Risikovurdering 2003

”Sikre samfunnsviktige objekter og informasjon”

Nasjonal sikkerhetsmyndighet

www.nsm.stat.no

Innhold

Forord

Nasjonal sikkerhetsmyndighet (NSM) ble etablert som direktorat 1 januar 2003. Direktoratet erstatter Forsvarets overkommando/Sikkerhetsstaben som nasjonal fag- og tilsynsmyndighet innen forebyggende sikkerhetstjeneste. Opphenget til det nye direktoratet er todelt idet det er rapporteringspliktig både til Forsvarsdepartementet (FD) og Justis- og politidepartementet (JD). Administrativt er NSM underlagt FD.

Det nye direktoratet skal koordinere og kontrollere utøvelsen av den forebyggende sikkerhetstjenesten som skjer i alle offentlige, militære og private virksomheter som er underlagt sikkerhetsloven.

I denne risikovurderingen har NSM forsøkt å beskrive sentrale forhold innen det nasjonale sikkerhetsbildet. Dette er gjort innenfor rammen av ansvarsområdet til den forebyggende sikkerhetstjenesten. Forebyggende sikkerhetstjeneste omfatter i Norge alle tiltak som iverksettes for å sikre skjermingsverdig informasjon[1] og skjermingsverdige objekter mot sikkerhetstruende virksomhet (spionasje, sabotasje og terrorhandlinger).

NSMs forhåpning er at denne risikovurderingen bidrar til å bedre det forebyggende sikkerhetsarbeidet. Ikke minst er det en målsetning at vurderingen bidrar til større forståelse og motivasjon for det forebyggende sikkerhetsarbeidet. Håpet er at dette igjen skal resultere i at alle aktuelle virksomheter gir forebyggende sikkerhetstjeneste den nødvendige prioritet. Det er en kjensgjerning at forebyggende sikkerhetstjeneste i dag i mange virksomheter ikke gis den nødvendige prioritet – denne risikovurderingen er et bidrag for å imøtegå dette.

NSM er svært interessert i tilbakemeldinger på vurderingens form og innhold. Slike kommentarer vil bidra til å forbedre kommende risikovurderinger.

Bakerst i vurderingen finnes et vedlegg med definisjoner av sentrale begreper.

Jan Erik Larsen

Direktør for NSM

[1] Med skjermingsverdig informasjon forstås her informasjon som bærer graderingen BEGRENSET, KONFIDENSIELT, HEMMELIG, STRENGT HEMMELIG eller ekvivalente NATO eller andre internasjonale organisasjoners eller nasjoners graderinger.

1 Hensikt og rammefaktorer

Alle virksomheter som håndterer sikkerhetsgradert informasjon eller skjermingsverdig objekt er gjennom sikkerhetsloven pålagt å utøve forebyggende sikkerhetstjeneste. Med utøvelse av forebyggende sikkerhetstjeneste menes alle defensive sikkerhetstiltak som er iverksatt for å beskytte informasjon og objekter med sikkerhetsgradering.

Hensikten med NSMs risikovurdering er å hjelpe virksomhetene til å forstå hvorfor det er nødvendig å utøve forebyggende sikkerhetstjeneste. Dette gjøres gjennom å formidle et overordnet nasjonalt sikkerhetsbilde. Vurderingen avgrenses til ansvarsområdet som tilligger den forebyggende sikkerhetstjenesten. Forebyggende sikkerhetstjeneste omfatter i Norge alle tiltak for å sikre skjermingsverdig informasjon og skjermingsverdige objekter mot sikkerhetstruende virksomhet som spionasje, sabotasje og terrorhandlinger. Dette er informasjon og objekter som er av betydning for rikets sikkerhet og andre nasjonale sikkerhetsinteresser.

Den forebyggende sikkerhetstjenesten er regulert gjennom sikkerhetsloven. Et viktig formål med loven er å bidra til sikring av informasjonens konfidensialitet, integritet og tilgjengelighet. Sikringstiltakene skal dekke hele livssyklusen til informasjonen og tiltakene etableres overalt der informasjonen befinner seg (for eksempel i informasjonssystemer, kommunikasjonsutstyr eller papirdokumenter). I tillegg bedømmes sårbarheter til personellet som har tjenestemessig behov for tilgang til gradert informasjon. Sikkerhetsklarering skjer derfor ved å vurdere personens lojalitet, pålitelighet og sunne dømmekraft.

Sikkerhetsloven pålegger også virksomhetene å beskytte skjermingsverdige objekter av betydning for rikets sikkerhet og andre vitale nasjonale sikkerhetsinteresser. Dette vil eksempelvis kunne være militære installasjoner og materiell, eller samfunnsviktig infrastruktur innen vannforsyning, telekommunikasjon, kraftforsyning, olje- og gassvirksomhet. Innholdet og omfanget av objektsikkerhetsbegrepet er imidlertid ennå ikke fastsatt, men en tverrsektoriell arbeidsgruppe har ferdigstilt et utkast til forskrift med definisjoner, virkeområde og krav til overordnede tiltak. Arbeidsgruppens rapport vil bli sendt ut på høring til relevante virksomheter.

Et formalisert og målrettet nasjonalt beskyttelsesregime for objekter vil i økende grad utgjøre en sentral del av egenbeskyttelsen mot spionasje, terror- og sabotasjehandlinger. I påvente av at objektsikkerhetsforskriften vedtas, fokuseres dette fagfeltet i mindre grad i denne risikovurderingen. Det er derimot en ambisjon at objektsikkerhet i større grad vil bli belyst i NSM sine fremtidige risikovurderinger.

