Rapport

En metastudie om innsidetrusselen

Forfattere:
Marte Høiby, Pål Brennhovd, Anita Øren

Rapportnummer:
2023:01616 - Åpen

Oppdragsgiver:
Sivil klareringsmyndighet

Bildet på forsiden er laget ved hjelp av kunstig intelligens og tjenesten Shutterstock AI Generator

SINTEF Digital
Postadresse:
Postboks 4760 Torgarden
7465 Trondheim

Sentralbord: 40005100

info@sintef.no

Foretaksregister:
NO 919303808 MVA

Rapport

En metastudie om innsidetrusselen

EMNEORD
Innsidetrussel, innsider, personellsikkerhet

VERSJON
Versjon 1

DATO
2023-12-22

FORFATTER(E)
Marte Høiby, Pål Brennhovd, Anita Øren

OPPDRAGSGIVER(E)
Sivil klareringsmyndighet

OPPDRAGSGIVERS REFERANSE
Kathinka Skott Hansen

PROSJEKTNUMMER
102030060

ANTALL SIDER
57

SAMMENDRAG
Denne rapporten skal gi økt forskningsbasert kunnskap om hvordan personellsikkerhet kan håndteres og innsiderisiko reduseres, og er basert på en metastudie av forsknings- og grålitteratur innen personellsikkerhet og innsiderisiko. Målet med studien er å fremlegge en oversikt over eksisterende kunnskap på feltet og synliggjøre eventuelle mangler i denne. Oversikten gir utgangspunkt for anbefalinger om hvilke retninger, tema og tilnærminger det er behov for i videre forskning.

UTARBEIDET AV
Marte Høiby

SIGNATUR
Marte Høiby
Marte Høiby (Feb 2, 2024 11:19 GMT+1)

KONTROLLERT AV
Stine Skaufel Kilskar

SIGNATUR
Stine SKaufel Kilskar
Stine SKaufel Kilskar (Feb 2, 2024 11:36 GMT+1)

GODKJENT AV
Anita Øren

SIGNATUR
Anita Øren
Anita Øren (Feb 2, 2024 11:19 GMT+1)

RAPPORT NR.
2023:01616

ISBN
978-82-14-07139-9

GRADERING
Åpen

GRADERING DENNE SIDE
Åpen

Innholdsfortegnelse

BILAG/VEDLEGG

Klikk eller trykk her for å skrive inn tekst.

Sammendrag

Denne rapporten skal gi økt forskningsbasert kunnskap om hvordan personellsikkerhet kan håndteres og innsiderisiko reduseres, og er basert på en metastudie av forsknings- og grålitteratur innen personellsikkerhet og innsiderisiko. Målet med studien er å gi innsikt i eksisterende kunnskap på feltet og synliggjøre eventuelle mangler i denne. Oversikten gir utgangspunkt for anbefalinger om hvilke retninger, tema og tilnærminger det er behov for i videre forskning.

Studien finner et stort utvalg av forskningslitteratur som omhandler innsidetrussel, men en betydelig andel er basert på annen eksisterende litteratur og kun et fåtall studier bringer inn ny empiri og kunnskap fra praksis. Deler av forskningsfeltet, særlig forskning om innsidetrusselen sett i et cyberperspektiv, virker godt teoretisert og innehar et betydelig antall metastudier med teoretiske rammeverk, modellutvikling og taksonomi. Innsidetrusselen sett i sammenheng med personellsikkerhet får mindre oppmerksomhet i forskningslitteraturen, og studier som ser på dette benytter gjerne casestudier med kjente spionsaker fra virkeligheten eller rammeverk for identifisering og deteksjon av innsideren. Heller ikke her er forskningen i særlig grad basert på ny empiri og førstehånds erfaringer.

Forskningslitteraturen peker på at innsidetrussel fortsatt er et uavklart begrep. Hvordan innsidertrussel defineres påvirker hvilken ny innsikt forskningen kan opparbeide, og kan dermed bidra til å begrense eller øke forståelse. Forskningen viser et stort utvalg av ulike definisjoner av innsidetrussel. Disse vektlegger gjerne en sammenheng mellom definisjon av innsidetrusselen og innsideren. Innsideren er i definisjonene den som utgjør trusselen og er en som har, eller har hatt, tilhørighet til organisasjonen. Definisjonene sier imidlertid lite om dynamikk mellom individ og gruppe, mellom individ og organisasjon og mellom de som er på innsiden og utsiden. Omfanget av ubevisste/uintenderte innsidere beskrives i litteraturen som antatt stort, men ukjent, og forskningen virker ikke å være forenlig om problemforståelse hva gjelder den ubevisste innsideren. Denne type innsider omtales mest i tilknytning til cyberdomenet og i mindre grad det sosiale rom, på møteplasser og i livet utenfor arbeidsplassen.

Litteraturen om innsidetrusselen retter betydelig oppmerksomhet mot enkeltindividet. Det kan være en motsetning mellom streng ansvarliggjøring av enkeltindivider og muligheten for organisasjonen til å lære og utvikle robusthet mot innsidetrusselen. Manglende innsikt begrenser mulighet til å forstå hvilke tiltak som kan forebygge og begrense innsidetrussel. For å kunne møte dagens utfordringer knyttet til innsidetrusler, er det behov for bedre og mer konsistent begrepsbruk.

Rapporten anbefaler at videre forskning i større grad bør være basert på empiriske studier om innsidevirksomhet for å bedre relatere forskningsresultatene til innsikt som bedrifter og foretak behøver for å bygge opp robuste organisasjoner i møte med innsidetrusselen.

Summary

This report offers research-based knowledge for personnel security and insider risk reduction. The report presents findings from a meta-study of research and gray literature in personnel security and insider threat. The aim of the study is to provide insight into existing knowledge in the field and highlight any shortcomings. This overview provides a starting point for recommendations on which directions, themes and approaches are needed in further research.

The study finds a large selection of research literature that deals with insider threats; however, a significant proportion is based on other existing literature and only a small number of studies bring new empirical evidence and knowledge from practice. Parts of the research field, especially research on the insider threat in a cyber perspective, seem well theorized and contain a significant number of meta-studies with theoretical frameworks, model development and taxonomy. The insider threat in context of personnel security receives less attention in the research literature, and studies investigating this tend to use case studies with well-known espionage cases or frameworks for identification and detection of insiders.

The research literature indicates that insider threat is still an unsettled concept. How insider threat is defined affects what new insights research may provide and thus contributes to limiting or increasing an understanding of what it entails. The research shows a significant scope of different definitions, of which most emphasize a connection between the insider threat and the insider as an individual. In the definitions, the insider is the person who poses the threat and has had, or had, affiliation with the organization. However, the definitions do not elaborate on dynamics between individual and group, between individual and organization and between those on the inside and on the outside. The number of unconscious or unintended insiders is described in the literature as assumed to be high but unknown, and there is little consensus on the prevalence or significance of the unintended insider. This type of insider is mostly studied through a cyber lens and to a lesser extent in the social space, in meeting places or in life outside the workplace.

The insider threat literature pays considerable attention to the individual. But placing accountability on individuals may be counterproductive to the opportunity for an organization to learn and develop resilience against the insider threat. Lack of insight limits understanding of which measures can prevent and limit insider threats. To meet today's challenges of managing insider threats, there is a need for better and more consistent use of terms.

The report recommends that further research offers empirical studies to give insights that companies and enterprises need to build robust organizations resilient to the insider threat. Suggested recommendations are listed at the end of the report.

1 Innledning: Innsidetrusselen – en gammel problemstilling i ny drakt

Studier som undersøker bevisstgjøringsstrategier for å redusere innsiderisiko i virksomheter viser at akademiske tilnærminger til denne problemstillingen omfatter både fysisk og digital sikring. Mens noen studier vektlegger en integrert cyberdimensjon, eller et integrert menneskelige faktorer-perspektiv, viser likevel mange eksempler fra litteraturen på dette fagfeltet at forskning i stor grad holder fast ved tradisjonelle fagdisipliner (Høiby m.fl., 2023). At personlige og individuelle forhold kan bidra til økt risiko er viet betydelig oppmerksomhet i litteraturen (f.eks. Jacobsen, 2021; Pareira, 2023; Marbut & Harms, 2023). I et annet spor, og ofte innen samfunnspsykologi, belyses kontekstuelle faktorer og miljømessige hensyn som kan legge til rette for å øke eller redusere risiko. Testing og rekrutteringsverkstøy som skal bidra til å styre ansettelsesprosesser er gjerne knyttet til begrepet personellsikkerhet, og belyser problemstillingen fra et sikkerhets- og sikringsperspektiv. Denne rapporten fremlegger funn fra en kartlegging av forsknings- og grålitteratur om innsidetrussel og personellsikkerhet, og drøfter litteraturens ulike innretninger, herunder blant annet metoder, problemstillinger, samt empirisk og teoretisk grunnlag. Videre går rapporten dypere i begrepsbruk og definisjoner knyttet til temaet og fremlegger eksempler på klassifisering, rangering og modellering av konsepter. Rapportens avsluttende del diskuterer hvilke bærende elementer som viser seg gjentagende eller kan være nyttige å trekke på både i forskning og praksis, og konkluderer om foreløpige blindsoner i litteraturen.

Begrepsbruk for innsidetrussel og innsideren har betydning for hvordan vi forebygger, identifiserer og begrenser skadene som innsidetrusselen utgjør. I både forskningslitteraturen og grålitteraturen observeres imidlertid sentrale svakheter knyttet til uklar bruk av definisjoner, forskningsmetoder, modeller og kritiske vurderinger om anvendelse av resultater (Schoenherr & Thomson, 2020). Disse svakhetene gir to sentrale begrensinger. Den første er at det er krevende å bygge videre på og sammenligne ulike kunnskapsgrunnlag, og derfor vanskelig å opparbeide en bred forståelse for problematikken. Det andre er at svakhetene gir usikkerhet om hvilke virkemidler som effektivt vil kunne forebygge og begrense skadene fra innsidetrusselen.

Mens forsknings- og grålitteratur[1] om innsiderisiko og personellsikkerhet i stor grad retter oppmerksomhet mot ansettelsesprosesser, personlighetstrekk, personlige egenskaper og karakteristika hos innsideren (DNV GL, 2019; Ringstad, 2019) kan funnene fra Krisino-undersøkelsen 2021 tyde på at det ikke bare er de bevisste innsiderne som utgjør en sikkerhetstrussel mot norsk næringsliv og Norges grunnleggende nasjonale funksjoner (NSR, 2021). Den viser til en høy andel såkalte utro tjenere, og mens disse, som utgjør en risiko for hver fjerde virksomhet i Norge, kanskje ikke handler med intensjon om å utlevere sensitiv informasjon, kan de likevel representere en sårbarhet for rekruttering til mer alvorlige hendelser og bli ledd i ondsinnede aktørers infiltrasjon. Mørketallsundersøkelsen (NSR, 2022) peker på at ledelsen spiller

[1] Med grålitteratur menes litteratur som ikke har blitt fagfellevurdert eller blitt publisert i formelle kommersielle kanaler, slik som bøker og tidsskriftartikler. For eksempel kan grålitteratur være rapporter og veiledere fra myndigheter eller private aktører.

en avgjørende rolle for hvor utsatt en virksomhet er for innsiderisiko, fordi rapportering av hendelser i Norge per i dag er svært lav og styringssystem for informasjonssikkerhet mangler.

Innsidetrussel er ikke nytt. Problematikken er velkjent fra antikk gresk litteratur som beskriver at denne utgjør en spesiell type trussel (Zimmer E., Burkert C., Federrath H. 2021). Diskusjonen om den trojanske hesten er et eksempel der bruk av definisjoner fra forsknings- og grålitteraturen argumenterer for at i et domene (bymuren i Troja), under de gitte omstendighetene (krig mellom Trojanere og Grekere utløst av at Paris av Troja berøvet vakre Helene fra hennes mann Menelaus, kongen av Sparta), er de greske krigerne som var gjemt inne i trehesten innsidere. Andre vil argumentere for at de er utsidere som har brutt (eller kanskje mer presist for historien, lurt) seg inn. Kan det også være et eksempel på at de greske krigerne som gjemte seg i trehesten var begge deler? I så fall taler det for en gradering (og ikke binært) mellom det å være på utsiden og innsiden. I historien om den trojanske hesten forstår vi hvem som utgjør innsidetrusselen, hvilke motiv de har og hva som kan gjøres for å forhindre og begrense skadene. For å kunne møte dagens ondsinnede programvarer og trojanske hester er det behov for bedre og mer konsistent begrepsbruk for å kunne beskrive hva disse truslene innebærer og hvordan de kan forhindres og begrenses. Målet bør være å opparbeide en organisasjon som er robust til å kunne motstå og begrense innsidetrusselen.

Det grunnleggende problemet med å definere omfanget av innsidetrusselen er at det ofte er krevende å skille mellom innsidere og utsidere av en organisasjon når de først opererer i et internt nettverk (Homoliak m.fl., 2019). En annen utfordring er å skille mellom innsidere og personer som bedriver kontraproduktiv atferd på arbeidsplassen, på engelsk, 'counterproductive workplace behaviour' (CWB). Kontraproduktivitet på arbeidsplassen kan dreie seg om holdninger og handlinger som virker destruktivt på kultur, arbeid eller systemer – som tyveri, sabotasje, mobbing eller trakassering. Det skiller seg fra innsidevirksomhet på den måten at det ikke gjøres som en (bevisst eller ubevisst) anskaffelse for utenforstående. I tillegg er det krevende med avgrensing mellom en innsider og en varsler, altså en person som sier ifra om ulovlig eller uetisk virksomhet ('whistleblower'). I varslingssaker rettes spørsmål mot en virksomhets praksis i forhold til etikk og lov, der varsleren vurderer at denne kan være til skade for de verdiene og reglene samfunnet styres etter. Avgrensingen fra innsidevirksomhet er vanskelig grunnet ulike interesser på innsiden og utsiden, ulik praksis og oppfatninger knyttet til etiske prinsipper. Aktørene som varselet rettes mot og aktørene som varselet søker å beskytte er derfor avgjørende i å definere handlingen, i tillegg til gjeldende jurisdiksjon. Dette underbygger derfor behovet for å beskrive hensiktene som ligger bak innsidetrusselen. Økonomisk vinning er eksempel på et av de vanligste motivene for innsidevirksomhet, samtidig som den ofte ikke opptrer i et vakuum og har vært del av flere kjente spionasjesaker.

Innsidetrusselen er altså langt ifra ny, men med introduksjon av datateknologi kreves nye måter å forstå og kategorisere den på. Med stadig mer og bedre IT-sikkerhet blir det vanskeligere for trusselaktører å angripe fra utsiden, og veien til innsiden blir igjen kortere via mennesket. I dagens sammensatte trusselbilde kan aktører som vil infiltrere en organisasjon kombinere ny teknologi

med tradisjonelle fysiske metoder. I tillegg, har utbredelsen av sosiale medier og delingssystemer bidratt til at store datasett om menneskers tanker og levesett tilgjengeliggjøres i aggregert format og øker sårbarhet for strategisk påvirkning – uten at en fysisk eller digital infiltrasjon i det hele tatt er nødvendig. Samspillet mellom fysiske objekter, mennesker, systemer og organisasjon blir mer konsentrert og sammensatt, og gjør det krevende å se eventuelle følger av endringer.

Arbeidet fremlagt i denne rapporten ser på innsidetrusselen generelt, både i statlig og kommersiell virksomhet. Utvalget av litteratur er ikke begrenset til spesifikke mål og motivasjon for innsidetrusselen, men valgt med hensyn til at rapporten skal belyse innsidetrusselen forbundet med personellsikkerhet. Utover dette, er alt innen feltet innsidetrussel inkludert i utvalget. Dette er gjort for blant annet å kunne antyde hva forskningen er rettet mot og om den dekker problemstillingen bredt. Begrepet innsidetrussel brukes om vinningskriminalitet, informasjonstyveri, datatyveri, spionasje m.m., og utvalget selekteres ikke etter kriterier for dette.

Personellsikkerhet er et lite brukt begrep i forskningslitteraturen, og generelle søk på dette gir få akademiske treff. Organisasjoner og statlige enheter ser imidlertid ut til å bruke begrepet knyttet til personellsikring og klarering, og omtaler dette i sine rapporter, altså i grålitteratur. Denne undersøkelsen vil derfor inkludere observasjoner og betraktninger knyttet til personellsikkerhet der det oppstår i grålitteraturen, men ikke gjøre en egen kartlegging av akademisk litteratur for dette begrepet.

Rapportens funn fra kartleggingsundersøkelsen redegjør for de mest anvendte definisjoner, modeller og taksonomier og diskuterer deretter funnene med anbefalinger for videre teoretisering av faget, eventuelle mangler innen forskningen og behov for ny empiri.

1.1 Oppdragets art

Undersøkelsen er utført på oppdrag for Sivil klareringsmyndighet og skal bidra til økt forskningsbasert kunnskap om hvordan personellsikkerhet håndteres og innsiderisiko reduseres og håndteres. Målet med en slik metastudie av forsknings- og grålitteraturen innen personellsikkerhet og innsiderisiko er å fremlegge en oversikt over eksisterende kunnskap på feltet og synliggjøre trender og eventuelle mangler i denne. Med utgangspunkt i oversikten innebærer oppdraget å gi anbefalinger om behov for videre forskning. Anbefalingene beskriver hvilke retninger og tema som vurderes mest relevant. Forskerteamet har relevant erfaring fra andre tidligere og pågående metastudier, slik som kartlegging av forskningslitteratur på hybride trusler, datakriminalitet i internasjonal forskningslitteratur og bevisstgjøringsstrategier som kan motvirke rekruttering av ubevisste innsidere. Arbeidet er inndelt i følgende fem delmål; forarbeid og planlegging; litteraturgjennomgang, analyse av litteratur og sammenfatting av data; diskusjon og anbefalinger om videre forskning; og å skrive sluttrapport. Oppdraget er utført i perioden september til desember 2023. Sluttleveransen for oppdraget er denne rapporten.

1.2 Tilnærming og metode

For kartleggingen gjennomført i rapportens første del, ble det gjort søk på engelsk etter relevans i Scopus, Academia.edu, ResearchGate.net og Google Scholar. Ved snøballmetoden har forskerteamet samlet et utvalg relevant litteratur, i tillegg til hjelp fra algoritmer som er innebygd i søketjenestene. Målet er å samle den mest relevante litteraturen om innsidetrusselen sett i sammenheng med personellsikkerhet.

Innsidetrussel er ikke et avklart og avgrenset konsept. I cyberforskningen kan for eksempel innsidetrusselen motvirkes med mer tekniske grep enn i psykologien. Det er ulike tilnærminger til problemstillingen, og forskerteamet har derfor søkt å ekskludere en del litteratur vurdert som for teknisk til å bidra med innsikt om innsidetrusselen i et samfunnsvitenskapelig og sosioteknisk perspektiv. Grunnet prosjektets rammer, er mengden litteratur avgrenset til en skjønnsmessig vurdering av grad av relevans, basert på litteraturens tittel og sammendrag (abstract). Oppdraget skal se på litteratur om innsidetrussel i lys av personellsikkerhet og i tillegg belyse forståelsen av innsidetrusselen i litteraturen. Bruk av definisjoner og taksonomi er derfor viktig. Relevans er særskilt vurdert opp til oppdragets mål knyttet til personellsikkerhet. Nasjonal sikkerhetsmyndighet (NSM) beskriver at "med personellsikkerhet menes tiltak, handlinger og vurderinger for å hindre at personer som kan utgjøre en sikkerhetsrisiko, plasseres eller er plassert i stillinger eller roller slik at det er aktuelt å frykte brudd på sikkerhetsloven" (NSM, 2023). Vi finner at denne tilnærmingen anvendes lite i forskningslitteraturen. Vi har derfor tatt utgangspunkt i begrepene *innsidetrussel* og *innsider* i arbeidet med å søke etter forskningslitteratur. I denne forståelsen av innsiderbegrepet inngår blant annet forsøk på rekruttering av innsidere, både før og etter at informanten er bevisst sin rolle.

