FFI Forsvarets forskningsinstitutt

23/00546

FFI-RAPPORT

Hva vet vi om innsiderisiko?

Betina Slagnes

Hva vet vi om innsiderisiko?

Betina Slagnes

Forsvarets forskningsinstitutt (FFI) 6. mars 2023

Emneord
Innsiderisiko
Innsidevirksomhet
Nasjonal sikkerhet
Personellsikkerhet
Spionasje

FFI-rapport
23/00546

Prosjektnummer
1619

Elektronisk ISBN
978-82-464-3461-2

Engelsk tittel
What do we know about insider threats?

Godkjennere
Stig Rune Sellevåg, *forskningsleder*
Janet Blatny, *forskningsdirektør*

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Sammendrag

Denne rapporten gir et kunnskapsbidrag om innsiderisiko. Den er bygget opp rundt åpent tilgjengelig og relevant forskning. Rapporten legger vekt på egenskaper ved sosiale medier og ulike tilnærminger til påvirkning. Rapporten ser også nærmere på faktorer knyttet til hvordan en kan vurdere sikkerhetsmessig skikkethet. Her er individuelle personlighetstrekk viktig. Et annet viktig tema er sikkerhetskultur og sikkerhetsledelse. Dette omfatter jobbtilfredshet, sikkerhetsbevissthet og rapportering av sikkerhetstruende hendelser.

Rapporten avdekker at det er et stort behov for nasjonal forskning på personellsikkerhet som tar hensyn til norske forhold. For det første bør det forskes på hvordan påvirkningsoperasjoner i det digitale rom kan føre til økt innsidevirksomhet. For det andre bør forskningen se på faktorer knyttet til vurderinger av sikkerhetsmessig skikkethet. For det tredje bør forskningen ta for seg innsiderisiko og sikkerhetskultur ut fra norske kulturelle forhold, ettersom nasjonale kulturer og organisasjonskulturer ofte er unike. For det fjerde bør det forskes mer på hvordan eksisterende kunnskap og kompetanse innenfor ledelse, organisasjonsutvikling og pedagogikk kan anvendes i en sikkerhetssammenheng.

Rapporten konkluderer med at forskning på personellsikkerhet bør etableres som et bærekraftig fagområde i Norge, der forskningen kontinuerlig utvikles og oppdateres. Med den rette tilnærmingen kan Norge bli et foregangsland innenfor forskning på personellsikkerhet.

Summary

This report is a contribution to the literature on insider threats. The report treats openly available and relevant research. It emphasizes characteristics of social media and malicious actors' different approaches of influencing their targets. The report also examines factors that can contribute in assessing persons' suitability related to security. Here, individual personality traits are important. Another important area is security culture and security management, which include job satisfaction, security awareness and reporting of security-threatening behaviors or incidents.

Moreover, the report reveals that there is a great need for national research on personnel security that considers Norwegian conditions. First, the research should investigate how influence operations in the digital space can increase insider activities. Second, the research should examine relevant factors in assessments of persons' suitability related to security. Third, research on insider threats and security culture should include Norwegian cultural parameters, as national cultures and organizational cultures are often unique. Fourth, the research should further explore the possibility of applying existing knowledge and competence within management, organizational development and pedagogy in the context of security.

The report recommends establishing personnel security as a sustainable research area in Norway, and continuously developing and updating this research. With the right approach, Norway can become a leading country in the field of personnel security research.

Innhold

Forord

En stor takk rettes til sjefsforsker Stig Rune Sellevåg, seniorforsker Nina Hellum, Dr. Paul Martin og Dr. Margaret Wilson for gode diskusjoner og faglige råd. Tusen takk til seniorforsker Arild Bergh for faglige råd og skriftlig bidrag i forbindelse med kapittel 3 om sosiale medier og påvirkning. Takk også til grafisk designer Grete Foss Alvestad for god hjelp med designet av figurene, bibliotekar Caroline Musæus for god hjelp med litteratursøkene, koordinator Frida Skjei for god hjelp med gjennomlesing av rapporten og grafisk rådgiver Brita Øvreås for god hjelp med å ferdigstille rapporten.

Kjeller, 6.mars 2023
Betina Slagnes

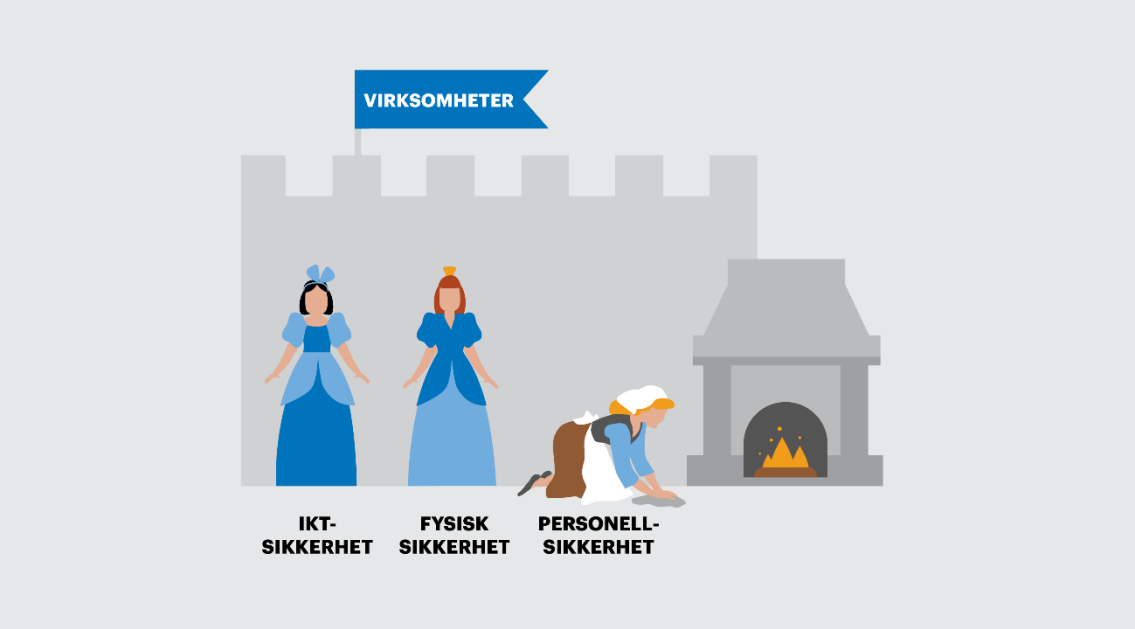
1 Innledning

Myndighetene og ulike sikkerhetsfaglige miljøer har en rekke ganger påpekt et behov for kunnskapsutvikling relatert til personellsikkerhet og innsiderisiko. Blant annet fremkommer det i en Stortingsmelding om samfunnssikkerhet (Meld. St. 5 (2020–2021), 2020, s. 69) at regjeringen ønsker å øke den forskningsbaserte kunnskapen om motvirkning av innsiderisiko. Videre fremhever Nasjonal sikkerhetsmyndighet (NSM) i sitt sikkerhetsfaglige råd et behov for akademisk kunnskap i flere disipliner innenfor personellsikkerhet (NSM, 2015, s. 31-32, 45).

Behovet for akademisk kunnskap rundt personellsikkerhet kan knyttes til diverse utfordringer innenfor arbeid med forebyggende sikkerhet. Enkelte av disse utfordringene er beskrevet i en temarapport om innsiderisiko av NSM (2015, s. 28-30). Blant annet er det en økning av antall klareringssaker der klareringsmyndighetene foretar komplekse vurderinger rundt temaer som privatøkonomi, psykisk helse og utenlandsk tilknytning. Disse vurderingene skal balanseres med et krevende regelverk. Til sammen fører dette til at klareringsmyndighetene må ha stor breddekunnskap, forklarer NSM. Breddekunnskapen inkluderer fagfelt som psykologi, statsvitenskap, sosiologi, antropologi, rettsvitenskap, religionsvitenskap, kriminologi og etterforskning (eksemplene er ikke uttømmende).

Kunnskapsbehovet forsterkes av at truslene mot norske interesser er sammensatte og endres raskt (Etterretningstjenesten, 2021, 2022, 2023; NSM, 2021, 2022, 2023; PST, 2020, 2021, 2023). Disse truslene er også sektorovergripende, det vil si at alle samfunnssektorer kan utsettes for maktbruk og press. Dette trusselbildet fører til utfordringer i arbeid med forebyggende sikkerhet, da klareringsmyndighetene, sikkerhetstjenestene, og virksomheter underlagt sikkerhetsloven må være dynamiske i deres vurderinger for å ivareta våre nasjonale sikkerhetsinteresser. Slike sammensatte vurderinger krever at alle som arbeider med forebyggende sikkerhet har tilgang til en god og oppdatert kildeportefølje.

Det er også et særskilt behov for å utvikle et bedre kunnskapsgrunnlag og forståelse for personellsikkerhet og innsiderisiko ut fra norske forhold. Foruten enkelte temarapporter om innsiderisiko, samt masteroppgaver om personellsikkerhet, eksisterer det i liten grad nasjonal forskning omkring disse temaene. I tillegg er det usikkert om internasjonal forskning på personellsikkerhet og innsiderisiko har en direkte overføringsverdi til forebyggende sikkerhetsarbeid i Norge, ettersom ulike kulturelle og samfunnsmessige forhold spiller inn. Dessuten vier akademia og virksomheter for lite oppmerksomhet til personellsikkerhet sammenlignet med sikkerhet innenfor informasjons- og kommunikasjonsteknologi (IKT-sikkerhet) og fysiske objekter (Martin, 2019, s. 203). På bakgrunn av dette kan personellsikkerhet omtales som «sikkerhetens Askepott» (figur 1.1) (Martin, 2019, s. 203).



Figur 1.1 Martin (2019, s. 203) omtaler personellsikkerhet som «sikkerhetens Askepott». Illustrasjon: FFI

1.1 Samfunnseffekter

Myndigheters evne til å administrere effektivt blir redusert dersom de kontinuerlig må forklare og rettferdiggjøre sine beslutninger (Tyler & Lind, 1992). For at myndighetene skal fungere effektivt i sitt virke, er det derfor avgjørende at det er etablert positive holdninger og aksept knyttet til beslutningene deres i befolkningen (Bos et al., 1998, s. 1449; Tyler & Degoey, 1996, s. 332). Imidlertid har Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) kritisert Forsvarets sikkerhetsavdeling (FSA) og NSM for manglende innsyn i ulike klareringssaker (EOS-utvalget, 2020-2021, s. 28, 31). Videre får klareringsmyndighetene og utfallet av klareringsprosesser ofte negativ omtale i media (Haugsbø, 2021b, 2022; Haugsbø & Skålevik, 2021; Karlsen, 2020a, 2020b; Kristoffersen et al., 2019; Pang, 2022; Strand, 2022; Tennøy et al., 2020), og Justis- og beredskapsminister Emilie Enger Mehl har varslet en gjennomgang av praksisen i klareringssakene (Haugsbø, 2021a). Klareringssaker har også i økende grad blitt et eget fagfelt blant advokater og akademikere, som argumenterer for at rettssikkerheten blir satt på prøve i klareringssaker (Bakke, 2017, 2019; Graver, 2021; Skotvedt, 2019). Forskningsbasert kunnskapsutvikling innenfor personellsikkerhet kan i så måte gi muligheter for økt tillit til klareringsmyndighetenes personellsikkerhetsvurderinger. Dette kan igjen bidra til økt effektivitet.

Forskningsbasert kunnskapsutvikling innenfor personellsikkerhet kan gi muligheter for økt tillit til klareringsmyndighetenes personellsikkerhetsvurderinger. Dette kan igjen bidra til økt effektivitet.

Kunnskapsutvikling innenfor forebyggende sikkerhet har også en større samfunnsmessig betydning. Det er en veletablert oppfatning om at politisk tillit er nødvendig for å sikre stabiliteten i demokratiske politiske systemer (Almond & Verba, 1963). Nyere studier viser at politisk tillit også omhandler tillit til grunnleggende demokratiske institusjoner og prosedyrer (Dalton, 2004; Pharr & Putnam, 2000; Putnam, 2002; Stolle & Hooghe, 2005). Befolkningens tillit til klareringsmyndighetene kan sies å være en forlengelse av befolkningens tillit til politikere og de demokratiske institusjonene, ettersom klareringsmyndighetene er underlagt demokratisk og politisk kontroll, og statsrådene konstitusjonelt har ansvaret for de offentlige forvaltningsorganene som er underlagt dem. Således kan fremtidig forskning innenfor personellsikkerhet gi muligheter for økt tillit til klareringsmyndighetene. Dette kan igjen bidra til demokratisk stabilitet.

