FFI-RAPPORT

18/00466

En morfologisk analyse av tilsiktede uønskede handlinger rettet mot Forsvarets informasjonsinfrastruktur

–
Bodil Hvesser Farsund
Geir Enemo

En morfologisk analyse av tilsiktede uønskede handlinger rettet mot Forsvarets informasjonsinfrastruktur

Bodil Hvesser Farsund
Geir Enemo

Forsvarets forskningsinstitutt (FFI) 21. mars 2018

Emneord

Informasjonsinfrastruktur
Morfologisk analyse
Risikoanalyse

FFI-rapport
FFI-RAPPORT 18/00466

Prosjektnummer
1464

ISBN
P:978-82-464-3032-4
E: 978-82-464-3033-1

Godkjent av
Nils Nordbotten, *forskningsleder*
Jan Erik Voldhaug, *forskningsleder*
Espen Skjelland, *forskningsdirektør*

Sammendrag

Forsvarets informasjonsinfrastruktur (INI) skal knytte sammen Forsvarets sensorer, effektorer og beslutningstakere slik at disse kan samvirke på en effektiv måte. INI er derfor en kritisk ressurs i Forsvaret, og det kan forventes at INI i gitte situasjoner vil kunne utsettes for ulike typer angrep fra en motpart.

I denne rapporten har vi definert et angrep på Forsvarets informasjonsinfrastruktur (INI) til å bestå av én eller flere tilsiktede uønskede handlinger som utføres i serie/og eller parallell. Vi har forsøkt å finne alle mulige tilsiktede uønskede handlinger som kan rettes mot INI. Dette utfallsrommet omfatter ikke bare handlinger som kan utføres i cyberdomenet, men også angrep som fysisk ødeleggelse av infrastrukturkomponenter og angrep rettet direkte mot nøkkelpersonell. Dette utfallsrommet kan videre danne grunnlaget for ulike analyser relatert til Forsvarets INI og sikkerhet. Eksempler på dette er analyser knyttet til risiko, hendelseshåndtering, ansvarsfordeling og behovet for ulike sikkerhetsmekanismer. Ved å bruke dette utfallsrommet tvinges man til å ta bevisste valg med tanke på hvilke handlinger man velger å inkludere i analysen og hvilke handlinger man velger å utelate.

For å finne alle disse handlingene som potensielt kan rettes mot Forsvarets INI, har vi benyttet morfologisk analyse. Dette er en metode som egner seg for å analysere komplekse problemstillinger, og hvor resultatet er en matrise som beskriver utfallsrommet. Motivasjonen for å benytte morfologisk analyse er å inkludere handlinger som kan være vanskelige å forutse, men som likevel kan få store konsekvenser. Målet er at beslutningstakere og planleggere skal se hele bildet med utfordringer, og på den måten være forberedt på et bredere spekter av handlinger. Slik kan Forsvaret bli bedre rustet til å beskytte seg mot, eller å håndtere, disse handlingene.

Vi har utviklet en morfologisk matrise, og deretter beskrevet to ulike angrep ved hjelp av matrisen. Vi viser også hvordan matrisen kan brukes med en annen innfallsvinkel, der vi finner hvilke tilsiktede uønskede handlinger ulike sikkerhetsmekanismer og hendelseshåndteringsmekanismer vil virke mot. Vi beskriver også noen nærliggende modeller som Cyber Kill Chain og STRIDE, og diskuterer disse modellene opp mot vår morfologiske matrise.

I tillegg til å beskrive utfallsrommet for tilsiktede uønskede handlinger som kan rettes mot Forsvarets INI, viser matrisen også hvor stort og komplekst dette utfallsrommet er. Den tydeliggjør derfor behovet for å bruke helhetlige og etterprøvbare metoder når det arbeides med problemstillinger relatert til sikkerhet og INI.

Summary

The Norwegian Armed Forces' Information Infrastructure (INI) connects the sensors, effectors and decision makers of the Norwegian Armed Forces in order to collaborate efficiently and effectively. The INI is therefore a critical resource, and it can be assumed that the INI will be considered as an important target for an adversary.

In this work we have defined an attack against the INI to contain one or several intentional unwanted actions that can be performed in serial and/or parallel. We have tried to identify all possible intentional unwanted actions that can be directed against the INI. This spectrum of actions contains not only actions in the cyber domain, but also actions like physical destruction of infrastructure components, and attacks directly targeting critical staff. The entire spectrum can be used as a basis for further analysis related to the Norwegian Armed Forces' INI and security. Examples include analysis related to risk assessment, incident response, responsibilities, and the need for security mechanisms. By using this proposed spectrum, one is forced to make conscious choices in relation to which actions to include and which actions to exclude in the analysis.

We have used morphological analysis to extract all actions that can be directed against the Armed Forces' INI. This method is suitable for analysing complex issues and provides a framework that contains the different solutions, which in this case is the entire spectrum of intentional unwanted actions. The motivation for using morphological analysis is to include actions that may be difficult to predict, but which can still have major consequences. The goal is to help decision makers and planners to see the whole picture with challenges, thus being prepared for a wider range of actions. This enables the Norwegian Armed Forces to work out the robustness required to protect itself from, or to handle, these actions.

We have developed a morphological framework, and we show two examples of how to use it. Furthermore, we show how the framework can be utilised to identify the intentional unwanted actions in which the different security mechanisms and incident response mechanisms will mitigate. We describe some related methods like Cyber Kill Chain and STRIDE, and compare and contrast these methods with our morphological framework.

Finally, our analysis illustrates how large and complex the spectrum of intentional unwanted actions is, thus demonstrating the need for comprehensive and traceable methods when working with security for the INI.

Innhold

1 Innledning

Forsvarets informasjonsinfrastruktur (INI) skal, svært forenklet sagt, knytte sammen Forsvarets sensorer, effektorer og beslutningstakere slik at disse kan samvirke på en effektiv måte. INI ses derfor på som en kritisk ressurs, nærmest uavhengig av hvilke oppgaver Forsvaret skal løse. Gitt viktigheten for Forsvaret, er det derfor sannsynlig at INI i gitte situasjoner vil kunne utsettes for ulike typer angrep fra en motpart.

I denne rapporten defineres et angrep på INI til å være en kjede av tilsiktede, uønskede handlinger utført i serie og/eller parallell av en motpart. Rapporten ser kun på tilsiktede uønskede handlinger, fordi disse kan få større konsekvenser og være vanskeligere å håndtere enn utilsiktede uønskede hendelser. Et angrep på INI vil kunne være koordinert med angrep rettet mot andre deler av forsvarssektoren, eller mot andre sektorer, for å oppnå større effekt. De vil ofte også kunne være vanskeligere å oppdage fordi de i mange tilfeller vil være konstruert for nettopp ikke å bli oppdaget, for eksempel ved å fremstå som utilsiktede fenomener som strømbrudd, brann og så videre.

Denne rapporten beskriver en metode som systematisk spenner ut utfallsrommet for tilsiktede uønskede handlinger rettet mot Forsvarets INI. Dette kan i sin tur danne grunnlag for analyser knyttet til for eksempel risikovurdering for ulike typer angrep, behov for sikkerhetsmekanismer, ansvarsfordeling relatert til cyberhendelser og hendelseshåndtering. Vi har benyttet metoden morfologisk analyse, som blir nærmere beskrevet i kapittel 3, for å finne dette utfallsrommet.