Scopus, og i noen grad Google Scholar, tilbyr andre søkemuligheter enn Academia og Researchgate, og derfor er søkene her avgrenset på en annen måte. Søk i Scopus er avgrenset til innsidetrussel i en- og flertall ('Limited to Insider Threat' og 'Limited to Insider Threats'). I tillegg er søk avgrenset til treff på samfunnsvitenskapelig litteratur ('Limited to Social Science'). Det har likevel gitt treff i flere cybertekniske tidsskrift, da sosiotekniske problemstillinger er relativt godt forsket på. Men i sum blir treff langt mer relevant for samfunnsfaglige problemstillinger enn om søket for eksempel hadde inkludert en avgrensning til treff innen informatikk ('Limited to Computer Science'), et søk som gir nesten like mange treff på innsidetrussel som et søk avgrenset til samfunnsvitenskap. Disse to vitenskapene gir betydelig flere treff enn andre, henholdsvis 127 treff i samfunnsvitenskap og 100 treff i informatikk, mens 'Engineering' og 'Decision Sciences' gir hhv. 33 og 13 treff. Søk er også avgrenset til funn i konferanseprosederinger og tidsskrift. Bøker og bokkapitler er ikke inkludert i utvalget både grunnet omfang og begrenset tilgang. Det ble også søkt spesifikt på taksonomi og spionasje både i tittel og sammendrag, for å finne litteratur som kunne bidra til kunnskap om hvordan dette er dekket i litteraturen.

Google Scholar tilbyr også mulighet for avgrensing gjennom søkekriterier. Her ble søk også avgrenset til artikler og konferansebidrag, med de samme søkebegrepene som benyttet i Scopus,

og deretter skjønnsbasert utvalg etter relevans i tittel og sammendrag. Søk i Academia.edu, ResearchGate.net ble gjort med stadig seleksjon etter relevans i tittel og sammendrag, og søketjenestens forslag til andre relevante artikler ble benyttet deretter.

For annen litteratur, som rapporter og veiledere, ble det gjort søk i Google og i referanselistene i den litteraturen som til enhver tid var samlet inn, i tråd med snøballmetoden.
Søk ble gjennomført i september og oktober 2023.

Den samlede litteraturen er gjennomgått av forskerteamet, som har lest sammendragene og notert detaljer om publiseringsår, forfatterskap, utgiver, nøkkelord og mer, i tillegg til informasjon om metoder, problemstillinger og forskningsspørsmål, kontekst, om det tilfører ny empiri eller om det er teoribasert og hvorvidt det er cyberteknisk eller innlemmer menneskelige faktorer. Artikler som fremstår særskilt relevante er studert mer inngående for mer kunnskap.

2 Kartlegging av litteratur

Utvalget som danner grunnlag for denne rapportens undersøkelse omfatter forskningsartikler, konferanseartikler og -bidrag og grålitteratur, som guider og rapporter. All litteraturen er publisert i perioden 2003 til 2023, med en betydelig større andel innenfor det siste tiåret. Nedenfor følger tabeller over forskningsartikler publisert i vitenskapelige tidsskrift, konferanseartikler og -bidrag publisert i konferansetidsskrift, og til slutt over de rapportene og veilederne som er inkludert i utvalget. Samtlige vitenskapelige tidsskrifter har fagfellevurdering, men det er her ikke tatt hensyn til om de vitenskapelige tidsskriftene er nivå 1 eller 2. Det er heller ikke tatt stilling til hvorvidt konferansetidsskriftene har fagfellevurdering.

2.1 Utvalg

2.1.1 Forskningsartikler i tidsskrift

Tabell 1. Oversikt over forskningsartikler publisert i vitenskapelige tidsskrifter

Risk Assessment of Insider Threats Based on IHFACS-BN	Zeng m.fl. (2023) *Sustainability*
Queen of Cuba	Pereira (2023) *Journal of Applied Security Research*
Industrial espionage from a human factor perspective	Mészáros & Kelemen-Erdős (2023) *Journal of International Studies*
A Taxonomic Classification of Insider Threats: Existing Techniques, Future Directions & Recommendations	Rauf m.fl. (2023) *Journal of Cyber Security and Mobility*
Fiends and Fools: A Narrative Review and Neo-socioanalytic Perspective on Personality and Insider Threats	Marbut & Harms (2023) *Journal of Business and Psychology*
Techniques and countermeasures for preventing insider threats	Alsowail & Al-Shehari (2022) *Peer J computer science*

Exposing the darkness within: A review of dark personality traits, models, and measures and their relationship to insider threats	Harms m.fl. (2022) *Journal of Information Security and Applications*
The Missing Case of Disinformation from the Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats	Caramancion m.fl. (2022) *Data*
Insiders Dissected: New Foundations and a Systematisation of the Research on Insiders	Zimmer m.fl. (2021) *Digital Threats: Research and Practice*
Review of insider and insider threat detection in the organizations	Subhani m.fl. (2021) *Journal of Advanced Research in Social Sciences and Humanities*
A Multi-Tiered Framework for Insider Threat Prevention	Alsowail & Al-Shehari (2021) *Electronics*
A damage assessment framework for insider threats to national security information: Edward Snowden and the Cambridge Five in comparative historical perspective	Gioe & Hatfield (2020) *Cambridge Review of International Affairs*
The dark triad and insider threats in cyber security	Maasberg m.fl. (2020) *Communications of the ACM*
Insider threats in Cyber Security: The enemy within the gates	Mazzarolo & Jurcut (2020) *European Cybersecurity Journal*
Insight into insiders and IT: A survey of insider threat taxonomies, analysis, modeling, and countermeasures	Homoliak m.fl. (2019) *ACM Computing Surveys*
SoK: A systematic review of insider threat detection	Kim m.fl. (2019) *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*
Under the Corporate Radar: Examining Insider Business Cybercrime Victimization through an Application of Routine Activities Theory	Williams m.fl. (2019) *Deviant Behavior*
Insider Threats: It's the HUMAN, Stupid!	Greitzer (2019) *Journal of Advanced Research in Social Sciences and Humanities*
The Wolf of SUTD (TWOS): A dataset of malicious insider threat behavior based on a gamified competition	Harilal m.fl. (2018) *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*
The Enemy Within the Insider: Detecting the Insider Threat Through Addiction Theory	Maasberg & Beebe (2014) *Journal of Information Privacy and Security*
Secure Team Composition to Thwart Insider Threats and Cyber-Espionage	Laszka m.fl. (2014) *ACM Transactions on Internet Technology*
Insider threat assessment: A model-based methodology	Nostro m.fl. (2014) *Operating Systems Review, ACM*
Corporate espionage: The insider threat	Vashisth & Kumar (2013) *Business Information Review*
Insiders and Insider Threats: An Overview of Definitions and Mitigation Techniques	Hunker & Probst (2011) *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*
Unconventional Spies: The Counterintelligence Threat from Non-State Actors	Harber (2009) *International Journal of Intelligence and CounterIntelligence*
Thwart the insider threat: a proactive approach to personell security	Power & Forte (2006) *Computer Fraud and Security*

2.1.2 Konferanseartikler og -bidrag

Tabell 2. Oversikt over konferanseartikler og -bidrag

Scenarios for Process-Aware Insider Attack Detection in Manufacturing	Macak m.fl. (2022) The 17th International Conference on Availability, Reliability and Security (ARES 2022)
Conversations around Organizational Risk and Insider Threat	Osterritter & Carley (2021) IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining
SOFIT: Sociotechnical and Organizational Factors for Insider Threat	Greitzer m.fl. (2018) IEEE Symposium on Security and Privacy Workshops
Cognitive and Affective Eye Tracking Metrics for Detecting Insider Threat: A Study of Simulated Espionage	Matthews m.fl. (2018) Human Factors and Ergonomics Society 2018 Annual Meeting
Network Packet Analysis for Detecting Malicious Insider	Patil & Meshram (2018) 3rd International Conference for Convergence in Technology (I2CT)
Insider Threat Detection Using Time-Series-Based Raw Disk Forensic Analysis	Beebe, Liu & Ye (2017) IFIP International Conference on Digital Forensics
Critical Analysis in the Research Area of Insider Threats	Zaytsev, Malyuk & Miloslavskaya (2017) IEEE 5th International Conference on Future Internet of Things and Cloud
Organizational values fostering secure knowledge sharing	Dulipovici (2017) European Conference on Knowledge Management, ECKM
Social engineering and Insider threats	LiuXiangyu m.fl. (2017) International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery
A critical reflection on the threat from human insiders - Its nature, industry perceptions, and detection approaches	Nurse m.fl. (2014a) 2nd International Conference on Human Aspects of Information Security, Privacy, and Trust, HAS
Insider Espionage: recognising ritualistic behavior by abstracting technical indicators from past cases	Maasberg (2014) 20th Americans Conference on Information Systems
Understanding insider threat: A framework for characterising attacks	Nurse m. gl. (2014b) IEEE Symposium on Security and Privacy
Toward the development of a psycholinguistic-based measure of insider threat risk focusing on core word categories used in social media	Brown, Watkinson & Greitzer (2013) The Nineteenth Americas Conference on Information Systems
Insider threat detection using virtual machine introspection	Crawford & Peterson (2013) Annual Hawaii International Conference on System Sciences
Trust enhanced security architecture for detecting insider threats	Typakula & Varadharajan (2013) 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom
Predicting insider threat risks through ligustic analysis of electronic communication	Brown, Watkinson & Greitzer (2013) Hawaii International conference on system sciences
The optimization of situational awareness for insider threat detection	Brancik & Ghinita (2011) Acm conference on Data and application security and privacy
Intent-driven insider threat detection in intelligence analyses	Santos m.fl. (2008) IEEE/WIC/ACM International Conference on Intelligent Agent Technology, IAT

Applying role based access control and genetic algorithms to insider threat detection	Hu m.fl. (2006) Annual Southeast Conference
A Multidiscipline Approach to Mitigating the Insider Threat	Butts m.fl. (2006) AFIT Scholar
Honeypots: Catching the insider threat	Spitzner (2003) Annual Computer Security Applications Conference, ACSAC

2.1.3 Rapporter og veiledere

Tabell 3. Oversikt over rapporter og veiledere

Hva vet vi om innsiderisiko?	Slagnes (2023) Forsvarets forskningsinstitutt (FFI)
The resource exfiltration project: Findings from DoD Cases, 1985-2017	Jaros m.fl. (2019) Office of People Analytics (OPA) og Defence Personnel and Security Research Center (PERSEREC)
Hvordan holde innsidere på utsiden?	Jacobsen (2021) Universitetet i Stavanger (UiS)
Håndtering av innsiderisiko	Jerre, Funnemark & Angelsen (2019) Det Norske Veritas (DNV-GL) for Petroleumstilsynet
Assessing the mind of the malicious insider: Using a behavioral model and data analytics to improve continous evaluation	Intelligence and National Security Alliance (INSA, 2017) Security Policy Reform Council, Insider Threat Subcommittee
Common Sense Guide to Mitigating Insider Threats, Sixth Edition	CERT (2019) Carnegie Mellon University
Common Sense Guide to Mitigating Insider Threats, 7th ed	CERT National Insider Threat Center, Carnegie Mellon University
Sikkerhetsstyringens utvikling	Ringstad (2020) Universitetet i Stavanger (UiS)
Sikkerhet ved ansettelsesforhold	Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet, Politiet og Næringslivets Sikkerhetsråd (2017)

2.2 Publiseringskanal

En stor andel av litteraturen finnes innen cyberfeltet. Det kan leses ut ifra at tidsskriftene der forskningen dukker opp i søk, både i form av tidsskriftartikler og konferanseartikler, i stor grad er relatert til cyber. Omtrent halvparten av forskningsartiklene publisert i tidsskrift kan sies å ha en direkte samfunnsvitenskapelig innretning, nemlig Journal of Applied Security Research (Routledge, Taylor & Francis); Deviant Behavior (Routledge, Taylor & Francis); Journal of Information Privacy and Security (Routledge, Taylor & Francis); International Journal of Intelligence and CounterIntelligence (Routledge, Taylor & Francis); Business Information Review (SAGE); Cambridge Review of International Affairs (Taylor & Francis); Journal of Business and Psychology (Springer); Sustainability (MDPI); og Journal of Advanced Research in Social Sciences and Humanities. Utenom sistnevnte er disse internasjonale, fagfellevurderte og åpne tidsskrift.

Journal of Applied Security Research publiserer forskning på teori og praksis innen sikkerhetsfaget; *Deviant Behavior* publiserer forskning på avvikende atferd, inkludert kriminalitet og avhengigheter; *Journal of Business and Psychology* og *Business Information Review* har begge forskning innen organisasjonsvitenskap; *Journal of Information Privacy and Security* publiserer forskning på informasjonssikkerhet og personvern; *Cambridge Review of International Affairs* har internasjonale studier inkludert IR, internasjonal lov, politisk økonomi og historie; *Sustainability* har miljømessig, kulturell, økonomisk og sosial bærekraft for mennesker; og *Journal of International Studies* publiserer sosioøkonomiske analyser av samfunn, institusjoner, organisasjoner, grupper og nettverk.

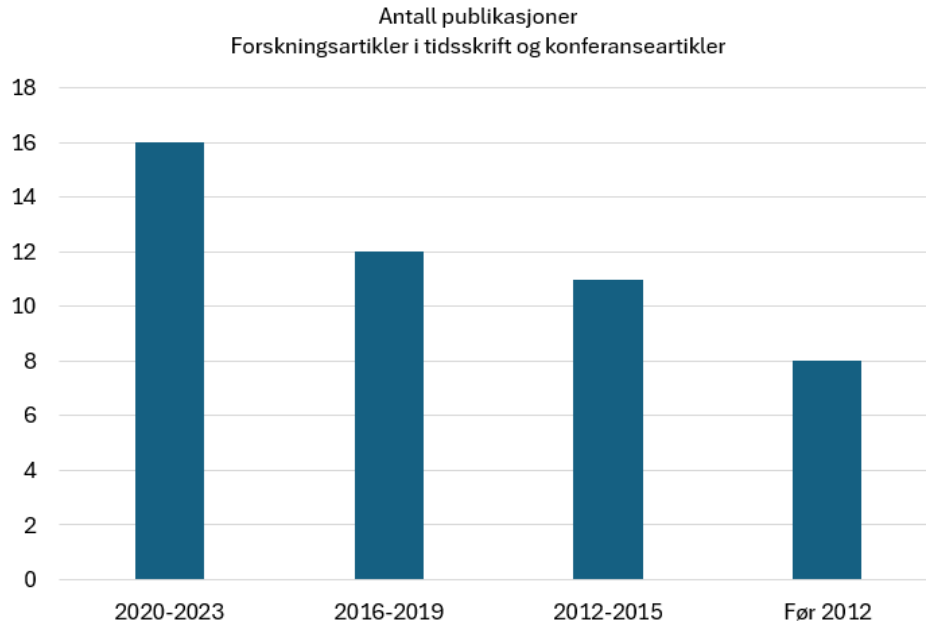
Resten av tidsskriftene er i betydelig grad relatert til cyberdomenet. Av disse, er flere underlagt forlaget Association for Computing Machinery (ACM), som *Communications of the ACM; ACM Computing Surveys; ACM Transactions on Internet Technology; Operating Systems Review* og *Digital Threats: Research and Practice.* AMC er ett av verdens største utdannings- og vitenskapelige samfunn, som samler utdanningsansvarlige, forskere og fagfolk for å inspirere til dialog, dele ressurser og møte feltets utfordringer. Tidsskrift som ikke er publisert av AMC, er blant annet *Data* og *Electronics*, som begge er underlagt forlaget MDPI; *Journal of Cyber Security and Mobility* er fra River publishers; *Journal of Information Security and Applications* fra Elsevier; *Peer J Computer science* fra Peer J, et forlag som utgir åpen og fagfellevurdert datavitenskap; *Computer Fraud and Security* er overført fra Elsevier til Mark Allen Group i 2022 og *European Cybersecurity Journal* er underlagt European Cybersecurity Forum.

Tre av forskningsartiklene er publisert i tidsskriftet *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* (JoWUA), et online fagfellevurdert tidsskrift som har som mål å tilby et internasjonalt forum for forskere, fagfolk og industrielle utøvere om emner relatert til trådløse mobilnettverk, databehandling og pålitelige applikasjoner. Tidsskriftet utgis av Innovative Information Science & Technology Research Group (ISYOU).

Konferanseartiklene er presentert på internasjonale konferanser, hvor noen har egne tidsskrift for publisering av disse artiklene, ofte kalt "proceedings". De fleste av disse konferansetidsskriftene har fagfellevurdering, slik vitenskapelige tidsskrift har, der andre forskere går igjennom artiklene til hverandre og vurderer kvalitet og gir kommentarer/ønsker om andre tilnærminger, og på den måte kvalitetssikrer forskningen. Systemforskning, informasjonssikkerhet og cyber- og kommunikasjonsfag er fremtredende blant konferanseartiklene. IEEE er tydelig representert i denne delen av utvalget, og særlig i konferanseartikler. IEEE er en av verdens største fagorganisasjoner og har som mål å fremme innovasjon og forskning innenfor el, elektronikk og databehandling ved å organisere og drifte en rekke tidsskrifter og konferanser (www.ieee.org). IEEE er videre en av de største aktørene innen standardisering.

2.3 Publiseringsår og geografi

Forskningsartikler og konferanseartikler utgjør til sammen 47 publikasjoner. 16 av artiklene er publisert i perioden 2020-2023, mens 12 andre i perioden 2016-2019, se figur nedenfor. I perioden 2012-2015 var 11 publisert. Resterende 8 artikler er publisert før 2012, hvorav den eldste er fra 2003. mesteparten av litteraturen i utvalget er altså publisert etter 2015. Litteraturen har ingen særskilt oppmerksomhet rettet mot enkeltland eller regioner, men fem hadde søkelys på USA, fire var internasjonale, en kanadisk, en fra India og en Tsjekkia.



Figur 1. Antall forsknings- og konferanseartikler fordelt over tidsperioder

2.4 Problemstillinger

I forskningsartikler innen samfunnsvitenskapen er det vanlig å fremsette forskningsspørsmål eller problemstillinger, som er styrende for hva den enkelte studie søker å besvare. Rapporter kan også ha en tydelig problemstilling, mens dette sjeldnere benyttes i veiledere. Veiledere har i stedet som mål å formidle tekniske grep eller etiske prinsipper som kan følges for å oppnå en ønsket effekt.

Forskningsspørsmål og problemstillinger i litteraturen om innsidetrusselen, er blant annet knyttet til deteksjon og identifisering av innsideren og trusselen. Et eksempel på dette finner vi i studien til Nurse m.fl. (2014a), som spør hva truslene består i, hvilke som er mest fremtredende, hva som motiverer innsidere til å angripe, om noen er mer mottakelig for å bli en trussel, og hvilke atferder som kan indikere et forestående angrep. De forsøker også å belyse eventuelle effekter av ny teknologi på problemstillingen.

Det er ikke en rett frem øvelse å definere hvorvidt en artikkel er rent cyberteknisk eller ikke, da teknologi og IoT blir stadig mer integrert i menneskers liv og samfunnets funksjoner. Likevel er det i denne undersøkelsen forsøkt å gi et bilde av en fordeling. Om lag halvparten av litteraturen har et sterkt cyberteknisk fokus, og litt under halvparten kombinerer et cyberteknisk tema med sosiale og menneskelige faktorer. Kun fire artikler og to veiledere har lite søkelys på cyber og teknologi, og blant disse er dem som tar for seg historier fra virkeligheten og psykologiske faktorer. Litteratur som handler om innsidetrusselen i et organisatorisk perspektiv virker å inkludere cyberdimensjonen i stor grad, antageligvis fordi det i dag er en vesentlig del av virksomheters arbeidsform og er viktig for blant annet beskyttelse av informasjon.