Således kan fremtidig forskning innenfor personellsikkerhet gi muligheter for økt tillit til klareringsmyndighetene. Dette kan igjen bidra til demokratisk stabilitet.

1.2 Litteratursøk

Innholdet i rapporten baseres på nasjonal og internasjonal forskningslitteratur som er identifisert ved hjelp av samfunnsvitenskapelige og pålitelige databaser som ISI Web of Knowledge (Web of Science), International Bibliography of the Social Sciences (IBSS), Sociological Abstracts, Scopus og Idunn, samt Google Scholar. Databasene dekker samtlige fagområder innenfor samfunnsvitenskap. Utvalgskriteriene for valg av litteratur fra høyest til lavest rangering, er:

1. Vitenskapelige artikler i høyt rangerte internasjonale tidsskrifter med fagfellevurdering
2. Vitenskapelige artikler i vitenskapelige tidsskrifter med fagfellevurdering
3. Analyser og rapporter fra tenketanker og liknende forskningsinstitusjoner
4. Fagbøker
5. Andre internettkilder

Litteratursøkene ga få treff på nasjonal og fagfellevurdert forskning på personellsikkerhet (se vedlegg side 30). Samtidig er det en mulighet for at relevant litteratur ikke har blitt kartlagt. Det skriftlige materialet som derimot har blitt identifisert vil bli gjennomgått og diskutert nærmere i de neste kapitlene.

1.3 Rapportens oppbygging

Rapporten er delt inn i 6 kapitler. Kapittel 2 gjennomgår definisjoner av innsidevirksomhet og innsiderisiko, samt eksempler på motivasjoner bak innsidevirksomhet. Kapittel 3 inneholder en kunnskapsstatus om moderne utviklingstrekk og potensielle sårbarheter som kan medføre økt risiko for innsideaktivitet. Kapittel 4 gjennomgår faktorer knyttet til vurdering av sikkerhetsmessig skikkethet. Kapittel 5 undersøker om det eksisterer tilstrekkelig kunnskap rundt daglig sikkerhetsledelse, sikkerhetskultur og sikkerhetsbevissthet. Kapittel 6 inneholder anbefalinger om fremtidig kunnskapsutvikling. I tillegg inneholder rapportens vedlegg en oversikt av litteratursøkene.

2 Hva er innsiderisiko?

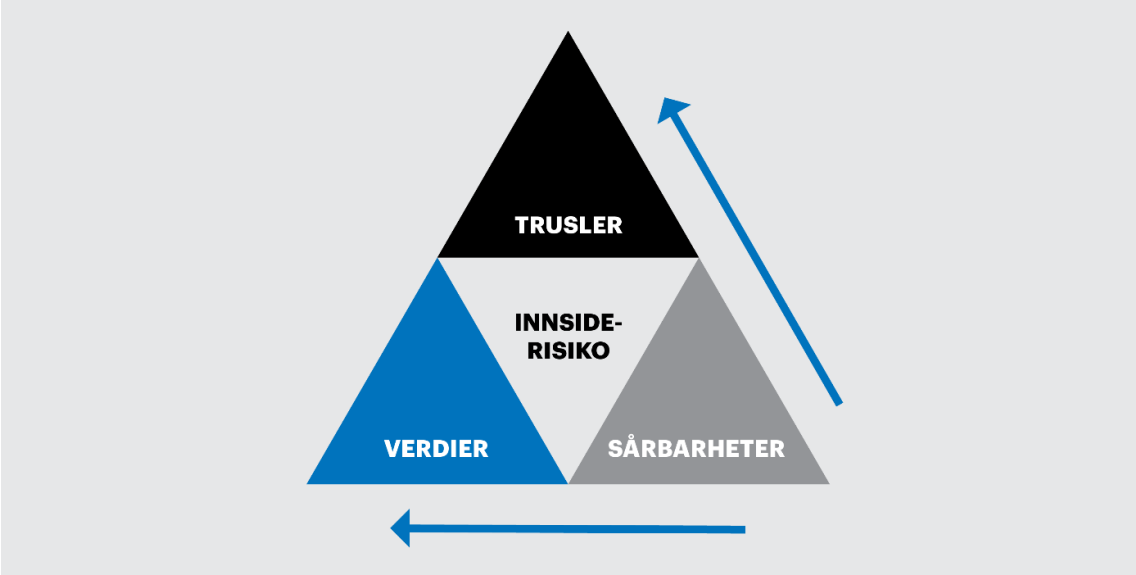
Dette kapittelet inneholder en gjennomgang av forskjellene mellom en ubevisst og en bevisst innsider, samt eksempler på motivasjoner bak innsidevirksomhet. I tillegg vurderes det i hvilken grad det eksisterer forskning på innsidevirksomhet ut fra norske forhold.

2.1 Innsider

Det finnes ulike definisjoner på en innsider. NSM (2020b, s. 9) definerer en innsider som «en nåværende eller tidligere ansatt, konsulent eller kontraktør som har eller har hatt legitim tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, og som misbruker denne kunnskapen og tilgangen for å utføre handlinger som påfører virksomheten skade eller tap.» Politiets sikkerhetstjeneste (PST) (2020, s. 10) definerer en innsider «som en person som utnytter, eller har intensjon om å utnytte, sin legitime tilgang til en virksomhets verdier til uautoriserte formål». Martin (2019, s. 98) definerer en innsider som «en person som utnytter, eller har til hensikt å utnytte, sin autoriserte tilgang på uautoriserte formål».

NSM (2020b, s. 9-10) argumenterer for at innsiderisikoen er både statisk og dynamisk. Risikoen er statisk fordi det vil alltid være personer innenfor en virksomhet som kan skade verdiene til virksomheten gjennom blant annet å «kompromittere, sabotere eller manipulere informasjon og prosesser» (NSM, 2020b, s. 9). Risikoen er også dynamisk, ettersom motivasjoner, prioriteringer og lojalitet hos en arbeidstager kan forandres. På samme måte kan trusselaktører endre sine mål og arbeidsmetoder. Forhold i en virksomhet kan i tillegg ha innflytelse på innsiderisikoen, blant annet ved at sikkerhetstiltak, arbeidsoppgaver og prosesser blir endret.

Innsiderisiko kan forstås ut fra en enkel modell som er skissert i figur 2.1 (DNV-GL, 2019, s. 7). Sikkerhetsloven (2019) §8-4 a) - o) identifiserer sårbarheter som kan føre til økt innsiderisiko. En person som innehar en eller flere av disse sårbarhetene kan bli hindret i å få tilgang til skjermingsverdige objekter og informasjon. Samtidig kan våre nasjonale sikkerhetsinteresser stå i fare dersom relevante sårbarheter ikke er tilstrekkelig identifisert, eller sårbarhetene endres over tid. I de kommende kapitlene skal rapporten derfor undersøke hvordan dagens system for personellsikkerhet er innrettet, og hvilke faktorer som kan være viktige for fremtiden.



Figur 2.1 Innsiderisikoen kan forstås ut fra en kombinasjon av trusler, sårbarheter og verdier (DNV-GL, 2019, s. 7). Illustrasjon: FFI

2.2 Ubevisste og bevisste innsidere

2.2.1 Ubevisste innsidere

Det finnes ulike definisjoner av ubevisste innsidere. DNV-GL (2019, s. 10-11) forklarer at en «uforvarende innsider er en som uten å forstå eller ville det, gjennomfører en handling som resulterer i økt sårbarhet, skade eller tap for virksomheten. Vedkommende kan ha blitt manipulert eller forledet eller vedkommende har ikke kompetanse til å forstå konsekvensene av handlingen sin. Eventuelt kan vedkommende være i en sinnstilstand der uoppmerksomhet eller sløvhet medfører at handlingen blir utført uten at dette er tilsiktet.»

En nærmere forklaring på ubevisste innsidere beskrives av NSM (2020b, s. 11-12). En ubevisst innsider har ikke en intensjon om å være en innsider. Personen har eller har hatt tilgang til verdiene i en virksomhet, og uten onde hensikter er personen årsaken til at en virksomhet opplever skade eller tap. Disse handlingene har ofte en sammenheng med at personen har en lav sikkerhetsbevissthet[1], kombinert med at sikkerhetsstyringen og den daglige sikkerhetsledelsen i virksomheten er ufullstendig. Dessuten kan en trusselaktør forlede, manipulere eller utnytte en person på en måte som fører til at personen utfører innsideaktivitet ubevisst, selv om personen ikke har et ønske om å begå disse handlingene i utgangspunktet. For eksempel kan en trusselaktør manipulere en person til å dele informasjon om verdiene og sårbarhetene i en virksomhet, uten at personen selv er klar over dette. Videre kan den ubevisste innsideren bli utsatt for press etter at

[1] For eksempel kan den aktuelle personen være uoppmerksom, naiv eller ha manglende kjennskap til virksomhetens sikkerhetsprosedyrer. I tillegg kan muntlig lekking av informasjon på offentlig transport, sosiale sammenkomster eller liknende være mindre sporbart enn for eksempel datasikkerhetsbrudd.

virksomhetens verdier har blitt eksponert eller kompromittert. Trusselaktøren kan for eksempel presse personen til å begå mer innsideaktivitet dersom personen frykter for potensielle konsekvenser av at de tidligere ubevisste handlingene blir avdekket. Dermed har personen blitt en bevisst innsider – selv om motivasjonen for dette ikke var der i utgangspunktet.

2.2.2 Bevisste innsidere

En bevisst innsider har andre motivasjoner sammenlignet med en ubevisst innsider. Ifølge NSM (2020b, s. 12-13) har en bevisst innsider en intensjon. Personen er klar over at vedkommende utfører en handling som er uforenlig med virksomhetens interesser. Derimot er ikke nødvendigvis personen klar over konsekvensene av handlingene sine på virksomheten og/eller nasjonale sikkerhetsinteresser. En bevisst innsider kan videre være selvmotivert, en infiltratør eller rekruttert. En selvmotivert innsider tar selv initiativet til innsideaktivitet, og kan utføre disse handlingene uten at en ekstern aktør er innblandet, eller ved at personen henvender seg til en aktør og tilbyr tjenestene sine. Med et ønske om å utføre innsideaktivitet, arbeider en infiltratør bevisst for å få legitim tilgang til en virksomhet og verdiene til virksomheten. På forhånd kan infiltratøren være fra en fremmedstatlig etterretningstjeneste eller rekruttert av en trusselaktør over en kortere eller lengre periode. Som nevnt i avsnittet ovenfor kan en innsider også bli rekruttert av en trusselaktør etter at personen har fått tilgang til verdiene i virksomheten. I begynnelsen har ikke personen et ønske om å bli innsider, men kan bli kultivert, påvirket eller presset av en trusselaktør som vil ha tilgang til virksomhetsverdiene. Innsideren kan raskt gå fra å være en lojal ansatt, som ikke ønsker å skade virksomheten, og over til å bli en bevisst innsider. Generelt velger trusselaktøren å etablere en positiv relasjon til innsideren med hensikt på å skape et forretningsmessig forhold, i stedet for å bruke press, ettersom press innebærer en større risiko. Til tross for dette bruker trusselaktøren de metodene som er nødvendige for å oppnå sine mål.[2]

> Trusselaktøren bruker de metodene som er nødvendige for å oppnå sine mål.

2.2.3 En gråsone mellom ubevisste og bevisste innsidere

Det finnes argumenter for at det eksisterer en gråsone mellom ubevisste og bevisste innsidere. Mange innsidere er et sted midt mellom å være en ubevisst og bevisst innsider. Mange mennesker ser ikke på seg selv som sabotører eller spioner. De forstår ikke at de påfører skade på en virksomhet eller en stat, selv om handlingen tilsier at de er innsidere ut fra enhver definisjon. Mange innsidere vil egentlig ikke innse hva de gjør, selv om de kanskje innerst inne vet at de utfører handlinger som er skadelige for virksomheten og/eller staten.

Videre er det vanskelig å fange opp handlinger som er på grensen til å være ulovlige og som dermed er i en gråsone (DNV-GL, 2019, s. 16). Summen av slike handlinger av en eller flere

[2] Les mer om rekrutteringsfasen på side 18 og 19 i NSMs temarapport om innsidere (2020).

personer kan medføre større sårbarhet, skade eller tap for en virksomhet eller stat enn enkelthandlingene alene.

2.2.4 Eksempler på ulike typer motivasjon for innsidevirksomhet

Årsaken til at mennesker blir innsidere er sammensatt. Det er komplisert og vanskelig å klassifisere innsidere ut fra deres motivasjon – kanskje spesielt fordi motivasjonen kan endres over tid. Mange innsidere klarer heller ikke å forklare hvorfor de handlet som de gjorde, eller de har endret forklaringene sine flere ganger i etterkant. Selv om innsideres motivasjoner i noen tilfeller er klare og tydelige, kan det altså se ut til at dette er unntaket snarere enn regelen.