Motivasjonen for å benytte morfologisk analyse er å ikke utelate handlinger som potensielt kan få store konsekvenser, men som allikevel kan være vanskelige å forutse. Målet er at beslutningstakere og planleggere ikke låser seg i noen spor, men heller prøver å se hele bildet med utfordringer. Hensikten er å gjøre Forsvaret forberedt på et bredere spekter av handlinger slik at de kan opparbeide robusthet til å beskytte seg mot dem eller å håndtere dem. Forsvaret vil da ha større sjanse til å områ seg raskt og få kontroll på situasjonen. Hovedtanken er at handlingene skal være realiserbare, selv om sannsynligheten for at de inntreffer i seg selv kan være liten.

Det er også viktig å påpeke at vi i denne rapporten ikke bare ser på handlinger som gjøres i programvare, det vil si ved hjelp av virus, phishing, Denial of Service -angrep og så videre. I mange tilfeller kan det være enklere og mer treffsikkert å angripe INI med for eksempel direkte angrep mot nøkkelpersonell eller fysisk ødeleggelse av infrastrukturkomponenter. Det er derfor viktig også å inkludere dette.

Et angrep på INI kan som sagt ofte være en del av et større angrep som rammer bredere. I denne rapporten ser vi ikke på hvilken aktør som står bak angrepet, hva den overordnede hensikten med angrepet er, eller hvilke følger ulike angrep kan få i stort. Vi har kun konsentrert oss om de

handlingene som kan ramme INI, og hvilke følger dette får for INIs egenskaper. Ved for eksempel hendelseshåndtering må man selvfølgelig se på handlingene i en større sammenheng.[1]

Selv om hovedhensikten med denne rapporten er en helhetlig og bred oversikt over mulige tilsiktede handlinger som kan ramme Forsvarets INI, mener vi metoden som presenteres også kan være nyttig for lignende problemstillinger utenfor Forsvaret. Selv om truslene mot Forsvaret i en krise eller krig vil kunne være annerledes enn for en sivil etat eller bedrift, vil potensielt også mye kunne være likt.

Rapporten starter med å definere en del sentrale begreper, mens vi i kapittel 3 beskriver morfologisk analyse. I kapittel 4 gjør vi denne analysen for tilsiktede uønskede handlinger rettet mot Forsvarets INI, og i kapittel 5 beskrives eksempler på bruk av metoden. Kapittel 6 beskriver noen nærliggende kjente modeller, mens vi i kapittel 7 diskuterer modellen vi har kommet frem til samt metoderammeverket som er benyttet.

2 Definisjoner

Forsvarets informasjonsinfrastruktur (INI) knytter sammen alle relevante sensorer, effektorer og beslutningstakere, slik at disse kan samvirke på en effektiv måte. I denne rapporten har det vært mest hensiktsmessig å definere *Forsvarets informasjonsinfrastruktur (INI)* som de *tekniske systemene*, *informasjonen* som utveksles på de tekniske systemene og de *menneskelige prosessene* tilknyttet bruk, drift og vedlikehold av de tekniske systemene. Dette er illustrert i Figur 2.1.

Figur 2.1 Forsvarets INI.

Vi har valgt å definere en *uønsket handling* på samme måte som en *uønsket hendelse* er definert i [2], nemlig som en handling/hendelse som kan utsette en verdi for uønsket påvirkning.

[1] Det er en tidligere FFI-rapport som omhandler cyberhandlinger, ansvarsfordeling og morfologisk analyse [1], men hvor selve angrepene på INI ikke blir behandlet like bredt. Derimot inkluderes konteksten rundt cyberhandlingene, og det utvikles mer overordnede scenarioer.

En *tilsiktet uønsket handling* definerer vi til å være en handling forårsaket av en aktør som handler med hensikt. Dette er samme definisjon som er brukt i [2].

I vårt tilfelle vil *verdien* være knyttet til Forsvarets INI sine egenskaper. En uønsket handling vil således være en handling som påvirker negativt dens tekniske systemer, informasjon og/eller menneskelige prosesser. Vi mener at de viktigste egenskapene for Forsvarets INI og dets elementer er:

- Konfidensialitet – hindre at uvedkommende får uautorisert tilgang til informasjon som ligger på systemene, informasjon om de tekniske systemene eller informasjon om de menneskelige prosessene tilknyttet INI. Verdien er her avhengig av to faktorer. Den ene faktoren er hvor stor operativ nytte en motpart vil ha av informasjonen, mens den andre faktoren er hvor lenge informasjonen vil ha operativ nytte for motparten. Jo større operativ nytte en motpart vil ha, og jo lengre holdbarhet, jo større verdi.

- Integritet – hindre at uvedkommende kan endre på informasjon, eller endre på de tekniske systemenes eller prosessenes egenskaper. Verdien er igjen avhengig av hvor stor operativ nytte motparten vil få av å endre dette, og hvor lang holdbarhet denne endringen vil ha.

- Tilgjengelighet – hindre at uvedkommende kan forhindre eller forsinke tilgangen til informasjon, tekniske systemer eller menneskelige prosesser. Verdien er avhengig av hvor lang tid det tar før dette gir operativ nytte for motparten og hvor stor operativ nytte motparten får av dette.

3 Morfologisk analyse

Det å modellere komplekse sosio-tekniske systemer og trusselscenarioer gir oss store utfordringer. Mange av egenskapene er ikke kvantifiserbare, og det kan være mye usikkerhet knyttet til blant annet de involverte aktørene. Hvis problemstillingen inkluderer å se frem i tid, er det også store usikkerheter blant annet til hva slags teknologiske nyvinninger som vil bli utviklet. Morfologisk analyse er en metode for å utforske forholdene i slike multidimensjonale og ikke kvantifiserbare problemstillinger. Metoden ble utviklet av Fritz Zwicky i 1930- og 40-årene [3].

Morfologisk analyse blir brukt til å definere, strukturere og analysere komplekse systemer, ofte med det formål å utvikle fremtidsscenarioer. Ved FFI har morfologisk analyse blitt benyttet flere ganger, blant annet som grunnlag for scenarioutvikling i Forsvarsstudie 2007 [4]. Disse scenarioene har blitt oppdatert [5] og brukes blant annet i forbindelse med Forsvarets

langtidsplanlegging [6]. I NATO kalles metoden *Creative Combinations* [7]. Metoden kan også brukes for å kartlegge forholdet mellom formål og virkemidler i strategisk planlegging [8].

Fremgangsmåten ved morfologisk analyse er følgende:

1. Problemstillingen som skal studeres formuleres så presist som mulig.

2. De viktigste *parameterne* som beskriver problemstillingen identifiseres. Det er viktig at parameterne i størst mulig grad er uavhengige.

3. Til hver parameter blir det tilordnet *tilstander* som denne parameteren kan inneha. Det er viktig at tilstandene man velger ikke er overlappende, samtidig som alle mulige tilstander for parameteren skal være representert.

4. Parameterne settes mot hverandre i et n-dimensjonalt rom, der *n* er antall parametre. Denne konstruksjonen omtales ofte som en *morfologisk boks* eller et *morfologisk rom*.