2.5 Metoder benyttet i litteraturen

Metoder som går igjen i litteraturen, er metaforskning, litteraturstudier og i noen grad casestudier. Noen studier har sett på hvordan å utvikle metoder for å identifisere innsidere, der de bruker teoretiske spillmodeller. Andre har utviklet metoder for å detektere innsideres aktiviteter i cyberrommet. Én studie ser på hvordan en ved å detektere personers øyebevegelser kan forutse hvem som har illegale intensjoner. I tillegg til å utvikle metoder, har flere artikler utviklet rammeverk og da gjerne basert på eksisterende litteratur.

Det er noen eksempler på kvantitative innholdsanalyser, som analyse av tekstprøver i sosiale medier, overvåking av elektronisk kommunikasjon, og sosial og dynamisk nettverksanalyse. Kun én artikkel bruker kvalitativ innholdsanalyse.

Det er en forholdsmessig liten andel av litteraturen som bidrar med ny empiri til feltet. Metastudier, som enten konseptualiserer fenomener eller forsøker å bygge eller utbygge rammeverk, er betydelig flere – og dette kan ha sammenheng med andel teori og empiri. Empiri er gjerne basert på casestudier av tidligere kjente hendelser og tar i liten grad inn førstehånds erfaringer fra praksisfeltet.

2.6 Nøkkelord

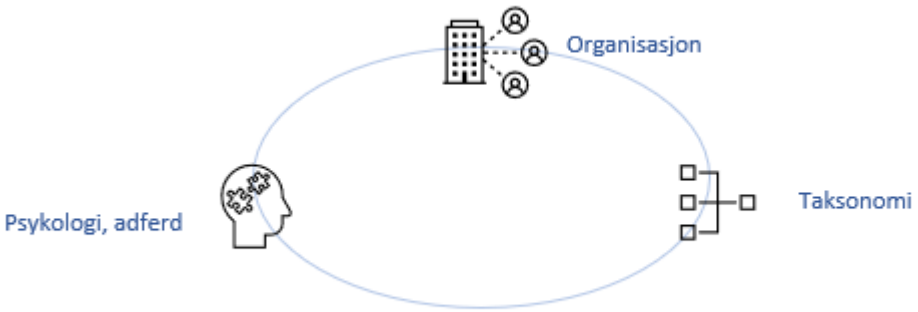
Nøkkelordene i forskningsartiklene, plassert under tittel og sammendrag, oppsummerer tema for innholdet og skal sikre relevans ved søk. Både tidsskriftsartikler og konferansebidrag har nøkkelord, men det er mindre vanlig i rapporter og guider. Ordskyen under (Figur 2) viser hvilken tematikk som ligger i nøkkelordene, og i hvilken grad den er representert.

Figur 2. Ordsky med nøkkelord fra litteraturen

Innsider er det mest brukte nøkkelordet, mens andre fremtredende er trussel, sikkerhet, cyber, risiko, nettverk, deteksjon, modell, informasjon, ondsinnet, system, modell, faktor og spionasje.

2.7 Innsidetrusselen er tverrfaglig

En atskillig del av forskningslitteraturen om innsidetrusselen handler om å klassifisere og å definere, eller forebygge og detektere, på individ-nivå eller fra organisatorisk perspektiv, være seg digital eller fysisk infrastruktur og system i en organisasjon. Derfor ender vi med en tredeling av litteraturen, der taksonomi, psykologi og organisasjonsforskning står sentralt som tre tradisjonelle og etablerte felt, se Figur 3.



Figur 3. Tverrfaglig problemstilling

Nurse m.fl. (2014a) adresserer denne multidisiplinærheten, som de beskriver som bestående av forskning innen psykologi og atferd, utvikling av deteksjonssystemer og bevisstgjøringsstrategier for organisasjoner. Her er også cyberdimensjonen viet særlig oppmerksomhet gjennomgående. En metastudie gjennomført av Subhani m.fl. (2021) fremhever også denne tverrdisiplinærheten og beskriver forskningsfeltet i tre deler: en om innsideren, inkludert ulike typer innsidere, deres motiver, metoder, innsidertilgang, profilering og nivåer av innsidervirksomhet; en annen om metoder for trusseldeteksjon inkludert tilnærming, teknikker, datasett teknikker baserer seg på og former for atferdsanalyser, og den tredje evalueringsmatriser som benyttes. En taksonomi av feltet er også grundig studert og beskrevet i Homoliak (2019), der forskningsarbeidet kategoriseres innenfor fire hovedkategorier: 1) hendelser og datasett, 2) analyse av hendelser, 3) simuleringer og 4) forsvarsløsninger (Figur 4). Innenfor første kategori, hendelser og datasett, plasserer de case-studier og studier av datasett som to underkategorier. I den andre plasserer de definisjoner og taksonomier i en underkategori, atferdsrammeverk i en annen og psykososiale rammeverk i en tredje.

Figur 4. Gjengivelse av arbeidsflyt for forskningsbidrag om innsidetrussel (Homoliak m.fl. 2019).

Strukturerte modeller og ontologiske rammeverk er tema for flere artikler i andelen litteratur som omhandler innsideren. Blant de mest siterte artiklene, finner vi både studier som tar for seg selve innsideren og som omhandler ulike angrep. Greitzer m.fl. (2018) hevder blant annet at modeller og rammeverk i utilstrekkelig grad hensyntar menneskelige faktorer og atferdspsykologi, og foreslår en ontologisk innretning der individuelle og organisatoriske sosiotekniske faktorer i større grad vektlegges. Hunker & Probst (2011) mener forskjellen på innsidere og utsidere blir mindre viktig ettersom IT-infrastruktur benyttes til å utføre angrep. De fastholder, i likhet med Greitzer m.fl., at både tekniske, sosiologiske og sosiotekniske tilnærminger må til for å håndtere innsidetrusselen.

Nurse m.fl. (2014b) foreslår et rammeverk basert på case-studier av tidligere angrep, samt annen forskningslitteratur og psykologi-teori. De identifiserer både tekniske og atferdsrelaterte nøkkelelementer fra angrepene og angriperen. Maasberg m.fl. (2020) er et eksempel der innsideren blir subjekt for analyse, og i dette tilfellet i lys av cybersabotasje som del av innsiderisiko. Her diskuteres patologiske personlighetstrekk som "den mørke triaden", et fenomen innen psykologien som omfatter et samspill mellom narsissisme, machiavellisme og psykopati (se 2.8.3 Figur 5).

Fra et organisasjonssikkerhetsfaglig perspektiv, skriver Osterritter & Carley (2021) at risiko og resiliens, inkludert insidetrusselen, har blitt studert gjennom sosiopsykologiske studier og informasjons- og informatikk. De bruker begrepet "industriell spionasje". Innsidetrusselen kan også ses fra et informasjonssikkerhetsperspektiv – der søkelys er på *sikring* av informasjonen i stedet for trusselen mot den. Feltet informasjonssikkerhet kan derfor inneha andre perspektiver på innsidetrusselen, som ikke fanges opp i denne studien.

Cyberdimensjonen har tilkommet med utbredelsen av internett og digitale systemer, og får derfor mye oppmerksomhet innen organisasjonsforskningen. Kanskje utgjør også cybersikkerhet og innsidetrussel et eget større felt, som ikke plukkes opp i denne undersøkelsen da en del studier som kun omfatter teknisk infrastruktur og system er forsøkt ekskludert i utvalgsprosessen. Med modernisering og integrering av digitale systemer i samfunn og organisasjoner, preger likevel cyber og ny teknologi det meste av litteraturen i utvalget. Fjerntilgang (‘remote access’), ‘cloud computing’ og sosiale medier har endret grunnlaget både for å utsettes for og for å utøve innsidevirksomhet (Williams m.fl., 2019). En del av forskningen handler om lingvistiske verktøy for deteksjon, også kalt "psycholinguistic insider threat research" (Brown, Watkinson og Greitzer, 2013). Dette er et fag innen informasjonsvitenskapen, som knyttes til cyberdomenet fordi det er teknologidrevet gjennom maskinlæring.

2.8 Tematikk i litteraturen

2.8.1 Kontraetterretning og spionasje

En begrenset del av litteraturen retter oppmerksomhet mot spionasje og kjente spion-saker. Blant eksempler er en artikkel om Ana Belén Montes og hvordan hun spionerte på Defense Intelligence Agency (DIA) for Cuba i 16 år uten å bli oppdaget, hennes operasjonelle metoder og hvilke faktorer som hindret DIA fra å detektere, identifisere og stoppe henne (Pareira, 2023). Pareira konkluderer blant annet med at kontroll av tidligere liv er svært viktig for å unngå infiltrasjon; at IT-sikkerhet ikke beskytter; at polygraf ikke er tilstrekkelig for å vurdere sannhet; at den beste måten å avdekke spionasje på er å spionere på fiendens etterretning og at dette er mye vanskeligere under etterforskning; at et godt mellommenneskelig forhold er avgjørende for å unngå spionasje; at memorering er en av de viktigste egenskapene til en spion; at støtteagenter er svært viktige for at spionasje kan finne sted; at spioner trenger psykologisk støtte; og at en god spion kan være veldig produktiv i mange år (s. 584). Pereira fokuserer også på rekruttering, og det refereres til en bok om hvordan universiteter og akademia benyttes til å rekruttere til spionasje (se Golden, 2017), samt et white paper fra Federal Bureau of Investigation (FBI) med tittelen *Higher Education and National Security: The Targeting of Sensitive, Proprietary, and Classified Information on Campuses of Higher Education*. White paperet er fra 2011 og retter oppmerksomhet mot hvordan utenlandsk etterretning og ikke-statlige aktører bruker høyskoler og universiteter for å fremme sine etterretnings- og operative behov (se FBI, 2011).

Et annet eksempel er en artikkel fra 2009, som også belyser tilfeller der tilgang til gradert informasjon er misbrukt av innsidere. Harber (2009) fremhever med Prouty-saken – ansettelsen av Nada Nadim Prouty i det amerikanske Central Intelligence Agency (CIA) etter terrorangrepet 9/11 – hvordan ikke-statlige aktører også kan operere som innsidere og utgjøre en trussel mot nasjonal sikkerhet. Problemstillingene her er knyttet til omfang av trusselen fra slike aktører, hvorvidt den tas på alvor i vurderinger for USAs nasjonale sikkerhet og eventuelle retningslinjer som kan redusere skade. Denne artikkelen er blant de eldste inkludert i denne undersøkelsen, og handler i essens om kontraetterretning som en neglisjert del av etterretningsdisiplinen.

En nyere studie, handler om samtidens store lekkasjer og varslingssaker, som fra Edward Snowden og Chelsea Manning. I denne artikkelen er innsidetrusselen mot nasjonale sikkerhetsinteresser og lekkasje av amerikansk hemmeligstemplet informasjon tema, og forfatterne av artikkelen er forskere i US Military- og US Naval Academy (Gioe & Hatfield, 2020). Til tross for at varsling ikke er en handling aktivert av andre staters etterretningsinteresser, mener artikkelforfatterne at det er interessant å vurdere om disse aktivitetenes skadeomfang kan sammenlignes. Artikkelen måler skadeomfang forårsaket av masselekkasjer opp mot eldre spionsaker, og kaller varslingssakene en ny transparens-drevet, digital generasjon innsidetrussel. Forskerne fremholder at slike er økende i frekvens. Denne nokså nye artikkelen hevder at en slik systematisk sammenligning av saker mangler i forskningsfeltet, og tilbyr derfor et rammeverk for å kartlegge skadeomfang. Snowden-lekkasjen og Cambridge Five-spionringen er brukt som casestudier for å måle moderne digitale sikkerhetsbrudd mot mer tradisjonelle

kontraetterretningsbrudd som de fra den kalde krigen. Forfatterne skiller mellom innsidere som enten "self-tasked" *eller* noen som får sine oppgaver fra et eksternt byrå (s. 706). Snowdens aktivitet blir beskrevet som "completely self-directed" mens Manning forklares som kultivert og semikontrollert av WikiLeaks-grunnlegger Julian Assange. Cambridge five beskrives som paradigmatisk for eksternt kontrollert aktivitet, som i regi av Moskva var rent etterretningsmessig organisert og kontrollert (ibid).

Denne delen av litteraturen virker å tilhøre et større forskningsfelt innen etterretningsstudier, der kontraetterretning hevdes å utgjøre et noe oversett og underteoretisert spor (Gioe & Hatfield, 2020; Harber, 2009). Artiklene forteller om kjente hendelser og personer for å synliggjøre problemet med innsidetrusselen (sett fra innsiden), men går ikke videre i å søke å utrede problemstillingen i særlig grad. Sporing av gradert informasjon, overvåking av bruk av tilganger, tilpasset trening av ansatte og bevisstgjøring om hvordan trusselaktører jobber, er anbefalinger som fremsettes i litteraturen.

2.8.2 Kartlegging, identifisering og forebygging

Å kartlegge hvem som er en mulig innsider har vært tema for flere forskningsmiljø igjennom tidene. Kartlegging vil i noen tilfeller bety en direkte overvåkning av ansatte og stille strenge krav til personvern og etikk. Videre kan overvåkning medføre stress, lavere grad av forpliktelse og redusere effektivitet. Overvåkning kan naturligvis også være med på å skape et anstrengt forhold mellom arbeidsgiver og arbeidstaker, og det kan gi falske negative signaler til en arbeidsgiver om en arbeidstaker (Greitzer, 2019; Brown m.fl., 2013).

En av utfordringene med å kartlegge innsidetrussel er å kunne skille når personenes atferd utgjør en innsiderisiko fra de tilfellene der atferden er kontraproduktivt for organisasjonen. For å møte denne utfordringen foreslår Marbut & Harms (2023) at innsidetrusselen bør omfavne når personen ikke har til hensikt å påføre organisasjonen skade, i tillegg til når personen har til hensikt å påføre skade. I forskningslitteraturen finner vi eksempler på studier som har til hensikt å identifisere psykososiale indikatorer for å gjenkjenne personkarakteristikker hos personer som kan ha ondsinnede hensikter (malicious insider). En studie lister opp tolv psykososiale indikatorer identifisert der de fem sterkeste indikatorene var i hvilken grad personen var misfornøyd, aksepterte tilbakemeldinger, hadde vanskeligheter med å beherske sinne, viste engasjement og hadde respekt for autoriteter (Greitzer & Frincke (2010) i Hunker & Probst, 2011).

I forskningslitteraturen finnes anbefalinger for å etablere en konvensjon som beskriver ulike typer av innsider- og utsiderkarakteristikker og at disse bør være graderbare (Zimmer m.fl. 2021; Zaytsev m.fl., 2017). Argumentasjonen tar utgangspunkt i at innsidekarakteristikker som ‘external penetrator’, ‘masquerader’, ‘legitimate user’, ‘clandestine user’, ‘real real insider’, ‘traitor’ og ‘errant insider’ er binære. De forutsetter at innsideren enten *er* en av disse typene eller *ikke*. En slik avgrensing tar dermed bort muligheten for at en innsider kan ha en gradering mellom å være på utsiden og innsiden. Argumentasjonen illustrerer et gjennomgående dilemma i forskningen,

nemlig at det ofte er krevende å skille mellom innsidere og utsidere av en organisasjon når de først opererer i et internt nettverk (Homoliak m.fl., 2019). I tillegg bruker forskningslitteraturen karakteristikkene om hverandre, slik som 'masquerader' og 'traitor', noe som gjøre det krevende å sammenligne og bygge videre på funnene mellom ulike studier (Zimmer m.fl., 2021).

Litteraturkartleggingen viser at det finnes en rekke studier som ser på både atferd og kultur, og teknisk overvåkning av uønsket datatrafikk, men som regel hver for seg. Mens noen studier ser på hva som typisk karakteriserer et menneske som kan være en innsidetrussel, har andre studier sett på hvordan identifisere innsidevirksomhet via å studere mønster i datatrafikk (Bebee m.fl., 2017; Patil og Meshram, 2018), eller identifisere sårbarheter via datasimuleringer (Laszka m.fl., 2014). Det er også i litteraturen beskrevet hvordan "honningfeller" er brukt som lokkemat i form av en falsk attraktiv komponent som lurer en potensiell innsider til å gå i fella (Spitzner 2003). Andre studier har utført fysiske målinger på øyebevegelser for å studere om en kan detektere de som jobber på innsiden som bevisste innsidere da disse har et annet bevegelsesmønster enn de som ikke har tilsiktede hensikter (Matthews m.fl., 2018).

Organisatoriske faktorer som kan forebygge innsidevirksomhet er tema for en betydelig andel av organisasjonsforskningen og mye av dette går ut på å kartlegge, identifisere og forebygge. Noen foreslår tiltak som å koble HR på i tidlig fase, ha fysisk sikring så vel som digitale sikre verktøy, og en årvåken ledelse (CERT Insider Threat Team, 2016). Andre foreslår økt bevissthet av sine ansatte om et eventuelt skadeomfang, for å øke deres eierskap, og vilje til å verne om sin egen organisasjon (Dulipovici, 2017). Sky- og mobilteknologi gjør veien fra utsiden til innsiden mindre tydelig, og gjør det vanskeligere å detektere eventuelle innsidere. Derfor ser noen studier også på hvordan cybersikkerhet ikke bare er en teknisk barriere, men også en kombinasjon av tekniske og menneskelige egenskaper som kan studeres via individers sosiale media, som igjen kan gi en større forståelse for hvordan innsidetrusselen kan begrenses (Mazzarolo, 2020).

Av norsk litteratur har NSM gitt ut en brukerveiledning "Grunnprinsipper for personellsikkerhet", hvor de gir veiledning til hvordan norske bedrifter og institusjoner kan ivareta personellsikkerhet og redusere mulig innsidetrussel. Grunnprinsippene er her delt inn i fire kategorier; identifisere og kartlegge, beskytte, opprettholde og oppdage, og håndtere og gjenopprette (NSM, 2020). Også Mazzarolo og kolleger (2020) påpeker at enkelte tiltak kan forebygge innsidetrusselen, slik som administrative tiltak som direktiver og regulering, teknisk kontroll, fysisk kontroll, risikobevissthet rundt denne tematikken, og håndteringsplan av en eventuell skade påført av en innsider.

Mye av kartleggings-forskningen på feltet foreslår kategorisering av innsidevirksomhet. Kont og kolleger (2015) deler innsidevirksomhet inn i fem forskjellige kategorier; bedrageri, sabotasje, tyveri av "intellectual property" (IP), spionasje og uintenderte handlinger (sitert i Mazzarolo 2020, s. 59)). CERT 2022 deler inn i tre kategorier; bedrageri, tyveri av "intellectual property" (IP) og sabotasje. Arkitektur, monitorering og brukerveiledning er også tema i Typakula & Varadharajan, 2013.

2.8.3 Psykologisk profilering av innsideren

Psykologisk profilering av mulige innsidere er ifølge Pfleeger (2008) etterspurt og i utgangspunktet en appellerende idé, men i realiteten vanskelig å få til. Dette er et syn som får støtte av blant annet Zimmer m.fl. (2021), og er redegjort for i denne rapportens kapittel om taksonomi for innsideren og dennes atferd og virksomhet. I likhet med tanker innen atferdspsykologien vektlegger Pfleeger at det vil være mer produktivt å trekke på psykologiske verktøy som oppfordrer til ønsket atferd blant ansatte. Noe av litteraturen refererer forholdsmessig mye til CIA og PERSEREC for hva som bør inngå i et rammeverk som skal identifisere innsideren (adferdsindikatorer) med begrunnelse i at dette er adferd demonstrert nært forestående avsløring (se Jacobsen, 2021; Jaros m.fl. 2020).