1.1 Virksomhetenes utøvelse av forebyggende sikkerhetstjeneste

NSM er fag- og tilsynsmyndighet innen forebyggende sikkerhetstjeneste. En hovedoppgave for NSM er å utforme de konkrete sikkerhetstiltakene slik de er uttrykt i forskriftene til sikkerhetsloven. I tillegg skal NSM føre tilsyn med virksomheter som faller inn under sikkerhetsloven, samt gi råd og veiledning i sikkerhetsspørsmål.

Selve utøvelsen av forebyggende sikkerhetstjeneste er som hovedregel desentralisert idet alle virksomheter som håndterer sikkerhetsgradert informasjon og sikkerhetsklassifiserte objekter, skal utøve nettopp forebyggende sikkerhetstjeneste. Dette omfatter virksomheter både innen Forsvaret, øvrig statsforvaltning, fylkeskommunene, kommunene og leverandører som leverer varer eller tjenester i forbindelse med sikkerhetsgraderte anskaffelser.

Virksomhetenes utøvelse av forebyggende sikkerhetstjeneste skal ta utgangspunkt i sikkerhetsloven med forskrifter. Bestemmelsene i forskriftene er dog bare å regne som minimumskrav. Virksomheten plikter løpende å vurdere om egne skjermingsverdige verdier er godt nok sikret i forhold til kjente sårbarheter og trusselsituasjonen. Gjennom utøvelse av

risikohåndtering[2] skal virksomhetene avdekke behov for å iverksette ytterligere tiltak utover minimumskravene. Dette systemet sikrer en tilpasset og fleksibel grunnsikring innen hver virksomhet og innenfor hver samfunnssektor - summen av dette bidrar til samfunnets totale sikkerhet.

En overordnet, nasjonal risikovurdering er et viktig utgangspunkt for den enkelte virksomhets utøvelse av risikohåndtering. Den overordnede risikovurderingen må her av den enkelte virksomhet ses i sammenheng med de lokale risikoforhold.

På samme tid understrekes betydningen av at virksomhetene rapporterer inn til NSM om sårbarheter, sikkerhetstruende hendelser, mistenkelige hendelser, sikkerhetsbrudd, skadevurderinger eller annen informasjon som anses som sikkerhetsmessig relevant. Informasjonen som tilkommer fra virksomhetene både i offentlig forvaltning, det private og Forsvaret utgjør en særlig viktig kilde for risikovurderingsarbeidet. Foruten å heve kvaliteten til risikovurderingene, bidrar innspill og rapporter fra virksomhetene til å forbedre alle deler av den forebyggende sikkerhetstjenesten. Det er her viktig å forstå vekselforholdet der NSMs risikovurderinger danner et viktig grunnlag for utøvelsen av sikkerhetsarbeidet i virksomhetene, samtidig som NSM er avhengig av innspill fra virksomhetene for å utarbeide de overordnede risikovurderingene.

1.2 Kilder til kompromittering

Den forebyggende sikkerhetstjenesten skal forhindre at informasjon og objekter blir kompromittert. Med kompromittering av informasjon menes her tap av konfidensialitet, integritet og tilgjengelighet. Kompromittering av objekter innbefatter også disse kravene til beskyttelse. Opprettholdelse av objektenes funksjonalitet og yteevne er imidlertid i mange sammenhenger en mer forståelig beskrivelse av formålet med beskyttelsen.

Kompromittering av skjermingsverdig informasjon og objekter kan noe forenklet skje på tre måter:

1) **Eksterne trusselaktører** – eksterne trusselaktører som gjennom bevisste handlinger prøver å få innsyn i sikkerhetsgradert informasjon, alternativt manipulere eller gjøre den utilgjengelig. For objekter vil en aktiv trusselaktører gjennom bevisste handlinger prøve å påvirke objekters funksjons- og yteevne. En trusselaktør vil alltid prøve å finne sårbare punkter som forsøkes utnyttet.
2) **Egeneksponering** – en virksomhet gjør seg selv mer sårbar dersom egensikringen ikke fungerer tilfredsstillende. Mangelfullt sikkerhetsarbeid vil kunne medføre at skjermingsverdig informasjon og skjermingsverdige objekter blir eksponert for omverdenen. Dette vil eksempelvis ofte bli resultatet dersom regelverket som regulerer sikkerhetstjenesten fravikes. Egeneksponeringen kan utløses både gjennom bevisste og ubevisste handlinger.
3) **Utro tjenere –** egne ansatte kan utgjøre en risiko og kan under visse omstendigheter bevisst bidra til at informasjon kompromitteres. Drivkreftene kan være egen vinning eller komme som et resultat av press fra eksterne aktører.

[2] Se §4-1 i Forskrift om sikkerhetsadministrasjon av 29 juni 2001 nr. 723.

De ulike kildene til kompromittering er forsøkt visualisert i denne modellen:

Det fremstår som en utfordring for den forebyggende sikkerhetstjenesten å rette fokuset mot samtlige tre kategorier. Aktivitet fra trusselaktører skal forsøkes vanskeliggjort gjennom situasjonstilpassede sikkerhetstiltak. Egeneksponeringen skal forsøkes minimalisert gjennom en riktig og målbevisst gjennomføring av sikkerhetstiltakene. Risikoproblematikk tilknyttet utro tjenere skal forsøkes avverget gjennom gode interne kontroll- og personellrutiner, samt sikkerhetsklarering og autorisasjonsprosessen.

1.3 Den samfunnsmessige rollen til forebyggende sikkerhetstjeneste

Den forebyggende sikkerhetstjenesten bidrar til å optimalisere den offentlige ressursbruken innen det totale beredskaps- og sikkerhetsarbeidet. Årlig øremerkes ressurser i form av store materielle investeringer i Forsvaret og innen annen offentlig virksomhet, driftsutgifter, omfattende menneskelige ressurser, kompetanse og øvelsesaktivitet. Samlet danner disse innsatsfaktorene grunnlaget for blant annet beredskapsplanverkene. Planverkene er særlig sentrale ettersom det er her synergieffekten av den samlede ressursbruk oppnås.