NSM (2020b, s. 23-26) skriver at innsidere har til felles at de innehar en eller flere menneskelige sårbarheter. Disse sårbarhetene kan enten føre til innsideaktiviteter eller bli utnyttet av trusselaktører som forsøker å tilnærme seg personen eller rekruttere vedkommende. Med dette som grunnlag deler NSM de motiverende faktorene inn i ulike kategorier. Rapporten gjennomgår noen av disse faktorene nå.

Både selvmotiverte og rekrutterte innsidere kan handle ut fra ideologi, skriver NSM (2020b, s. 23). Ideologiske overbevisninger kan bli etablert, styrket eller styrt av samfunnsendringer eller nasjonale og internasjonale forhold. Til felles har disse personene en overbevisning «om at deres meninger, oppfatninger eller opplevelser av en situasjon rettferdiggjør og legitimerer innsidevirksomhet» (NSM, 2020b, s. 23).

NSM (2020b, s. 24-25) belyser at negative forhold på arbeidsplassen kan føre til selvmotivert innsidevirksomhet i form av at personen ønsker å hevne seg eller skade virksomheten fordi personen opplever å bli behandlet urettferdig. Med andre ord kan det utgjøre en sårbarhet hvis en arbeidstaker ikke føler at kollegaer og ledere verdsetter, forstår eller ser arbeidstakeren på en tilstrekkelig måte. For eksempel kan en arbeidstager oppleve at hen ikke involveres i avgjørelser som påvirker vedkommende direkte, oppleve fravær av gode tilbakemeldinger eller føle seg tilsidesatt i forfremmelsesprosesser. På samme måte kan en ansatt gjennom skadelig aktivitet ha et ønske om å påvirke beslutningsprosesser i en virksomhet, slik som nedleggelser, omstruktureringer eller flytting. En trusselaktør kan igjen utnytte sårbarheter som er relatert til forhold på en arbeidsplass ved å påvirke en misfornøyd arbeidstager til å utføre innsideaktiviteter, eller skape en ubevisst innsider ved å utnytte at en person ønsker anerkjennelse. Blant annet kan personen dele sensitive detaljer om virksomheten gjennom samtaler, uten å vite at vedkommende kommuniserer med en trusselaktør.

Mange innsidesaker er knyttet til økonomi (NSM, 2020b, s. 25). Økonomiske sårbarheter kan føre til selvmotivert innsidevirksomhet i form av et ønske om å bli gjeldfri, eller så kan en person bli rekruttert gjennom tilbud om økonomiske gevinster.

Endringer i en livssituasjon som skjer plutselig eller gradvis har ved mange tilfeller forårsaket eller indikert innsideaktivitet (NSM, 2020b, s. 25-26). Hendelser som skilsmisse, sykdom, dødsfall eller liknende kan være traumatisk og skape sårbarheter, som kan føre til ubevisste og bevisste innsidere. Endringer i en livssituasjon kan også aktualisere eller styrke andre sårbarheter

hos en person. Dette kan en trusselaktør enten kultivere ved å tilby hjelp til vedkommende, eller bruke som pressmiddel ved å true om å offentliggjøre hendelsen(e). Til felles er trusselaktørens krav om at vedkommende blir en innsider.

3 Utviklingstrekk

Mennesker og virksomheter påvirkes av ulike forhold i samfunnet som igjen kan påvirke sårbarheter, motivasjoner og kapasiteter. Dette kan føre til at personer og virksomheter blir mottakelige for sikkerhetsmessig uønsket adferd. For å forhindre uønsket aktivitet er det viktig å ha oppdatert kunnskap om hvordan forskjellige trusselaktører opptrer for å nå sine mål og ramme andres verdier. Det eksisterer i liten grad kunnskap om hvordan teknologiske, sosiale, økonomiske, politiske og geopolitiske utviklinger påvirker innsiderisikoen i en norsk kontekst. Med andre ord er det et ytterligere behov for å forske på hvordan ulike trusselaktører opererer mot norske interesser i en personellsikkerhetskontekst.

Forskning på digitale påvirkningsaktiviteter kan gi oss kunnskap om noen av metodene som brukes av trusselaktører, samt hvordan en kan forebygge, avdekke, og håndtere påvirkning og manipulasjon av mennesker med hensyn til innsiderisiko. I dette kapittelet skal rapporten derfor se nærmere på moderne utviklingstrekk som kan føre til innsidevirksomhet. Rapporten gjennomgår først sosiale medier som fenomen. Deretter ser den på mulige tilnærminger til påvirkning (som er skjult eller skadelige for virksomhetene).

3.1 Sosiale medier

3.1.1 Egenskaper

Sosiale medier har en rekke egenskaper som kan gjøre dem til unike verktøy for datainnsamling om, og påvirkning av, mennesker over hele verden. For det første tilrettelegger sosiale medier for pseudonymitet, det vil si muligheten til å utgi seg for å være en annen enn den en er – som oftest for å gjøre informasjonen mer tillitsvekkende for en eventuell målgruppe. For det andre forflater sosiale medier innhold ved å bruke en standard formattering på alt innhold. Brukere har dermed ingen kontekstuelle hint om hvorvidt profiler og innhold er autentiske eller ikke.

Sosiale medier har en verdensomspennende og umiddelbar distribusjon av innhold uten redaksjonelt ansvar. Sosiale medier er dessuten spesielt tilrettelagt for personlig «godkjenning» av informasjon gjennom enkel deling og flagging av innhold en liker. Dette øker troverdigheten til innhold, uten at de kontaktene som har videreformidlet eller flagget innlegg nødvendigvis har sjekket innleggenes sannhetsgehalt. Disse faktorene endrer hvordan vi tolker og håndterer informasjon.

Informasjonen som individuelle brukere ser, er videre valgt automatisk via bruk av algoritmer. Algoritmer er en programvare som automatisk evaluerer og velger innhold som gir mest mulig oppmerksomhet og engasjement. Forskjellige brukere av den samme sosiale medie-plattformen kan av den grunn ha vidt forskjellige inntrykk av samme hendelse. Dette kan igjen styrkes via selvutvelgelse i form av deltakelse i spesialistfora eller grupper rundt ulike temaer. Til sammen kan denne aktiviteten gi en såkalt ekkokammer-effekt, der en kun opplever at andre er enig i det en selv tror.

Sist, men ikke minst, er informasjon som genuine brukere legger ut om seg selv, sine interesser, og sine aktiviteter, åpent tilgjengelig og lett søkbart for alle andre brukere på den samme plattformen og/eller gruppen.

I tillegg til disse egenskapene har vi en stadig økende grad av såkalte sensordata. Dette er data som samles inn om ting en gjør (løper, sover, og så videre), og som ikke krever direkte handlinger (Farsund et al., 2022, s. 18, 19). Et eksempel på dette er smartklokker og liknende, som måler hvor fort en går eller løper, samt hvor en gjør det. Ofte vises disse dataene på sosiale medier. Den økte datainnsamlingen kan gi utfordringer for nasjonal sikkerhet (Farsund et al., 2022, s. 41). For eksempel ble amerikanske soldater i militærleirer i forskjellige land eksponert gjennom bruk av fitnessapper som samlet inn data fra treningsøktene deres. Fra disse dataene kunne en regne ut hvor amerikanske leire befant seg (BBC, 2017; Lockie, 2018; Sly, 2018).

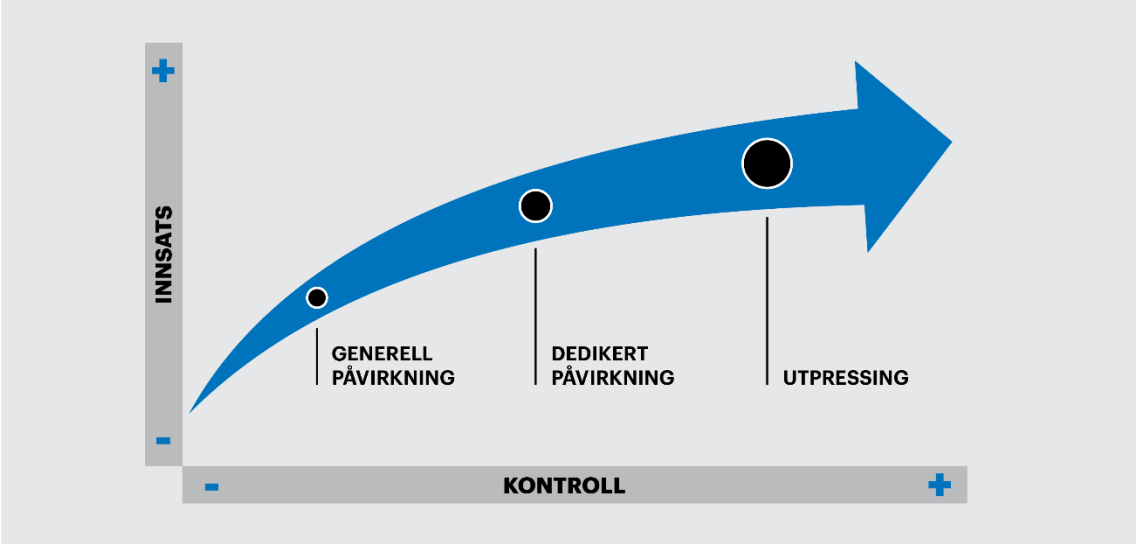
3.1.2 Implikasjoner

En trusselaktør har klare insentiver for å benytte sosiale medier, ettersom bruk av sosiale medier er billige med hensyn til tid, penger og mulige straffetiltak. Der det tidligere var behov for manuell arbeidskraft ved diverse operasjoner, som for eksempel å kartlegge alle som jobber for en bestemt bedrift, er det nå mulig å utføre mange operasjoner automatisk. Det er derfor skalerbart å påvirke eller benytte andre former for sosial manipulasjon av innsidere gjennom sosiale medier. Med skalerbarhet menes det at en evner å gjøre sosial manipulasjon i større omfang enn før, uten at kostnadene eller behovet for arbeidskraft stiger nevneverdig.

Til tross for disse problemene har sosiale medier blitt en del av hverdagen vår. Imidlertid er de «globale sosiale medie-selskapene utenfor Norges jurisdiksjon med hensyn til regulering» og kontroll (Bergh, 2020, s. 33). «Det er mulig å innføre lokal lovgivning om innhold, men … det er uklart hva som kan fjernes innenfor demokratiske rammer» (Bergh, 2020, s. 33). Egenskapene ved sosiale medier gjør det dessuten vanskelig for virksomheter å oppdage eventuelle forsøk på sosial manipulasjon av ansatte. Hvilke konsekvenser har dette for vår nasjonale sikkerhet?

3.2 Mulige påvirkningstilnærminger

Figur 3.2 illustrerer den glidende overgangen mellom de nye mulighetene for påvirkningsaktiviteter gjennom sosiale medier. Disse aktivitetene kan gå fra stor-skala påvirkning av visse målgrupper, til former for utpressing som utenifra vil se ut som klassisk utpressing – men som nå kan forsterkes og automatiseres gjennom tilgang til store mengder data på sosiale medier. Av den grunn vil dette kapittelet belyse potensielle tilnærminger på et overordnet nivå, og kombinere det med eksempler som illustrerer hva som kan oppnås av en trusselaktør.



Figur 3.2 *En fremmed aktør kan utøve generell påvirkning (som kan være både indirekte og direkte), dedikert påvirkning og utpressing. Det krever mindre innsats å utøve generell påvirkning, og dette er vanskeligere for virksomhetene å kontrollere. På den andre siden krever utpressing større innsats, men kan samtidig kontrolleres i større grad sammenlignet med generell påvirkning. Illustrasjon: FFI*

3.2.1 Desinformasjon og misinformasjon

Vi har i liten grad kunnskap om hvordan påvirkningsoperasjoner i det digitale rom – og med langsiktig målsetting – kan føre til økt innsidevirksomhet. Spredning av desinformasjon og misinformasjon er varianter av «cyber-sosiale påvirkningsoperasjoner» (Bergh, 2020, s. 15). Sivertsen et al. (2021, s. 11) beskriver desinformasjon som «utvikling og spredning av bevisst feilaktig eller villedende informasjon i den hensikt å påvirke menneskers virkelighetsoppfatning, holdninger og handlinger.» Forfatterne forklarer at fenomenet ikke er nytt, men at internett og sosiale medier har ført til at en rekke aktører – alt fra fremmede stater til terrororganisasjoner, svindlere og ulike interessegrupper – har fått nye muligheter til å spre desinformasjon med bakgrunn i ulike motiver og formål. Deretter beskriver Sivertsen et al. (2021, s. 11) misinformasjon eller feilinformasjon som «falsk eller misvisende informasjon som en deler fordi en faktisk tror den er sann». Forskjellen mellom desinformasjon og feilinformasjon er hvorvidt det er et bevisst og manipulativt formål bak spredningen av informasjonen, eller om det gjøres i god tro. En aktør som sprer desinformasjon bevisst vil antageligvis ikke stoppe dersom noen gjør aktøren oppmerksom på at informasjonen er feil. En aktør som sprer feilinformasjon vil likevel korrigere adferden dersom det blir påpekt at informasjon er feil, med mindre vedkommende har en sterk overbevisning som er basert på desinformasjon eller konspirasjonsteorier.