Innsideren er derfor forsøkt klassifisert og kategorisert ut ifra personlighetstrekk og antisosial atferd. 'Den mørke triaden' kommer stadig frem i litteraturen som referanse til slik psykologisering av individet, en eldre teori fra personlighetsforskning introdusert av Robert og Joyce Hogan (2001), og popularisert av Delroy Paulhus (sitert i Harms m.fl. 2022 s.2). Den mørke triaden viser i kortfattethet til et samspill mellom narsissisme, machiavellisme og psykopati, og skal forklare avvikende og antisosial atferd innenfor et spekter som ikke er tilsynelatende (illustrert i Figur 5). Forskning på dette feltet argumenterer for at såkalte mørke personlighetstrekk, eller sosialt avvikende kognitive mønstre, kan trigges ved stress eller ekstra belastning, og mener derfor at dette bør inngå i forskning på innsidetrusselen (Harms m.fl. 2022, s. 2214). Normbrytende, egoistisk og egennyttig fremferd kjennetegner mennesker med såkalte mørke trekk, og det rettes kritikk mot eksisterende forskning på innsidetrusselen for ikke å tilstrekkelig vektlegge slike trekk som betydelig for truende atferd.

Figur 5. Den mørke triaden

Marbut & Harms (2023) argumenter imot denne ideen om å se unyansert til innsiderens personlighet, og fremfører bevis for at biologisk natur hele tiden står i dynamisk samspill med omgivelsene. De mener at intenderte innsidehendelser for ofte kategoriseres som motivert av egoisme og rasjonalisering av umoralsk oppførsel, mens ikke-ondsinnede trusler assosieres med

mistilpasning og nysgjerrighet. De legger frem det de kaller et neo-sosioanalytisk rammeverk som skal bidra til en mer nyansert kartlegging av innsideaktivitet.

3 Definisjoner av innsidetrussel og innsideren

Definisjon av begrepene innsidetrussel og innsider er sentralt i forskningslitteraturen. Hvordan disse to begrepene defineres har betydning for hvordan forskningen tilnærmer seg problematikken, men også hvilke avgrensinger som er gjort. Definisjonene danner dermed utgangspunkt for hva litteraturen problematiserer, men også hva som utelates. De fleste definisjonene skiller mellom innsidetrussel og innsideren, samtidig som de to definisjonene henger nøye sammen (Homoliak m.fl., 2019).

Denne delen av rapporten gir først eksempler på hvordan de to begrepene defineres. Hensikten er å få frem bredden av definisjoner som utvalget av forskningslitteraturen viser. Deretter ses definisjonene av de to begrepene i sammenheng, slik det ofte fremkommer av litteraturen. Videre følger en analyse av hva disse definisjonene inneholder. Dette gir et overblikk av hva som kjennetegner definisjonene, og tegner et utgangspunkt for hva de i mindre grad inneholder og utelater.

3.1 CERT Common Sense Guide to Mitigating Insider Threats

Nedenfor gjengis et utvalg definisjoner av innsidetrussel og innsider fra forskningslitteraturen. Fra den akademiske litteraturen ser vi ofte referanse til CERT for definisjon av innsidetrusselen. Den nyeste versjonen fra CERT definerer innsidetrusselen slik:

> Insider Threat—The potential for an individual who has or had authorized access to an organization's critical assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization. (CERT, 2022, s.3)

CERT definerer at trusselen er et potensiale som kan påvirke organisasjonen negativt. Individet er en person som har eller har hatt tilgang til kritisk verdi for organisasjonen. CERT vektlegger at verdiene må være kritiske for organisasjonen og anslår dermed en avgrensing i alvorlighetsgrad. Definisjonen beskriver også at hensikten for individet kan være et ønske om å forvolde skade (malicious[2]), eller at personen ikke har til hensikt å forvolde skade (unintentional). De to siste elementene av definisjonen beskriver at personen har eller har hatt tilgang til organisasjonens kritiske verdier, og utfører handlinger på en slik måte at det kan medføre en negativ konsekvens

[2] Malicious er antageligvis et juridisk begrep i lovgivningen til USA.

for organisasjonen. Scenarioer av innsidertrusler brukes for å beskrive mønster for hvordan en innsider negativt kan påvirke organisasjonen.

I tillegg definerer CERT innsiderisiko. Denne definisjonen er basert på anerkjent definisjon av risiko:

> Insider Risk—The impact and likelihood associated with the realization of an insider threat. (CERT, 2022, s.3)

CERT sin tilhørende definisjon av innsideren tilfører at dette er et individ som har eller har hatt tilgang til organisasjonens kritiske verdier. CERT bruker scenario-tilnærming for å beskrive hvordan en innsider kan påføre organisasjonen skade.

> With this perspective, an insider threat actor (or simply, an insider) is an individual who has or had authorized access to an organization's critical assets. The distinct patterns of how an insider threat actor can negatively affect the organization are referred to as insider threat scenarios. Each insider threat scenario has impact potential (typically measured in dollars as direct and indirect loss, or as a qualitative low to high anticipated magnitude) and likelihood potential (typically measured as a probability or percentage, or as a qualitative low to high anticipated probability of occurrence). (CERT, 2022, s.3)

Sitatene overfor er basert på CERT sin siste revisjon fra 2022. Hovedforskjellene fra tidligere definisjoner er introduksjonen av innsiderisiko og bruk av trusselscenarioer. Definisjonene har blitt revidert flere ganger de senere årene og en del av litteraturen peker på disse oppdateringene. Det beskrives endringer fra femte utgave, der *muligheten* for individet til å misbruke sin tilgang tillegges vekt, og at den nyere varianten inkluderer både intenderte og ikke-intenderte trusler samt vold på arbeidsplassen (CERT Insider Threat Team, 2016).

> The definition of insider threat has changed since the fifth edition and is now defined as the potential for an individual who has or had authorized access to an organization's assets to use that access, either maliciously or unintentionally, to act in a way that could negatively affect the organization. This definition has been updated to include both intentional and unintentional insider threats as well as workplace violence. (CERT Insider Threat Team, 2016).

3.2 Andre definisjoner i litteraturen

Mazzarolo & Jurcut (2020) viser også til CERT sine (tidligere) definisjoner av intenderte og uintenderte innsidere. CERT sin rapport 'The CERT Guide to Insider Threats' publisert av Cappelli, Moore og Trzeciak i 2013, har en spesifikk definisjon av hvem den ondsinnede innsideren kan være:

> A malicious insider threat may be either a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems. (Cappelli m.fl. 2013 sitert i Mazzarolo & Jurcut, 2020 s. 58)

Den ondsinnede innsideren kan her være motivert av økonomisk vinning, misnøye på arbeidet, ideologi med mer. Mazzarolo & Jurcut peker på at omfanget av uintenderte innsidesaker innenfor IT på arbeidsplassen er virksomheters største utfordring, og definerer den ubevisste innsideren som

> [a] current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and who, through action or inaction without malicious intent, causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems. (CERT Insider Threat Team, 2013, sitert i Mazzarolo & Jurcut, 2020 s. 58)

Definisjoner i forsknings- og konferanselitteraturen

Maasberg & Beebe (2014) tar utgangspunkt i definisjonen til Pfleeger & Stolfo, (2009) og definerer innsideren som en trussel representert av individer som er autoriserte, eller på annen måte tilkjent tillit, i en organisasjon, og som oppfører seg på en måte som setter data, systemer, organisasjonen og i noen tilfeller hele forretningens levedyktighet på spill. Det er altså individer tilkjent tillit og tilgang som begår innsidevirksomhet i deres definisjon:

> The term insider threat refers to the danger posed by trusted members of an organization who 'behave in ways that put our data, our systems, our organizations, and even our businesses' viability at risk'. (Maasberg & Beebe, 2014, s. 60 siterer Pfleeger & Stolfo, 2009, s. 10)

Mens Maasberg & Beebe tar utgangspunkt i at trusselen befinner seg på innsiden, er Greitzer i følgende formulering opptatt av at trusselen kommer utenfra. Det er innsideren som eksponerer virksomheten for en utenforstående trussel og/eller trusselaktør. Greitzer m.fl. (2019, s. 2) inkluderer i tillegg at innsideren ikke nødvendigvis må ha intensjon om å begå innsideaktivitet, at deres handlinger kan være utilsiktede. De legger utover dette vekt på type skadelig utfall, som destruksjon, eksfiltrering eller lekking av sensitiv informasjon, altså konsekvenser av handlinger eller ugjerninger:

> Insider threats refer to threats posed by individuals who intentionally or unintentionally destroy, exfiltrate, or leak sensitive information, or expose their organization to outside attacks. (Greitzer, 2019 s. 2)

Tilsvarende inndeling i om trusselen er med hensikt eller ikke finner vi i artikkelen til Liu Xiangyu m.fl. (2017), med særskilt oppmerksomhet rettet mot cybertrusler. Den intenderte versus den uintenderte trusselen definerer de slik:

> Intentional insider threat is current employees or former employees, business partners and other people who unintentionally or maliciously authorize one's website or allows software access to their own company's network, system and data, which causes a series of data leakage resulting in interests of the current phase damaged or income expected reduced. (Liu Xiangyu m.fl., 2017 s. 1)

De mener denne definisjonen er både inkluderende og åpen slik at den kan omfatte både intenderte og uintenderte innsidehandlinger. Andre eksempler på definisjoner som skiller mellom tilsiktet og utilsiktet insideraktivitet, er situasjoner hvor en insider bryter sikkerhetsreglene til organisasjonen:

> Insiders can be classified into intended insiders and unintended insiders. Intended insiders are who can conduct deliberately malicious activities targeted at any organization by a variety of motivations, including revenge, financial need, greed, dissatisfaction, health problems, proclaimed patriotism, notoriety, and political ideology. Intended insiders also can be divided into Traitor and Masquerader […] The unintended insiders are who inadvertently launch attacks inside an organization due to inadvertent actions such as breaking security policy. (Kim m.fl., 2019, s. 49)

Hunker & Probst (2011) beskriver at skillet mellom å være en innsider og en utsider virker å miste betydning når IT infrastruktur brukes til å utføre innsiderangrep. Forfatterne definerer at innsidetrusselen utgjør et individ med privileger som personen misbruker eller ved at personen har tilgang til privileger som resulterer i misbruk. Det sentrale i denne definisjonen er individets privilegerte tilgang, underforstått til verdier som organisasjonen besitter. Definisjonen gir rom for at tilgangen misbrukes eller at det resulterer et misbruk. Denne formuleringen unngår å beskrive til hvilken hensikt misbrukes oppstår.

> An insider threat is [posed by] an individual with privileges who misuses them or whose access results in misuse. (Hunker & Probst, 2011, s.7)

Tidlige definisjoner av innsideren kommer til uttrykk i Hunker & Probst (2011) sin studie, som viser til en definisjon utarbeidet av en tverrfaglig arbeidsgruppe i 2008:

> [A]n insider is a person that has been legitimately empowered with the right to access, represent, or decide about one or more assets of the organization's structure. (2011, s. 6)

Selv om disse definisjonene i utgangspunktet søker å beskrive trusselen, har de betydelig søkelys på innsideren og dennes gjerninger, og det virker vanskelig å skille utføreren og utførelsen fra utføringen, altså individ og metode fra gjerning. Spitzner (2003) peker på den *avanserte* innsideren, som ligner mer på det vi kjenner fra litteraturen om spionasje, og hvordan denne er vanskeligere å avbøte.

> This trusted individual knows your networks and organization. Often, these individuals are not after computers, but specific information. This is a risk that has proven far more dangerous, and far more difficult to mitigate. (Spitzner, 2003, s.1)

Nurse m.fl. (2014a) underbygger oppfatningen om at det er vanskelig å skille innsidetrusselen fra innsideren. I tillegg til hvem innsideren kan være og hens privilegerte tilgang beskriver forfatterne også hvilke hensikter innsideren kan ha. Dette kan være hevn og å oppnå økonomisk vinning, og påføre skade på organisasjonen.

> The essence of most definitions, however, is that an insider threat is a member of trusted personnel (e.g., employee, contractors, business partners) that used their privileged access for some unauthorised purpose such as revenge or financial gain, and to the detriment of their enterprise. (Nurse m.fl., 2014a, s. 271)

Truslene fra ondsinnede trusler kan være bedrageri, tyveri av intellektuell eiendom (IP) og sabotasje av infrastruktur. Nurse m.fl. (2014a) mener oppmerksomheten om trusler fra insidere som uforvarende påfører virksomheten trusler, såkalte 'accidental insiders', har økt. Tilsvarende kobling mellom innsidetrussel og innsideren finner vi i definisjonen gjengitt i Subhani m.fl., (2012).

> According to the author Chan (2019), an insider threat is defined as "A person who has the potential to harm an organization for which they have inside knowledge or access". (Chan 2019 sitert i Subhani m.fl. 2012, s. 1)

Sammenkoblingen kommer også til uttrykk i definisjonen til Nostro m.fl. (2014). De definerer innsideren som følger. Definisjonen fremhever personen bruk av privilegier.

> In general, we can simply define an insider as an entity that has been given the privileges to act within a specific environment. What is of interest is the use of privileges (being it an abuse or misuse of privilege, or simply a mistake) in such a way that it constitutes a threat (being it malicious or accidental) i.e., an insider threat. (Nostro m.fl., 2014, s. 4)

Selv om definisjonen bruker ordet enhet (entity), noe som favner vidt og kan tolkes til å inkludere programvare, leder forfatternes diskusjon til at betydningen av enhet i hovedsak handler om person.

Crawford og Peterson (2013) beskriver relasjonen til en organisasjon på en tilsvarende måte som det er flere andre eksempler på i definisjon av innsidetrusselen. I deres definisjonsbruk er ondsinnede innsidere en undergruppe.

> Insiders are frequently … defined as individuals who are current or former members of an organization, contractor or partner, who are trusted and have or had access or knowledge of the organization's information systems,

> and objectives. Malicious insiders are a subset of individuals who intentionally misuse their trusted position through a set of actions and against a target or targets that result in a violation of confidentiality, integrity and/or availability (CIA). Malicious insiders may be disgruntled employees, employees who see an opportunity for financial benefit or spies who join an organization in order to commit espionage or financial fraud. (Crawford & Peterson, 2013, s. 1821)

En innsider kan være rekruttert, frivillig og/eller mål for en stikkoperasjon (Jaros m.fl., 2019 s.12). Jaros og kolleger bruker dualiteten indirekte, ved å antyde at innsideren er enten rekruttert (altså bevisst), frivillig (også bevisst) eller lurt inn i operasjon (ubevisst). Det er her to varianter av den bevisste, mens den tredje er enten helt ubevisst eller i en fase fra ubevisst til bevisst. En stikkoperasjon er en villedende operasjon designet for å fange en annens lojalitet og villighet til å utføre oppgaver og oppdrag.

Lignende beskrivelser av innsideren, der bevissthet og ubevissthet vektlegges, finner vi også i FFI-rapporten "Hva vet vi om innsiderisiko?" (Slagnes, 2023). Her kategoriseres også innsidere i ubevisste og bevisste, og videre herunder rekrutterte, selvmotiverte og dem som til enhver tid befinner seg i gråsonen imellom. Videre kategoriseres ulike faktorer for motivasjon ut ifra NSM sin kategorisering, som ideologi eller omstendigheter. Søkelys på opplevelse av urettferdig behandling på arbeidsplassen, ønske om hevn eller lignende, vitner igjen om forsøk på å finne "feilen" hos vektoren, snarere enn å studere problemet per se. Både individer og omstendigheter rundt dem vil stadig være gjenstand for endringer, og av den grunn argumenterer andre forfattere for at søkelys i stedet bør rettes mot faktorer som kan være styrende for forhold av mer varig karakter.

Til sammenligning definerer the Cybersecurity and Infrastructure Security Agency (CISA) innsidetrussel som gjengitt under. Definisjonen retter oppmerksomhet mot bruk av autorisert tilgang, som med tilsiktet eller utilsiktet hensikt kan påføre skade for departementet, samt ulike typer av innsidetrusler, slik som voldsutøvelse, spionasje, osv.

> The threat that an insider will use their authorized access, intentionally or unintentionally, to do harm to the department’s mission, resources, personnel, facilities, information, equipment, networks, or systems. Insider threats manifest in various ways: violence, espionage, sabotage, theft, and cyber acts. (CISA)

I CISAs definisjon av innsideren utdypes personens tilgang til eller kunnskap om organisasjonen.

> Any person who has or had authorized access to or knowledge of an organization's resources, including personnel, facilities, information, equipment, networks, and systems. (CISA)

Blant forskningsartikler som er av eldre dato finnes en definisjon som knytter hacker-aktivitet til en person som er eller har vært ansatt i organisasjonen.

> It often happens that the "hacker" turns out to be a current or former employee who engages in unauthorized system usage for personal advantages or even revenge. The perpetrator in this situation is called an insider, and the menace caused by his actions to the organization's computer assets is known as an insider threat. (Hu m.fl., 2006, s. 1)

Eldre forskningslitteratur beskriver også tilgangen en person har til en organisasjon, slik som gjengitt nedenfor fra Santos m.fl. (2008). Forfatterne problematiserer at en trussel kan være å manipulere beslutningstakere ved å innlemme feilinformasjon i deres informasjonsgrunnlag.

> An insider is either a current or previous member of an organization who has access to privileged resources and whose output has an impact on decision makers. (Santos m.fl., 2008, s. 345)

I en upublisert rapport av Levi & Gundu fra 2015, gjengitt i Zimmer m.fl. (2021), inndeles det de kaller for innsider-viktimisering i fire kategorier. Inndelingen er basert på omkring 100 tilfeller rapportert i pressen. De fire kategoriene er:

i. Viktimisering uten ondsinnede hensikter. Dette er ansatte som ikke følger beste praksis eller som av vanvare engasjerer seg i handlinger som er ødeleggende for de økonomiske interessene til selskapet.
ii. Viktimisering med altruistisk hensikt. Dette kan være der ansatte varsler om uforsvarlige forhold. Edvard Snowden sin varsling inngår i denne kategorien.
iii. Viktimisering med ondsinnet hensikt som kan resultere i sivil rettstvist. Dette kan være der en ansatt bytter jobb og tar med seg konfidensiell informasjon til en konkurrent.
iv. Viktimisering med ondsinnet hensikt som kan resultere i straffesak. Denne kategorien kan inndeles i fem undergrupper; i) avbrudd eller destruksjon; ii) underslag; iii) industrispionasje; iv) innsidehandel; og v) datatyveri (som også inkluderer identitetstyveri).

En viktig kritikk av trusselen som innsidefenomen fremlegges også i forskningen til Zimmer m.fl., (2021). De argumenterer med at definisjon av innsidetrusselen bør gå utover det å definere og karakteriserer individet, altså innsideren. De beskriver *innsidigheten* ('insiderness') som en gradering mellom en insider og en utsider.

> An insider threat is not a threat of an insider, but more precisely a threat of an insider, where his insiderness is involved (intentionally or accidentally) and where this insiderness actually enables or compounds the threat. (Zimmer m.fl., 2021, s. 2:17)

Forfatterne argumenter for å utarbeide innsiderhetskarakteristikker. Beskrivelsen av karakteristikkene bør beskrives i relasjon til et domene, i form av at innsideren har en gradert form for tilgang til eller har klart å få tilgang til domenet. Et domene trenger ikke nødvendigvis å være så vidt som en organisasjon. Det kan for eksempel være avgrenset til et informasjonssystem, datanettverk, programvaresystem eller sikkerhetssystemer.

> Insider characteristics can only be provided, granted, or are controlled by a specific domain or by authorities of that domain[3] either deliberately or inadvertently. One can see that the domain of an insider constitutes an important area of reference. Examples of domains, which can also be referred to throughout this article, are organisations, information systems, computer networks, software or hardware products, or security mechanisms. Another key observation is the one that the distinction between an insider and an outsider is not binary. There evidently exists a graduation in the distinction between an insider and an outsider, which in the literature has been named insiderness. (Zimmer m.fl., 2021, s. 5)

Forfatterne foreslår å beskrive innsidigheten (insiderness), altså karakteristikker som synliggjør hvilken grad en person står mellom å være på utsiden og innsiden av et domene. De foreslår at innsidigheten utvikles fra det de kaller for innsidighetsmodellering. Denne modelleringen består av en eksplisitt beskrivelse av domenet, beskrivelse av innsidighetskarakteristikker som baserer seg på fem ulike typer og graderinger, noe som samlet sett gir en karakteristikk av innsidigheten til en person for det spesifikke domenet (Zimmer m.fl., 2021).

