NTNU CCIS
Center for Cyber and
Information Security

Årsrapport 2020

NTNU Center for Cyber and Information Security

Gjøvik, 17.02.2021

CENTER FOR CYBER AND INFORMATION SECURITY v/IIK, NTNU, Pb 191, N-2902 Gjøvik, Norway post@ccis.no
www.ccis.no

Innholdsfortegnelse

1 Innledning

NTNUs Center for Cyber and Information Security (NTNU CCIS) er et nasjonalt senter for 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 som 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, og 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 informasjonssikkerhet i -Europa.

NTNU CCIS har i 2020 følgende 30 partnere i tillegg til vertsinstitusjonen NTNU: Atea, Cyberforsvaret, Datatilsynet Domstolene i Norge, Eidsiva, Forsvarets Høgskole, Forsvarets forskningsinstitutt, Høgskolen i Innlandet, IBM, Innlandet politidistrikt, KINS, KPMG, Kripos, mnemonic AS, Nasjonal sikkerhetsmyndighet, Nasjonalt ID-senter, NC-Spectrum AS, Norsk senter for informasjonssikring, Innlandet Fylkeskommune, Oslo Politidistrikt, Politidirektoratet, Politiets sikkerhetstjeneste, Politihøgskolen, PwC, Sykehuset Innlandet HF, Statkraft, Statnett, Telenor, Watchcom Security Group og Økokrim.

2 Årsberetning

2.1 Styrets arbeid og generalforsamling

Styret i NTNU CCIS består etter generalforsamlingen 2020 av:

- Norges teknisk-naturvitenskapelige universitet (NTNU), styreleder ved Ingrid Schjølberg (2018-2022)
- Nasjonal sikkerhetsmyndighet (NSM), nestleder ved Mona Strøm Arnøy (2017-2021)
- Cyberforsvaret, ved Knut Ivar Rønning (2017-2021)
- mnemonic AS, ved Tønnes Ingebrigtsen (2018-2022)
- Telenor, ved Hanne Tangen Nilsen (2017-2021)
- Politidirektoratet, ved Olav Skard Jørgensen (2017-2021)
- 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.

2.2 Organisasjon og ledelse

NTNU CCIS har Institutt for informasjonssikkerhet og kommunikasjonssikkerhet (IIK) ved Fakultet for informasjonsteknologi og elektroteknikk (IE) som sitt vertsinstitutt i Norges teknisk-naturvitenskapelige universitet (NTNU). I 2020 har Nils Kalstad, instituttleder for IIK, også fungert som leder av og koordinator for aktiviteten i NTNU CCIS. Senteret har en ordning med en konstituert vitenskapelig styringsgruppe som i 2020 har bestående av førsteamanuensis Basel Katt, førsteamanuensis Bian Yang, professor Colin Boyd, førsteamanuensis Geir Olav Dyrkolbotn, professor Katrin Franke, professor Patrick Bours, professor Sokratis Katsikas. Seniorrådgiver Inge Øystein Moen har i 2020 administrativt understøttet aktiviteten i NTNU CCIS i tillegg til at senteret har bred administrativ støtte fra vertsinstitutt og -fakultet.

NTNU CCIS' aktivitet er basert på de delene av IIK utdannings- og forskningsportefølje som er av særlig relevans for partnerne i senteret. Aktiviteten i senteret er samlet i de tematiske gruppene

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

Gruppene har ulik historikk, oppbygning og modenhetsgrad. Det de har til felles er at de er svært relevante for å adressere de utfordringene som partnerne i NTNU CCIS står ovenfor. Det er også gjennom samarbeidet i disse gruppene at kunnskapsoverføringen mellom partnerne finner sted. Det er derfor av stor viktighet at partnerne engasjerer seg i de grupper de finner relevante.