Desinformasjon og misinformasjon kan derimot føre til at en kun ser en sterk og villet kampanje som problematisk, mens det over tid være vil sosiale mediers natur som er problemet. Dette skyldes økosystemet[3] til sosiale medier. Bergh (2020, s. 15) forklarer at økosystemet i cyber-sosiale påvirkningsoperasjoner består av en rekke aktører. Iverksetteren lager og laster opp innhold som består av desinformasjon. Deretter sprer iverksetteren, deres ansatte samt direkte støttespillere denne desinformasjonen. Andre aktører kan igjen spre narrativet videre fordi de er enige i narrativet eller ønsker å tjene penger på å spre det videre. De to sistnevnte aktørene er ikke klar over hensikten bak påvirkningsoperasjonen. Miljøet rundt alle disse aktørene består igjen av infrastrukturen[4] til de sosiale mediene, samt automatiserte ressurser som bots og algoritmer. Myndighetene må derfor balansere mellom en potensiell sensurering av egne innbyggere og å stoppe slike påvirkningsforsøk (Bergh, 2020, s. 33).

Myndighetene må balansere mellom en potensiell sensurering av egne innbyggere og å stoppe påvirkningsforsøk.

3.2.2 Generell og indirekte påvirkning

Ansatte bli eksponert for innhold fra pågående påvirkningsforsøk mot demokratier på samme måte som alle andre sosiale medier-brukere. Slikt innhold er en indirekte påvirkning som kan ramme alle uten at noen er utpekt som et spesifikt mål. Dette kan for eksempel skje i forbindelse med valg, diskusjoner rundt temaer som Nato-medlemskap eller massevaksinering i forbindelse med en pandemi. Ekkokammer-effekten som ble diskutert innledningsvis (punkt 3.1.1) kan i tillegg forsterke syn og holdninger rundt et tema ytterligere. Denne type påvirkning er altså ikke direkte rettet mot potensielle innsidere i en virksomhet. Påvirkningsaktiviteten er i stedet en implisitt trussel. Trusselen vil være skadelig dersom personer ender opp med å ha redusert tillit til en virksomhet, og hvis denne reduserte tilliten igjen fører til endrede lojalitetsfølelser overfor virksomheten.

Trusselen vil være skadelig dersom personer ender opp med å ha redusert tillit til en virksomhet, og hvis denne reduserte tilliten igjen fører til endrede lojalitetsfølelser overfor virksomheten.

[3] «Et økosystem er, i overført betydning fra biologien, alle aktørene som er samlet et sted og miljøet rundt dem. I et økosystem er aktører i samspill med miljøet. De forskjellige elementene i økosystemet knyttes sammen gjennom distribusjon av ting de behøver for å overleve.» (Bergh, 2020, s. 15).

[4] Profiler på sosiale medier som legger ut originalt innhold eller interagerer med andre brukere ved å like eller videresende andres innlegg, og som kontrolleres helt eller delvis av operatører eller av bots (Bergh, 2020, s. 14).

3.2.3 Generell og direkte påvirkning

Hvis potensielle innsidere i en virksomhet oppfattes som en klart definert målgruppe, for eksempel ansatte som har sterk interesse for miljøvern eller distriktspolitikk, kan en trusselaktør prøve å utøve mer eksplisitt påvirkning. Metodene ville være de samme som for indirekte påvirkning, det vil si opprettelse, distribusjon og popularisering av innhold som vil appellere til brukeren. Innholdet vinkles i trusselaktørens favør, enten det er sant eller usant. Forskjellen er at målgruppene vil defineres ut fra gruppen som utgjør potensielle innsidere i en virksomhet, og ikke befolkningen generelt. Gjennom sosiale mediers automatiske valg av innhold som matcher brukerens interesser, vil trusselaktøren forsøke å påvirke disse personene mer direkte.

3.2.4 Dedikert påvirkning

Dedikert påvirkning benytter individfokuserte metoder, men baseres fortsatt på påvirkning i motsetning til belønninger eller utpressing. Metodene består ofte av å kartlegge en person, eller en viss type person, og deretter kontakte personene direkte med utgangspunkt i ting som interesserer vedkommende. Målet vil i starten ofte være å få tak i (sensitiv) informasjon, og mindre på at personen endrer oppførsel innenfor virksomheten. En ofte brukt metode er å utgi seg for å være en person i samme bransje, spørre om å få kontakt og etter hvert kanskje invitere personen til å delta i konferanser, seminarer, workshops, og liknende. Ofte betaler fremmede aktører for billetter og benytter smiger, for eksempel ved å spørre om vedkommende kunne tenke seg å holde en presentasjon fordi de er så dyktige innenfor sitt fagfelt. Keir Giles, en britisk forsker som jobber med russisk påvirkning, ble for eksempel kontaktet via LinkedIn av en person som så ut til å være en yngre kvinne i sikkerhetsbransjen, men som viste seg å være en falsk konto med et såkalt «deepfake» bilde (Bridge, 2019).

3.2.5 Utpressing

Dedikert påvirkning kan over tid dreie mot direkte utpressing, der trusselaktøren er i stand til å forlange informasjon eller handlinger direkte fra innsideren. Utpressing kan også være startpunktet. Rollen til sosiale medier vil da være en kilde for informasjon som kan misbrukes (for eksempel at en ansatt har ytret seg hatefullt gjennom falske kontoer eller har vært med i fora som kan føre til pinligheter dersom det oppdages). Ansatte i særs utsatte posisjoner kan dessuten bli oppdaget gjennom sosiale medier, og deretter bli tvunget til å utføre handlinger som forhindrer at trusler mot deres familier realiseres.

NSM (2020a, s. 30) påpeker at utstrakt bruk av sosiale medier fører til at det er enklere for trusselaktører å etablere kontakt med deres målpersoner. Sosiale medier vil da benyttes til å gjennomføre sosial manipulasjon i form av å danne lojalitetsbånd, samt kultivere og å følge opp innsidere. Selv om det er forståelse for at målsøking eller målutvelgelse skjer i åpne kilder og på sosiale medier, har vi i liten grad kunnskap om hvordan innsiderisikoen påvirkes av sosial manipulasjon i det digitale rom – og med langsiktig målsetting. Det er derfor et behov for forskning rundt effekten av sosiale medier på innsidevirksomhet, samt at denne forskningen tilpasses norske forhold.

Det er et behov for forskning rundt effekten av sosiale medier på innsidevirksomhet, samt at denne forskningen tilpasses norske forhold.

4 Faktorer knyttet til vurdering av sikkerhetsmessig skikkethet

En stor del av den nasjonale litteraturen rundt personellsikkerhet kan deles inn i fire hovedområder:

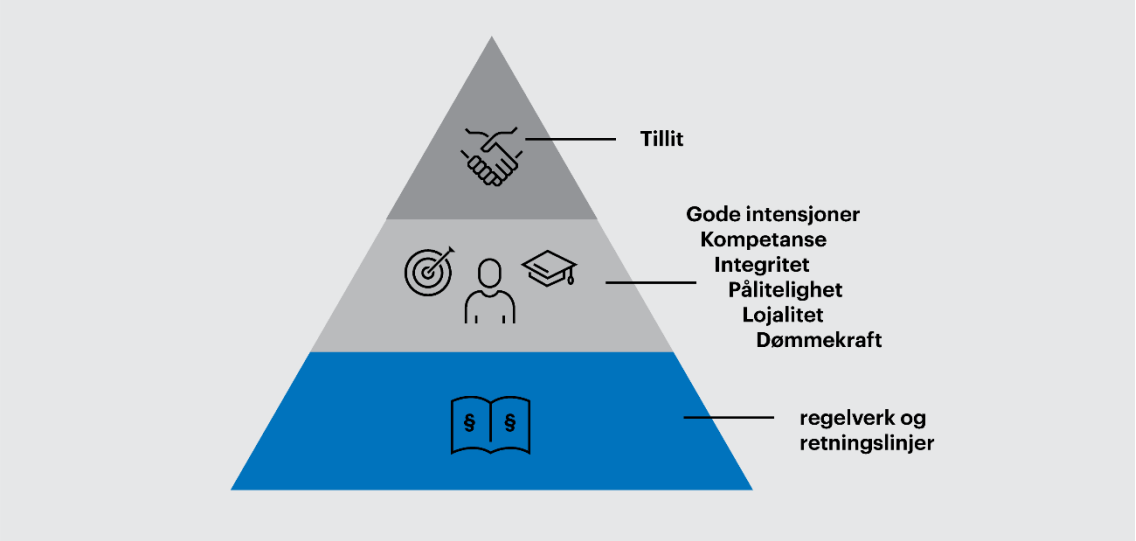
- En rettspolitisk og akademisk debatt omkring personkontroller og sikkerhetsklareringer (Bae, 1983; Bakke, 2017, 2019; Graver, 2021).
- IKT-sikkerhet knyttet til innsidevirksomhet (Abomhara et al., 2018; Gonzalez et al., 2006).
- Studier av personellsikkerhet i masteroppgaver (Benjaminsen, 2017; Berdal, 2018; Hove, 2022; Jacobsen, 2021; Ringstad, 2020; Syvertsen, 2007).
- Veiledningsmateriell utgitt av sikkerhetsmyndighetene (NSM, 2020a; PST et al., 2017).

Et femte alternativ er å se mot den internasjonale litteraturen og vurdere om noe av denne litteraturen kan anvendes i nasjonal forskning på personellsikkerhet. Rapporten skal litt se nærmere på dette alternativet.

4.1 Tillit: Gode intensjoner, kompetanse, integritet og pålitelighet

For å være i stand til å stole på en person eller en organisasjon må en ha grunnlag for å tro på at de har velmenende og vennlige holdninger, er i stand til å gjøre det en forventer av dem, opptrer ærlig og rettferdig i møte med andre, og er konsekvente i sine handlinger i form at de gjør det de sier at de skal gjøre. Martin (2019, s. 117-118) bryter derfor tillit ned i fire hovedelementer. Elementene består av gode intensjoner overfor andre, kompetansen til å gjøre det omgivelsene forventer av en, integritet[5] og pålitelighet[6]. Han anbefaler videre at disse elementene vurderes i en ansettelsesprosess og ved daglig sikkerhetsledelse. De rette psykometriske testene (se delkapittel 4.2) og grundige intervjuer kan dermed kaste lys over personens intensjoner, kompetanse, integritet og pålitelighet, konkluderer han. Disse faktorene kan være viktige når en vurderer sikkerhetsmessig skikkethet.

[5] Integritet defineres som «en person eller institusjons evne og vilje til å handle selvstendig, ærlig og redelig uten å ta hensyn til uvedkommende eller utenforliggende interesser; ubestikkelighet» (Det norske akademis ordbok (NAOB)).
[6] Ektehet; Noen en kan stole eller lite på.