Samme forfattere argumenter med at i deres forslag til innsidigheten av en person (insiderness) er det ikke relevant å betrakte hensikten til insideren. Hensikten er relevant å inkludere i

definisjonen av innsidetrussel, men altså ikke om i hvilken grad en person er på innsiden (insiderness). På den måten omslutter hensikter, slik som ondsinnede, utilsiktete og gode hensikter i deres forslag til bruk av 'insiderness'. Karakteristikker av innsideren, slik som personens kapasitet eller kapabilitet, er heller ikke relevant for innsidigheten hos en person (the insiderness of an individual).

Marbut & Harms (2023) argumenterer for noe annet. I stedet for å beskrive om en person er dårlig eller god, bør innsidetrusselen være rettet mot hvilken atferd personen har. De begrunner dette med at atferd ofte i litteraturen er inndelt i om den er ondsinnet eller ikke. Ondsinnet atferd kan relateres til særskilte personer (insidere) ved at de har ulike motiver eller ferdigheter for å kunne utføre handlingene. Ikke-ondsinnet trusler kan relateres til særskilte personer ved at disse har kognitive prosesser eller typiske atferdsmønster som gjør det mer sannsynlig med at det oppstår ulykker.

3.3 Hvordan de to definisjonene henger sammen

Som demonstrert i eksemplene overfor henger definisjon av innsidetrussel (insider threat) og innsider (insider) nøye sammen. Homoliak m.fl. (2019) mener at definisjon av innsider som oftest er en statisk beskrivelse av individer, der begreper slik som tilgang (access), kunnskap, tillit, eller retningslinjer for sikring (security policy) ofte er inkludert. Definisjoner av innsidetrussel viser ofte til handlinger, slik som misbruk av tilgang, eller kunnskap som innsideren har, eller brudd på retningslinjer for sikring (Homoliak m.fl., 2019).

Forskjellene mellom de to definisjonene kan også forklares på en annen måte. Den ene tilnærmingen er at innsidetrusselen defineres som trusselen for at virksomheten kan bli påført skade. I denne tilnærmingen utgjør tilhørighet som individet har til virksomheten, hensikt, tilgang, kunnskap, osv., selve trusselen. Denne tilnærmingen virker å være mest utbredt i vårt utvalg av forskningslitteratur. Mange av disse refererer til CERT sin definisjon, som er gjengitt tidligere. CERT sin siste revisjon av definisjonene har blitt tilpasset tankegangen for risikostyring, men dette endrer ikke de prinsipielle forskjellene i definisjonene, som er beskrevet nedenfor.

En annen tilnærming vi observerer med bruk av definisjonene, er at det er innsideren som er innsidetrusselen. I denne type tilnærming er det graderingen i hvordan individet oppfører seg på innsiden av et domene som utgjør trusselen (og et domene kan være noe annet enn en virksomhet). Denne tilnærmingen fremstår likevel mindre utbredt. Definisjonen til Zimmer m.fl., (2021), som brukes i flere av de nyere artiklene, eksemplifiserer denne tilnærmingen. Forfatterne beskriver at innenforskapet (the insiderness), dvs. en gradering mellom å være på utsiden og innsiden, ble beskrevet av Bishop m.fl., allerede i 2010, men uten at årsakene til- og implikasjonene av begrepet har blitt utdypet tidligere.

Zimmer m.fl. (2021) gjør et poeng av at en innsiders hensikt ikke er relevant for definisjonen av innenforskapet (the insiderness), men at det er relevant for innsidetrusselen. Ved å sammenligne

de to tilnærmingene er det likevel ikke tegn til at dette utgjør vesentlig forskjell. Noen definisjoner og tilnærminger er mer utbredt enn andre, men sett opp mot hverandre omfavner de mye av det samme.

3.4 Utvikling av definisjonene av innsidetrussel

En gjennomgang av ulike definisjoner brukt i litteraturutvalget for denne studien viser at definisjonene har inkludert en del av de samme elementene over tid. Trusselen om at virksomheten kan lide skade av at verdier kommer på avveie eller på annen måte blir misbrukt er tydelig.

Det er som regel en person, et individ, som utgjør denne trusselen. Unntaket er der relasjon mellom person og organisasjon inkluderes. Personen har eller har hatt en relasjon til virksomheten, og kan ha til hensikt å utføre handlinger som påfører virksomheten skade. Men personen kan også uforvarende utføre handlinger som utilsiktet medfører skade for virksomheten. I hvilken grad definisjonene vektlegger hensikt for handlingene varierer, og det er også noe variasjon i hvorvidt definisjoner vektlegger person-karakteristikker, konkretisering av handlinger og konkretisering av hva trusselen om skade for virksomheten innebærer.

I noen definisjoner som inkluderer personens hensikt for handlingene brukes begreper som malicious og non-malicious. Andre bruker begreper som intentional og un-intentional. De førstnevnte ordvalgene (malicious/non-malicious) kan relateres til et juridisk begrep som brukes i USA og dermed knyttes en definisjon som bruker disse ordene sterkere opp mot juridisk vurdering av om handlingene er i henhold til lover og regler. Det andre alternativet (intentional/un-intentional) knyttes ikke på samme måte opp til lover og regler som en referanse. Denne type valg av begreper kan ha betydning for hvordan forskningen tilnærmer seg problematikken. For begge alternativene uttrykker det individets (selvstendige) handlinger, intensjoner, osv., til å være en innsidetrussel.

Analyse av definisjonene i neste kapittel utdyper mer om hvordan definisjonene karakteriserer innsideren, dens handlinger og motivasjon og også hvordan definisjonene beskriver hvilke verdier for virksomhetene som trues.

3.5 Analyse av definisjonene om innsidetrussel og innsideren

En sammenfatting av definisjonene som er funnet i denne studien, kan tydeliggjøre hvilke elementer de er konstruert av[4]. Under følger en analyse av definisjonenes innhold. Ingen av

[4] Analysen er basert på femten ulike definisjoner funnet i følgende av utvalgets forskningsartikler: Spitzner, 2003; Hu m.fl., 2006; 2008; Hunker & Probst, 2008 i Marbut & Harms, 2023; Pfleeger & Stolfo, 2009 i Maasberg & Beebe, 2014; Hunker & Probst, 2011;

definisjonene fra utvalget inneholder alle elementene. Elementer som er identifisert vises i venstre kolonne i tabellen nedenfor. Høyre kolonne sammenstiller typiske ord som anvendes i de ulike definisjonene.

Tabell 4. Analyse av hvilke karakteristikker definisjonene av innsidetrussel inneholder.

Threat	• Threats; danger; fraud; theft. • Dangerous. • Malicious or accidental threat.
Posed by	• Insider, individuals, internal actor; employee, contractors, business partners; current or former members, trusted individual. • Malicious insiders. • Insiderness.
Purpose/motivation	• An abuse or misuse of privilege; intentionally misuse. • Disgruntled employees, see an opportunity for financial benefit; personal advantage, revenge or financial gain. • Benign/accidental; a mistake; unintentionally. • Unauthorised purpose. • Spies who join an organisation.
Insider's knowledge/ skills/ characteristics	• Trusted and have or had access or knowledge of the organisation's information systems and objective. • Knows your networks and organisation. • Given the privileges to act within a specific environment. • Legitimately empowered with the right to access, represent, or decide about one or more assets of the organisation's structure.
Insider's behaviour/act	• Malicious or non-malicious. • Behave in ways, through a set of actions, destroy, exfiltrate, or leak, or expose. • Commit espionage or financial fraud. • Use of privileges; engages in; unauthorized system usage; misuses the privileges. • Have access to.
Object (values)	• Put our data, our systems, our organizations, and even our businesses' viability; intellectual property (IP); sabotage of infrastructure. • Sensitive information; expose their organisation. • Specific information. • The organisation's computer assets.
Consequences	• To the detriment of their enterprise. • Violation of confidentiality, integrity and/or availability. • Make different types of accidents more likely.
External actor's behaviour	• Outside attacks.

Tilsvarende, er definisjoner av *innsider* i utvalgets litteratur analysert[5]. Ingen av definisjonene fra utvalget inneholder alle elementene. Elementene som er identifisert vises i venstre kolonne i

Crawford and Peterson, 2013; Nurse m.fl., 2014a; Nostro m.fl., 2014; CERT, 2014 og Nurse m.fl., 2014b i Marbut & Harms, 2023; Greitzer, 2019; Eftimie m.fl., 2020 i Marbut & Harms, 2023; CERT, 2022; Zimmer m.fl., 2021; Marbut & Harms, 2023. I de tilfellene der eksempler er beskrevet i tilknytning til definisjon, er disse inkludert i analysen.

[5] Analysen er basert på femten ulike definisjoner funnet i forskningsartiklene vi tidligere har omtalt: Spitzner, 2003; Hu m.fl., 2006; 2008; Hunker & Probst, 2008 i Marbut & Harms, 2023; Pfleeger & Stolfo, 2009 i Maasberg & Beebe, 2014; Hunker & Probst, 2011; Crawford and Peterson, 2013; Nurse m.fl., 2014a; Nostro m.fl., 2014; CERT, 2014 og Nurse m.fl., 2014b i Marbut & Harms, 2023; Greitzer, 2019; Eftimie m.fl., 2020 i Marbut & Harms, 2023; CERT, 2022; Zimmer m.fl., 2021; Marbut & Harms, 2023. I de tilfellene der eksempler er beskrevet i tilknytning til definisjon, er disse inkludert i analysen.

tabellen nedenfor. Høyre kolonne sammenstiller typiske ord som anvendes i de ulike definisjonene.

Tabell 5. Analyse av hvilke elementer definisjonene av innsider inneholder

The actor	• A person; individuals; insider threat actor. • A trusted entity; any user. • Hacker; perpetrator. • A person or an organisation.
Behaviour/characteristics	• Intended insiders - Traitor or Masquerador; malicious insiders; malicious users; malicious behaviour. • insider victimization with malicious intent that may result in civil litigation or in criminal litigation. • Unintended insiders; unintentional users; non-malicious behaviour; insider victimization without malicious intent. • Insider victimization with altruistic intent. • The insiderness of an individual - a graduation between an insider and an outsider.
Relation to the organisation	• A current or former employee; current or previous member; current or former members of an organization, contractor or partner. • Authorised; legitimately empowered; given the privileges to act within a specific environment; can conduct; inside knowledge; who has or have been authorised. • Insider characteristics can only be provided, granted, or are controlled by a specific domain or by authorities of that domain, either deliberately or inadvertently.
Access to the value (object)	• Engages in unauthorised system usage. • Access to priviledge resources; with the right to access, represent or decide about one or more assets of the organisation's structure; the privileges to act within a specific environment. • Uses inherent trusts. • Are trusted and have or had access or knowledge of the organization’s information systems, and objectives; with confidential data or knowledge from his/her previous employer. • Access to an organisation's critical assets (people, information, technology, and facilities). • A set of insider characteristics, which are important in the context of the domain: Credentials, Knowledge, Privileges, Trust, Uncertainty (Structural Trust).

Tabell 5. forts. Analyse av hvilke elementer definisjonene av innsider inneholder

Intention/purpose	• For personal advantage or even revenge; malicious; dis-information of decision makers; intentionally misuse their trusted position; deliberately malicious; intentionally harm the institutions; intentionally harmful or for selfish gain. • Non-malicious; failing to follow best practices or by inadvertently engaging in an act; inadvertent actions; accidentally expose confidential data; damaging behaviour. • "Whistle-blowers" (e.g. Edward Snowden). • Pending on insider threat scenarios. • Not relevant for insiderness (but relevant for insider threat).
Motivation	• Disgruntled employees, employees who see an opportunity for financial benefit or spies; revenge, financial need, greed, dissatisfaction, health problems, proclaimed patriotism, notoriety, and political ideology; monetary gain, a disgruntled employee, entitlement, ideology, or outside influence. • Different motives or accidental in nature. • Individual factor or organisational factor. • Not relevant for insiderness (but relevant for insider threat). • Pending on insider threat scenarios.
Method	• Compromise; manipulation; spies who join an organization in order to commit espionage or financial fraud; breaking security policy. • Through a set of actions; activities. • Using unsecured systems, employing weak passwords, etc., disruption or destruction; embezzlement; industrial espionage; insider trading; secure data theft (including but not restricted to identity theft). • Actions performed by employees (as insiders) or actions performed by organisations (such as problematic responses to potential threats, poor institutional policies, or security practices). • Pending on the set of insider characteristics. • Pending on insider threat scenarios. • Require different skills to implement or the insider's cognitive processes and typical behavioural responses make different types of accidents more likely. • Succumbing to phishing attempts or interpersonal manipulation, surfing unsafe websites, failing to notice malicious hardware such as infected USBs. • Failure to report problems, unintentionally deleting data, and granting access to unauthorized parties.
Target	• Information within a system. • Decision-makers in the organisation. • At any organisation. • Endanger confidentiality, integrity, and availability of a business (of the organization). • Pending on insider threat scenarios. • An explisit denotation of the domain. An insider for one domain does not have to be the same insider for another domain. • Intellectual property (IP) theft, steganography, fraud, espionage, gatekeeping software, administrator lockout, salami attacks, kiting, and wire closet attacks. • Losing sensitive documents while taking them home, disclosure of sensitive information.
Consequences	• Violation of confidentiality, integrity and/or availability; detrimental to the economic interests of the company; fraud, sabotage, espionage, and theft or loss of confidential information; harm organisations or their members. • Potential to harm the organisation; Impact potential (direct and indirect loss, or as a product of consequence and probability of occurence). • Not relevant for insiderness (but relevant for insider threat).

Analysen over viser at innsideren får mye oppmerksomhet i definisjonene av innsidetrussel. Innsideren defineres som et enkeltindivid, men interaksjon mellom individ og gruppe eller individ og organisasjon er ofte neglisjert. I stor grad beskrives innsideren som en person som har eller har hatt tilgang til organisasjonen. Dette kan være ved at personen har vært ansatt, er/har vært leid inn eller er en forretningspartner. Noen av definisjoner skiller mellom en innsider som er tilkjent en form for tillit i organisasjonen, f.eks. “trusted innsider” og en som har onde hensikter, f.eks. "malicious insider". Definisjonene vier mye oppmerksomhet til innsiderens hensikt/motivasjon og individets kunnskap, ferdigheter, rettigheter og privileger.

Det er forståelig at definisjonene beskriver enkeltindividet, men ingen av definisjonene inkluderer gruppe av personer som innsidere. Unntaksvis finner vi litteratur som beskriver dynamikk mellom individ og gruppe og mellom individ og organisasjon (Greitzer m.fl., 2018).

Ved at definisjonene er begrenset til enkeltindividet er det fare for at forskningslitteraturen ikke i tilstrekkelig grad fanger opp situasjoner som involverer flere personer. Definisjonenes reduksjon til enkeltindividet begrenser også muligheten til innsikt i dynamikken mellom enkeltpersoner og andre i eller utenfor organisasjonen. Dette kan muligens være relevant i situasjoner der enkeltindivider går fra å være en ‘ufrivillig’ eller ‘ubevisst’ innsider til en innsider som med hensikt påfører skade.

Objektet/verdiene som trues dekkes godt gjennom eksempler. Noen av definisjonene inkluderer objektet, eller verdiene, som kan påføre organisasjonen skade. Ofte gis det eksempler på hva dette kan være, slik som data, systemer, informasjon om organisasjonen, forretningshemmeligheter, sensitiv informasjon, åndsverk (IP), sabotasje av infrastruktur, men eksemplene skiller ikke nødvendigvis mellom verdier som trues og hvordan de trues, se for eksempel (Hunker & Probst, 2008) og (Marbut & Harms, 2023, s2). Definisjonene og eksemplene virker å dekke dette elementet godt.

Konsekvensene som innsidetrusselen kan forårsake, er i liten grad inkludert i definisjonene, verken i form av alvorlighetsgrad, sannsynlighet eller klassifisering av ulike typer. Det kan hende at konsekvenser og alvorlighetsgrad bedre beskrives basert på domene og at det derfor vurderes som mindre hensiktsmessig å inkludere i en generisk definisjon.

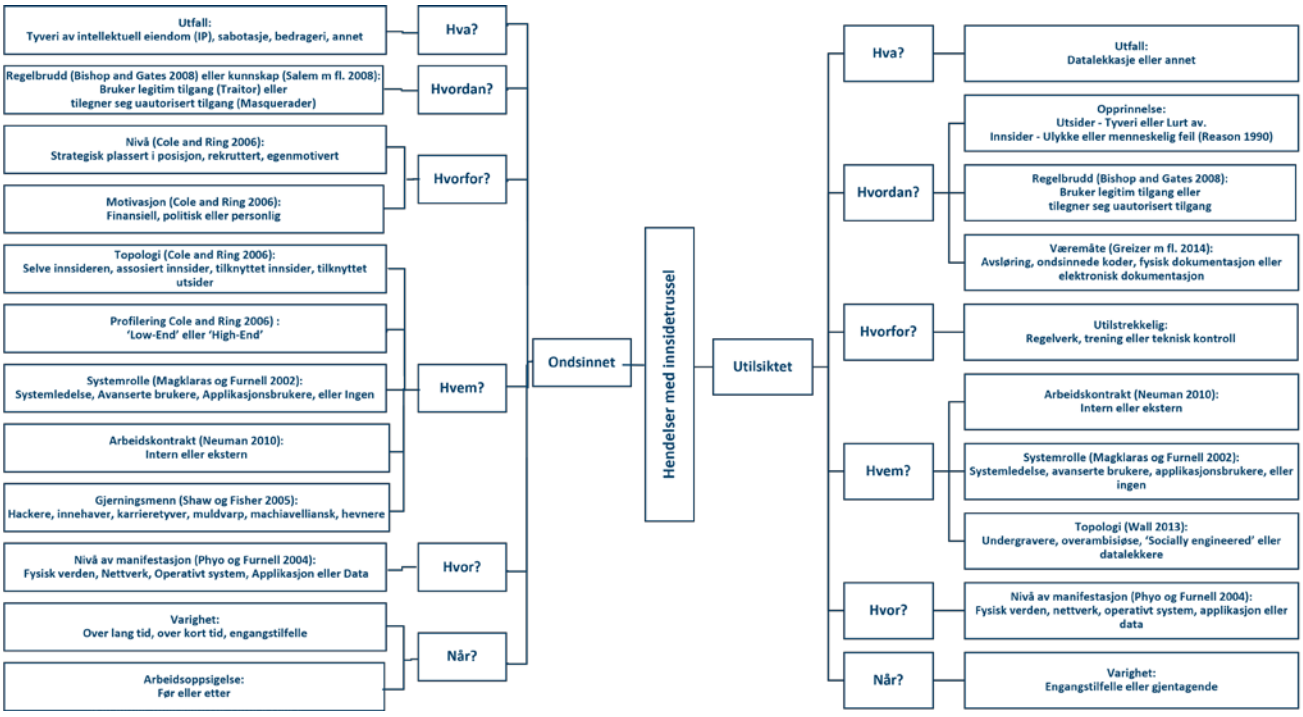
Definisjonene sier svært lite om interaksjonen mellom utsiden og innsiden, dvs. ‘insiderness’. Noen av definisjonene inkluderer ekstern aktør ("outside attack") (Greitzer m.fl., 2014; Maasberg m.fl., 2015; Cohen, 1997; Brackney & Anderson, 2004, sitert i Margot & Harms, 2023). Ekstern aktør er også inkludert i de tidligere nevnte eksemplene på objekt/verdiene. Ingen av definisjonene inkluderer beskrivelse av motivasjon eller hensikt til en ekstern aktør. Disse fraværene i definisjonene av innsidetrusselen resulterer i at det er svært lite oppmerksomhet rettet mot dynamikken i å være mellom utsiden og innsiden, dvs. innsidigheten.