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 de samfunnsmessige utfordringene som må adresseres knyttet til cyber- og informasjonssikkerhet. Dette bruker vi til å gi innspill til relevante forskningsstrategier og forskningsprogrammer, både nasjonalt og internasjonalt. Norges forskningsråd (NFR), Justis- og Beredskapsdepartementet (JD), NordForsk (Nordisk ministerråd), Europakommisjonen og National Institute of

Technologies and Standards (NIST) er eksempler på organer som er av særlig relevans for NTNU CCIS, våre partnere og våre nettverk. Dette gjøres i form av senterets samarbeide med NTNU om myndighetskontakt gjennom en rekke møter med statsråder, statssekretærer, departementer, andre forvaltningsenheter, og politiske partier. I en annen dimensjon gjøres dette gjennom for eksempel deltagelse i Justisdepartementets forum for digital sikkerhet, Nasjonalt cybersikkerhetssenter (NSM NCSC) sin referansegruppe, Digital Enlightenment Forum, European Cyber Security Organization, North European Cyber Security Cluster og Norges forskningsråds referansegruppe for H2020 Secure Societies. I en tredje dimensjon gjøres dette gjennom ekspertdeltagelse i internasjonale organisasjoner som EUROPOL, INTERPOL, ENISA og NATO, som i tur gir sine innspill til samfunnsutfordringene.

NTNU CCIS har i 2020 hatt svært gode resultater i konkurransebasert forskningsfinansiering med fire nye EU prosjekter, to NF- prosjekter 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. Særlig gledelig er det for 2020 å kunne rapportere at SFI Norwegian Center for Cybersecurity in Critical Sectors (SFI NORCICS) ble en realitet med finansiering fra Norges Forskningsråd. Det å etablere et SFI-senter har fra starten vært en målsetning for CCIS, og dette er nå en realitet.

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

NTNU er partnerskapets hovedleverandør av studier innen cyber- og informasjonssikkerhet. Utdanninger ved NTNU med særlig fokus på områder av høy relevans for NTNU CCIS er:

- PhD. i informasjonssikkerhet og kommunikasjonsteknologi
- 5-årig masterstudium i teknologi/sivilingeniør i kommunikasjonsteknologi
- 2-årig engelskspråklig masterstudium «Information Security»
- 4-årig deltid engelskspråklig masterstudium «Information Security»
- 2-årig engelskspråklig masterstudium «Kommunikasjon og digital sikkerhet»
- 3-årig deltid erfaringsbasert masterstudium «Information Security»
- 3-årig bachelorstudium i Digital infrastruktur og cybersikkerhet
- Partner i Erasmus-program SECCLO «Security and Cloud Computing»

Erfaringsbasert mastergrad i informasjonssikkerhet tilbys i samarbeid med Politihøgskolen, Cyberforsvaret og NorSIS. Alle masterutdanningene tilbys både på heltid og deltid, og er derfor svært aktuelle tilbud for virksomheter som ønsker å gjennomføre målrettede kompetanseutviklingstiltak for sine ansatte. I 2020 ble det etablert et 7.5 studiepoengs valgemne i digital sikkerhet for alle sivilingeniørstudenter i NTNU. 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 adressert gjennom å organisere og være tilstede på en rekke møteplasser. I så måte har 2020 vært et helt spesielt år med Covid-19 og strenge restriksjoner på fysiske møteplasser. Viktige aktiviteter som CCIS lecture, Sikkerhetsfestivalen, Cyber Symposiet, COINS Finse Winter School, Immatrikulering ved NTNU, SikkertNOK og European Cyber Security Challenge ble alle sterkt berørt eller avlyst på grunn av dette. Men i samarbeid med gode partnere har vi klart å opprettholde god aktivitet.

2.5.1 Ekskursjon til Israel og Cybertech 2020

NTNU CCIS var representert på en studietur til Israel siste uke i januar 2020 for å studere og få kontakt med miljøer innen cyber- og informasjonssikkerhet. Det deltok også representanter for kommunale og fylkeskommunale myndigheter på Innlandet og fra innovasjonsbedriften Total Innovation. Turen var tilrettelagt av den israelske ambassaden. Vi mottok nyttig og inspirerende informasjon og knyttet flere kontakter. Vi besøkte bl.a. cyberhovedstaden Beer Sheva, samt Tel Aviv. I ettertid er kontakten opprettholdt, bl.a. har professor I. Ben-Israel, direktør ved Blavatnik Interdisiplinary Cyber Research Center, holdt innledninger på 3 konferanser i Norge til nå, han er også invitert inn på en nordisk konferanse. Oppfølgingen fortsetter.