5. Hver konfigurasjon (i vårt tilfelle: hver tilsiktet uønsket handling) består av en tilstand fra hver parameter.

6. Konfigurasjoner som inneholder en inkonsistens fjernes og blir ikke med videre i analysen. Dette gjøres vanligvis ved en krysskonsistenssjekk hvor parametertilstandene vurderes parvis i forhold til konsistens.

Utgangspunktet for punkt 6 er at svært mange av de teoretiske løsningene ikke vil være realiserbare i praksis. Disse omtales som *inkonsistente*. Løsninger som inneholder minst ett par av tilstander som ikke kan opptre sammen, kan fjernes fra den videre analysen. En vanlig metode for å fjerne inkonsistente konfigurasjoner er å undersøke alle par av tilstander i matrisen med tanke på om de kan opptre sammen. Dette er en arbeidsbesparende metode, siden antall par i en matrise er langt mindre enn antall konfigurasjoner.

Ved konsistensvurderingene (syntesen) finner en ofte ut at enkelte tilstander bør endres, slettes eller tilføyes. Det kan også være at man vil innføre nye parametre og/eller slette eksisterende for å få parametre som er mer relevante, eller for å få mest mulig uavhengige parametre. En må da hoppe tilbake til henholdsvis punkt 2 eller 3 i fremgangsmåten.

Etter konsistensvurderingene kan vi markere ut et utfallsrom. Dette utfallsrommet kan til slutt deles inn i ulike klasser. Det er da viktig at klassene ikke overlapper og at hele utfallsrommet dekkes. Det vil si at ethvert utfall skal høre inn under én, og bare én klasse. Vi har ikke funnet det hensiktsmessig å dele inn i ulike klasser i dette arbeidet.

4 Morfologisk analyse av tilsiktede uønskede handlinger rettet mot Forsvarets INI

Når det gjelder sivile systemer har historien vist oss at det er mange ulike måter å angripe IKT-systemer på. Noen av de mest kjente angrepene på sivile systemer er Stuxnet [9] og WannaCry [10]. Ofte er det vanlig å tenke på angrep utført med programvare når man tenker på handlinger som kan ramme Forsvarets INI. Det er derimot ikke sikkert at en motpart alltid vil benytte dette virkemiddelet. Andre former for angrep som fysisk ødeleggelse av infrastrukturkomponenter og angrep på sentralt nøkkelpersonell kan være mer effektivt og treffsikkert i noen scenarioer.

Angrepene, slik de fremstilles i media, går ofte på at det oppstår en eller annen form for feil med systemene. Ofte har det imidlertid foregått en informasjonsinnsamling på forhånd. Denne er ofte vanskelig å oppdage. Det er derfor viktig å understreke at et angrep som kan ramme Forsvarets INI ofte består av flere steg, der hvert steg består av en tilsiktet uønsket handling. Man kan sammenligne dette med dominobrikker, der hver handling er en dominobrikke, og hvor siste brikke representerer handlingen som fullfører angrepet på INI. En motpart vil i mange tilfeller prøve å gjøre hver handling slik at den ikke blir oppdaget, men i sum ønsker motparten å oppnå en effekt. Motparten kan også skreddersy en handling for å fremtvinge en spesiell reaksjon. Hensikten med en fremtvunget reaksjon kan for eksempel være å skaffe informasjon om menneskelige prosesser eller tekniske systemer. Alle disse tilsiktede handlingene blir plukket fra utfallsrommet av alle mulige tilsiktede uønskede handlinger som kan rettes mot Forsvarets INI, eller med andre ord en slags verktøykasse som motparten besitter.

Første steg i en morfologisk analyse er å formulere problemstillingen presist. Problemstillingen i vårt tilfelle er: *Hva er utfallsrommet av alle mulige tilsiktede uønskede handlinger som kan ramme Forsvarets INI?*

Det neste steget er å finne de parameterne som best beskriver problemstillingen. I dette tilfelle mener vi at følgende parametere vil gi en god beskrivelse:

- Utgangsposisjon
- INI-element
- Middel
- INI-verdi angrepet

Hva som ligger i de ulike parameterne blir beskrevet nærmere i det videre, og til slutt i kapittelet gjøres det en konsistensvurdering. Det neste kapittelet viser noen eksempler på tilsiktede uønskede handlinger, samt en alternativ måte å bruke den morfologiske matrisen på.

Å finne de relevante parameterne kan betraktes som en «prøv og feil»-prosess, som har bestått i at vi har sett på ulike angrep og prøvd å beskrive disse ved hjelp av ulike parametre. Vi har

deretter endret parameterne til vi synes vi kan beskrive angrepene på en konsistent og hensiktsmessig måte. En svakhet med morfologisk analyse er at det ikke finnes noen metode for å komme fram til de mest optimale parameterne, og at man derfor ikke har noen garanti for at et gitt sett med parametre er de som beskriver problemstillingen best.

4.1 Utgangsposisjon

Denne parameteren beskriver hvilken posisjon den som utfører handlingen har. Han kan på en eller annen måte ha en befatning med Forsvarets INI, eller han kan stå helt utenfor. Befatningen han har med INI kan være som en bruker av INI, å arbeide med drift og vedlikehold av INI eller å være en produsent av utstyr eller utvikler av programvare som brukes i INI. I tillegg velger vi å ta med muligheten for at skadevare kan opptre autonomt etter installasjon. Tilstanden *autonomt* kan ikke inngå i den første handlingen i et angrep, da angrepet forutsettes startet av en menneskelig handling.

Parameteren *utgangsposisjon* kan derfor ha følgende tilstander:

- Bruker
- Driftspersonell
- Produsent av utstyr eller utvikler av programvare
- Ekstern
- Autonomt

De ulike utgangsposisjonene vil gi ulike muligheter til å påvirke INI. De tre første tilstandene inkluderer både bevisste insidere og handlinger hvor den som utfører ikke er klar over at han gjør noe galt. For eksempel kan en bruker sette en minnepinne med skadevare inn i en maskin med viten og vilje, eller han kan være helt uvitende om at noen har lagt skadevare på minnepinnen hans. I sistnevnte tilfelle er selve overføringen av skadevare utilsiktet for brukeren som gjør det, men vi definerer allikevel dette til å være en tilsiktet handling, fordi det da står noen bak som har sørget for at dette skjer.

Merk at vi konsentrerer oss om hvilken posisjon den som utfører handlingen har, og ikke hvem denne aktøren er eller hvem han eventuelt utfører handlingen på vegne av. Vi ser som tidligere nevnt ikke på hva det overordnede målet er utover å ramme INI.

4.2 INI-element

INI-element er en parameter som sier noe om hva som angripes. Vi har definert INI til å bestå av *endeutstyr* som enten kommuniserer med hverandre eller med *sentrale infrastruktur-komponenter*. Endeutstyr kan for eksempel være faste terminaler, håndholdte telefoner og

sensorsystemer, mens sentrale infrastrukturkomponenter for eksempel kan være databaser og webservere. For å muliggjøre kommunikasjon mellom endeutstyr og sentrale infrastrukturkomponenter har vi *kommunikasjonsinfrastruktur* som også er en del av INI. Man kan også angripe INI mer indirekte ved å angripe eksterne elementer som INI er avhengig av. Dette kan være strømtilførsel, fysisk sikring rundt de tekniske systemene og sivil kommunikasjonsinfrastruktur, og dette har vi kalt *eksterne avhengigheter*. Til slutt kan man også angripe INI ved å angripe *menneskelige prosesser tilknyttet INI*, for eksempel prosesser som deployering av sambandsutstyr på kommandoplasser, ordinær drift og vedlikehold av utstyr og ordinær bruk.