Vår slagkraft og motstandsdyktighet mot sikkerhetstruende hendelser tappes dersom ikke slike planverk omgis av et velfungerende sikkerhetsregime. Kompromitteres våre planer, undergraves også vår evne til å motstå sabotasje og terroranslag. En helhetlig sikkerhetstjeneste, integrert i den daglige aktivitet, utgjør derfor en styrkemultiplikator i våre samlede anstrengelser mot spionasje-, terror- og sabotasjetrusselen.

Den forebyggende sikkerhetstjenesten må til enhver tid kritisk evalueres i forhold til det rådende risikobildet. I Osama bin Laden og al-Qaida har den vestlige verden møtt en asymmetrisk motstander som er villig til å gjennomføre omfattende terroroperasjoner mot samfunnsvitale installasjoner, gjerne med høy symbolverdi og med store tap av menneskeliv. Forberedelsen til operasjonene gjennomføres både profesjonelt og over lengre tidsspenn. Et avgjørende element i terroraktørers arbeid er å samle inn informasjon omkring sannsynlige måls sårbarheter. Dette kan være informasjon fra åpne kilder, men sikkerhetsgradert informasjon vil være særlig verdifull. Et

måls attraksjon kan noe forenklet sagt øke i takt med trusselaktørens kunnskap om nettopp målobjektet. Inngående kjennskap til rutiner, sårbarheter, kapasiteter og planverk forenkler både planleggingen og eventuell gjennomføring av anslag. Bekjempelsen av terrornettverket utgjør en betydelig utfordring ettersom de råder over betydelige ressurser, har høy kompetanse og er usynliggjort som tilsynelatende "vanlige borgere". Den forebyggende sikkerhetstjenesten fungerer i denne forbindelse som en barriere som skal hindre at terroraktører erverver tilstrekkelig kunnskap omkring våre skjermingsverdige verdier.

Kampen mot al-Qaida anskueliggjør behovet for at den forebyggende sikkerhetstjenesten samarbeider internasjonalt. Forebyggingen av terror kan ikke skje utelukkende innenfor nasjonalstaten. En god sikkerhetstjeneste er viktig for vår anseelse utad. Vi er aktive internasjonalt, eksempelvis innen NATO, og det forventes her at vi opprettholder en nasjonal robusthet mot sikkerhetstruende aktiviteter, slik at vi også evner å håndtere vår felles risiko. En godt fungerende nasjonal sikkerhetstjeneste på alle nivåer bidrar således til å gjøre Norge til en tillitvekkende medspiller. Vårt betydelige engasjement i internasjonale militæroperasjoner krever også at sikkerheten ivaretas. Dette også for å unngå tap av liv og materielle verdier.

1.4 Rammefaktorer for den forebyggende sikkerhetstjenesten

Den forebyggende sikkerhetstjenesten opererer innenfor ytre rammer gitt av myndighetene. Sikkerhetsloven er allerede nevnt. Gjennom lovens formål gis det klare begrensninger for utøvelse av sikkerhetstjenesten. I følge formålsparagrafen skal forholdene legges til rette for effektivt å kunne motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser. Videre heter det at loven skal ivareta den enkeltes rettssikkerhet, og trygge tilliten til og forenkle grunnlaget for kontroll med forebyggende sikkerhetstjeneste.

Andre rammefaktorer som begrenser den forebyggende sikkerhetstjenestens handlingsrom utover de juridiske kan være av etisk og økonomisk karakter. Disse rammefaktorene setter samlet grenser for den forebyggende sikkerhetstjenestens virksomhet, samtidig som myndighetene gjennom slik grensesetting setter terskelen for akseptabel restrisiko.

1.5 Kontroll med den forebyggende sikkerhetstjenesten

Stortingets kontrollutvalg for etterretnings- overvåkings- og sikkerhetstjenestene (EOS-tjenestene) gjennomfører jevnlig kontroll med NSM. Denne kontrollordningen er uavhengig av EOS-tjenestene og forvaltningen for øvrig. Utvalgets medlemmer velges av Stortinget, og utvalget rapporterer til Stortinget i form av årsmeldinger og særskilte meldinger.