4 Taksonomi

Taksonomi er grunnleggende for beregnende modeller og analyse der fenomener og konsepter kan systematiseres i kategorier og klasser. Følgende gjengir eksempler på taksonomi for innsidetrussel, vurdering og deteksjon av innsidevirksomhet og beskrivelser av prosesser for å detektere og reagere på innsidetrussel. Eksemplene er hentet fra utvalget beskrevet i første del av rapporten og hensikten er å vise bredden fra utvalget. Det er ikke foretatt vurderinger av hvilke erfaringer og effekt disse forslagene har til å håndtere innsidetrusler. Taksonomiens formål er gjerne å belyse deler av eller hele økosystemet for innsidetrusselen, og illustreres i stor grad i modeller i litteraturen.

4.1 Innsidetrusselen

Basert på gjennomgang av litteratur foreslår Homoliak m.fl. (2019) taksonomi for hendelser av innsidetrusselen som vist i figuren nedenfor. Som tidligere beskrevet skiller noe av forskningslitteraturen mellom tilsiktet og utilsiktet innsidetrussel (Homoliak m.fl., 2019). Derfor foreslår forfatterne inndeling mellom om hensikten er ondsinnet eller ikke. Grupperingen tar utgangspunkt i seks spørsmål (Figur 6); hva, hvordan, hvorfor, hvem, hvor og når? Taksonomien setter mange forhold i en sammenheng med tidligere forskningslitteratur. I Scopus har artikkelen 127 siteringer, noe som er mye i forhold til forskningslitteraturen på feltet.



Figur 6. Gjengivelse av taksonomi for innsidetrussel (Homoliak m.fl. 2019)

Et annet forslag til taksonomi er SOFIT Ontology Classes hvor hovedgruppene består av tre deler (Greitzer m.fl., 2018), se Figur 7. På samme måte som i Homoliak m.fl. (2019) inkluderer hovedgrupperingene om intensjonen er ondsinnede eller ikke. I tillegg tar hovedgrupperingene høyde for om handlingene er utført av en person eller om det er handlinger utført av en organisasjon (slik som problematisk håndtering av en innsidetrussel, svakheter i regelverket eller sikkerhetspraksis) (Greitzer m.fl., 2018). Denne artikkelen har betydelig færre siteringer (29) enn Homoliak et. al. (2019).

Figur 7. Gjengivelse av SOFIT ontologiklassifisering (Greitzer m.fl., 2018)

Tupakula & Varadharajan (2013) demonstrerer hvordan en insider kan utnytte svakheter i et datasystem til å utvikle angrep. De argumenterer med hvordan deres arkitektur kan bidra til å forhindre denne type angrep ved å overvåke brukeraktivitet og tilstanden til systemet.
Flere av forskningslitteraturen viser til CERT sin kategorisering av ondsinnede trusler. Et eksempel på dette er i Kim m.fl. (2019), som gjengir de fire klassifiseringene av ondsinnet innsideraktivitet; IT-sabotasje, bedrageri, tyveri av intellektuell eiendom og annet.

> Insider Activities: The report, published by the CERT Insider Threat Team, categorized four classes of malicious insider activity and analyzed 1,154 actual insider incidents in the United States [5]. Four classes of malicious insider activity are IT Sabotage (179 cases), Fraud (728 cases), Theft of Intellectual Property (268 cases), and Miscellaneous (65 cases). The numbers in parentheses indicate the number of events that occur in each class. (Kim m.fl., 2019, p50)

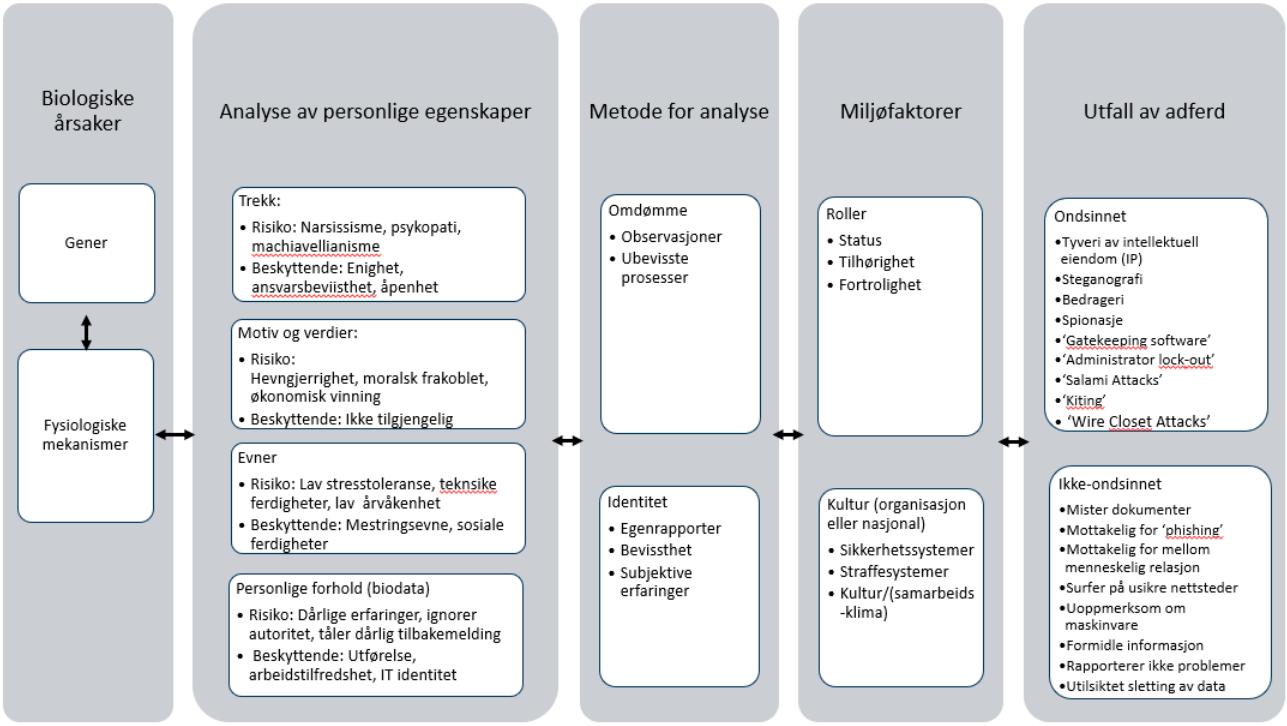
Kim m.fl. (2019) systematiserte deteksjonsmetode av innsideaktivitet ved å utvikle insiderkategorier og karakteristikker. Inndelingen er basert på om innsideren kan kategoriseres

som forræder (‘traitor’), maskerade (‘masquerader’) eller om trusselen var utilsiktet (‘unintended’), gjengitt i tabellen nedenfor. I den andre dimensjonen beskrives teknologinivå, i hvilken grad innsideren hadde tilgang til verdiene. Dette eksempelet får frem hvilken tid som er til rådighet i planleggings- og gjennomføringsfasen, som er en del av den andre dimensjonen. Den siste parameteren er hvordan innsidevirksomheten kan oppdages i planleggings- og gjennomføringsfasen.

Tabell 6. Gjengivelse av innsidekategorier og karakteristikker (Kim m.fl. 2019)

		Forræder (‘traitor’)	Maskerade (‘masquerader’)	Utilsiktet (‘unintended’)
Teknologinivå		Lav	Middels	Lav
Intensjon om å påføre skade		Ja	Ja	Nei
Legitim tilgang til verdiene		Egne privileger	Eskalering av privileger	Egne privileger
Frekvens		Sjeldent	Av og til (‘infrequent’)	Av og til (‘infrequent’)
Tidsbegrensing	**Forberedelse**	Ofte	Ofte	Ikke relevant
	Gjennomføring	Ofte	Begrenset	Ikke relevant
Deteksjons-faktor	**Forberedelse**	Adferd Psykologisk	Adferd Psykologisk	Regelbrudd
	Gjennomføring	Systembruk Netverksbruk	Systembruk Netverksbruk	Systembruk Netverksbruk

En modell for taksonomi er blant annet basert på eldre forskningslitteratur om innsideren (Roberts & Wood, 2006 og Roberts, 2006 i Marbut & Harms, 2023) og metode for å analysere atferd av komplekse systemer over tid (Hunker & Probst, 2011). Modellen knytter biologiske forklaringer til områder for analyse av personlige egenskaper, metode for analyse, kontekstuelle forhold og resultatene av handlingene fra innsidevirksomhet, se Figur 8. Begrunnelsen for denne tilnærmingen er at biologi og miljø interagerer med hverandre.



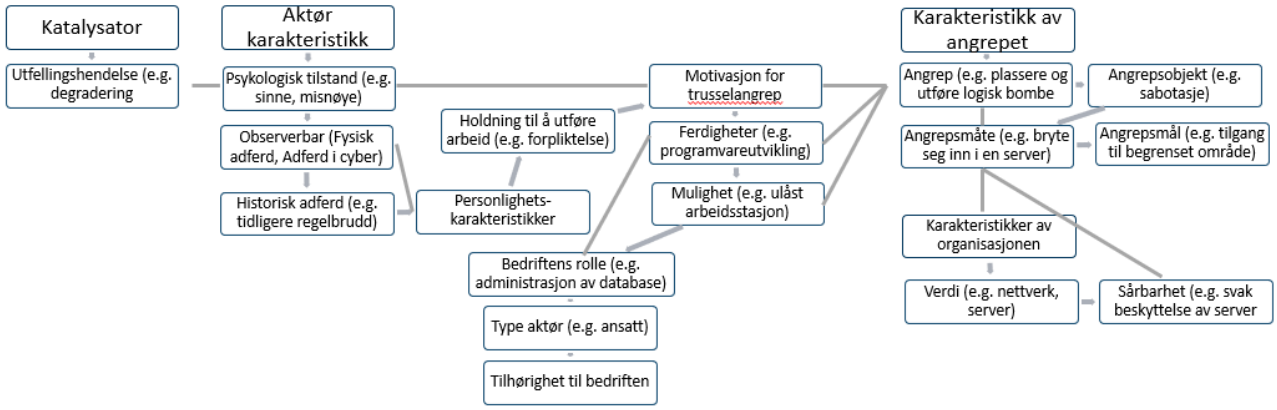
Figur 8. Gjengivelse av sosioanalytisk teorimodell av personlige og kontekstuelle forhistorier til innsidetrusler (Marbut & Harms, 2023). Forfatterne baserte denne fremstillingen på Roberts & Wood (2006) og Roberts (2006).

4.2 Innsideangrepet

Hunker og Probst (2011, s.8) mener fokuset på intensjon må nyanseres, da konsekvenser kan ha uventet innvirkning og ikke nødvendigvis stå i samsvar med alvorlighetsgraden i motivasjonen bak en innsiderhandling. Det de kaller bonus-runde innsidetrussel – altså handlinger utført i sinne og som hevn for manglende kompensasjon for arbeid – kan ha like alvorlige konsekvenser for organisasjonen som en uintendert forseelse, og målet må derfor være å begrense konsekvenser uavhengig av motivasjonen for innsidetrusselen. De klassifiserer utfall av innsidetrusselen i økonomisk tap, skade på organisasjon, skade på omdømme og langsiktige innvirkninger på organisasjonskultur. Forfatterne foreslår å kategorisere innsiderangrep i tre hovedtyper; misbruk av tilgang, omgåelse av forsvarsmekanismer og feil i adgangskontrollsystemer (2011, s. 9). De argumenterer med at effektiviteten av tekniske og ikke-tekniske tilnærminger for å imøtegå innsidetruslene varierer mellom disse tre hovedtypene.

CERT (2022) forslår å katalogisere og prioritere innsidetruslene basert på utarbeidelse av et register av innsidetrusler som kan være relevant for organisasjonen. Denne fremgangsmåten tar utgangspunkt i tradisjonell anvendelse av risikomodellering og utarbeidelse av trussel-scenarioer (se tidligere omtale CERT sine definisjoner i del 2).

Et eksempel på rammeverk for karakterisering av innsideangrepet, er her gjengitt fra Nurse m.fl. (2014b), se figur nedenfor. Her gis utløsende faktorer (katalysator) og karakteristikker av organisasjonen i denne situasjonen mindre oppmerksomhet, mens aktørens handling i gjerningsrommet og karakteristikker av selve hendelsesforløpet får størst oppmerksomhet.



Figur 9. Gjengivelse av rammeverk for å karakterisere innsiderangrep (Nurse m.fl., 2014b)

4.3 Innsideren og "the insiderness"

Utvalget av forskningslitteratur viser til en rekke forslag til metoder og tilnærminger for å kunne avdekke innsidevirksomhet, slik som uregelmessighetsdeteksjon eller å vurdere psykologiske faktorer og profilering (gjengitt i Nurse m.fl. 2014a), biometrisk og verdi-basert vurderinger (Alsowail & al-Sherari, 2022), profilering av mulige innsidere basert på hensikt, tilgang, utfall, begrensninger, ressurser, ferdighetsnivå, objekt og synlighet (Nostro m.fl., 2014), vurdere muligheter for å utføre og motiv for å indikere potensiale for ondsinnet innsidevirksomhet (Heuer 2001).

Inndelingen av forræder ('traitor'), maskerade ('masquerader') finner vi igjen i flere av forskningslitteraturen, blant annet gjengitt i Harilal m.fl. (2018). Forfatterne beskriver at en forræder er en ondsinnet innsider som misbruker ens privileger til å utføre ondsinnet aktiviteter. Maskerade er en annen type ondsinnet innsider som utfører ulovlige handlinger på vegne av en legitim bruker av systemet.

Men vi finner også andre tilnærminger og utdypinger av forhold som påvirker innsideren, slik som Nurse m.fl. (2014a). Forskere har hevdet at innsidere har spesifikke psykologiske egenskaper og karakteristikker. Kortsiktige psykologiske eller emosjonelle tilstander kan bidra til å identifisere et individ som er mer sannsynlig å utføre en innsidehandling enn andre. Slike psykologiske tilstander kan inkludere stress, depresjon eller angst, og en ekstern hendelse kan utløse eller forsterke en psykologisk tilstand som utløser et angrep. I tillegg til eksterne hendelser kan psykologiske lidelser

og personens holdning til arbeidsplassen være relevant å vurdere, hevder Nurse m.fl. (2014a, s. 273).

Lignende tilnærming ser vi der Intelligence and National Security Alliance (2017) har utviklet en modell som baserer seg på forskning om ondsinnede innsidere. Modellen antar at denne type innsidere ikke er individer som i utgangspunktet er lojale ansatte som brått får ondsinnede hensikter. De forklarer at noen personegenskaper kan gjøre en person disponibel for spionasje, tyveri, vold og ødeleggelse. Disse disposisjonene kan bli forsterket gjennom stress fra omgivelsene og i organisasjonen. Forfatterne foreslår en modell som kan anvendes som et tidlig varsling-system for innsidevirksomhet og øke forståelsen for hvordan faktorer knyttet til individ og miljø kan begrense eller forsterke uønsket atferd (Intelligence and National Security Alliance, 2017, s. 1).

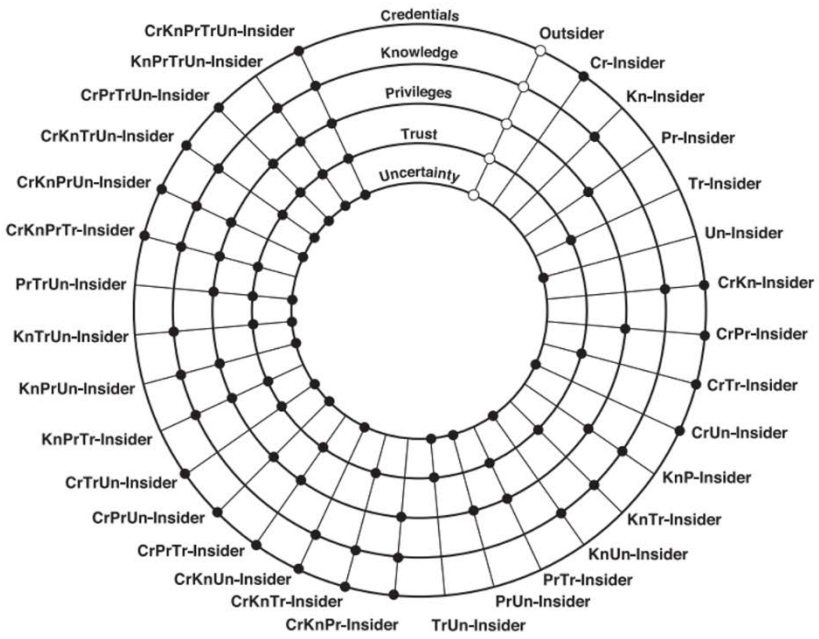
For klassifisering av innsideren tar Maasberg og Beebe (2014) utgangspunkt i Kramer, Heuer, and Crawford (2005), Chivers m.fl. (2013) i Willison & Warkentin (2013). De klassifiserer innsidere ut ifra fire dimensjoner, som er: rolle ('role'), avgrensing ('boundary'), tilgang ('access') og organisatorisk kunnskap ('organizational knowledge'). Rolle (fast eller midlertidig ansatt, selger, kontraktør, underleverandør eller tidligere ansatt) kan gi innsideren innflytelse til å utnytte organisasjonens verdier. Innsideren kan også karakteriserer opp mot i hvilken grad de har tillit og privileger innenfor den avgrensingen de opererer (avgrensing sett i sammenheng med tilgang). Den siste karakteristikken er i hvilken grad de har kunnskap om det indre liv i organisasjonen som de kan utnytte til sin fordel.

Marbut og Harms (2023) diskuterer egenskaper og forskjeller mellom innsidere som har ondsinnede hensikter og de som ikke har det. De argumenterer for at det er forhold som kan øke sannsynligheten for innsidevirksomhet. Disse forholdene er ulike om insideren har ondsinnede hensikter eller ikke. De med ondsinnede hensikter kjennetegnes blant annet ved at de er egoistiske, de begrunner hvorfor de kan være umoralske og de har en trøblete fortid. Innsidere som ikke har en ondsinnet hensikt kjennetegnes mer sannsynlig som å være sensitive, godtroende og nysgjerrige. For disse kan stress bidra til uønsket innsidetrussel.