Parameteren *INI-element* kan derfor ha følgende tilstander:

- Endeutstyr
- Sentrale infrastrukturkomponenter
- Kommunikasjonsinfrastruktur
- Eksterne avhengigheter
- Menneskelige prosesser tilknyttet INI

4.3 Middel

Parameteren middel sier noe om hvordan INI angripes. INI kan angripes ved hjelp av *programvare*, for eksempel «hacking», eller ved hjelp av *maskinvare*, for eksempel ved å bytte et kort i en maskin. INI kan også angripes ved *fysiske handlinger mot tekniske systemer* som å dra ut stikkontakten til en server, jamme en radiolinje eller bombe en satellittstasjon. Et annet middel en aktør kan bruke for å ramme INI har vi kalt *personpåvirkning.* Personpåvirkning kan foregå både fysisk, som for eksempel ved å lage trafikkork slik at sentrale personer innen drift ikke kommer seg på jobb, men også psykologisk ved for eksempel å presse en bruker av INI til å bli en insider.

Parameteren *middel* kan derfor ha følgende tilstander:

- Programvare
- Maskinvare
- Fysiske handlinger mot tekniske systemer
- Personpåvirkning

4.4 INI-verdi angrepet

Målet med en tilsiktet handling rettet mot INI kan være å skaffe seg informasjon om noe, det vil si å angripe verdien *konfidensialitet*. Det kan også være å endre på noe, det vil si å angripe verdien *integritet*, eller blokkere noe, det vil si å angripe verdien *tilgjengelighet*. Dette *noe* som angripes kan være både *informasjonen* som ligger på systemene, de *tekniske systemene* i INI og de *menneskelige prosessene* rundt det å bruke og operere INI. INI-verdiene som kan angripes blir dermed:

- Konfidensialitet (informasjon)
- Konfidensialitet (tekniske systemer)
- Konfidensialitet (menneskelige prosesser)
- Integritet (informasjon)
- Integritet (tekniske systemer)
- Integritet (menneskelige prosesser)
- Tilgjengelighet (informasjon)
- Tilgjengelighet (tekniske systemer)
- Tilgjengelighet (menneskelige prosesser)

Hvilken verdi som angripes vil påvirke hvilke muligheter en motpart har for neste handling. Hvis motparten for eksempel har klart å skaffe seg informasjon om prosesser rundt drift, *konfidensialitet (menneskelige prosesser)*, eller satt deler av et informasjonssystem ut av funksjon, *tilgjengelighet (tekniske systemer)*, vil dette gi ulike muligheter for neste handling.

4.5 Morfologisk matrise

Om vi setter alle parameterne med tilstander inn i en matrise, vil den se slik ut:

Utgangsposisjon	INI-element	Middel	INI-verdi angrepet
Bruker	Endeutstyr	Programvare	Konfidensialitet (informasjon)
Driftspersonell	Sentrale infrastruktur-komponenter	Maskinvare	Konfidensialitet (tekniske systemer)
Produsent av utstyr eller utvikler av programvare	Kommunikasjons-infrastruktur	Fysiske handlinger mot tekniske systemer	Konfidensialitet (menneskelige prosesser)
Ekstern	Eksterne avhengigheter	Personpåvirkning	Integritet (informasjon)
Autonomt	Menneskelige prosesser tilknyttet INI		Integritet (tekniske systemer)
			Integritet (menneskelige prosesser)
			Tilgjengelighet (informasjon)
			Tilgjengelighet (tekniske systemer)
			Tilgjengelighet (menneskelige prosesser)

4.6 Konsistensvurderinger

Den morfologiske matrisen vi har utviklet rommer til sammen 5x5x4x9 = 900 ulike kombinasjoner. Dersom alle relevante parametre og tilstander er representert i matrisen, skal derfor alle mulige tilsiktede uønskede handlinger som kan rettes mot INI være representert. Det å vurdere konsistensen til alle disse er svært ressurskrevende. Det er derfor mer vanlig å vurdere konsistensen til de ulike tilstandene parvis. På denne måten blir konsistensvurderingene enklere og antallet reduseres.

Ved å gå gjennom matrisen og se på parvis inkonsistens mellom de ulike tilstandene er det vanskelig å finne inkonsistens. Selv om noe i første omgang kan virke inkonsistent, for eksempel utgangsposisjonen *produsent av utstyr eller utvikler av programvare* og INI-verdi angrepet *integritet (menneskelige prosesser)*, er det mulig å finne eksempler på at det kan være en kobling. Måten man utvikler og produserer systemer på kan innvirke på hvordan drift og vedlikehold utføres, og i mange tilfeller vil opplæring i dette være inkludert i anskaffelsen av systemene. I neste omgang kan en motpart utnytte at drift og vedlikehold foregår på en spesiell måte til å utføre nye uønskede tilsiktede handlinger.

Vi finner det derfor lite hensiktsmessig å utelate noen av handlingene som er representert i matrisen. Kanskje kan nettopp de handlingene som inkluderer litt mer uvanlige kombinasjoner være de mest virkningsfulle, fordi vi ikke i samme grad er forberedt på dem. Brukt på en smart måte kan slike kombinasjoner derfor være ekstra vanskelige å oppdage, og de kan introdusere sårbarheter som kan utnyttes videre.

Hovedgrunnen til at det er vanskelig å finne inkonsistenser er at verdiene er såpass grove og lite spesifikke. Det finnes eksempler på at utgangsposisjonen *bruker* kan gjøre angrep ved hjelp av middelet *fysiske handlinger mot tekniske systemer*, for eksempel ved å flytte på en skjerm, så innholdet blir synlig for et kamera utenfor et vindu, eller at en bruker heller væske ned i en maskin for å ødelegge denne. Men hvis man ser på utgangsposisjonen *bruker* og en mer spesifikk *fysisk handling mot et teknisk system* som jamming av en radiolinje, så vil denne danne en inkonsistens på logisk og empirisk grunnlag. Det vil være veldig uvanlig at en bruker som har tilgang til systemene fra innsiden, vil benytte seg av jamming utenfra. En insider kan utnyttes mer effektivt enn til å jamme, siden dette er et virkemiddel som like gjerne kan utføres av *eksterne*.

Konklusjonen er derfor at siden verdiene er såpass overordnede og rommer såpass mange underkategorier, samtidig som parameterne er såpass uavhengige, er det vanskelig å finne parvis inkonsistens. Inkonsistens vil derimot inntreffe dersom tilstandene blir mer spesifikke.

5 Eksempler på bruk av den morfologiske matrisen

Som nevnt vil et angrep på Forsvarets INI kunne defineres som én eller flere tilsiktede uønskede handlinger som utføres i serie og/eller i parallell. Her vil vi beskrive disse handlingene for to ulike angrep. I tillegg vil vi vise et eksempel på hvordan den morfologiske matrisen kan brukes med en annen innfallsvinkel.