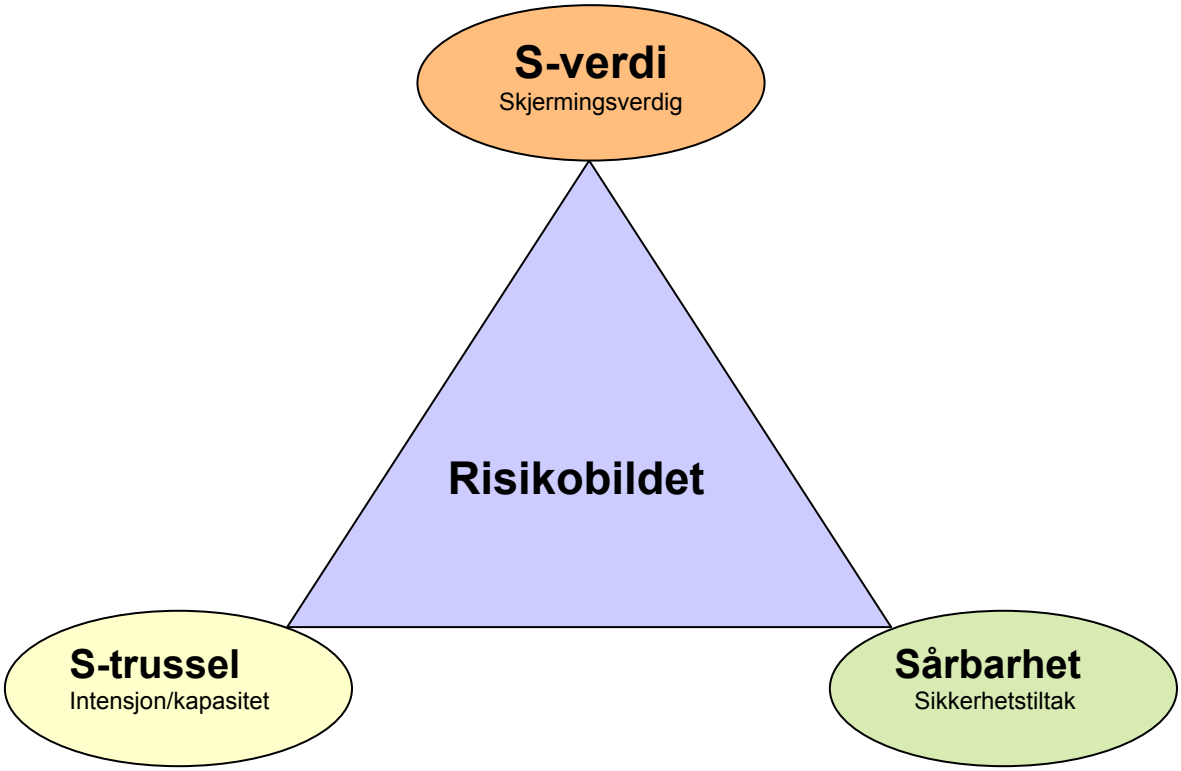
Den løpende kontrollen utføres ved regelmessige inspeksjoner av EOS-tjenestene, både sentralt og i de enkelte virksomheter. Utvalget behandler også klager fra enkeltpersoner og organisasjoner som mener EOS-tjenestene har begått urett mot dem.

Kontrollutvalgets arbeid er regulert gjennom Lov av 3. februar 1995 nr 7 om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste, med underliggende instruks.

Utover dette utøver regjeringen kontroll over NSM gjennom FD. NSM er også pålagt å rapportere til JD i enkelte saker, og er dermed underlagt en viss kontroll fra JD.

2 Risikobildet

Et helhetlig sikkerhetsbilde kan uttrykkes gjennom en risikovurdering. Følgende figur kan illustrere samspillet mellom faktorene som til sammen utgjør risikobildet.



Et viktig utgangspunkt for den forebyggende sikkerhetstjenesten er å vurdere hvilke verdier som trenger å skjermes (sikkerhetsmessig verdi). Videre vil det selvsagt være viktig å ha kjennskap til hvilke aktører som utgjør en trussel mot våre skjermingsverdige verdier. Følgelig er det viktig for det forebyggende sikkerhetsarbeidet å ha kjennskap til trusselaktørenes intensjoner og kapasiteter. For å kunne beskytte de skjermingsverdige verdiene er det viktig å ha oversikt over hvilke sårbarheter en trusselaktør kan tenkes å utnytte. På bakgrunn av en slik oversikt er utfordringen å finne frem til sikkerhetstiltak som bidrar til å redusere sårbarheten.

Hovedelementene i figuren vil bli beskrevet nærmere nedenfor.

3 Sikkerhetsmessig verdi – hva trenger beskyttelse ?

Den forebyggende sikkerhetstjenesten har som oppgave å etablere et system som gir skjermingsverdig informasjon og skjermingsverdige objekter den nødvendige beskyttelse. Denne beskyttelsen kommer til uttrykk gjennom sikkerhetstiltak innenfor ulike fagområder.

Et viktig utgangspunkt for den forebyggende sikkerhetstjenesten er likevel det som skjer før tiltakene utformes og implementeres. En verdivurdering må gjennomføres for å klarlegge hvilken informasjon og hvilke objekter som er skjermingsverdige. Dersom informasjon eller objekter vurderes som skjermingsverdig av hensyn til rikets sikkerhet eller andre vitale, nasjonale sikkerhetsinteresser, er utfordringen å definere riktig graderings- eller klassifiseringsnivå.

Hva som har sikkerhetsverdi, og følgelig er skjermingsverdig, vil aldri være statisk over tid. Mye vil regnes som skjermingsverdig over lang tid. Det vil imidlertid alltid være et tilsig av ny informasjon og nye objekter som bør beskyttes, samtidig som behov for beskyttelse av tidligere ansette verdier frafaller. Endringer i våre omgivelser, eksempelvis den overordnede

sikkerhetspolitiske, teknologiske, samfunnsmessige og økonomiske utviklingen, vil løpende påvirke hva vi ønsker å beskytte.

Det faktum at man anser noe for å ha en verdi, innebærer at det eksisterer et skadepotensiale. Skadepotensialet i forbindelse med en reduksjon eller et tap av sikkerhetsmessig verdi kan være knyttet til flere forhold. I tilknytning til informasjon vil det være særlig aktuelt å nevne muligheten for tap eller reduksjon av konfidensialitet, integritet og tilgjengelighet.

Konfidensialitet innebærer at informasjonen ikke er tilgjengelig for uautoriserte personer eller ikke-godkjente IKT-systemer. Integritet innebærer at informasjonen er nøyaktig og fullstendig, samt at transaksjoner kan skje på en pålitelig måte. Tilgjengelighet innebærer at man kan få tak i informasjonen, og at dette skal kunne skje uten nødvendig forsinkelse.