2.5.2 NBL annual workshop

Den 7. mars gjennomførte Norwegian Biometrics Laboratory sitt niende årlige workshop (NBLAW). NBLAW er et åpent og gratis arrangement og er for alle som er interessert i teknologi, policyer, applikasjoner og utvidet aksept av smarttelefonbiometri. NBLAW 2019 fokuserte på blockchain og biometri. NBLAW ble teknisk sponset av European Association for Biometrics (EAB) og økonomisk støttet av Norges forskningsråd (RCN) under prosjektet Secure Access Control over Wide Area Network (SWAN).

2.5.3 Cyber 9/12 Challenge

"The Norwegian Cyber Chiefs", bestående av studenter fra NTNU i Gjøvik (bachelor, master og doktorstudenter) deltok på Cyber 9/12 konkurransen. Arrangementet er i regi av Atlanterhavsrådet og arrangeres vanligvis 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 og laget tok seg i år til semifinalen i konkurransen. Det norske laget besto i år av Grethe Østby (lagleder og stipendiat ved Institutt for informasjonssikkerhet og kommunikasjonsteknologi), Mazaher Kianpourl, Philip Johannes Nyblom, Gaute Wangen (lagleder og ansatt ved Seksjon for digital sikkerhet ved NTNU), Bjørn Aune, John Andre Seem, Joachim Ulven, Job Nestor Bahner og Simen Bai.

2.5.4 Totalforsvaret cybersikkerhetskonferanse

Totalforsvarets Cybersikkerhetskonferanse 2020 ble arrangert 1. og 2. september på Lillehammer. Arrangørene var CyberLand, Innlandet fylkeskommune, Fylkesmannen i Innlandet, Cyberforsvaret, NSM, DSB, Politidirektoratet, NTNU CCIS, FFI og Næringslivets sikkerhetsråd. Formålet med konferanse er å etablere en arena for meningsutveksling, der det diskuteres utfordringer og løsninger for å nå vårt felles mål – et sterkere totalforsvar i Norge. Konferansen samlet 200 deltagere fysisk.

2.5.5 ovelse.no

Som del av øvelse Digital 2020 har NTNU hatt i oppdrag å utvikle og etablere en driftsplattform for øvelsespakkene. Prosjektet ledes av DSB og samarbeidspartnere i prosjektet utover NTNU er Digitaliseringsdirektoratet, Nasjonal sikkerhetsmyndighet og NorSIS. Plattformen ble lansert 14. oktober og inneholder 12 diskusjonsøvelser rettet mot virksomheter av ulik størrelse og i ulike sektorer. Innholdet i øvelsene er forskningsbasert, og det er også lagt til rette for følgeforskning på bruken av plattformen

2.5.6 SFI NORCICS

SFI NORCICS arrangerte sin kick-off i hybrid format den 20. oktober. SFI'en bygger på det gode partnerskapet og det gode samarbeidet som er etablert i NTNU CCIS, men inkluderer også en del partnere som ikke er i NTNU CCIS. Bakgrunnen for dette er behovet for et skreddersydd partnerskap som sammen skulle møte de spesifikke kriteriene og høye kravene som Forskningsrådet har for SFI instrumentet. Konsortiet består av Siemens, Helgeland Kraft, Yara, Lyse Energi,

Oslo Politidistrikt, Hydro, Kongsberg, Equinor, Sykehuset Innlandet HF, Elvia, mnemonic, NC-Spectrum, UiA og SINTEF. Senteret vil over 8 år 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 potensiale for samarbeid og synergier mellom NTNU CCIS og SFI NORCICS.

2.5.7 Etter- og videreutdanning (EVU)

Som en del av tiltakspakkene i og under Covid-19 har etterspørselen etter EVU vært betydelig. NTNU CCIS har arrangert to kurs med finansiering fra Kompetanse Norge rettet spesifikt mot personer som var direkte berørt av Covid-19 i form av å være permitterte i uke 33 og 34. Hver uke besto av 40 timer med undervisning og under tittelen «Digital sikkerhet og min nye arbeidshverdag» fikk deltagerne forelesninger og refleksjonsoppgaver under veiledning av bredden av fagmiljøet i NTNU CCIS. Etter dette har vi også levert en forelesningsserie til GCE Blue Maritime hvor vi fokuserer på cybersikkerhetsutfordringer i maritim sektor. Videre har vi fått tilslag på å etablere to kurspakker i digital sikkerhet, hvor den ene pakken skal være relevant for alle med generell studiekompetanse og den andre skal være relevant for de med bachelorgrad fra før. Begge etableringene støttes av kompetanse Norge og den siste er en del av bransjeprogrammet for petroleumssektoren