5.1 Angrep 1

I dette angrepet ønsker en fremmed stat muligheten til å hindre beslutningselementer tilgang til viktig informasjon i en tilspisset situasjon. Angrepet består av tre tilsiktede uønskede handlinger utført i serie. Disse handlingene er beskrevet under sammen med den morfologiske matrisen hvor den aktuelle handlingen er markert.

Tilsiktet uønsket handling nr. 1.1:

Her er det etterretningsorganisasjonen til en fremmed stat, altså en *ekstern* aktør, som angriper INI-elementet *menneskelige prosesser tilknyttet INI*. Dette gjøres med middelet *person-påvirkning* mot en person som jobber med drift. Resultatet er at den fremmede staten har fått en insider som jobber med drift, og INI-verdien som er angrepet er *integritet (menneskelige prosesser).*

Utgangsposisjon	INI-element	Middel	INI-verdi angrepet
Bruker	Endeutstyr	Programvare	Konfidensialitet (informasjon)
Driftspersonell	Sentrale infrastruktur-komponenter	Maskinvare	Konfidensialitet (tekniske systemer)
Produsent av utstyr eller utvikler av programvare	Kommunikasjons-infrastruktur	Fysiske handlinger mot tekniske systemer	Konfidensialitet (menneskelige prosesser)
Ekstern	Eksterne avhengigheter	Personpåvirkning	Integritet (informasjon)
Autonomt	Menneskelige prosesser tilknyttet INI		Integritet (tekniske systemer)
			Integritet (menneskelige prosesser)
			Tilgjengelighet (informasjon)
			Tilgjengelighet (tekniske systemer)
			Tilgjengelighet (menneskelige prosesser)

Tilsiktet uønsket handling nr. 1.2:

Insideren som jobber på drift installerer et script på sentrale nettverksnoder som angriper integriteten på de tekniske systemene.

Utgangsposisjon	INI-element	Middel	INI-verdi angrepet
Bruker	Endeutstyr	Programvare	Konfidensialitet (informasjon)
Driftspersonell	Sentrale infrastruktur-komponenter	Maskinvare	Konfidensialitet (tekniske systemer)
Produsent av utstyr eller utvikler av programvare	Kommunikasjons-infrastruktur	Fysiske handlinger mot tekniske systemer	Konfidensialitet (menneskelige prosesser)
Ekstern	Eksterne avhengigheter	Personpåvirkning	Integritet (informasjon)
Autonomt	Menneskelige prosesser tilknyttet INI		Integritet (tekniske systemer)
			Integritet (menneskelige prosesser)
			Tilgjengelighet (informasjon)
			Tilgjengelighet (tekniske systemer)
			Tilgjengelighet (menneskelige prosesser)

Tilsiktet uønsket handling nr. 1.3:

Ved en tilspisset situasjon kan den samme insideren endre tilgjengeligheten til enkelte systemer og informasjon ved å starte scriptet som han har installert tidligere. Dette vil lamme sentrale nettverksnoder, og medføre at beslutningselementer ikke får tilgang til informasjon i en kritisk situasjon.

Utgangsposisjon	INI-element	Middel	INI-verdi angrepet
Bruker	Endeutstyr	Programvare	Konfidensialitet (informasjon)
Driftspersonell	Sentrale infrastruktur-komponenter	Maskinvare	Konfidensialitet (tekniske systemer)
Produsent av utstyr eller utvikler av programvare	Kommunikasjons-infrastruktur	Fysiske handlinger mot tekniske systemer	Konfidensialitet (menneskelige prosesser)
Ekstern	Eksterne avhengigheter	Personpåvirkning	Integritet (informasjon)
Autonomt	Menneskelige prosesser tilknyttet INI		Integritet (tekniske systemer)
			Integritet (menneskelige prosesser)
			Tilgjengelighet (informasjon)
			Tilgjengelighet (tekniske systemer)
			Tilgjengelighet (menneskelige prosesser)

5.2 Angrep 2

I dette angrepet ønsker en fiendtlig aktør å ramme logistikksystemer slik at informasjonen som ligger i disse systemene blir feilaktig. Angrepet består av seks tilsiktede uønskede handlinger utført i serie og rettet mot Forsvarets INI. Disse handlingene er beskrevet i det følgende sammen med den morfologiske matrisen hvor den aktuelle handlingen er markert.

Tilsiktet uønsket handling nr. 2.1:

En maskin tilknyttet en gradert plattform står en begrenset periode i et lokale med kun rudimentær fysisk sikring grunnet ombygging av lokalitetene. Handlingen er her at en *ekstern* aktør klarer å komme seg forbi den fysiske sikringen, og angriper dermed INI-elementet *eksterne avhengigheter*, ved hjelp av middelet *fysiske handlinger mot tekniske systemer*. Han skaffer seg fysisk tilgang til maskinen, og angriper på denne måten prosessen rundt hvem som skal ha tilgang til systemene, det vil si *integritet (menneskelige prosesser).*

Utgangsposisjon	INI-element	Middel	INI-verdi angrepet
Bruker	Endeutstyr	Programvare	Konfidensialitet (informasjon)
Driftspersonell	Sentrale infrastruktur-komponenter	Maskinvare	Konfidensialitet (tekniske systemer)
Produsent av utstyr eller utvikler av programvare	Kommunikasjons-infrastruktur	Fysiske handlinger mot tekniske systemer	Konfidensialitet (menneskelige prosesser)
Ekstern	Eksterne avhengigheter	Personpåvirkning	Integritet (informasjon)
Autonomt	Menneskelige prosesser tilknyttet INI		Integritet (tekniske systemer)
			Integritet (menneskelige prosesser)
			Tilgjengelighet (informasjon)
			Tilgjengelighet (tekniske systemer)
			Tilgjengelighet (menneskelige prosesser)

Tilsiktet uønsket handling nr. 2.2:

Den fysiske tilgangen benyttes til å montere en keylogger på maskinen. En keylogger lagrer alle tastetrykkene som utføres på en maskin, og blir ofte brukt for å få tilgang til passord som brukes på maskinen. Maskinen brukes av ulike brukere, deriblant en superbruker av den aktuelle tjenesten som ønskes angrepet.

Utgangsposisjon	INI-element	Middel	INI-verdi angrepet
Bruker	Endeutstyr	Programvare	Konfidensialitet (informasjon)
Driftspersonell	Sentrale infrastruktur-komponenter	Maskinvare	Konfidensialitet (tekniske systemer)
Produsent av utstyr eller utvikler av programvare	Kommunikasjons-infrastruktur	Fysiske handlinger mot tekniske systemer	Konfidensialitet (menneskelige prosesser)
Ekstern	Eksterne avhengigheter	Personpåvirkning	Integritet (informasjon)
Autonomt	Menneskelige prosesser tilknyttet INI		Integritet (tekniske systemer)
			Integritet (menneskelige prosesser)
			Tilgjengelighet (informasjon)
			Tilgjengelighet (tekniske systemer)
			Tilgjengelighet (menneskelige prosesser)

Tilsiktet uønsket handling nr. 2.3:

Aktøren skaffer seg fysisk tilgang til maskinen på ny, og logger seg nå inn som superbrukeren. Handlingen er her at aktøren henter ut system- og tjenesteinformasjon.