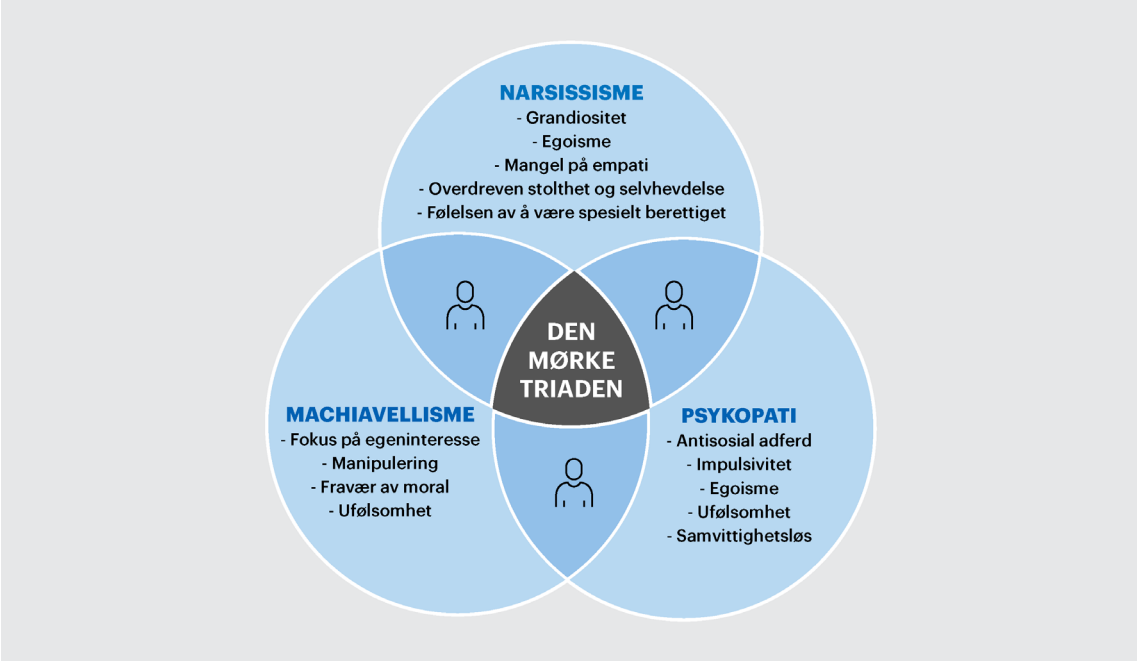
Figur 4.1 Viktige faktorer i en vurdering av sikkerhetsmessig skikkethet. Illustrasjon: FFI

4.2 Personlighetstrekk

En rekke studier fremhever tre personlighetstrekk som assosieres med problematisk adferd, bedre kjent som «den mørke triaden» (Baweja et al., 2019; Central Intelligence Agency, 2014, s. 8-10; CPNI, 2013, s. 11; Jacobsen, 2021; Nurse et al., 2014; Paulhus & Williams, 2002; Shechter & Lang, 2011; Wilder, 2017). Disse mørke trekkene består av *narsissisme*, *psykopati* og *machiavellisme*, der spesielt narsissistiske egenskaper er indikatorer på innsiderisiko (Defense Personnel and Security Research Center, 2014, s. 264-268; Martin, 2019, s. 107). Figur 4.2 inneholder en ikke-uttømmende oversikt over noen av indikatorene for de ulike personlighetstrekkene.

Det er ofte vanskelig å håndtere mennesker som viser slike egenskaper, i og med at de er sjarmerende, overbevisende og ikke ser noe galt i hvordan de oppfører seg. Forskning viser derimot at psykometriske tester kan være særlig nyttige innenfor personellsikkerhet hvis formålet er å avdekke slike personlighetstrekk, ettersom testene har en høy indre og ytre validitet[7].

[7] Med indre validitet menes det at det trekkes korrekte slutninger rundt årsakssammenhenger i en studie. Med ytre validitet menes det hvorvidt funnene kan generaliseres til andre områder.



Figur 4.2 Et utvalg av egenskaper som inngår i den mørke triaden (Jakobwitz & Egan, 2006, s. 332; Lee et al., 2013, s. 169-170; Skeem et al., 2011, s. 98-100). Illustrasjon: FFI

5 Sikkerhetskultur og sikkerhetsledelse

En god sikkerhetskultur og et godt lederskap er viktig for å redusere risikoen for innsidevirksomhet også etter at personer eventuelt har fått tilgang til, eller blitt en del av, en virksomhet. Heyerdahl (2022) har blant annet publisert en vitenskapelig artikkel om risikostyring i Norge der hun har intervjuet 40 respondenter som arbeider med sikkerhet til daglig, som er verdt å lese. Utover dette arbeidet kan temaer som jobbtilfredshet og sikkerhetsbevissthet belyses mer gjennom forskning. Rapporten skal se nærmere på disse temaene i dette kapittelet.

5.1 Jobbtilfredshet

Martin (2019, s. 102) legger særlig vekt på at risikoen for innsidevirksomhet kan øke med manglende jobbtilfredshet. Han viser til forskning som er utført av CPNI (2013). Blant annet har de kommet frem til at en gjentagende årsak til innsidevirksomhet er at innsidere føler seg undervurdert og dårlig behandlet på arbeidsplassen sin. En innsider kan derfor være en middels rangert ansatt som har jobbet i en organisasjon i mange år, og som ikke føler seg anerkjent. I noen tilfeller kan disse personene bli manipulert eller presset av eksterne trusselaktører.

Misnøye på jobb kan altså potensielt være en risikofaktor for en virksomhet. I tillegg kan det være utfordrende for ledere å balansere kontroll og autonomi opp mot jobbtilfredshet blant arbeidstagere. For å kunne innføre målrettede tiltak er det derfor behov for å undersøke hvilke forhold som fører til manglende jobbtilfredshet, samt hvordan disse forholdene kan utvikles til uønsket adferd. Flere spørsmål kan belyses gjennom forskning, som hva jobbtilfredshet er, hvordan det kan skapes og styrkes (for eksempel gjennom stolthet), samt hvilke faktorer hos ansatte, i en virksomhet og i samfunnet for øvrig som kan øke misnøye og eventuelt utgjøre en risiko for en virksomhet.

5.2 Sikkerhetsbevissthet

Sikkerhetsbevissthet handler om at en har vilje og evne til å håndtere virksomhetens verdier i tråd med gitte retningslinjer og regelverk (NSM, 2020b, s. 26). Mennesker med lav eller manglende sikkerhetsbevissthet kan imidlertid kompromittere sensitiv informasjon og dermed bli ubevisste innsidere. De kan også være mer sårbare for tilnærming og kultivering fra trusselaktører (NSM, 2020b, s. 26), for eksempel gjennom sosiale medier.

Forskning på digital sikkerhetsbevissthet og kunnskap er med andre ord essensielt i arbeidet med å videreutvikle forebyggende sikkerhet som fagfelt. Blant annet kan forskning bidra til at en kan måle sikkerhetsbevissthet. Videre kan forskning føre til mer kunnskap om effekten av sikkerhetsbevissthet på å håndtere egne sårbarheter, samt andre sikkerhetsrelaterte forhold. I tillegg kan analyser av rapporterte sikkerhetsbrudd brukes til å evaluere effekten av eventuelt konkrete tiltak som tidligere har blitt innført for å motvirke sikkerhetsbrudd, og om disse tiltakene må forbedres.

Forskning på digital sikkerhetsbevissthet- og kunnskap er essensielt i arbeidet med å videreutvikle forebyggende sikkerhet som fagfelt.

5.3 Rapportering av sikkerhetstruende hendelser og sårbarheter

Ledere og medarbeidere i virksomhetene kan være i stand til å fange opp adferd som ikke blir oppdaget gjennom en ansettelsesprosess. Martin (2019, s. 107-108) belyser at en person som kan være på vei til å bli en bevisst innsider ofte viser tegn på misnøye, for eksempel ved at personen yter dårligere i arbeidet sitt, klager ofte, har et fiendtlig språk, eller viser symptomer på psykiske utfordringer eller rusavhengighet. Ledere og kollegaer er ofte godt egnet til å legge merke til disse faresignalene. I flere tilfeller der innsideaktivitet har blitt oppdaget har det kommet frem at kollegaer og ledere har vært kjent med unormal adferd og antydning til sårbarheter hos sin kollega, men valgt å ikke håndtere eller rapportere det. Den manglende responsen kan skyldes relasjonelle bånd, kognitive bias eller andre sosiale mekanismer. Det vil si at det er viktig å ha mekanismer som gir mulighet for å rapportere bekymringer på en diskret måte, og at det iverksettes passende tiltak.

Det er viktig å ha mekanismer som muliggjør rapportering av bekymringer på en diskret måte, og at det iverksettes passende tiltak.

6 Behov for kunnskapsutvikling

Hensikten med denne rapporten er å bidra til en kunnskapsoppsummering rundt innsiderisiko ut fra tilgjengelig og relevant litteratur. Rapporten avdekker at det er et stort behov for nasjonal forskning på personellsikkerhet som tar hensyn til norske forhold.

En rekke temaområder bør være gjenstand for nasjonal og åpen forskning:

- Det bør forskes på hvordan påvirkningsoperasjoner i det digitale rom kan føre til økt innsidevirksomhet.
- Forskningen bør se på faktorer knyttet til vurderinger av sikkerhetsmessig skikkethet.
- Forskningen bør ta for seg innsiderisiko og sikkerhetskultur ut fra norske kulturelle forhold, ettersom nasjonale kulturer og organisasjonskulturer ofte er unike.
- Det bør forskes mer på hvordan eksisterende kunnskap og kompetanse innenfor ledelse, organisasjonsutvikling og pedagogikk kan anvendes i en sikkerhetssammenheng.

Imidlertid smelter trusler i det fysiske og digitale rom sammen, og påvirker hverandre gjensidig. Dette innebærer at kun enkle trusler avgrenses innenfor ett enkelt domene, ettersom mer avanserte trusler umiddelbart får en større angrepsflate. Menneskelige faktorer forsterker i tillegg kompleksiteten i disse truslene. En tverrfaglig tilnærming må med andre ord til for å møte en sammensatt utfordring.

Forskning på personellsikkerhet bør etableres som et bærekraftig fagområde i Norge, der forskningen kontinuerlig utvikles og oppdateres. Med den rette tilnærmingen kan Norge bli et foregangsland innenfor forskning på personellsikkerhet.

Forskning på personellsikkerhet bør etableres som et bærekraftig fagområde i Norge, der forskningen kontinuerlig utvikles og oppdateres. Med den rette tilnærmingen kan Norge bli et foregangsland innenfor forskning på personellsikkerhet.

Vedlegg

A Treff på norske søkeord i samfunnsvitenskapelige databaser

Tabell A.1 Treff på norske søkeord, relatert til innsiderisiko og personellsikkerhetsarbeid, i samfunnsvitenskapelige databaser. Tallene i parentes viser antall relevante og fagfellevurderte vitenskapelige publikasjoner innenfor hvert søketreff. Mange av søketreffene er sammenfallende, og derfor inneholder siste rad totalt antall relevante søketreff: 3. (30.01.2023)

	ISI Web of Knowledge	IBSS	Sociological Abstracts	Scopus	Idunn
«innsiderisiko»	0	0	0	0	0
«innsidetrussel»	0	0	0	0	1 **(0)**
«innsidevirksomhet»	0	0	0	0	0
«innsideaktivitet»	0	0	0	0	0
«spionasje»	0	0	0	0	110 **(0)**
«kompromittere informasjon»	0	0	0	0	1 **(0)**
«lekke informasjon»	0	0	0	0	151 **(2)**
«sabotasje»	0	0	0	0	140 **(0)**
«personellsikkerhet»	0	0	0	0	5 **(3)**
«forebyggende sikkerhet»	0	0	0	0	1152 **(2)**
«forebyggende sikkerhetstjeneste»	0	0	0	0	61 **(3)**
«forebyggende sikkerhetsarbeid»	0	0	0	0	35 **(1)**
«sikkerhetsklarering»	0	0	0	0	33 **(3)**
«sikkerhetsmessig skikkethet»	0	0	0	0	15 **(3)**

«sikkerhetsmessig bevissthet»	0	0	0	0	84 **(0)**
«sikkerhetsbevissthet»	0	0	0	0	1 **(0)**
«sikkerhetsledelse»	0	0	0	0	6 **(0)**
«sikkerhetskultur»	0	0	0	0	19 **(0)**
Totalt	0	0	0	0	**3 (ulike artikler)**

B Treff på engelske søkeord i Brage

Tabell B.1 Treff på relevante engelske søkeord i Brage knyttet til vitenskapelige publikasjoner rundt personellsikkerhet fra et utvalg av norske forskningsinstitusjoner. Artikler som oppfattes som særlig relevante er fremhevet i parentes. (01.02.2023)

	UiO	BI	INN	Nord universitet	UiS	FHS	NTNU	UiB	PH	USN	UiA	Oslo-Met
«insider risk»	0	0	0	706	2539	0	0	0	0	0	0	0
«insider threat»	2 **(1 MA[8])**	3	200	370	1075	0	0	5	0	0	0	0
«espionage»	5 (0)	9	2	10	39 **(1)**	0	0	44	0	0	0	0
«personnel security»	1 **(1 MA)**	0	211	437	1260	0	0	1	0	0	0	0
«security clearance»	0	41	21	43	247	0	2	523	0	0	0	0
«vetting process»	868	0	0	0	0	0	0	0	0	0	0	0
«security management»	6 **(1)**	1941	842	1451	3414	0	101	4981	0	0	5	0
«security culture»	3	1182	641	1104	1993	0	78	4138	0	0	0	0
Antall relevante søketreff	**2**	**1**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