2.5.8 Mørketallsundersøkelsen 2020

Mørketallsundersøkelsen fra Næringslivets sikkerhetsråd (NSR) kartlegger IT-tilstanden i privat og offentlig næringsliv. Undersøkelsen er enestående i Norge og er et viktig bidrag til å kartlegge omfanget av datakriminalitet og IT-sikkerhetshendelser, samt bevissthet omkring informasjonssikring og omganger av sikringstiltak i norske virksomheter. NTNU CCIS bidro med analysekapitlet i Mørketallsundersøkelsen 2020.

2.5.9 Vurdere behovet for utdanningstilbud rettet spesifikt mot helsesektoren

Med bakgrunn i blant annet strategi for digital sikkerhetskompetanse har Helse- og omsorgsdepartementet gitt NTNU ved Institutt for informasjonssikkerhet og kommunikasjonsteknologi i oppdrag å utrede etter- og videreutdanningstilbud innen digital sikkerhet for helsesektoren. Utredningen skal utrede og 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. Resultatet skal fremlegges som en rapport innen utgangen av 2020. Det har blitt etablert en referansegruppe for arbeidet bestående av representanter fra Norsk Helsenett, HelseCERT, Direktoratet for e-helse, Helsetjenestens driftsorganisasjon for nødnett, KommuneCSIRT og Sykehuset Innlandet HF.

2.5.10 Norwegian Cyber Rage

Norwegian Cyber Range (NCR) er et tiltak som er nevnt eksplisitt i Nasjonal strategi for digital sikkerhet og som NTNU har ansvar for implementasjonen 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 vil ferdigstilles i 2020 og vi ser på mulighetene for en gjenåpning av NCR i moderne, tidsriktige og svært funksjonelle lokaler i begynnelsen av 2021. Disse lokalene vil by på innbydende mulighet for trening og øving av personell med fokus på både tekniske og organisatoriske ferdigheter.

2.5.11 Norwegian and European Cyber Security Challenge

På oppdrag fra Justis- og beredskapsdepartementet arrangerte IIK gjennom samarbeidet i NTNU CCIS Norwegian Cyber Security Challenge i 2020. Vi skulle også arrangere Norges deltagelse i European Cyber Security Challenge i Wien, Østerrike, i november 2020, men dette har blitt utsatt til 2021 på grunn av Covid-19. Norwegian Cyber Security Challenge (NCSC) har som målsetning å finne unge talenter (i aldersgruppen 16 - 25 år) innen cybersikkerhet og motivere disse til å utvikle seg videre. Det har i 2020 bitt arrangert en kvalifiseringsrunde i NCSC og vi jobber videre med å holde et 20 talls potensielle deltagere varme frem mot 2021. Vi har fått ansvaret for å arrangere European Cyber Security Challenge 2023 i Norge, og vi har startet arbeidet med å utrede Vikingskipet på Hamar som en mulig arena for dette. For mer informasjon se https://www.ntnu.no/ncsc.

2.5.12 CyberSmart

CyberSMART er 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 2020 har vi arbeidet for å finne partnere og sponsorer til prosjektet. Viktig inspirasjonskilde har vært det amerikanske prosjektet GenerationCyber: https://www.gen-cyber.com/

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

2.5.13 Digitale trusler i forsvarssektoren

I samarbeid med Norsk råd for digital etikk (NORDE) nådde NTNU CCIS opp i konkurransen for utredningsprosjektet Digitale trusler i forsvarssektoren. Prosjektet hadde oppstart i desember 2020 og vil foreta en gjennomgang av teknologiske områder og bruksområder for å identifisere digitaletiske problemstillinger som kan oppstå ved bruk eller utrulling av disse teknologiene i Forsvarsektoren. Videre vil prosjektet kartlegge og analysere hvor det kan oppstå etiske problemstillinger i fremtiden knyttet til trusler mot sikkerheten og demokratiet og hva som kan gjøres for å forhindre en uønsket utvikling.