Utgangsposisjon	INI-element	Middel	INI-verdi angrepet
Bruker	Endeutstyr	Programvare	Konfidensialitet (informasjon)
Driftspersonell	Sentrale infrastruktur-komponenter	Maskinvare	Konfidensialitet (tekniske systemer)
Produsent av utstyr eller utvikler av programvare	Kommunikasjons-infrastruktur	Fysiske handlinger mot tekniske systemer	Konfidensialitet (menneskelige prosesser)
Ekstern	Eksterne avhengigheter	Personpåvirkning	Integritet (informasjon)
Autonomt	Menneskelige prosesser tilknyttet INI		Integritet (tekniske systemer)
			Integritet (menneskelige prosesser)
			Tilgjengelighet (informasjon)
			Tilgjengelighet (tekniske systemer)
			Tilgjengelighet (menneskelige prosesser)

I mellomtiden skjer dette:

Maskinen tilknyttet den graderte plattformen fjernes fra lokalitetene grunnet omorganisering.

En flertrinns skadevarepakke rettet mot den aktuelle tjenesten utvikles. Et mindre nettsted på Internett som ofte besøkes av militært personell, blir kompromittert. Utvikling av skadevare-pakke og kompromittering av nettsted foregår utenfor Forsvarets INI og er utenfor Forsvarets kontroll. Disse handlingene vises derfor ikke i den morfologiske matrisen.

Tilsiktet uønsket handling nr. 2.4:

En bruker går inn på det kompromitterte nettstedet fra en ugradert maskin. Den ugraderte maskinen blir kompromittert, og den utviklede flertrinns skadevarepakken installeres på denne maskinen.

Utgangsposisjon	INI-element	Middel	INI-verdi angrepet
Bruker	Endeutstyr	Programvare	Konfidensialitet (informasjon)
Driftspersonell	Sentrale infrastruktur-komponenter	Maskinvare	Konfidensialitet (tekniske systemer)
Produsent av utstyr eller utvikler av programvare	Kommunikasjons-infrastruktur	Fysiske handlinger mot tekniske systemer	Konfidensialitet (menneskelige prosesser)
Ekstern	Eksterne avhengigheter	Personpåvirkning	Integritet (informasjon)
Autonomt	Menneskelige prosesser tilknyttet INI		Integritet (tekniske systemer)
			Integritet (menneskelige prosesser)
			Tilgjengelighet (informasjon)
			Tilgjengelighet (tekniske systemer)
			Tilgjengelighet (menneskelige prosesser)

Tilsiktet uønsket handling nr. 2.5:

Brukeren setter inn en minnepinne i den ugraderte maskinen. Minnepinnen blir kompromittert av skadevaren, og settes på et senere tidspunkt inn i en maskin tilknyttet det graderte nettverket. Skadevaren installeres og kompromitterer den aktuelle logistikktjenesten som kjører på den graderte plattformen. Dette er vist i matrisen under.

Dette kunne vært modellert som to handlinger, der den første handlingen ville være å infisere en minnepinne og den neste handlingen å sette minnepinnen i en maskin på det graderte nettverket slik at tjenesten her blir kompromittert. Vi har imidlertid valgt ikke å inkludere det å infisere en minnepinne som en handling rettet mot INI, før denne minnepinnen blir satt i en maskin tilknyttet INI. Vi har derfor valgt å fokusere på den siste handlingen.

Utgangsposisjon	INI-element	Middel	INI-verdi angrepet
Bruker	Endeutstyr	Programvare	Konfidensialitet (informasjon)
Driftspersonell	Sentrale infrastruktur-komponenter	Maskinvare	Konfidensialitet (tekniske systemer)
Produsent av utstyr eller utvikler av programvare	Kommunikasjons-infrastruktur	Fysiske handlinger mot tekniske systemer	Konfidensialitet (menneskelige prosesser)
Ekstern	Eksterne avhengigheter	Personpåvirkning	Integritet (informasjon)
Autonomt	Menneskelige prosesser tilknyttet INI		Integritet (tekniske systemer)
			Integritet (menneskelige prosesser)
			Tilgjengelighet (informasjon)
			Tilgjengelighet (tekniske systemer)
			Tilgjengelighet (menneskelige prosesser)

Tilsiktet uønsket handling nr. 2.6:

Skadevaren som er installert sprer seg autonomt over nettverket, angriper over tid databaser som inneholder logistikkinformasjon, og endrer dataene i disse. Alt skjer i henhold til en forhåndsdefinert plan.

Utgangsposisjon	INI-element	Middel	INI-verdi angrepet
Bruker	Endeutstyr	Programvare	Konfidensialitet (informasjon)
Driftspersonell	Sentrale infrastruktur-komponenter	Maskinvare	Konfidensialitet (tekniske systemer)
Produsent av utstyr eller utvikler av programvare	Kommunikasjons-infrastruktur	Fysiske handlinger mot tekniske systemer	Konfidensialitet (menneskelige prosesser)
Ekstern	Eksterne avhengigheter	Personpåvirkning	Integritet (informasjon)
Autonomt	Menneskelige prosesser tilknyttet INI		Integritet (tekniske systemer)
			Integritet (menneskelige prosesser)
			Tilgjengelighet (informasjon)
			Tilgjengelighet (tekniske systemer)
			Tilgjengelighet (menneskelige prosesser)

5.3 Eksempel på annen bruk av matrisen

Den morfologiske matrisen kan også brukes med en annen innfallsvinkel. Det vil si at man kan bruke matrisen til å se hvilke tilsiktede uønskede handlinger en gitt sikkerhetsmekanisme vil virke mot. Den kan også brukes på tilsvarende måte for å vise hvilke handlinger en gitt hendelseshåndteringsprosess vil motvirke. Dette kan igjen brukes for å finne ut om det er handlinger Forsvarets INI mangler beskyttelse mot.

Et eksempel på en sikkerhetsmekanisme er tofaktorautentisering. Tofaktorautentisering er en mekanisme for tilgangskontroll hvor brukeren kun gis adgang etter å ha verifisert sin identitet på to ulike måter. Denne mekanismen vil beskytte mot *eksterne* som ønsker tilgang til systemene i INI for å gjøre et angrep i *programvare*. Potensielt kan et slikt angrep rettes mot både *endeutstyr*, *sentrale infratrukturkomponenter* og *kommunikasjonsinfrastrukturen.* Denne mekanismen kan være med på å beskytte mot handlinger som potensielt kan ramme alle INI-verdiene vi har angitt. Dette er vist i matrisen under. Mekanismen vil derimot ikke ha noen betydning for handlinger utført fra andre utgangsposisjoner, eller med andre midler. For å beskytte seg mot dette, må man ha andre mekanismer.

Det er imidlertid viktig å være klar over at det fins andre måter for *eksterne* å angripe ulike elementer i INI på med *programvare* som vil omgå tofaktorautentiseringen. Dette kan for eksempel gjøres ved å sende en epost med et vedlegg som inneholder skadevare. Tofaktorautentisering vil derfor være med på å beskytte mot alle tilsiktede uønskede handlinger som er en kombinasjon av tilstandene vist i matrisen under, men ikke gi en fullstendig beskyttelse mot disse handlingene.