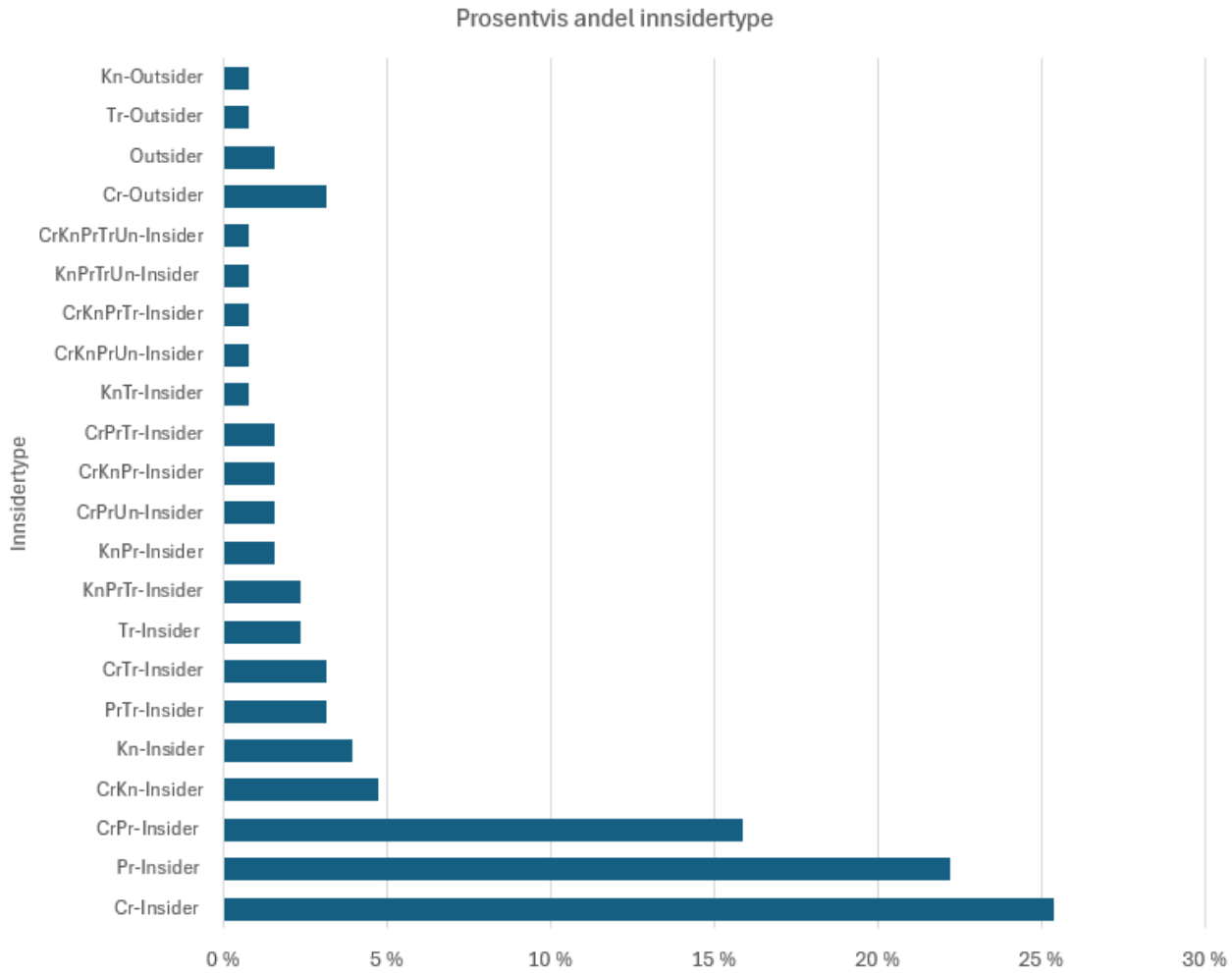
Nostro m.fl. (2014) mener at for å kunne beskytte seg mot innsidetrussel er det nødvendig med tilpasset sosioøkonomisk profilering av brukerne, hvilke verdier de bruker (verdier som trues), deres handlinger og hvilke konsekvenser det får for verdiene, systemene og organisasjonen. For å vurdere potensielle innsidere foreslår de å bruke åtte attributter; hensikt, tilgang, utfall, begrensniger, ressurser, ferdighetsnivå, objektiv og synlighet.

Zimmer og kolleger (2021) foreslår en annen tilnærming. De vil heller enn å beskrive innsideren som person, holde seg til hva som er aktuelt for problemstillingen, noe de kaller *innsidigheten*. Det er altså graderingen mellom å være på utsiden og innsiden sett i forhold til et domene. Deres forslag tar også utgangspunkt i individet, men argumenterer for at blant annet individets hensikt ikke er relevant for å beskrive innsidigheten (men hensikt er relevant for å vurdere

innside*trusselen*). Forfatterne forslår å bruke fem typer av innsidekarakteristikker som til sammen utgjør en innsidetype. Disse er Legitimasjon (eller godkjenning, 'Cr - Credentials'), Kunnskap ('Kn – Knowledge'), Privileger ('Pr – Privileges'), Tillit ('Tr – Trust') og Usikkerhet (kalles også Systemisk tillit, 'Un – Uncertainity'). Ved å bruke disse karakteristikkene til å vurdere kategoriene og gradere personens forhold til et domene uttrykkes innsidetypen i forhold til et domene. Kombinasjonen av alle de ulike innsidetypene utgjør til sammen forfatternes forslag til innsidertaksonomi, som vist i figuren nedenfor.



Figur 10. Gjengivelse av innsidertaksonomi av alle kombinasjoner av innsidertype (Zimmer m.fl., 2021)



Figur 11. Gjengivelse av prosentvis andel innsidertype (Zimmer m.fl., 2021). Analysen var av 85 definisjoner fra 49 ulike forskningslitteratur.

Zimmer m.fl. (2021) analyserte 85 definisjoner av innsider fra 49 ulike forskningslitteratur og gruppert disse i deres foreslåtte taksonomi, se figur gjengitt overfor. Resultatene av denne analysen viser at et klart flertall av definisjonene vektlegger innsiderens Legitimasjon (Cr) og Privileger (Pr) i en organisasjon, eller en kombinasjon av disse to. Forfatterne forklarer resultatet med at denne type innsiderkarakteristikker, altså innsidere som har en legitim tilgang til et domene i kombinasjon med privileger, er den mest åpenbare type innsider. Det er også disse innsidertypene som er lettest å rette tiltak mot og utføre analyse av. Videre viser deres analyse at noen få av definisjonene vektlegger kombinasjonene Legitimitet, Kunnskap, Privileger og Tillit. Andre kombinasjoner av innsidertyper er svært lite beskrevet i den litteraturen de gjennomgikk. De uttrykker usikkerhet til om utvalget de har sett på kan ha skjevheter. Forfatterne beskriver at de vil arbeide videre med hvordan deres forslag til taksonomien kan anvendes i arbeidet med innsidetrussel.

5 Innsidetrusselen i praksis

Grålitteraturen viser at mange foretak har essensiell informasjon om egen virksomhet som det er svært viktig for dem at ikke faller i andres hender. Slike fortrolige eller hemmelige opplysninger må vernes. Å vurdere mulig lekkasje av informasjon via innsidere bør være et fast punkt i foretakets risikoanalyse. Hvorvidt dette gjøres, sier litteraturen lite om, og det er også lite empirisk evidens knyttet til hvorvidt innsidetrussel er diskusjonstema i bedrifter og foretaks sikkerhetsstyring.

Et tiltak for å redusere sannsynligheten for at personer som har tilgang på hemmelig informasjon skal bli utnyttet på noe vis av en trusselaktør, er å sikkerhetsklarere personene. En sikkerhetsklarering er "en avgjørelse foretatt av en klareringsmyndighet om en persons antatte sikkerhetsmessige sikkerhet" (www.nsm.no). Klareringen gir derimot ingen garanti for at personen ikke kan være, eller bli, en innsider. Videre er det er bare personer som har et dokumentert behov for å ha tilgang til gradert informasjon som blir vurdert for sikkerhetsklarering.

I mars 2023 la Etterretningstjenesten, Politiets sikkerhetstjeneste (PST) og Nasjonal sikkerhetsmyndighet frem sine åpne trussel- og risikovurderinger (se hhv. Fokus 2023, NTV 2023, og Risiko 2023). Fremmede stater vil også dette året bruke mye ressurser på etterretnings-operasjoner for å stjele informasjon blant forskjellige mål i Norge og Russland blir nevnt som den største etterretningstrusselen. Dette bør tolkes som en klar beskjed til bedrifter eller foretak i Norge om at det vil være en relativt stor risiko for at nettopp din organisasjon, kan bli utsatt for nettopp dette.

NSM har gitt ut en veileder *Grunnprinsipper for personellsikkerhet* (NSM, 2020) hvor de presenterer et sett med tiltak som virksomheter kan bruke i sitt arbeid med å ivareta en god personellsikkerhet. Grunnprinsippene beskriver hva som bør gjøres og hvorfor de bør gjennomføres, men det er opp til virksomhetene selv å lage et design for gjennomføring av disse. Ett tiltakene som NSM anbefaler er å ha sårbarhetssamtaler med ansatte fra høyrisikoland (Russland, Iran, Kina og Pakistan). Det er flere grunner til å ha slike sårbarhetssamtaler, først og fremst for å forklare den enkelte medarbeider at hen kan bli satt i en presset situasjon, og at arbeidsgiver har plikt å ivareta alle enkeltpersoners sikkerhet. Det kan videre bli utøvd press mot familie til vedkommende. Disse personene kan også være attraktive ubevisste innsidere av statlige aktører. Ved å ha en sårbarhetssamtale kan enkeltpersoner bli klar over hvordan en selv bidrar til trusselbildet, og ved økt egen bevissthet dermed redusere trusselen.

Sårbarhetssamtalene kan bygge tillitt mellom potensielt utsatte enkeltindivider og ledelsen, noe som vil redusere innsidetrusselen. Det er derfor viktig at slike samtaler blir godt forankret i organisasjonen og at ledelsen, både nærmeste og overordnet leder, har kompetanse på utførelse av samtaler. Videre anbefaler Direktoratet for høyere utdanning og kompetanse institusjonene

om at det bør vurderes å innføre sårbarhetssamtaler med ansatte der det er aktuelt[1]. Noen forskningsmiljø har etablerte rutiner for dette, mens andre velger å følge eventuelle etiske retningslinjer for ansatte for egen institusjon.

6 Diskusjon og konklusjoner

Innsidetrusselen fremstår fra litteraturen som særskilt vanskelig å oppdage til tross for at praksis innen sikkerhetsfaget mener dette er den alvorligste trusselen mot organisasjoner, både hva gjelder tap av økonomiske verdier og statshemmeligheter (Butts, Mills og Peterson, 2006).

6.1 Lite empiri, stort cyberfokus og manglende sosiotekninsk integrering

Det er svært lite empiri i forskningen, som i stedet er preget av metastudier og litteraturstudier som tilbyr rammeverk og taksonomi. I tilfeller der det er benyttet case-studie som metode, er også forskningen basert på litteratur om hendelser snarere enn eksempelvis intervjuer med personer som kan ha førstehånds kunnskap om hendelsene. En årsak, kan naturligvis være at slik kunnskap av mange er regnet for sårbart å utgi, og kan være hemmeligstemplet. Til gjengjeld, er det i forskningen mange forsøk på å tyde og forstå problemstillinger knyttet til innsidetrusselen fra et teoretisk ståsted. Utfordringen med dette, er at det forblir en videre teoretisering av mulig utdatert kunnskap og resirkulering av antagelser som ikke tar høyde for at problemstillingen kan ha endret seg betydelig i praksis. En vurdering av rapporter og veiledere sett opp mot forskningslitteraturen indikerer et gap mellom teori og praksis, som kanskje også kan forklares med det manglende empiriske grunnlaget i forskningen på feltet.

Det finnes relativt mye litteratur som ser på den uintenderte innsideren i et cyberteknisk perspektiv (unintended insider, ofte forkortet UIT) med argumentasjon i dennes utbredte omfang (f.eks. Liu Xiangyu m.fl., 2017; Mazzarolo & Jurcut 2020; Maasberg & Beebe, 2014). Men søkelyset er i stor grad rettet mot cyberdimensjonen av disses aktivitet fremfor det som foregår i det fysiske rom og mellom mennesker der. Uintenderte innsidetrusler utenfor cyberrommet, eller trusler som altså ikke er cyberavhengig eller cybertilrettelagt, men som skjer på fysiske møteplasser og i livet utenfor arbeidet, får lite oppmerksomhet. Noe forskning peker på at den største utfordringen er å identifisere og innlemme adferdsindikatorer for risiko i de cybertekniske indikatorene for å oppnå en godt integrert sosiotekninsk tilnærming – og at programmer som skal motvirke innsidetrussel for ofte neglisjerer den menneskelige delen av problemet (Greitzer, 2019).

Rapporter og veiledere indikerer et fokus på å "holde innsideren ute" med grep som grundige rekrutteringsprosesser og testing. Ser vi likevel på aktørbildet som tredelt, der den egentlige trusselaktøren befinner seg på utsiden av organisasjonen og innsideren kun er en benyttet vektor i en prosess, er det kanskje ikke bærende over tid å fokusere så mye på personen på innsiden – men heller hvordan den kan bli brukt i en prosess av en utsider.

[1] https://hkdir.no/retningslinjer-og-verktoy-for-ansvarlig-internasjonalt-kunnskapssamarbeid/risiko-og-sikkerhetsstyring-ved-kunnskapsinstitusjonen/ansatte-ved-norske-institusjoner

6.2 Dynamikk og gradering mellom innside og utside

Denne studiens analyser av definisjoner av innsidetrussel og innsider illustrerer hvordan disse vektlegger enkeltindividenes tilhørighet til den organisasjonen som er utsatt for trusselen. I svært liten grad inneholder definisjonene noe om dynamikk mellom individ og gruppe, mellom individ og organisasjon og mellom de som er på innsiden og utsiden. Sistnevnte kan være relevant i situasjoner der enkeltindivider går fra å være en ubevisst eller ufrivillig innsider til en innsider med hensikt om å påføre skade. Definisjonene som forskningslitteraturen i stor grad bruker, kan dermed bidra til å begrense forståelse av overganger der innsidetrusselen kan oppstå og foregå.

Hvordan innsidetrussel defineres påvirker også hvilken ny innsikt forskningen kan opparbeide. Uforholdsmessig stor oppmerksomhet rettet mot enkeltindividet i definisjoner og taksonomi kan medføre mindre fokus på andre tiltak som virksomheten kan gjøre for å forhindre og begrense farene for innsideaktivitet. Som individ, men også gruppe og virksomhet står en jevnlig overfor målkonflikter og problemstillinger i komplekse systemer der det er krevende å forutse alle konsekvensene. Vurderinger, motiver, handlinger og hensikt kan være basert på dynamikk som oppstår mellom personer og teknologier innenfor en virksomhet, men også med andre som står på utsiden av virksomheten, slik som tjenester og produkter fra underleverandører og samarbeidspartnere, kunder, konkurrenter og myndighetsutøvere – og aktører som har som motiv å utgjøre en trussel. Det kan også være krevende å forutsi hvordan trusler i en sektor kan få konsekvenser i en annen sektor, noe som blant annet problematiseres av NSM (2023). Målkonflikter og dynamikk mellom aktører i komplekse systemer er tematikk som i svært liten grad behandles i definisjoner og taksonomier funnet i utvalget for denne rapportens undersøkelser. Manglende innsikt om dette er begrensende for forståelsen av hvilke tiltak som kan forebygge og motvirke innsideaktivitet.

Begrepet innsidetrussel kan virke misvisende fordi det antyder an trussel på innsiden, altså individet som har infiltrert eller kan bli rekruttert. Det er viktig å huske på at selve trusselen ikke befinner seg på innsiden, men på utsiden. For å kunne forstå og begrense innsideaktivitet er det behov for bedre og mer konsistent begrepsbruk. En mulighet kan være å inkludere i definisjon og taksonomi dynamikk og gradering mellom utside og innside. Det vil kunne gi et bedre utgangspunkt for å forstå hvem som er de utenforstående, hvilke verdier de truer og hva som er interaksjonene og ellers samspillet mellom de som står på utsiden og den eller de som utgjør innsidigheten. Dette vil kunne gi et bedre utgangspunkt for andre tiltak som kan forebygge og begrense innsidetrusselen enn de som er direkte rettet mot enkeltindivid og verdiene som trues.

6.3 Organisatorisk læring for å øke robusthet mot innsidetrussel

Det er på mange måter forståelig at innsidetrusselen retter sterk oppmerksomhet mot enkeltindividet. I arbeidet med å forhindre og forfølge innsideaktivitet har det vært viktig at enkeltindivider ansvarliggjøres. Den store oppmerksomheten mot enkeltindividet i definisjonene for innsidetrusselen antas å være basert på juridiske og økonomiske føringer og interesser. Dette

reflekteres muligens også i prosessene for klarering av personell, der individet og omstendigheter tilknyttet individet tillegges betydelig vekt.

Det kan være en motsetning mellom streng ansvarliggjøring av enkeltindivider og muligheten for organisasjonen til å lære og utvikle robusthet mot innsidetrusselen. En rapport utarbeidet av Sikkerhetsforum for Petroleumstilsynet beskriver blant annet om fremmere og hemmere for organisatorisk læring (Sikkerhetsforum, 2019). Åpenhet og høyde under taket i en organisasjon er eksempler på fremmere. Lukkethet, sanksjoner og straff er eksempler på hemmere for organisatorisk læring. Sagt på en annen måte; hvis oppmerksomheten er begrenset til handlingene og egenskapene til individet som har utført innsideaktivitet, kan dette redusere læringen som er nødvendig for å skape en robust organisasjon.

6.4 Er påvirkning og åpen informasjon en innsidetrussel?

Utover de ubevisste innsiderne som beskrives over, er innsidetrusselen som ligger utenfor individer og grupper som er tilkjent tillit og tilgang til informasjon og systemer på innsiden, viet lite oppmerksomhet i innsidelitteraturen. Demokratiske verdier og prinsipper om åpenhet kan utgjøre en større trussel i tider da sikkerhetspolitisk press øker, enn hva land som for eksempel Norge har vært vant med i fredstid. Dette er i omstilling i mange vestlige demokratier. Et sammensatt trusselbilde der stadig nye teknologier er drivende faktor, kan skape større opplevelse av usikkerhet og i en slik situasjon også bidra til overdreven 'sikkerhetisering' i samfunnet. Antagelsen om trusselen som frihet og åpenhet kan representere, kan paradoksalt bli en trussel mot demokratiet den søker å beskytte. Informasjon er i dag en flytende og lett tilgjengelig aggregerbar verdi som ligger tett opp mot kunnskap og forståelse om ulike samfunns kultur og levesett. Hvordan dette kan benyttes strategisk for innhenting av informasjon om andre stater, vil være et sammensatt tema for forskning og et tilsynelatende nytt tilskudd til samtidens forståelse av innsidetrusselen.

Påvirkning gjennom informasjonskampanjer og desinformasjonsoperasjoner, er trolig noe som kan forekomme oftere med økende fremvekst og utbredelse av sosiale medier. Caramancion m.fl. (2022) demonstrerer hvordan definisjonene av cybertrusler i stor grad mangler beskrivelse av desinformasjon. Påvirkningsoperasjoner mot samfunn og stater har fått mye oppmerksomhet i det siste tiåret, men hvordan mindre operasjoner kan ramme grupper av sikkerhetsklarert personell eller andre som utgjør kritiske samfunnsfunksjoner er ikke like mye diskutert. Videre, kan aggregert informasjon tilgjengelig i store datasett som samles opp av internasjonale medieplattformer avsløre mye både om statlig og kommersiell virksomhet – på helt lovlig vis. Etterretning i den digitale tid byr derfor på nye muligheter for innsamling og analyse av data enn tidligere ifølge Steenslie, Haugom og Vaage (2019) og dagens sammensatte trusselbilde utnytter nettopp disse mulighetene til å orientere seg i gråsonen. Innsamling av informasjon som hver for seg ikke krever gradering, kan til sammen fortelle mye og det kan derfor ikke forventes at fremtidens spionasjesaker nødvendigvis fordrer innsidetilgang til gradert informasjon eller sikkerhetsklarert personell.

6.5 Anbefaling for videre forskning

Empiriske studier: Det er forholdsmessig lite empiri i litteraturen, og dette kan gjøre det vanskeligere å forstå problemstillingen i praksis. Andelen metaforskning er betydelig og mange søker å forstå innsidetrusselen, samtidig som få ser til praksisfeltet for å undersøke hva som foregår på arbeidsplasser og blant kolleger. Å kartlegge innsideaktivitet som har funnet sted og er avslørt kan utgjøre et verdifullt bidrag til litteraturen og gi kunnskapsbasert innsikt som kan være nyttig både for statlig og kommersiell virksomhet.

Norske forhold: Denne rapporten viser at det er svært lite dokumentasjon på hva norske bedrifter og foretak gjør for å adressere innsidetrussel. Det er heller ikke utført norske empiriske forskningsstudier av innsideaktivitet, ut ifra hva denne studien kunne finne. Som følge av at sikkerhetsloven gjøres gjeldende for flere virksomheter må disse øke andel sikkerhetsklarert personell, og det kan være aktuelt å undersøke hvordan dette påvirker dem – kanskje særskilt forholdet mellom de som klareres og de som ikke klareres. Klarering av personell i virksomheter eller deler av virksomheter kan skape ulike rom for meningsdannelse og forsterke skiller mellom virksomheter og personell som skal samarbeide, og resultere i mer fraksjonert forståelse av risiko og sikkerhet. Vilje og evne til å utføre arbeid i kritiske situasjoner avhenger av at kunnskap om trusler og risiko når bredt ut, og det er derfor viktig å opprettholde åpenhet der det er mulig.