2.5.14 Nærings-PhD

I samarbeid med partnere i NTNU CCIS har det i 2020 levert og innvilget flere søknader om nærings/offentlig PhD til Norges forskningsråd. Særlig aktive har kraftsektoren vært med innvilgede initiativer fra Statnett, Elvia og NVE. Disse har alle hatt oppstart i 2020.

2.6 Regnskapsrapport

Regnskapsrapporten under viser totaløkonomien for NTNU CCIS. Dette inkluderer bevilgninger, partnerbidrag og NTNU sine bidrag som vertsinstitusjon. På bevilgningssiden ser vi for 2020 en redusert bevilging fra HOD på grunn av Covid-19, men det er signaler om at det kan være håp en normal bevilgning i 2021. Videre ser vi at en del av den planlagte aktiviteten i 2020 har blitt utsatt eller avlyst. Derav svært lave utgifter til reiser og parter oppfølging. For at ikke disse uforutsatte hendelsene skal medføre betydelige avsetninger vurderer vi å investere noe av de udisponerte midlene inn i infrastruktur, utstyr og løsninger som vil gjøre NTNU CCIS til enda sterkere senter i fremtiden. Dette inkluderer å understøtte øvelsesplattformen ovelse.no, fullføre installasjonen av HANSKEN og ferdigstillelse av ombyggingsprosjektet i Norwegian Cyber Range. Det er i 2020 også lagt betydelig resurser i utvikling og leveranse av hybride og heldigitale løsninger for etter- og videreutdanning innen våre fagområder.

Årsregnskap CCIS

Finansieringskilde	Sum	HOD	JD	NTNU	PARTNER
Inntekter					
Overføring udisponerte midler 2019	1 984 719	1 577 708	407 011		
Bevilgning statsbudsjettet – JD	5 000 000		5 000 000		
Bevilgning statsbudsjettet – HOD	600 000	600 000			
Bidrag partnere	8 272 564				8 272 564
Bidrag NTNU	5 785 351			5 785 351	
Totale inntekter 2020	**21 642 634**	**2 177 708**	**5 407 011**	**5 785 351**	**8 272 564**
Utgifter					
Administrasjon	2 096 718			1 397 862	698 856
Lønn	752 400	250 800	501 600		
Reiser	0				
Utstyr	0				
Utvikling	0				
Partner- og avtaleoppfølging	0				
Forskning, utdanning og formidling	11 961 197			4 387 489	7 573 708
Lønn	3 075 433	1 366 722	1 708 711		
Reiser	134 528	17 972	116 556		
Utstyr	313 719	63 441	250 278		
FoU aktiviteter	0				
Publikasjoner, trykking, annonser	0				
Møter og arrangementer	38 291	6 305	31 986		
Formidling og markedsføring	681 159	170 290	510 869		
Utvikling	0				
Totale utgifter 2020	**19 053 445**	**1 875 530**	**3 120 000**	**5 785 351**	**8 272 564**
Udisponerte midler for 31.12 2020	**2 589 189**	**302 178**	**2 287 011**	**0**	**0**


POLITIET
KRIPOS


Eidsiva


FORSVARET


FFI
Forsvarets
forskningsinstitutt
Norwegian Defence Research Establishment


POLITIET
POLITIDIREKTORATET


Nasjonalt ID-senter


PST
POLITIETS
SIKKERHETSTJENESTE


telenor


NorSIS
Norsk senter for
informasjonssikring

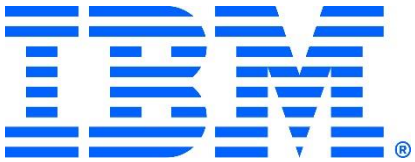

ØKOKRIM


pwc


NC-Spectrum


ATEA
Sykehuset Innlandet HF


mnemonic


IBM


WATCHCOM
Security Group


NASJONAL
SIKKERHETSMYNDIGHET


KPMG


POLITIET
OSLO POLITIDISTRIKT


Datatilsynet


Innlandet
fylkeskommune


Statnett


POLITIHØGSKOLEN


Statkraft