Utgangsposisjon	INI-element	Middel	INI-verdi angrepet
Bruker	Endeutstyr	Programvare	Konfidensialitet (informasjon)
Driftspersonell	Sentrale infrastruktur-komponenter	Maskinvare	Konfidensialitet (tekniske systemer)
Produsent av utstyr eller utvikler av programvare	Kommunikasjons-infrastruktur	Fysiske handlinger mot tekniske systemer	Konfidensialitet (menneskelige prosesser)
Ekstern	Eksterne avhengigheter	Personpåvirkning	Integritet (informasjon)
Autonomt	Menneskelige prosesser tilknyttet INI		Integritet (tekniske systemer)
			Integritet (menneskelige prosesser)
			Tilgjengelighet (informasjon)
			Tilgjengelighet (tekniske systemer)
			Tilgjengelighet (menneskelige prosesser)

6 Andre relaterte modeller

Det fins flere modeller som er relatert til problemstillingen som omhandles i denne rapporten. I dette kapittelet beskriver vi kort angrepstrær, Cyber Kill Chain og STRIDE som er tre av de mest kjente.

Angrepstrær [11] er en teknikk som tar utgangspunkt i hva en angriper ønsker å oppnå, og deretter finner man de ulike måtene en angriper kan oppnå dette målet på. Utfallsrommet vi har utviklet vil kunne være til hjelp for å finne ulike kombinasjoner av tilsiktede uønskede handlinger som kan føre til at dette målet oppnås.

Cyber Kill Chain [12] og STRIDE [11] er relativt kjente modeller for henholdsvis å modellere et angrep og analysere trusler i cyberdomenet.

Cyber Kill Chain er utviklet av Lockheed Martin, og er en metode for å modellere inntrengning i datanettverk. Metoden beskriver en fast kjede man må igjennom for å utføre et angrep i cyberdomenet. Denne kjeden kjeden består av følgende:

- "Reconnaissance" – Inntrenger definerer målet og samler informasjon om blant annet sårbarheter hos dette målet.
- "Weaponization" – Inntrenger lager et våpen, som for eksempel et virus eller en orm, som utnytter én eller flere sårbarheter hos målet.
- "Delivery" – Inntrenger leverer våpen til målet via epost, web, USB eller lignende.
- "Exploitation" – Når våpenet er levert trigges våpenets kode slik at sårbarheter i applikasjoner eller systemer hos målet utnyttes.
- "Installation" – Bakdør/kommunikasjonskanal på målets system som tillater fjernaksess blir installert.
- "Command and Control" – En server på utsiden kommuniserer med våpenet og tilbyr "Hands on Keyboard"-aksess på innsiden av målets nettverk.
- "Action on objectives" – Inntrenger fullfører angrepet som kan være å hente ut data, endre data eller lignende.

Denne beskrivelsen danner en kjede av hendelser der utgangsposisjonen / den som utfører angrepet ser ut til å være *ekstern* og hvor middelet i alle stegene ser ut til å være *programvare*. Den omfatter derfor bare en del av det utfallsrommet vi definerer med vår morfologiske analyse.

STRIDE er en metode for å identifisere trusler rettet mot et programvaresystem. Metoden er utviklet av Microsoft, og STRIDE er et akronym som står for *Spoofing*, *Tampering*, *Repudiation*, *Information Disclosure*, *Denial of Service* og *Elevation of Privilege*. Den deler altså trusler rettet mot et programvaresystem inn i seks kategorier, og hensikten er at disse kategoriene skal være til hjelp med å finne ut hva som kan gå galt med et slikt system. Metoden blir ofte brukt sammen med et dataflytdiagram over systemet, hvor de ulike truslene markeres i diagrammet.

STRIDE ser derfor på angrep rettet mot de tilsvarende verdiene autentisitet (*spoofing*), integritet (*tampering*), ikke-fornektelse (*repudiation*), konfidensialitet (*information disclosure*), tilgjengelighet (*denial of service*) og autorisasjon (*elevation of privilege*). Dette er om lag de samme verdiene som vi har definert (se kapittel 4.4), men vi har i tillegg spesifisert hvilken del av Forsvarets INI som rammes (*menneskelige prosesser, tekniske systemer* eller *informasjon)*.

STRIDE beskriver ikke noe metodikk for å finne alle truslene under hver kategori, men her kan den morfologiske matrisen vi har utviklet brukes som et utgangspunkt.

7 Diskusjon

Vi har i denne rapporten brukt morfologisk analyse for å spenne ut utfallsrommet av tilsiktede uønskede handlinger som kan ramme Forsvarets INI. Vi har sett bredere enn bare angrep utført i programvare, i motsetning til Cyber Kill Chain, som ser ut til å ha hovedfokus på dette. I mange scenarioer kan det være enklere, billigere og mer forutsigbart med tanke på effekt å utføre et fysisk angrep på for eksempel infrastruktur, eller å påvirke de menneskelige prosessene rundt INI, enn å måtte gå veien om et angrep utført med programvare.

Rapporten er ment som et grunnlag for å gjøre ulike analyser. Ved for eksempel risikoanalyser kan denne modellen brukes til å velge seg ut handlinger det skal beregnes risiko for. Ved å bruke denne matrisen tvinges man til å ta et bevisst valg også med tanke på hvilke handlinger man velger å ikke vurdere risikoen for.

Samtidig som rapporten gir et grunnlag for videre analyser, viser den også hvor omfattende og stort dette utfallsrommet av tilsiktede uønskede handlinger er. Selv om den morfologiske matrisen er laget på et overordnet nivå, viser den at det vil være nærmere tusen ulike tilsiktede uønskede handlinger på dette nivået. Siden vi definerer et angrep til å være en kombinasjon av handlinger, enten i serie og/eller i parallell, vil det være nærmest et uendelig antall ulike angrep.

Et annet poeng er at denne matrisen er svært overordnet. Hver tilstand inneholder i realiteten mange underkategorier. For eksempel vil tilstanden *bruker* inneholde brukere i alle de ulike forsvarsgrener og på mange ulike nivå, mens *nettverk og kommunikasjonsinfrastruktur* vil kunne inneholde ulike typer infrastrukturkomponenter fra mange ulike systemer. Dette viser at om vi hadde økt detaljeringsnivået, så hadde matrisen og antall mulige handlinger, blitt betydelig større. Eksemplene i kapittel 5 viser også at det er ulike måter å realisere hver handling på. Til sammen gir dette mange muligheter for en angriper.

Noe som øker kompleksiteten ytterligere er at en tilsiktet uønsket handling vil gi ulik risiko for INI, kreve ulik håndtering og ha ulik ansvarsfordeling og så videre, avhengig av hvilket scenario man er i. For eksempel vil risikoen for at noen tilsiktet kutter en fiber som knytter en radar til et beslutningselement i et gitt geografisk område, være avhengig av hvilket scenario vi befinner oss i. I følge [9] kan risikoen for en handling beskrives ved å se på de berørte verdiene, sårbarhetene og truslene knyttet til handlingen. Både verdien denne fiberforbindelsen har for oss og hvilke trusler som eksisterer vil være scenarioavhengig. Selv om vi ikke har sett på disse problemstillingene i denne rapporten, er det viktig å være klar over at den videre analysen av handlingene vil være avhengig av en slik kontekst.