Utover virksomhet underlagt sikkerhetsloven foreslås forskning som undersøker hva andre bedrifter og foretak gjør for å adressere innsidetrusselen, herunder i hvilken grad og hvordan de eventuelt er bevisste trusselen, hvordan den adresseres i sikkerhetsstyring, hvilke opplevelser de har og har hatt inkludert en utvikling over de seneste år og hvor mange som har inkludert innsideaktivitet i ROS-analyser og sikkerhetsstyring.

'Innsidepåvirkning': Ny teknologi medfører nye metoder og muligheter for informasjonsinnhenting. I dag har mange stater et godt cyberforsvar, men slik har det ikke alltid vært og sårbarhetene i teknologiens frammarsj har kostet både stater og kommersielle virksomheter store hemmeligheter og mye penger. I dag er etterretning i åpne kilder og sosiale medier i utstrakt bruk, og dette ser ikke ut til å ta særskilt plass i innsidelitteraturen – antageligvis fordi begrepet 'innside' fordrer en (falsk) barriere som åpen informasjon befinner seg på utsiden av. I dagens åpne demokratier kan en sette spørsmålstegn ved hvor flytende denne barrieren er, og undersøke i hvilken grad det kognitive domenet benyttes for innsidevirksomhet. Det kan være verdifullt å undersøke hvordan og i hvilken grad påvirkningsoperasjoner rettes mot mindre grupper (f.eks. sikkerhetsklarerte) og hvilken trussel dette kan representere. Hvorvidt påvirkning og åpen informasjon er en innsidetrussel, og forholdet i gråsonen imellom, er ikke undersøkt i særlig grad i denne rapportens litteratur om innsidetrusselen og foreslås derfor for videre forskning.

Kontraetterretningsstudier: Etterretningsstudier og spesielt kontraetterretningsstudier, er nært beslektet med innsideproblematikken sett fra et personellsikkerhetsperspektiv. Dette

forskningsfeltet er spesielt opptatt av behandling av hemmeligstemplet informasjon og gangen i større avsløringer av spionasje. Selv om det kan være vanskelig å få tilgang til empirisk kunnskap om saker som angår nasjonal sikkerhet aner vi en økende åpenhet knyttet til etterretningsarbeid og utviklingen i faget, som bruk av analyse av data fra åpne kilder. Aggregert informasjon kan uansett avhjelpe utfordringer knyttet til forskning på sensitiv informasjon. For å utvikle denne delen av litteraturen teoretisk, kan det i tillegg være verdifullt å overføre metode for strukturert analyse fra innsidelitteraturen til kontraetterretningsstudier. Gioe & Hatfield (2023) kritiserer eksisterende forskningslitteratur innen etterretning- og kontraetterretningsstudier for å være underteoretisert og ikke å benytte strukturert analyse og rammeverk i særlig grad. Her kan tilnærminger fra innsidestudier ha overføringsverdi i ny forskning.

Forskning på sikkerhetsklarering og klareringsprosesser er et annet lite dekket felt. Det kan være aktuelt å undersøke i hvilken grad sikkerhetsklarering fanger opp sentrale forhold forbundet med innsidetrusselen; hvordan klareringsprosesser eventuelt kan styrkes, eller effektiviseres der det ikke er behov for grundigere vurderinger; hvor stor utbredelsen av klarering er eller bør være for ulike ansvarsroller og om det finnes alternativer til sikkerhetsklarering som kan gi effekt. Det bør forskes på omfang og effekt av sårbarhetssamtaler i bedrifter eller foretak som utfører slike, hva disse inneholder og eventuelle innvirkninger knyttet til kultur, trivsel og miljø på arbeidsplassen.

Organisatorisk læring med aksjonsforskning og følgeforskning: Empiriske studier om hvordan organisasjoner kan fremme læring for å bli mer robust mot innsidetrussel vil kunne være verdifullt for norske og nordiske virksomheter i framtiden. Geopolitisk endring og sikkerhetspolitisk uro gjør innsidetrusselen mer aktuell og i et sammensatt trusselbilde er informasjon essensielt. Fra blant annet petroleumssektoren er det godt kjent hva som fremmer og hemmer organisatorisk læring (f.eks. robuste løsninger vs. kapasitetspress og målkonflikter). Denne kunnskapen kan være relevant for arbeidet med å møte innsidetrusselen. Aksjonsforskning er en forskningsform der forskerne er tett på dem som det forskes på. Forskningen kan for eksempel starte med at det innføres tiltak, og hvor forskerne og personer fra virksomhetene jobber sammen i fellesskap og diskuterer utfordringer, deler kunnskap og erfaringer. Siden forskerne er tett på i gjennomføring av tiltak, kan de studere virking av tiltakene og gjøre eventuelle endringer underveis. Denne form for forskning er motsetningen til observasjoner, der forskerne kun skal studere for eksempel en organisasjon uten å ha noen interaksjon med dem som er forskingsobjektet. Følgeforskning er en annen mulighet der en kan følge forskjellige bedrifter eller foretak over tid for å se forskjellige utviklinger eller trender. I motsetning til aksjonsforskning, der forskerne er involvert i gjennomføring av tiltak, er man i følgeforskning en mer passiv aktør, men ikke nødvendigvis bare en observatør. Mål med følgeforsking er å kunne lære viktige momenter fra prosesser som går over tid. Dette er metoder som kan være godt egnet for en tilnærming til å forstå og forebygge innsidetrusselen i norske virksomheter.

7 Referanser

Alsowail RA, Al-Shehari T. A (2021) Multi-Tiered Framework for Insider Threat Prevention. *Electronics*. 2021; 10(9):1005.

Alsowail RA, Al-Shehari T. (2022). Techniques and countermeasures for preventing insider threats. *PeerJ Computer Science* 8:938.

Beebe, N., Liu, L., Ye, Z. (2017). Insider Threat Detection Using Time-Series-Based Raw Disk Forensic Analysis. In: Peterson, G., Shenoi, S. (eds) *Advances in Digital Forensics XIII. DigitalForensics 2017*. IFIP Advances in Information and Communication Technology, vol 511. Springer, Cham.

Bishop M., Engle S., Frincke D.A., Gates C., Greitzer F.L., Peisert S., & Whalen S. (2010). A RiskManagement Approach to the "Insider Threat." In: Probst, C., Hunker, J., Gollmann, D., Bishop, M. (eds) *Insider Threats in Cyber Security. Advances in Information Security*, vol 49.

Brown C.R., Watkinson A. & Greitzer F.L. (2013). Toward the development of a psycholinguistic-based measure of insider threat risk focusing on core word categories used in social media. *The Nineteenth Americas Conference on Information Systems.*

Brown C.R., Watkinson A. & Greitzer F.L. (2013). Predicting insider threat risks through linguistic analysis of electronic communication. *46th Hawaii International Conference on System Sciences* (HICSS-46), 2013, pp.1849-1858.

Brancik K. & Ghinita G. (2011). The optimization of situational awareness for insider threat detection. First ACM Conference on Data and Application Security and Privacy.

Butts, J., Mills, R. F., & Peterson, G. L. (2006). A multidiscipline approach to mitigating the insider threat. *International Conference on I-Warfare and Security, ICIW* 2006, 29–36.

Caramancion, K.M., Li, Y., Dubois, E., & Jung, E.S. (2022). The Missing Case of Disinformation from the Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats. *Data;* 7, 49.

Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes. Carnegie Mellon University, Software Engineering Institute's Digital Library.

CERT Insider Threat Team. (2013). Unintentional Insider Threats: A Foundational Study. Technical note CMU/SEI-2013-TN-022 Carnegie Mellon University.

CERT Insider Threat Team (2016). Common Sense Guide to Mitigating Insider Threats, 5th ed. Carnegie Mellon University.

CERT National Insider Threat Center. (2022). Common Sense Guide to Mitigating Insider Threats, 7th ed. Carnegie Mellon University.

CISA, The Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/

Ponemon Institute Research Report (2018). Cost of Insider Threats: Global. https://www.insiderthreatdefense.us/pdf/Ponemon%20Institute%202018%20Report%20-%20The%20True%20Cost%20Of%20Insider%20Threats%20Revealed.pdf

Crawford M. & Peterson G. (2013) Insider threat detection using virtual machine introspection. *46th Hawaii International Conference on System Sciences* pp. 1821-1830

Dulipovici A. (2017). Organizational values fostering secure knowledge sharing. *European Conference on Knowledge Management,* ECKM

Federal Bureau of Investigation. (2011). Higher education and national security: The targeting of sensitive, proprietary and classified information on campuses of higher education. https://www.fbi.gov/file-repository/higher-education-national-security.pdf/view

Fokus (2023). Etteretningstjenestens åpne trusselvurdering.

Gioe D.V. & Hatfield J.M. (2021). A damage assessment framework for insider threats to national security information: Edward Snowden and the Cambridge Five in comparative historical perspective, *Cambridge Review of International Affairs*, 34:5, 704-738

Golden, D. (2017). Spy schools: How the CIA, FBI, and foreign intelligence secretly exploit America's universities. [Synopsis]. https://www.coleurope.eu/fr/spy-schools

Greitzer, F.L. (2019). Insider Threats: It's the HUMAN, Stupid! *Proceedings of the Northwest Cybersecurity Symposium.*

Greitzer F., Purl J., Leong Y.M., & Becker D.E.S. (2018) "SOFIT: Sociotechnical and Organizational Factors for Insider Threat," *2018 IEEE Security and Privacy Workshops (SPW)*, pp. 197-206

Harber J.R. (2009) Unconventional Spies: The Counterintelligence Threat from Non-State Actors. *International Journal of Intelligence and CounterIntelligence*, 22:2, 221-236

Harilal A., Toffalini F., Homoliak I. (2018). The Wolf of SUTD (TWOS): A dataset of malicious insider threat behavior based on a gamified competition. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications;* 9:1:1-32.

Harms P.D., Marbut A., Johnston A.C., Lester P., & Fezzey T. (2022). Exposing the darkness within: A review of dark personality traits, models, and measures and their relationship to insider threats. *Journal of Information Security and Applications,* Volume 71.

Heuer, R. (2001). The Insider Espionage Threat. Defense Personnel Security Research Center. Online: http://www.dss.mil/search-dir/training/csg/security/Treason/Insider.htm

Homoliak I., Toffalini F., Guarnizo J., Elovici Y., Ochoa M. (2019). Insight Into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures. *ACM Computing Surveys*; 52, 2.

Hu N., Bradford P.G., Liu J. (2006). Applying role based access control and genetic algorithms to insider threat detection. *In Proceedings of the 44th annual Southeast regional conference* (ACM-SE 44). Association for Computing Machinery, New York, NY, USA, 790–791.

Hunker J. & Probst C.W. (2011). Insiders and Insider Threats: An Overview of Definitions and Mitigation Techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*;2:1:1-27.

Høiby M., Vatn D.M.K., Fiskvik J.T., & Thaulow K. (2022). Kunnskapsgrunnlag om bevisstgjøringsstrategier som skal motvirke rekruttering av ubevisste innsidere i norske virksomheter. *SINTEF Rapport* 2022:01518.

INSA, Intelligence and National Security Alliance. (2017). Assessing the Mind of the Malicious Insider: Using a Behavioral Model and Data Analytics to Improve Continuous Evaluation. Security Policy Reform Counsil. Insider Threat Subcommittee.

Jaros S.L., Rhyner K.J., McGrath S.M., Gregory E.R. (2019). The resource exfiltration project: Findings from DoD Cases, 1985-2017, *Office of People Analytics (OPA) og Defence Personnel and Security Research Center (PERSEREC).*

Jacobsen J.D. (2021) Hvordan holde innsidere på utsiden? *Masteroppgave* Universitetet i Stavanger (UiS).

Jerre J., Funnemark E., & Angelsen S. (2019). Håndtering av innsiderisiko, *Det Norske Veritas (DNV-GL)* for Petroleumstilsynet. Rapportnr:2019-0280.

Kim, A., Oh, J., Ryu, J., Lee, J.J., Kwon, K., & Lee, K.H. (2019). SoK: A Systematic Review of Insider Threat Detection. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, 10, 46-67.

Kont M., Pihelgas M., Wojtkowiak J., Trinberg L., & Osula A-M. (2015). CCDCOE. *NATO Cooperative Cyber Defence Centre of Excellence*.

Kramer, L. A., Crawford, K. S., & Heuer, R. J. (2005). Technological, social and economic trends that are increasing us vulnerability to insider espionage. Monterey, CA: *Defense Personnel Security Research Center*.

KRISINO. (2021). Kriminalitets- og sikkerhetsundersøkelsen i Norge (KRISINO). Næringslivets sikkerhetsråd (NSR).

Laszka A., Johnson B., Schöttle P., Grossklags J., & Böhme R. (2014). Secure Team Composition to Thwart Insider Threats and Cyber-Espionage. *ACM Trans. Internet Technol;* 14, 2–3.

Maasberg M. (2014). Insider Espionage: recognising ritualistic behavior by abstracting technical indicators from past cases. *20th Americans Conference on Information Systems.*

Maasberg M., & Beebe N. (2014). The Enemy Within the Insider: Detecting the Insider Threat Through Addiction Theory. *Journal of Information Privacy and Security*;10:59-70.

Maasberg M., Slyke C.V., Ellis S., & Beebe N. (2020). The dark triad and insider threats in cyber security. *Communications of the ACM*;63:12, 64-80.

Macak M., Vaclavek R., Kusnirakova D., Matulevičius R., & Buhnova B. (2022). Scenarios for Process-Aware Insider Attack Detection in Manufacturing, *The 17th International Conference on Availability, Reliability and Security (ARES 2022);*1,10.

Marbut A., & Harms P.D. (2023). Fiends and Fools: A Narrative Review and Neo-socioanalytic Perspective on Personality and Insider Threats. *Journal of Business and Psychology*;1:18.

Matthews, G., Wohleber, R., Lin, J., Reinerman-Jones, L., Yerdon, V., & Pope, N. (2018). Cognitive and Affective Eye Tracking Metrics for Detecting Insider Threat: A Study of Simulated Espionage. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 62(1), 242-246.

Mazzarolo G., & Jurcut A. (2020). Insider threats in Cyber Security: The enemy within the gates. *European Cybersecurity Journal*

Mészáros A., & Kelemen-Erdős A. (2023). Industrial espionage from a human factor perspective. *Journal of International Studies*; 16:97-116.

Nostro N., Ceccarelli A., Bondavalli A., & Brancati F. (2014). Insider Threat Assessment: A Model-Based Methodology. *SIGOPS Oper. Syst. Rev*. 48. 3-12.

NSM, Nasjonal sikkerhetsmyndighet (2020). Grunnprinsipper for personellsikkerhet.

NSM, Nasjonal sikkerhetsmyndighet (2023). Personellsikkerhet – Nasjonal sikkerhetsmyndighet (nsm.no). Desember 2023.

NTV (2023). Nasjonal trusselvurdering for 2023. Utgitt av Politiets sikkerhetstjeneste (PST).

Nurse J., Legg P., Buckley O., Agrafiotis I., Wright G., Whitty M., Upton D., Goldsmith M., & Creese S. (2014a). A Critical Reflection on the Threat from Human Insiders – Its Nature, Industry Perceptions, and Detection Approaches. *2nd International Conference on Human Aspects of Information Security, Privacy and Trust at the 16th International Conference on Human-Computer Interaction (HCII).*

Nurse J., Buckley O., Legg P., Goldsmith M., Creese S., Gordon R.T., % Whitty M. (2014b). Understanding insider threat: A framework for characterising attacks. *IEEE Symposium on Security and Privacy Workshops.*

Osterritter L. & Carley K.M. (2021). Conversations around Organizational Risk and Insider Threat. *In Proceedings of the 2021 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM '21)*. Association for Computing Machinery, New York, NY, USA, 613–621.

Patil D., & Meshram B. (2018). Network Packet Analysis for Detecting Malicious Insider. *3rd International Conference for Convergence in Technology (I2CT)*;1-8.

Pereira A.R. (2023). Queen of Cuba. *Journal of Applied Security Research*;18:3:576-587.

Pfleeger, C.P. (2008). Reflections on the Insider Threat. In: Stolfo, S.J., Bellovin, S.M., Keromytis, A.D., Hershkop, S., Smith, S.W., Sinclair, S. (eds*) Insider Attack and Cyber Security. Advances in Information Security,* vol 39. Springer, Boston, MA.

Pfleeger S. & Stolfo S. (2009). Addressing the Insider Threat. *IEEE Security & Privacy*; 7. 10-13.

Power R. & Forte D. (2006). Thwart the insider threat: a proactive approach to personell security. *Computer Fraud and Security*;10-15.

Rauf U., Mohsen F., & Wei Z. A. (2023). A Taxonomic Classification of Insider Threats: Existing Techniques, Future Directions & Recommendations. *Journal of Cyber Security and Mobility*;12:2.

Ringstad P. (2020). Sikkerhetsstyringens utvikling. *Masteroppgave.* Universitetet i Stavanger (UiS).

Risiko (2023). Økt forutsigbarhet krever høyere beredskap. Utgitt av Nasjonal sikkerhetsmyndighet (NSM).

Santos E., Nguyen H., Yu F., Kim K., Li D., Wilkinson J., Olson A., & Russell J. (2008). Intent-Driven Insider Threat Detection in Intelligence Analyses. *IEEE/WIC/ACM International Conference on Intelligent Agent Technology;*2:345-349.

Schoenherr, J.R., & Thomson, R. (2020). Insider Threat Detection: A Solution in Search of a Problem. *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security),* 1-7.

Slagnes B. (2023). Hva vet vi om innsiderisiko? *Forsvarets forskningsinstitutt (FFI*), FFI-rapport 2/00546.

Spitzner L. (2003). Honeypots: Catching the Insider Threat. *In Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC '03)*. IEEE Computer Society, USA, 170.

Sikkerhetsforum (2019). Læring etter hendelser. Rapport fra Sikkerhetsforum. Petroleumstilsynet.

Steenslie S., Haugom L., & Vaage B.H. (2019). Etterretningsanalyse i den digitale tid – En innføring. Bok utgitt av Fagbokforlaget.

Subhani A., Khan I.A., & Zubair A. (2021). Review of insider and insider threat detection in the organizations. *Journal of Advanced Research in Social Sciences and Humanities*;6:4.

Theis, M., Trzeciak, R., Costa, D., Moore, A., Miller, S., Cassidy, T., & Claycomb, W. (2019). *Common Sense Guide to Mitigating Insider Threats, Sixth Edition.* Technical Report CMU/SEI-2018-TR-010.

Tupakula U., & Varadharajan V. (2013). Trust enhanced security architecture for detecting insider threats. *12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2013*.

Vashisth A., & Kumar A. (2013). Corporate espionage: The insider threat. *Business Information Review*;30:2.

Williams M., Levi M., Burnap P., & Gundur, R.V. (2019). Under the Corporate Radar: Examining Insider Business Cybercrime Victimization through an Application of Routine Activities Theory. *Deviant Behavior*;40:9.

Willison R., & Warkentin M. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS* Quarterly; 37. 1-20.

Xiangyu L., Qiuyang L., & Chandel S. (2017). Social Engineering and Insider Threats. *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*;25-34.

Zaytsev A., Malyuk A., & Miloslavskaya N. (2017). Critical Analysis in the Research Area of Insider Threats. *IEEE 5th International Conference on Future Internet of Things and Cloud*;288-296.

Zeng M., Dian C., & Wei Y. (2022). Risk Assessment of Insider Threats Based on IHFACS-BN. *Sustainability*; 15(1):491.

Zimmer E., Burkert C., & Federrath H. (2021). Insiders Dissected - New Foundations and a Systematisation of the Research on Insiders. *Digital Threats: Research and Practice*; 3(1).

SINTEF

Teknologi for et bedre samfunn