I forhold til skjermingsverdige objekt vil begrep som funksjonalitet og legitim kontroll være aktuelle. Et objekt må ha sin funksjonalitet i behold, dersom man skal kunne si at objektet ikke har vært utsatt for skade. Et objekt må også være under legitim kontroll. Et objekt som er overtatt av fiendtlige aktører, vil ikke være tilgjengelig for legitime aktører, og har dermed tapt sin sikkerhetsmessige verdi.

3.1 Oversikt over verdier

Hva som må beskyttes av hensyn til rikets sikkerhet og andre vitale, nasjonale sikkerhetsinteresser, må ta utgangspunkt i ønsket om nasjonal handlefrihet og integritet. Nasjonal handlefrihet og integritet kan igjen brytes ned til en rekke underpunkter. Innenfor alle disse underpunktene finnes det igjen en kjerne av informasjon og objekter som av hensyn til rikets sikkerhet må beskyttes.

Nedenfor gis det en grov punktliste over ulike områder der nasjonale verdier må sikres:

- konstitusjonell handlefrihet
- økonomisk og finansiell handlefrihet
- juridisk handlefrihet
- militær handlefrihet
- sikkerhets- og utenrikspolitisk handlefrihet
- territoriell integritet

Oversikten er ikke utfyllende, men er ment å gi en pekepinn på bredden av områder der skjerming av informasjon og objekter alltid i større eller mindre grad vil være nødvendig. Viktig i denne sammenheng er at beskyttelsesbehovene vil forefinnes på alle nivåer i samfunnet. Utfordringen for den enkelte virksomhet blir å definere hva som er kritiske verdier for egen del, samtidig som virksomhetene ser seg selv i en større sammenheng.

Opprettholdelsen av nasjonal handlefrihet og integritet er igjen avhengig av en rekke funksjoner. Et fellestrekk for disse funksjonene er at de er gjensidig avhengige av hverandre for å kunne yte sine tjenester. Sentrale funksjoner i denne sammenheng er:

- ledelse og informasjon
- kraftforsyning
- telekommunikasjon
- olje og drivstoff
- transport
- Forsvar og beredskap
- arbeidskraft

- vannforsyning
- bank- og pengevesen
- bygg og anlegg
- industri og varehandel
- helsevesen
- ernæring
- brann/redning
- politi/orden

Heller ikke denne opplistingen er utfyllende, men indikerer likevel mangfoldet av funksjoner som bidrar til opprettholdelse av nasjonal handlefrihet og integritet. Behov for å skjerme informasjon og objekter vil gjelde alle disse funksjonene.

4 Sikkerhetstrusselen – fokus, aktører og tiltak

Den forebyggende sikkerhetstjenesten må ha inngående kjennskap til trusselen av flere årsaker. Nedenfor angis noen årsaker til hvorfor kjennskap til trusselens kapasiteter, intensjoner og handlinger er av interesse for den forebyggende sikkerhetstjenesten.

4.1 Hva fokuserer trusselaktører på?

Det vil alltid være viktig å ha kjennskap til hva trusselaktørene fokuserer på. Dette er viktig som et korrektiv til vår egen formening om hvilke verdier som bør beskyttes. Et samsvar mellom det vi definerer som beskyttelsesverdig og det trusselaktørene fokuserer på, kan gi en bekreftelse på at vi beskytter riktige verdier. Et avvik kan være en spore til å revurdere de verdier vi beskytter, eller ikke beskytter. Uavhengig av den foreliggende trusselaktiviteten vil imidlertid konsekvensene som en kompromittering av informasjon eller objekter innebærer, alltid fremstå som et selvstendig kriterium for skjerming.

Nedenfor følger en liste over aktuelle områder hvor trusselaktører har drevet aktiv etterretning. Listen er ikke nødvendigvis utfyllende.

- Norsk utenriks- og sikkerhetspolitikk
- Forsvaret
- Internasjonalt samarbeid
- Bilaterale relasjoner
- Utenlandske etablissementer i Norge
- Norsk virksomhet i utlandet
- Personell og beslutningstakere
- Industri, forskning og teknologi
- Kritisk infrastruktur
- Kystfarvann
- Objekter med symbolverdi
- Farlig materiell

4.1.1 Trusselaktørenes metoder

For den forebyggende sikkerhetstjenesten vil det alltid være avgjørende å ha kjennskap til de arbeidsmetoder og teknikker en trusselaktør benytter. Kjennskap til metoder og teknikker er

viktig for å kunne fastsette og dimensjonere sikkerhetstiltakene. En trusselaktørs metoder og teknikker vil alltid utbedres og raffineres, noe som i sin tur får konsekvenser for utformingen av de forebyggende sikkerhetstiltakene.

En trusselaktør vil ha et utall av mulige teknikker for å innhente informasjon. Nedenfor listes en del plattformer som gjerne blir benyttet i etterretningssammenheng. Listen er ikke uttømmende.

- Ambassadepersonell
- Skipsfart
- IKT-systemer
- Elektroniske innsamlingssatellitter
- Fotosatellitter
- Teknisk avlyttingsutstyr
- Reiser og delegasjoner
- Personkontakt
- Åpne kilder
- Observasjon
- Bruk av vervede personer

4.1.2 Aktivitetsnivå

Det er videre avgjørende for den forebyggende sikkerhetstjenesten å ha kjennskap til trusselaktørenes aktivitetsnivå. Dersom trusselens aktivitetsnivå antas høynet, eksempelvis at det foreligger indikasjoner på et nært forestående anslag, må den forebyggende sikkerhetstjenesten være parat og implementere ytterligere tiltak. Dette gjøres for eksempel gjennom Forsvarssjefens terrorberedskapsdirektiv der ulike beredskapsnivåer og tiltak iverksettes i takt med trusselens intensitet. De samme prinsippene som for Forsvarssjefens terrorberedskapsdirektiv er lagt til grunn i NSMs veileder for egenbeskyttelse mot terrorhandlinger. Veilederen ble publisert i september 2002.

4.1.3 Motivasjon

Kjennskap til trusselaktørers kapasiteter og intensjoner vil virke motiverende for personell som er i befatning med skjermingsverdig informasjon eller objekt. Kunnskaper om trusselaktiviteten gir igjen forståelse for viktigheten av det forebyggende sikkerhetsarbeidet. Forståelse og motivasjon vil videre sikre bedre rapporteringsrutiner. Rapportering av sikkerhetstruende virksomhet, sikkerhetsbrudd og kompromitteringer er avgjørende for at den enkelte virksomhet selv skal ha oversikt over sikkerhetstilstanden. Virksomhetens rapportering til NSM er igjen avgjørende for at NSM skal kunne danne seg et bilde av den nasjonale sikkerhetstilstanden.

4.2 Trusselaktørene

Trusselbildet under den kalde krigen var relativt oversiktlig og enkelt å forholde seg til, og motpartens intensjoner var forholdsvis enkle å identifisere. I dagens situasjon derimot, er trusselbildet mer kompleks. Sikkerhetstruslene er mange og mer uforutsigbare, og potensielle aktører og deres intensjoner kan være ukjente. Nedenfor angis enkelte trusselaktører som den forebyggende sikkerhetstjenesten må fokusere på fordi deres aktiviteter kan true våre nasjonale sikkerhetsinteresser. Listen er ikke utfyllende, men beskriver sentrale aktørkategorier.

4.2.1 Nasjonale aktører

Flere nasjoner driver etterretningsinnhenting i og mot Norge. Slik aktivitet retter seg både mot åpne informasjonskilder og mot sikkerhetsgradert informasjon. I tillegg rettes slik aktivitet mot objekter, installasjoner og personell. Andre nasjoner gjennomfører etterretning både i Norge og mot norske interesser i utlandet, herunder norske militære styrker i utlandet, ambassader og industri. Aktuelle etterretningsmål og metoder er tidligere beskrevet i dette kapitlet.

Bruk av åpen informasjon fremstår som den mest brukte etterretningskilden. Dette kan for eksempel dreie seg om tidsskrifter, aviser, TV, internett og offentlige dokumenter. Denne formen for innhenting er i utgangspunktet legal, men kan likevel ha visse sikkerhetsmessige implikasjoner. Det er et dilemma for den forebyggende sikkerhetstjenesten at bestemte kategorier ugradert informasjon som settes sammen i en større helhet kan utgjøre et gradert bilde. Dersom den systematiske innsamlingen og sammensettingen av åpen informasjon danner et gradert bilde, vil dette kunne falle inn under Lov om forsvarshemmeligheter og straffeloven.

Tilgang til gradert informasjon vil selvsagt være særlig verdifull for en nasjonal etterretningsaktør. Dette fordi gradert informasjon gjerne beskriver våre sårbarheter, handlingsmønstre og kapasiteter. Tilgang til gradert informasjon vil også kunne bekrefte eller eventuelt avkrefte de konklusjoner som er trukket på bakgrunn av de åpne kildene.

4.2.2 Terroraktører

Terrortrusselen fremstår som en mer aktuell trussel mot både vestlig sikkerhet og vår nasjonale sikkerhet enn tidligere. Terrorens potensial åpenbarte seg med større kraft enn hva de fleste trodde var mulig 11 september 2001. USA og verden våknet opp til ”superterrorismen” da al-Qaida brutalt slo til mot finansverdenens nervesenter på Manhattan og forsvarsmaktens hovedkvarter i Pentagon. Al-Qaida viser videre vilje til å gå svært langt i valg av virkemidler for et terroranslag. Bruk av passasjerfly mot World Trade Center og Pentagon viser dette med all tydelighet. I al-Qaidas arsenal finnes også mer tradisjonelle virkemidler som lastebiler eller småbåter fullastet av sprengstoff. Den påviste interessen for kjemiske, biologiske og radioaktive våpen åpner videre for skremmende scenarier.

Gjennom den forebyggende sikkerhetstjenesten etableres det en betydelig grunnsikring mot terrorhandlinger. Dette kommer mellom annet til uttrykk gjennom det forebyggende informasjonssikkerhetsarbeidet. Tilgang til informasjon er en viktig del av forberedelsene for en terroraksjon. I tillegg til å være et terrornettverk kan al-Qaida også betegnes som et etterretningsnettverk.

Innhenting, systematisering og analyse av informasjon er en kjerneaktivitet for al-Qaida. Dette fremgår av beslaglagte al-Qaida dokumenter hvor det fremheves at enhver organisasjon som ønsker å delta i en global jihad må samle så mye informasjon som mulig om fienden. Al-Qaida opererer med to hovedmetoder for informasjonsinnhenting; 1) gjennom fordekte midler og 2) gjennom bruk av åpne kilder. Det stilles høye krav til informasjonens integritet. Informasjonen må mellom annet være oppdatert, pålitelig og være bekreftet. Dette forholdet indikerer at informasjonsinnhenting anses som en løpende aktivitet for nettverkets medlemmer.

Informasjonsinnhentingen kan i grovt tenkes å ha to utgangspunkt; 1) innhenting omkring faktiske terrormål, og 2) innhenting omkring potensielle terrormål. Et avgjørende element i en al-Qaida operasjon er å samle inn informasjon omkring sannsynlige måls sårbarheter og styrke. Inngående kjennskap til rutiner, sårbarheter, kapasiteter og planverk forenkler både planleggingen og en eventuell gjennomføring av anslag. Dette sammenfaller med det generelle forholdet at et måls attraksjon noe forenklet sagt øker i takt med trusselaktørens kunnskap om nettopp målobjektet.