[8] Masteroppgave

C Treff i Web of Science knyttet til norske utdanningsinstitusjoner

Tabell C.1 Avansert søk i Web of Science (WoS) på fagfellevurderte artikler i tilknytning til UiO. Artikler som omhandler innsiderisiko innenfor personellsikkerhet – og ikke IKT-sikkerhet eller fysisk sikkerhet – ansees som et relevant treff. (01.02.2023)

Søkestreng i avansert søk i WoS	**Antall treff**	**Antall relevante treff**
(OG=(University of Oslo)) AND TS=(insider AND risk)	4	0
(OG=(University of Oslo)) AND TS=(insider AND threat)	2	0
(OG=(University of Oslo)) AND TS=(espionage)	4	0
(OG=(University of Oslo)) AND TS=(security AND clearance)	0	0
(OG=(University of Oslo)) AND TS=(vetting AND process)	1	0
(OG=(University of Oslo)) AND TS=(protective AND security)	1	1
(OG=(University of Oslo)) AND TS=(security AND management)	117	2
(OG=(University of Oslo)) AND TS=(safety AND management)	346	0
(OG=(University of Oslo)) AND TS=(risk AND management)	1684	0
(OG=(University of Oslo)) AND TS=(security AND culture)	17	0
(OG=(University of Oslo)) AND TS=(safety AND culture)	76	0
(((OG=(University of Oslo)) AND TS=(Personnel AND Security)) AND DT=(Article)) AND ALL=(Norway)	6	0
(((OG=(University of Oslo)) AND TS=(Insider AND Threat)) AND DT=(Article)) AND ALL=(Norway)	0	0
(((OG=(University of Oslo)) AND TS=(Insider AND Risk)) AND DT=(Article)) AND ALL=(Norway)	4	0
Totalt	2262	**3 (2 ulike artikler)**

Tabell C.2 Avansert søk i Web of Science (WoS) på fagfellevurderte artikler i tilknytning til OsloMet, Artikler som omhandler innsiderisiko innenfor personellsikkerhet – og ikke IKT-sikkerhet eller fysisk sikkerhet – ansees som et relevant treff. (01.02.2023)

Søkestreng i avansert søk i WoS	**Antall treff**	**Antall relevante treff**
(OG=(Oslo Metropolitan University)) AND TS=(insider AND risk)	0	0
(OG=(Oslo Metropolitan University)) AND TS=(insider AND threat)	0	0
(OG=(Oslo Metropolitan University)) AND TS=(espionage)	0	0
(OG=(Oslo Metropolitan University)) AND TS=(security AND clearance)	0	0
(OG=(Oslo Metropolitan University)) AND TS=(vetting AND process)	0	0
(OG=(Oslo Metropolitan University)) AND TS=(protective AND security)	0	0
(OG=(Oslo Metropolitan University)) AND TS=(security AND management)	0	0
(OG=(Oslo Metropolitan University)) AND TS=(risk AND management)	0	0
(OG=(Oslo Metropolitan University)) AND TS=(safety AND management)	0	0
(OG=(Oslo Metropolitan University)) AND TS=(security AND culture)	0	0
(OG=(Oslo Metropolitan University)) AND TS=(safety AND culture)	0	0
(((OG=(Oslo Metropolitan University)) AND TS=(Personnel AND Security)) AND DT=(Article)) AND ALL=(Norway)	0	0
(((OG=(Oslo Metropolitan University)) AND TS=(Insider AND Threat)) AND DT=(Article)) AND ALL=(Norway)	0	0
(((OG=(Oslo Metropolitan University)) AND TS=(Insider AND Risk)) AND DT=(Article)) AND ALL=(Norway)	0	0
Totalt	0	**0**

Tabell C.3 Avansert søk i Web of Science (WoS) på fagfellevurderte artikler i tilknytning til NTNU. Artikler som omhandler innsiderisiko innenfor personellsikkerhet – og ikke IKT-sikkerhet eller fysisk sikkerhet – ansees som et relevant treff. (01.02.2023)

Søkestreng i avansert søk i WoS	**Antall treff**	**Antall relevante treff**
(OG=(Norwegian University of Science & Technology (NTNU))) AND TS=(insider AND risk)	0	0
(OG=(Norwegian University of Science & Technology (NTNU))) AND TS=(insider AND threat)	0	0
OG=(Norwegian University of Science & Technology (NTNU))) AND TS=(espionage)	0	0
(OG=(Norwegian University of Science & Technology (NTNU))) AND TS=(security AND clearance)	0	0
(OG=(Norwegian University of Science & Technology (NTNU))) AND TS=(vetting AND process)	9	0
(OG=(Norwegian University of Science & Technology (NTNU))) AND TS=(protective AND security)	5	0
(OG=(Norwegian University of Science & Technology (NTNU))) AND TS=(security AND management)	4	0
(OG=(Norwegian University of Science & Technology (NTNU))) AND TS=(risk AND management)	997	0
(OG=(Norwegian University of Science & Technology (NTNU))) AND TS=(safety AND management)	413	0
(OG=(Norwegian University of Science & Technology (NTNU))) AND TS=(security AND culture)	0	0
(OG=(Norwegian University of Science & Technology (NTNU))) AND TS=(safety AND culture)	111	0
(((OG=(Norwegian University of Science & Technology)) AND TS=(Personnel AND Security)) AND DT=(Article)) AND ALL=(Norway)	0	0
(((OG=(Norwegian University of Science & Technology)) AND TS=(Insider AND Threat)) AND DT=(Article)) AND ALL=(Norway)	0	0
(((OG=(Norwegian University of Science & Technology)) AND TS=(Insider AND Risk)) AND DT=(Article)) AND ALL=(Norway)	0	0
Totalt	1539	**0**

Tabell C.4 Avansert søk i Web of Science (WoS) på fagfellevurderte artikler i tilknytning til UiB. Artikler som omhandler innsiderisiko innenfor personellsikkerhet – og ikke IKT-sikkerhet eller fysisk sikkerhet – ansees som et relevant treff. (01.02.2023)

Søkestreng i avansert søk i WoS	**Antall treff**	**Antall relevante treff**
(OG=(University of Bergen)) AND TS=(insider AND risk)	0	0
(OG=(University of Bergen)) AND TS=(insider AND threat)	0	0
(OG=(University of Bergen)) AND TS=(espionage)	2	0
(OG=(University of Bergen)) AND TS=(security AND clearance)	1	0
(OG=(University of Bergen)) AND TS=(vetting AND process)	2	0
(OG=(University of Bergen)) AND TS=(protective AND security)	5	0
(OG=(University of Bergen)) AND TS=(security AND management)	61	0
(OG=(University of Bergen)) AND TS=(risk AND management)	711	0
(OG=(University of Bergen)) AND TS=(safety AND management)	167	0
(OG=(University of Bergen)) AND TS=(security AND culture)	9	0
(OG=(University of Bergen)) AND TS=(safety AND culture)	49	0
(((OG=(University of Bergen)) AND TS=(Personnel AND Security)) AND DT=(Article)) AND ALL=(Norway)	5	0
(((OG=(University of Bergen)) AND TS=(Insider AND Threat)) AND DT=(Article)) AND ALL=(Norway)	0	0
(((OG=(University of Bergen)) AND TS=(Insider AND Risk)) AND DT=(Article)) AND ALL=(Norway)	0	0
Totalt	1012	**0**

Tabell C.5 Avansert søk i Web of Science (WoS) på fagfellevurderte artikler i tilknytning til UiS. Artikler som omhandler innsiderisiko innenfor personellsikkerhet – og ikke IKT-sikkerhet eller fysisk sikkerhet – ansees som et relevant treff. (01.02.2023)

Søkestreng i avansert søk i WoS	**Antall treff**	**Antall relevante treff**
(OG=(University of Stavanger)) AND TS=(insider AND risk)	0	0
(OG=(University of Stavanger)) AND TS=(insider AND threat)	0	0
(OG=(University of Stavanger)) AND TS=(espionage)	0	0
(OG=(University of Stavanger)) AND TS=(security AND clearance)	0	0
(OG=(University of Stavanger)) AND TS=(vetting AND process)	0	0
(OG=(University of Stavanger)) AND TS=(protective AND security)	0	0
(OG=(University of Stavanger)) AND TS=(security AND management)	0	0
(OG=(University of Stavanger)) AND TS=(risk AND management)	0	0
(OG=(University of Stavanger)) AND TS=(safety AND management)	0	0
(OG=(University of Stavanger)) AND TS=(security AND culture)	0	0
(OG=(University of Stavanger)) AND TS=(safety AND culture)	0	0
(((OG=(University of Stavanger)) AND TS=(Personnel AND Security)) AND DT=(Article)) AND ALL=(Norway)	0	0
(((OG=(University of Stavanger)) AND TS=(Insider AND Threat)) AND DT=(Article)) AND ALL=(Norway)	0	0
(((OG=(University of Stavanger)) AND TS=(Insider AND Risk)) AND DT=(Article)) AND ALL=(Norway)	0	0
Totalt	0	**0**

Tabell C.6 Avansert søk i Web of Science (WoS) på fagfellevurderte artikler i tilknytning til UiT. Artikler som omhandler innsiderisiko innenfor personellsikkerhet – og ikke IKT-sikkerhet eller fysisk sikkerhet – ansees som et relevant treff. (01.02.2023)

Søkestreng i avansert søk i WoS	**Antall treff**	**Antall relevante treff**
(OG=(The Arctic University of Norway)) AND TS=(insider AND risk)	0	0
(OG=(The Arctic University of Norway)) AND TS=(insider AND threat)	0	0
(OG=(The Arctic University of Norway)) AND TS=(espionage)	0	0
(OG=(The Arctic University of Norway)) AND TS=(security AND clearance)	0	0
(OG=(The Arctic University of Norway)) AND TS=(vetting AND process)	0	0
(OG=(The Arctic University of Norway)) AND TS=(protective AND security)	0	0
(OG=(The Arctic University of Norway)) AND TS=(security AND management)	0	0
(OG=(The Arctic University of Norway)) AND TS=(risk AND management)	0	0
(OG=(The Arctic University of Norway)) AND TS=(safety AND management)	0	0
(OG=(The Arctic University of Norway)) AND TS=(security AND culture)	0	0
(OG=(The Arctic University of Norway)) AND TS=(safety AND culture)	0	0
(((OG=(The Arctic University of Norway)) AND TS=(Personnel AND Security)) AND DT=(Article)) AND ALL=(Norway)	0	0
(((OG=(The Arctic University of Norway)) AND TS=(Insider AND Threat)) AND DT=(Article)) AND ALL=(Norway)	0	0
(((OG=(The Arctic University of Norway)) AND TS=(Insider AND Risk)) AND DT=(Article)) AND ALL=(Norway)	0	0
Totalt	0	**0**

Tabell C.7 Avansert søk i Web of Science (WoS) på fagfellevurderte artikler i tilknytning til Nord universitet. Artikler som omhandler innsiderisiko innenfor personellsikkerhet – og ikke IKT-sikkerhet eller fysisk sikkerhet – ansees som et relevant treff. (01.02.2023)

Søkestreng i avansert søk i WoS	**Antall treff**	**Antall relevante treff**
(OG=(Nord University)) AND TS=(insider AND risk)	0	0
(OG=(Nord University)) AND TS=(insider AND threat)	0	0
(OG=(Nord University)) AND TS=(espionage)	0	0
(OG=(Nord University)) AND TS=(security AND clearance)	0	0
(OG=(Nord University)) AND TS=(vetting AND process)	1	0
(OG=(Nord University)) AND TS=(protective AND security)	0	0
(OG=(Nord University)) AND TS=(security AND management)	7	0
(OG=(Nord University)) AND TS=(risk AND management)	54	0
(OG=(Nord University)) AND TS=(safety AND management)	45	0
(OG=(Nord University)) AND TS=(security AND culture)	2	0
(OG=(Nord University)) AND TS=(safety AND culture)	15	0
(((OG=(Nord University)) AND TS=(Personnel AND Security)) AND DT=(Article)) AND ALL=(Norway)	1	0
(((OG=(Nord University)) AND TS=(Insider AND Threat)) AND DT=(Article)) AND ALL=(Norway)	0	0
(((OG=(Nord University)) AND TS=(Insider AND Risk)) AND DT=(Article)) AND ALL=(Norway)	0	0
Totalt	125	**0**

Tabell C.8 Avansert søk i Web of Science (WoS) på fagfellevurderte artikler i tilknytning til UiA. Artikler som omhandler innsiderisiko innenfor personellsikkerhet – og ikke IKT-sikkerhet eller fysisk sikkerhet – ansees som et relevant treff. (01.02.2023)