Noen vil kanskje mene at det er noen tilstander som mangler, for eksempel firmware som vanligvis blir regnet som å ligge mellom programvaren og maskinvaren. Er firmware viktig for analysen, kan man utvide parameteren *INI-element* med tilstanden firmware, eller man kan definere at man inkluderer firmware i for eksempel tilstanden *programvare*.

På samme måte kan man velge å fokusere på bare én tilstand under én parameter. Er det Forsvarets kommunikasjonsinfrastruktur (FKI) som er i fokus, kan man velge bare å konsentrere seg om tilstanden *kommunikasjonsinfrastruktur* under parameteren *INI-element*. Eller hvis man bare ønsker å se på middelet *programvare*, kan man kutte ut de andre tilstandene under parameteren *middel*. Det kan i slike tilfeller være aktuelt å utvide tilstandene *kommunikasjons-infrastruktur* og *programvare* med henholdsvis aktuelle deler av kommunikasjons-infrastrukturen og ulike måter å benytte programvare på. Modellen kan derfor tilpasses ulike behov.

Ved bruk av morfologisk analyse i andre sammenhenger er det vanlig å dele utfallsrommet inn i ulike klasser. Dette har vi ikke gjort her, men det kunne vært interessant å se om det er handlinger som på en eller annen måte hører mer sammen. Finnes det for eksempel en fredstidsklasse av handlinger, hvor INI-verdiene som angripes i stor grad omhandler konfidensialitet? Er det noen handlinger som vil være mer typiske i krig, hvor man kanskje vil se mer bruk av fysiske virkemiddel? Er det noen handlinger som vil være mer typisk for grupper og nasjoner med lite ressurser kontra grupper og nasjoner med mye ressurser? Det kunne også vært interessant å se om det er mulig å dele handlingene inn i ulike klasser basert på hvilke former for sikkerhetsmekanismer og hendelseshåndtering som vil være aktuelle for å beskytte seg mot dem.

Denne rapporten, er som tidligere nevnt, ment som grunnlag for å gjøre ulike analyser. Samtidig som den gir et slikt grunnlag, synes vi også den gir et godt bilde på hvor kompleks problemstillingene rundt sikkerhet og INI er. Den viser hvor viktig det er med etterprøvbare og helhetlige metoder når problemstillinger knyttet til Forsvarets INI og sikkerhet skal vurderes.

Referanser

[1] H. Fridheim og S. Malerud, "Scenarioer for vurdering av Forsvarets ansvar og roller i cyberdomenet [BEGRENSET]," FFI-rapport 2014/01151: 2014.

[2] Norsk Standard, "Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger - Terminologi," NS 5830:2012: 2012.

[3] F. Zwicky og A. G. Wilson, "New Methods of Thought and Procedure: Contributions to the Symposium on Methodologies," New York: Springer Verlag, 1967.

[4] I. Johansen, "Scenarioklasser i Forsvarsstudie 2007: En morfologisk analyse av sikkerhetspolitiske utfordringer mot Norge," FFI-rapport 2006/02664: 2006.

[5] T. Bukkvoll, S. Glærum, I. Johansen, I. Diesen og B. Lia, "En gjennomgang av FFIs scenariogrunnlag for Forsvarets langtidsplanlegging [BEGRENSET]," FFI-rapport 2014/01154: 2014.

[6] E. Skjelland, S. Glærum, S. Gullichsen og S. Kvalvik, "Sammenhengen mellom Forsvarets oppgaver, struktur og budsjett - inspill til arbeidet med ny langtidsplan (2017-2020) [BEGRENSET]," FFI-rapport 2014/01338: 2014.

[7] NATO, "The NATO Alternative Analysis Handbook," 2017.

[8] T. Ritchey, "Strategic Decision Support using Computerised Morphological Analysis," Denmark: 9th International Command and Control Research and Technology Symposium, 2004.

[9] D. Veluz, "STUXNET Malware Targets SCADA Systems," Sist besøkt 16.02.2018: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/54/stuxnet-malware-targets-scada-systems: TREND MICRO, 2010.

[10] M. Reynolds, "Ransomware attack hits 200 000 computers across the globe," Sist besøkt 16.02.2018: https://www.newscientist.com/article/2130983-ransomware-attack-hits-200000-computers-across-the-globe/: New Scientist, 2017.

[11] A. Shostack, "Threat modeling - designing for security," John Wiley and Sons, 2014.

[12] "Sist besøkt: 19.02.2018: https://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html," 2018.

About FFI

The Norwegian Defence Research Establishment (FFI) was founded 11th of April 1946. It is organised as an administrative agency subordinate to the Ministry of Defence.

FFI's MISSION

FFI is the prime institution responsible for defence related research in Norway. Its principal mission is to carry out research and development to meet the requirements of the Armed Forces. FFI has the role of chief adviser to the political and military leadership. In particular, the institute shall focus on aspects of the development in science and technology that can influence our security policy or defence planning.

FFI's VISION

FFI turns knowledge and ideas into an efficient defence.

FFI's CHARACTERISTICS

Creative, daring, broad-minded and responsible.

Om FFI

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

FFIs FORMÅL

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

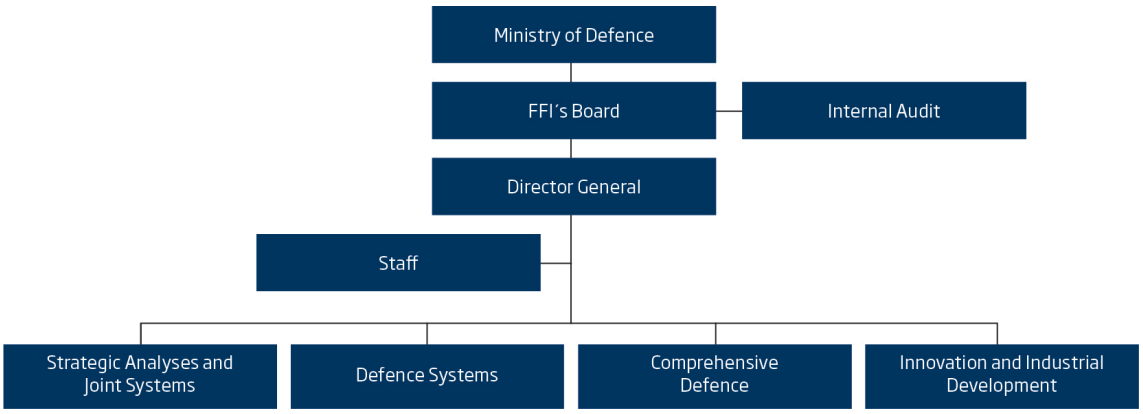
FFIs VISJON

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs VERDIER

Skapende, drivende, vidsynt og ansvarlig.

FFI's organisation



Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

Telefon: 63 80 70 00
Telefaks: 63 80 71 15
Epost: ffi@ffi.no

Norwegian Defence Research Establishment (FFI)
P.O. Box 25
NO-2027 Kjeller

Office address:
Instituttveien 20
N-2007 Kjeller

Telephone: +47 63 80 70 00
Telefax: +47 63 80 71 15
Email: ffi@ffi.no

FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment