenaen og samarbeider med Norsk senter for informasjonssikring (NorSIS) om å organisere og gjennomføre Norsk Sikkerhetstoppmøte tre ganger årlig. Gruppen deltar også i den årlige Nasjonale Sikkerhetsmåneden med konkurranse og presentasjon.

## Forskningsprosjekter

### PhD-forskning

*Hyper Contextual Information Security Management (Shao-Fang Wen)*

Kandidaten undersøker hvordan kunnskap og temaet teknologier best kan brukes til å støtte arbeidet for ledere innen informasjonssikkerhet og personvern. Forskningen skal utvikle sosio-tekniske modeller og tiltak for sikkerhets- og personvernlederfunksjoner og resultatene skal brukes til å evaluere og utvikle kunnskap om temaet teknologier i utviklingsprosjekter innen åpen kildekode.

## Avsluttede mastergrader

Steinar Nivlgard, Information Security Situation of BYOD as a Socio-Technical System in Norwegian SMEs.

Eirik L. Nesbakken, The Digital Shadow - The signification of intelligence to decrease Advanced Persistent Threat in cyberspace.

## Vitenskapelige publikasjoner

Al Sabbagh, B.; Kowalski, S., "A Socio-technical Framework for Threat Modeling a Software Supply Chain," in *Security & Privacy, IEEE*, vol.13, no.4, pp.30-39, July-Aug. 2015 doi: 10.1109/MSP.2015.72

## Faggruppens medlemmer

### Akademisk ansatte, fulltid

Professor Stewart Kowalski  
Professor Einar Snekkenes  
Førsteamanuensis Laura Georg

### Tilknyttede vitenskapelig ansatte

Richard McEvoy  
Professor Bernhard Markus Hammerli  
Professor, Dr.rer.nat Jose J. Gonzalez

### PhD-kandidater

Vivek Agrawal  
Wagas Aman  
Pankaj Pandey  
Gaute Wangen  
Shao-Fang Wen

### Administrativ støtte

Faggruppen har administrativ støtte fra CCIS sin ledelse og generelle administrasjonsstab.



**Norwegian University of Science and Technology**  
**Center for Cyber and Information Security**  
Pb 191, 2802 Gjøvik, Norge  
[www.ccis.no](http://www.ccis.no)