Søkestreng i avansert søk i WoS	**Antall treff**	**Antall relevante treff**
(OG=(University of Agder)) AND TS=(insider AND risk)	2	1
(OG=(University of Agder)) AND TS=(insider AND threat)	1	1
(OG=(University of Agder)) AND TS=(espionage)	1	1
(OG=(University of Agder)) AND TS=(security AND clearance)	0	0
(OG=(University of Agder)) AND TS=(vetting AND process)	0	0
(OG=(University of Agder)) AND TS=(protective AND security)	0	0
(OG=(University of Agder)) AND TS=(security AND management)	45	0
(OG=(University of Agder)) AND TS=(risk AND management)	107	0
(OG=(University of Agder)) AND TS=(safety AND management)	25	0
(OG=(University of Agder)) AND TS=(security AND culture)	5	0
(OG=(University of Agder)) AND TS=(safety AND culture)	5	0
(((OG=(University of Agder)) AND TS=(Personnel AND Security)) AND DT=(Article)) AND ALL=(Norway)	1	0
(((OG=(University of Agder)) AND TS=(Insider AND Threat)) AND DT=(Article)) AND ALL=(Norway)	0	0
(((OG=(University of Agder)) AND TS=(Insider AND Risk)) AND DT=(Article)) AND ALL=(Norway)	1	0
Totalt	193	3 **(2 ulike artikler)**

Tabell C.9 Avansert søk i Web of Science (WoS) på fagfellevurderte artikler i tilknytning til USN. Artikler som omhandler innsiderisiko innenfor personellsikkerhet – og ikke IKT-sikkerhet eller fysisk sikkerhet – ansees som et relevant treff. (01.02.2023)

Søkestreng i avansert søk i WoS	**Antall treff**	**Antall relevante treff**
(OG=(University of South-Eastern Norway)) AND TS=(insider AND risk)	0	0
(OG=(University of South-Eastern Norway)) AND TS=(insider AND threat)	0	0
(OG=(University of South-Eastern Norway)) AND TS=(espionage)	0	0
(OG=(University of South-Eastern Norway)) AND TS=(security AND clearance)	0	0
(OG=(University of South-Eastern Norway)) AND TS=(vetting AND process)	0	0
(OG=(University of South-Eastern Norway)) AND TS=(protective AND security)	0	0
(OG=(University of South-Eastern Norway)) AND TS=(security AND management)	0	0
(OG=(University of South-Eastern Norway)) AND TS=(risk AND management)	0	0
(OG=(University of South-Eastern Norway)) AND TS=(safety AND management)	0	0
(OG=(University of South-Eastern Norway)) AND TS=(security AND culture)	0	0
(OG=(University of South-Eastern Norway)) AND TS=(safety AND culture)	0	0
(((OG=(University of South-Eastern Norway)) AND TS=(Personnel AND Security)) AND DT=(Article)) AND ALL=(Norway)	0	0
(((OG=(University of South-Eastern Norway)) AND TS=(Insider AND Threat)) AND DT=(Article)) AND ALL=(Norway)	0	0
(((OG=(University of South-Eastern Norway)) AND TS=(Insider AND Risk)) AND DT=(Article)) AND ALL=(Norway)	0	0
Totalt	0	**0**

Tabell C.10 Avansert søk i Web of Science (WoS) på fagfellevurderte artikler i tilknytning til PH. Artikler som omhandler innsiderisiko innenfor personellsikkerhet – og ikke IKT-sikkerhet eller fysisk sikkerhet – ansees som et relevant treff. (01.02.2023)

Søkestreng i avansert søk i WoS	**Antall treff**	**Antall relevante treff**
(OG=(Norwegian Police University College)) AND TS=(insider AND risk)	0	0
(OG=(Norwegian Police University College)) AND TS=(insider AND threat)	0	0
(OG=(Norwegian Police University College)) AND TS=(espionage)	0	0
(OG=(Norwegian Police University College)) AND TS=(security AND clearance)	0	0
(OG=(Norwegian Police University College)) AND TS=(vetting AND process)	0	0
(OG=(Norwegian Police University College)) AND TS=(protective AND security)	0	0
(OG=(Norwegian Police University College)) AND TS=(security AND management)	2	0
(OG=(Norwegian Police University College)) AND TS=(risk AND management)	6	0
(OG=(Norwegian Police University College)) AND TS=(safety AND management)	0	0
(OG=(Norwegian Police University College)) AND TS=(security AND culture)	0	0
(OG=(Norwegian Police University College)) AND TS=(safety AND culture)	0	0
(((OG=(Norwegian Police University College)) AND TS=(Personnel AND Security)) AND DT=(Article)) AND ALL=(Norway)	0	0
(((OG=(Norwegian Police University College)) AND TS=(Insider AND Threat)) AND DT=(Article)) AND ALL=(Norway)	0	0
(((OG=(Norwegian Police University College)) AND TS=(Insider AND Risk)) AND DT=(Article)) AND ALL=(Norway)	0	0
Totalt	8	**0**

Tabell C.11 Avansert søk i Web of Science (WoS) på fagfellevurderte artikler i tilknytning til FHS. Artikler som omhandler innsiderisiko innenfor personellsikkerhet – og ikke IKT-sikkerhet eller fysisk sikkerhet – ansees som et relevant treff. (01.02.2023)

Søkestreng i avansert søk i WoS	**Antall treff**	**Antall relevante treff**
(OG=(Norwegian Defence University College)) AND TS=(insider AND risk)	0	0
(OG=(Norwegian Defence University College)) AND TS=(insider AND threat)	0	0
(OG=(Norwegian Defence University College)) AND TS=(espionage)	0	0
(OG=(Norwegian Defence University College)) AND TS=(security AND clearance)	0	0
(OG=(Norwegian Defence University College)) AND TS=(vetting AND process)	0	0
(OG=(Norwegian Defence University College)) AND TS=(protective AND security)	0	0
(OG=(Norwegian Defence University College)) AND TS=(security AND management)	2	0
(OG=(Norwegian Defence University College)) AND TS=(risk AND management)	1	0
(OG=(Norwegian Defence University College)) AND TS=(safety AND management)	1	0
(OG=(Norwegian Defence University College)) AND TS=(security AND culture)	0	0
(OG=(Norwegian Defence University College)) AND TS=(safety AND culture)	0	0
(((OG=(Norwegian Defence University College)) AND TS=(Personnel AND Security)) AND DT=(Article)) AND ALL=(Norway)	0	0
(((OG=(Norwegian Defence University College)) AND TS=(Insider AND Threat)) AND DT=(Article)) AND ALL=(Norway)	0	0
(((OG=(Norwegian Defence University College)) AND TS=(Insider AND Risk)) AND DT=(Article)) AND ALL=(Norway)	0	0
Totalt	4	**0**

Referanser

Abomhara, M., Køien, G. M., Oleshchuk, V. A. & Hamid, M. (2018). Towards Risk-aware Access Control Framework for Healthcare Information Sharing. 4th International Conference on Information Systems Security and Privacy (ICISSP), Funchal, Portugal.

Almond, G. A. & Verba, S. (1963). *The civic culture*. Princeton University Press.

Bae, O. J. (1983). Rikets hemmeligheter. *Lov og Rett*, *22*(6), 275-285. https://doi.org/10.18261/ISSN1504-3061-1983-06-02

Bakke, A. (2017). Individets rettsstilling ved sikkerhetstjenestens personkontrollundersøkelser. *Lov og Rett*, *56*(10), 571-589. https://doi.org/10.18261/issn.1504-3061-2017-10-02

Bakke, A. (2019). Refleksjoner over sikkerhetsklarering som virkemiddel. *Lov og Rett*, *58*(2), 82-93. https://doi.org/10.18261/issn.1504-3061-2019-02-03

Baweja, J. A., Mcgrath, S. M., Burchett, D. & Jaros, S. L. (2019). *An Evaluation of the Utility of Expanding Psychological Screening to Prevent Insider Attacks* (2019-067). PERSEREC. https://www.dhra.mil/Portals/52/Documents/perserec/reports/TR-19-05-Evaluation-of-Utility-Expanding-Psychological-Screen.pdf

BBC. (2017, 29.01.2018). *Fitness app Strava lights up staff at military bases*. BBC News. Hentet 03.03.2023 fra https://www.bbc.com/news/technology-42853072

Benjaminsen, T. (2017). *The Norwegian Downsizing Approach in Terms of the Insider Threat - An interpretive study* [NTNU].

Berdal, S. J. (2018). *A Holistic Approach to Insider Threat Detection* [Universitetet i Oslo].

Bergh, A. (2020). *Påvirkningsoperasjoner i sosiale medier - oversikt og utfordringer* (20/01694). Forsvarets forskningsinstitutt. https://www.ffi.no/publikasjoner/arkiv/pavirkningsoperasjoner-i-sosiale-medier-oversikt-og-utfordringer

Bos, K. v. d., Wilke, H. A. M. & Lind, E. A. (1998). When Do We Need Procedural Fairness? The Role of Trust in Authority. *Journal of Personality and Social Psychology*, *75*(6), 1449-1458. https://doi.org/10.1037//0022-3514.75.6.1449

Bridge, M. (2019, 21.06.2019). *Russians created AI redhead on LinkedIn to steal military secrets*. The Times. Hentet 03.03.2023 fra https://www.thetimes.co.uk/article/russians-created-ai-redhead-on-linkedin-to-steal-military-secrets-k2d20lc2z

Central Intelligence Agency. (2014). *Psychology of Treason*. The IC's Journal for the Intelligence Professional. https://www.cia.gov/readingroom/docs/DOC_0006183135.pdf

CPNI. (2013). *CPNI Insider Data Collection Study. Report of Main Findings.* https://www.cpni.gov.uk/system/files/documents/63/29/insider-data-collection-study-report-of-main-findings.pdf

Dalton, R. J. (2004). *Democratic Challenges, Democratic Choices: The Erosion of Political Support in Advanced Industrial Democracies*. Oxford University Press.

Defense Personnel and Security Research Center. (2014). *Adjucative Desk Reference. Assisting Security Clearance Adjudicators, Investigators, and Security Managers in Implementing the U.S. Government Personnel Security Program*. https://www.dhra.mil/Portals/52/Documents/perserec/ADR_Version_4.pdf

DNV-GL. (2019). *Håndtering av innsiderisiko*. https://www.ptil.no/fagstoff/utforsk-fagstoff/prosjektrapporter/prosjektrapporter-2019/hvordan-handtere-innsiderisiko/

EOS-utvalget. (2020-2021). *Årsmelding 2020 (Dokument 7:1)*. https://eos-utvalget.no/eos-utvalets-arsmelding-for-2020/

Etterretningstjenesten. (2021). *Fokus*. https://www.etterretningstjenesten.no/publikasjoner/fokus

Etterretningstjenesten. (2022). *Fokus*. https://www.etterretningstjenesten.no/publikasjoner/fokus
Etterretningstjenesten. (2023). *Fokus*. https://www.etterretningstjenesten.no/publikasjoner/fokus
Farsund, B. H., Søndrol, T., Nystuen, K. O., Hornfelt, L., Sellevåg, S. R. & Pham, V. (2022). *Utviklingen av nye IoT-baserte infrastrukturer i samfunnet – utfordringer for nasjonal sikkerhet (revidert rapport)* (22/00631). Forsvarets forskningsinstitutt. https://www.ffi.no/publikasjoner/arkiv/utviklingen-av-nye-iot-baserte-infrastrukturer-i-samfunnet-utfordringer-for-nasjonal-sikkerhet-revidert-rapport
Gonzalez, J. J., Sarriegi, J. M. & Gurrutxaga, A. (2006). A Framework for Conceptualizing Social Engineering Attacks. *Critical Information Infrastructures Security*, *4347*, 79-90. https://doi.org/10.1007/11962977_7
Graver, H. P. (2021). Sikkerhetsklarering og rettssikkerhet. *Lov og Rett*, *60*, 393-412. https://doi.org/10.18261/issn.1504-3061-2021-07-03
Haugsbø, F. (2021a, 12.11.2021). *Sikkerhetsklarering: Justisministeren varsler gjennomgang*. VG. Hentet 03.03.2023 fra https://www.vg.no/nyheter/innenriks/i/k6mGjk/sikkerhetsklarering-justisministeren-varsler-gjennomgang
Haugsbø, F. (2021b, 30.05.2021). *Tidligere toppdiplomat: − Det som skjer er kritikkverdig og feil*. VG. Hentet 03.03.2023 fra https://www.vg.no/nyheter/innenriks/i/41MWmg/tidligere-toppdiplomat-det-som-skjer-er-kritikkverdig-og-feil
Haugsbø, F. (2022, 21.03.2022). *Ble fratatt ambassadørjobben på grunn av thailandsk kjæreste: Nå har han fått tilbake sikkerhetsklareringen*. VG. Hentet 03.03.2023 fra https://www.vg.no/nyheter/innenriks/i/Qy24M8/ble-fratatt-ambassadoerjobben-paa-grunn-av-thailandsk-kjaereste-naa-har-han-faatt-tilbake-sikkerhetsklareringen
Haugsbø, F. & Skålevik, G. A. (2021, 19.09.2021). *Han var med og lage ny sikkerhetslov – nå kritiserer den tidligere toppdiplomaten hvordan den praktiseres*. VG. Hentet 03.03.2023 fra https://www.vg.no/nyheter/innenriks/i/ja3r4e/han-var-med-og-lage-ny-sikkerhetslov-naa-kritiserer-den-tidligere-toppdiplomaten-hvordan-den-praktiseres
Heyerdahl, A. (2022). From prescriptive rules to responsible organisations – making sense of risk in protective security management – a study from Norway. *European Security*. https://doi.org/10.1080/09662839.2022.2070006
Hove, M. (2022). *Innsiderisiko - hvordan påvirker sikkerhetsklarering vurderingen?* [UiS].
Jacobsen, J. D. (2021). *Hvordan holde innsidere på utsiden?* [UiS].
Jakobwitz, S. & Egan, V. (2006). The dark triad and normal personality traits. *Personality and individual differences*, *40*(2), 331-339. https://doi.org/10.1016/j.paid.2005.07.006
Karlsen, O. (2020a, 26.06.2020). *Forsvaret: 285 ble nektet klarering i 2019*. ABC nyheter. Hentet 03.03.2023 fra https://www.abcnyheter.no/nyheter/norge/2020/06/26/195686339/forsvaret-285-ble-nektet-klarering-i-2019
Karlsen, O. (2020b, 15.06.2020). *Russisk-gift romekspert vant mot sikkerhetsmyndighetene*. ABC nyheter. Hentet 03.03.2023 fra https://www.abcnyheter.no/nyheter/norge/2020/06/15/195684687/russisk-gift-romekspert-vant-mot-sikkerhetsmyndighetene
Kristoffersen, K. J., Lambertsen, O.-F. & Lyngmoe, H. (2019, 29.08.2019). *Alex (20) får ikke jobbe i Forsvaret på grunn av farens fødested*. NRK. Hentet 03.03.2023 fra https://www.nrk.no/nordland/alex-_20_-far-ikke-jobbe-i-forsvaret-pa-grunn-av-farens-fodested-1.14678520

Lee, K., Ashton, M. C., Wiltshire, J., Bourdage, J. S., Visser, B. A. & Gallucci, A. (2013). Sex, Power, and Money: Prediction from the Dark Triad and Honesty-Humility. *European journal of personality*, *27*(2), 169-184. https://doi.org/10.1002/per.1860

Lockie, A. (2018, 29.01.2018). *A map of fitness-tracker data may have compromised top-secret US military bases around the world*. Insider. Hentet 03.03.2023 fra https://www.businessinsider.com/secret-us-military-bases-world-strava-heat-map-operational-security-compromised-fitness-trackers-2018-1?r=US&IR=T

Martin, P. (2019). *The Rules of Security. Staying Safe in a Risky World*. Oxford University Press.

Meld. St. 5 (2020–2021). (2020). *Samfunnssikkerhet i en usikker verden*. Justis- og beredskapsdepartementet,. https://www.regjeringen.no/no/dokumenter/meld.-st.-5-20202021/id2770928/

NSM. (2015). *Sikkerhetsfaglig råd*. https://www.regjeringen.no/globalassets/departementene/fd/dokumenter/rapporter-og-regelverk/nsm-sikkerhetsfaglig_raad_2015_web.pdf

NSM. (2020a). *Grunnprinsipper for personellsikkerhet*. https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-personellsikkerhet/introduksjon/

NSM. (2020b). *Temarapport innsiderisiko*. https://nsm.no/regelverk-og-hjelp/rapporter/temarapport-om-innsidere/temarapport-om-innsidere

NSM. (2021). *Risiko 2021 - helhetlig sikring mot sammensatte trusler*. https://nsm.no/getfile.php/136419-1616673370/Demo/Dokumenter/Rapporter/NSM_Risiko_2021_web_enkeltside_1203.pdf

NSM. (2022). *Risiko 2022. Økt risiko krever økt årvåkenhet*. https://nsm.no/getfile.php/137798-1644424185/NSM/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enekeltsider.pdf

NSM. (2023). *Risiko 2023. Økt utforutsigbarhet krever høyere beredskap*. https://nsm.no/getfile.php/1312547-1676548301/NSM/Filer/Dokumenter/Rapporter/Risiko%202023%20-%20Nasjonal%20sikkerhetsmyndighet.pdf

Nurse, J. R. C., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R. T. & Whitty, M. (2014). *Understanding Insider Threat: A Framework For Characterising Attacks*. IEEE Symposium on Security and Privacy Workshops (SPW), San Jose, CA, USA.

Pang, X. (2022, 23.12.2022). VG. Hentet 03.03.2023 fra https://www.vg.no/nyheter/innenriks/i/gEv6Ra/skuffet-over-at-forsvaret-ikke-endrer-praksis-rundt-sikkerhetsklarering-for-foerstegangstjenesten

Paulhus, D. L. & Williams, K. M. (2002). The Dark Triad of personality: Narcissism, Machiavellianism, and psychopathy. *Journal of research in personality*, *36*(6), 556-563. https://doi.org/10.1016/S0092-6566(02)00505-6

Pharr, S. J. & Putnam, R. D. (2000). *Disaffected Democracies: What's Troubling the Trilateral Countries?* Princeton University Press.

PST. (2020). *Nasjonal trusselvurdering 2020*. https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2020/

PST. (2021). *Nasjonal trusselvurdering 2021*. https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/

PST. (2023). *Nasjonal trusselvurdering 2023*. https://www.pst.no/alle-artikler/trusselvurderinger/ntv-2023/

PST, NSM, Politiet & Næringslivets Sikkerhetsråd. (2017). *Sikkerhet ved ansettelsesforhold - før, under og ved avvikling*. https://pst.no/alle-artikler/utgivelser/sikkerhet-ved-ansettelseforhold/

Putnam, R. D. (2002). Conclusion. I R. D. Putnam (Red.), *Democracies in Flux: The Evolution of Social Capital in Contemporary Society* (s. 393-416). Oxford University Press.

Ringstad, P. (2020). *Sikkerhetsstyringens utvikling* [Universitet i Stavanger].

Shechter, O. G. & Lang, E. L. (2011). *Identifying Personality Disorders that are Security Risks: Field Test Results* (11-05). PERSEREC. https://www.dhra.mil/Portals/52/Documents/perserec/tr11-05.pdf

sikkerhetsloven. (2019). *Lov om nasjonal sikkerhet (LOV-2018-06-01-24)*. Lovdata. https://lovdata.no/dokument/NL/lov/2018-06-01-24

Sivertsen, E. G., Hellum, N., Bergh, A. & Bjørnstad, A. L. (2021). *Hvordan gjøre samfunnet mer robust mot uønsket påvirkning i sosiale medier*. Forsvarets forskningsinstitutt. https://www.ffi.no/publikasjoner/arkiv/hvordan-gjore-samfunnet-mer-robust-mot-uonsket-pavirkning-i-sosiale-medier

Skeem, J. L., Polaschek, D. L. L., Patrick, C. J. & Lilienfeld, S. O. (2011). Psychopathic Personality: Bridging the Gap Between Scientific Evidence and Public Policy. *Psychological science in the public interest*, *12*(3), 95-162. https://doi.org/10.1177/1529100611426706

Skotvedt, L. E. (2019, 03.07.2019). *I sikkerhetssaker bortfaller rettighetene nærmest umiddelbart*. Politiforum. Hentet 03.03.2023 fra https://www.politiforum.no/lars-e-skotvedt-politijuss/i-sikkerhetssaker-bortfaller-rettighetene-naermest-umiddelbart/153249

Sly, L. (2018, 29.01.2018). *U.S. soldiers are revealing sensitive and dangerous information by jogging*. The Washington Post. Hentet 03.03.2023 fra https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html

Stolle, D. & Hooghe, M. (2005). Innacurate, Exceptional, One-sided or Irrelevant? The Debate About the Alleged Decline of Social Capital and Civic Engagement in Western Societies. *British Journal of Political Science*, *35*(1), 149-167. https://doi.org/10.1017/S0007123405000074

Strand, T. (2022). *Norske «Håkon» måtte oppgi drømmen om å fly jagerfly fordi mor er russisk*. https://www.nrk.no/norge/matte-oppgi-drommen-om-a-fly-jagerfly-fordi-mor-er-russisk-1.15895024

Syvertsen, J. P. (2007). *Insider Threat* [Høgskolen i Gjøvik].

Tennøy, S.-L., Sandbakk, P.-K. & Taubo, V. (2020, 22.11.2020). *Drømmen om Forsvaret brast: – Staten sier at jeg ikke er norsk nok*. NRK. Hentet 03.03.2023 fra

Tyler, T. R. & Degoey, P. (1996). Trust in organizational authorities: The influence of motive attributions on willingness to accept decisions. I R. Kramer & T. Tyler (Red.), *Trust in Organizations: Frontiers of Theory and Research* (s. 331-356). SAGE Publications.

Tyler, T. R. & Lind, E. A. (1992). A Relational Model of Authority in Groups. *Advances in Experimental Social Psychology*, *25*, 115-191. https://doi.org/10.1016/S0065-2601(08)60283-X

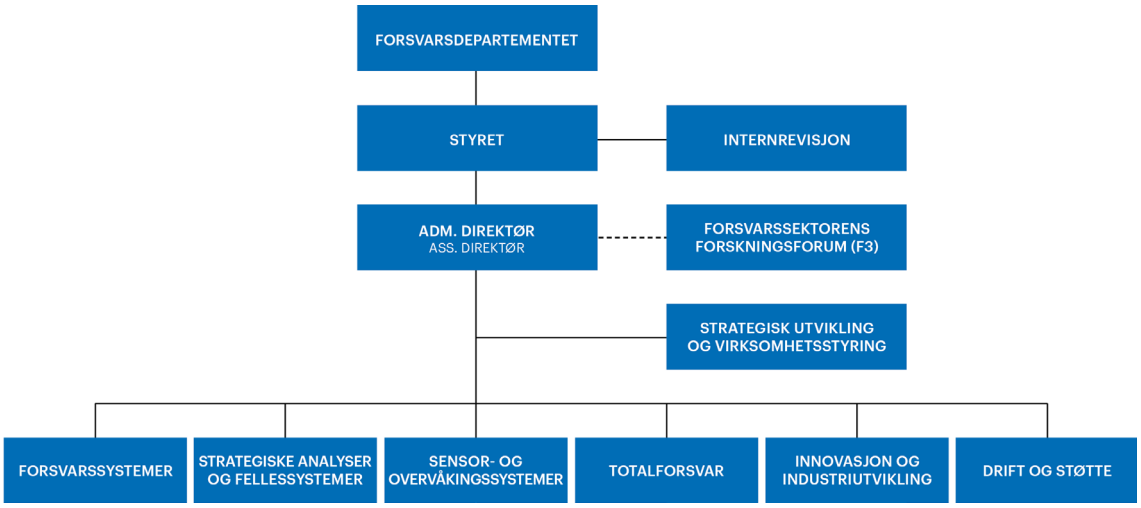
Wilder, U. M. (2017). The Psychology of Espionage. *Studies in Intelligence*, *61*(2). https://www.cia.gov/static/30b273c621d0896f13104ff48840b68f/psychology-of-espionage.pdf

Om FFI
Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan, med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs formål
Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

FFIs visjon
FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs verdier
Skapende, drivende, vidsynt og ansvarlig.



Forsvarets forskningsinstitutt (FFI)
Postboks 25
2027 Kjeller

Besøksadresse:
Kjeller: Instituttveien 20, Kjeller
Horten: Nedre vei 16, Karljohansvern, Horten

Telefon: 91 50 30 03
E-post: post@ffi.no
ffi.no

Norwegian Defence Research Establishment (FFI)
PO box 25
NO-2027 Kjeller
NORWAY

Visitor address:
Kjeller: Instituttveien 20, Kjeller
Horten: Nedre vei 16, Karljohansvern, Horten

Telephone: +47 91 50 30 03
E-mail: post@ffi.no
ffi.no/en