Det synes å være liten tvil om at terrorhandlingene 11. september 2001 var planlagt etter langvarig og systematisk informasjonsinnhenting, primært fra åpne kilder.

Al-Qaida fremstår ikke som den eneste terroraktøren som vil kunne ramme Norge, men fremstår likevel som den mest aktuelle.

4.2.3 Kriminelle aktører

Kriminell aktivitet gir den forebyggende sikkerhetstjenesten en rekke utfordringer. Her beskrives kort noen av disse utfordringene.

Dersom det totale omfanget av organisert kriminalitet blir stort nok, kan det utgjøre en trussel mot den nasjonale sikkerheten. Vårt nasjonale kriminalitetsbilde er imidlertid ikke av en slik karakter i dag, selv om kriminalitet fremstår som et økende samfunnsproblem.

Organisert kriminalitet er ofte en integrert del av terrororganisasjoners aktiviteter. Finansieringen av terrornettverkenes aktiviteter kommer i stor grad fra organisert kriminell aktivitet. Bekjempelse av organisert kriminalitet er således i mange sammenhenger en viktig del av bekjempelsen av terrornettverkene.

Kriminalitet fremstår som et problem innen cyberspace. Anslag mot informasjonssystemer i vinnings hensikt er et økende samfunnsproblem. Våre IKT-systemer har iboende en rekke sårbare punkter som kriminelle avdekker og utnytter. Ved siden av økonomiske motiver kan også innsyn i sensitiv informasjon være en drivkraft ved siden av å endre informasjonens integritet eller tilgjengelighet. Intensjonen bak illegal aktivitet innenfor informasjonssystem-nettverkene kan ofte være vanskelig å etterspore.

Kriminelle som en trussel mot Forsvarets våpenlagre ble synliggjort i 2002. En rekke militære våpen ble stjålet under anslag mot HV-lagre både i Oslo-området og i Finnmark. Heldigvis er disse våpnene kommet til rette. Generelt er det flere aktører som kan tenkes å ha interesse av å besitte militære våpen, herunder terrorister, geriljagrupper, kriminelle og ekstremister

Innbrudd og tyveri kan også være et sikkerhetsproblem. Under innbrudd kan sikkerhetsgradert materiale bli stjålet og således kompromittert. Dette kan for eksempel omfatte etterspurt IKT-utstyr der sensitiv informasjon ligger lagret. Selv om utstyret og ikke selve informasjonen er målet for innbruddet, vil likevel den graderte informasjonen komme på avveie.

Kriminelle rulleblad er av særlig interesse for våre nasjonale klareringsmyndigheter. Endringer i kriminalitetsbildet vil på den måten utgjøre en utfordring for våre klareringsmyndigheter. I overveiende grad begrunnes de negative klareringsavgjørelsene med straffbare forhold.

4.3 Asymmetriske virkemidler

Utviklingen i verdenssamfunnet har ført til at store, konvensjonelt utrustede, militære avdelinger stort sett ikke kriger mot hverandre lenger. Trusselen kommer i dag i større grad fra enheter og organisasjoner som ikke kan utfordre den militære styrken til statsmaktene. Det er altså et asymmetrisk forhold mellom statsmaktene og slike enheter og organisasjoner. Slike enheter og organisasjoner kan betegnes asymmetriske aktører. De asymmetriske aktørene benytter ulike virkemidler for å oppnå publisitet og om mulig gjennomslag for sin sak.

4.3.1 ABC-materiale

Radioaktivt, biologisk og kjemisk materiale (ABC-materiale) kan utnyttes som svært ødeleggende våpen. Ulike terrorgrupper har vist stor interesse for ABC-materiell, og utnyttelse av slikt materiell som våpen. Et av få eksempler på konkret bruk av ABC relaterte våpen, utført av en terrororganisasjon, er den japanske sekten Aum Shinrikyo, som i 1995 spredte nervegassen sarin på undergrunnsbanen i Tokyo. Angrepene i Tokyo må regnes som et lite vellykket anslag

hva angår fysisk skadeomfang, bare 12 personer omkom. Et annet eksempel, der gjerningsmennene foreløpig ikke er avslørt, er spredningen av anthrax-sporer i USA.

Målt ut i fra enkelte terrorgruppers interesse for å tilegne seg ABC-materiell til våpenproduksjon, må det påregnes at grupper før eller senere vil fremskaffe anvendbare kapasiteter. I beslaglagte dokumenter fra al-Qaida påvises det at nettverket har forsøkt å fremskaffe ABC-materiell og har hatt et ønske om å kunne produsere ABC-våpen. Det finnes også indikasjoner på at al-Qaida tilknyttede personer i USA har vist interesse for sprøytefly ment for landbruket, ikke usannsynlig med tanke på giftspredning. Videre er det kjent at al-Qaida har vist interesse for såkalte "skitne bomber". Slike bomber er enkle å produsere idet de består hovedsakelig av radioaktivt materiale og sprengstoff.

Med utgangspunkt i det skadepotensialet ABC-materiell vil kunne ha, er det viktig at informasjon omkring produksjon, lokalisering, bruk, lagring og transport av slikt materiell omgis av tilfredsstillende sikkerhetstiltak.

4.3.2 Informasjonsoperasjoner

Nasjonal integritet og konstitusjonell handlefrihet kan ikke lenger bare defineres innenfor rammen av et konvensjonelt, territorielt forsvar. Våre politiske og militære beslutningsprosesser integreres stadig tettere i større informasjons- og kommunikasjonssystemer med regionale og globale forgreninger. Tilgang på kritisk, relevant og tidsriktig informasjon utgjør således en stadig viktigere strategisk ressurs. På bakgrunn av dette får begrepet statlig suverenitet en bredere innholdsmessig betydning, som går ut over tradisjonell territoriell integritet. Nasjonal integritet og konstitusjonell handlefrihet berører i økende grad også vår nasjonale evne til å fatte egne beslutninger på et selvstendig, korrekt og tidsriktig informasjonsgrunnlag.

Med utgangspunkt i denne forståelsen av de utfordringer tilliggende fremtidig nasjonal integritet og konstitusjonell handlefrihet, fremstår Informasjonsoperasjoner (INFO OPS) som en betydelig utfordring. Med INFO OPS mener vi her koordinerte tiltak rettet mot å påvirke andre beslutningstakere for å oppnå egne overordnede mål ved å påvirke andres informasjon (fokusert mot utvalgte målgrupper), informasjonsbaserte prosesser og systemer, samtidig som vi utnytter og beskytter egen informasjon, informasjonsbaserte prosesser og systemer. Alternative virkemidler som kan brukes i en koordinert INFO OPS er psykologiske operasjoner, villedning, "Computer network operations", fysisk ødeleggelse og elektronisk krigføring.

Sikkerhetstjenesten må ha et særlig fokus rettet mot den defensive delen av INFO OPS. Sikkerhetsarbeidet må omstille seg i forhold til de teknologiske og samfunnsmessige utviklingstrekk som vil forme vår fremtid. En konsekvens av utviklingen er at en rekke nye aktører nå har reelle muligheter til å påvirke informasjonens integritet, konfidensialitet og tilgjengelighet. Dette gjelder også på felter som defineres som samfunnsvitale, og som er av betydning for evnen til å opptre selvstendig, fatte beslutninger på eget informasjonsgrunnlag og sikre opprettholdelsen av kritiske samfunnsfunksjoner. Ledelse og informasjon, Forsvar, lov og orden, kraft- og vannforsyning, olje og gass, økonomi og kommunikasjon på alle nivåer er bare noen eksempler på viktige sektorer som kan bli berørt av INFO OPS.

For sikkerhetstjenesten vil det særlig være viktig å bevisstgjøre seg hvordan man oppdager og beskytter seg mot motstanderes informasjonsoperasjoner. De sikkerhetsmessige mål må være å motstå eller begrense skadeomfanget av et angrep.

4.3.3 Psykologiske anslag

Psykologiske virkemidler innrettes mot mennesket og kan blant annet ha til hensikt å true, skremme, skape kaos eller gi falske varsel om forestående anslag. Psykologiske trusler kan formidles gjennom telefon, brev, direktekontakt, elektronisk post eller media.

Målgrupper for slike virkemidler kan være hele befolkningen, bestemte befolkningsgrupper, myndighetspersoner med familie, beslutningstakere, profilerte personer med familie og enkeltpersoner. Slike trusler kan komme eksempelvis fra rasjonelle kriminelle, terrorgrupper eller mentalt forstyrrede personer. Det finnes flere eksempler på at psykologiske trusler er blitt rettet mot norsk personell. Ett konkret eksempel er under Kosovo-krisen, der familiemedlemmer til militært personell ble utsatt for grove trusler.

Den forebyggende sikkerhetstjenesten må bistå med å forebygge slike psykologiske anslag. Det er selvsagt viktig å sikre nødvendig skjerming av sikkerhetsgradert informasjon. For virksomhetene vil det også være nødvendig å vurdere å beskytte informasjon som i utgangspunktet ikke er gradert. Dette kan være konkret informasjon om enkeltpersoner som finnes i personellister, lønningslister, beordringslister, vaktlister, adresselister og så videre. I tillegg bør det vurderes hvem som skal eksponeres i media.

5 Sårbarhet og forebyggende sikkerhetstiltak

Den forebyggende sikkerhetstjenesten utgjør en grunnsikring mot de aktører som anses som en trussel mot vår nasjonale sikkerhet. En konsekvens av dette er at den forebyggende sikkerhetstjenesten må kjenne til aktørenes overordnede målsetninger, drivkrefter, kapasiteter og aktiviteter. I tillegg er det avgjørende for utøvelsen av en situasjonstilpasset sikkerhetstjeneste å kjenne til den faktiske trusselaktiviteten som rettes mot norske interesser både i og utenfor Norge. Kjennskap til trusselens aktiviteter, slik som det er beskrevet tidligere i denne vurderingen, er derfor et nødvendig grunnlag for å finne frem til de sikkerhetstiltak vi til enhver tid må ha på plass.

Den forebyggende sikkerhetstjenestens oppgave er mer spesifikt å avdekke hvor egne virksomheter er sårbare. En trusselaktør vil i mange tilfeller gjennomføre en parallell vurdering av hvor våre virksomheter er sårbare. Disse sårbarhetene vil igjen trusselaktøren kunne forsøke å utnytte for å tilegne seg gradert informasjon, eventuelt manipulere eller slette informasjonen. Sikkerhetstjenestens forsøk på å demme opp for trusselaktørers eventuelle kartlegging og utnyttelse av sårbarheter, må nødvendigvis skje gjennom faktiske beskyttelsestiltak. Det heter gjerne at målsettingen med sikkerhetstiltakene er å snu sårbarheter som trusler kan utnytte til motstandsdyktighet. De forebyggende tiltakene er med andre ord sårbarhetsfokuserende.

De forebyggende mottiltak kan, uavhengig av de ulike sikkerhetsfaglige områdene, deles inn i tre kategorier;

- barrierer
- deteksjon
- reaksjon

Når den enkelte virksomhet skal utøve forebyggende sikkerhetstjeneste, er det viktig at det foreligger en forståelse for innholdet i disse kategoriene av tiltak.

5.1.1 Barrierer

Barrierer er her å forstå som de faktiske sikkerhetstiltakene som omgir skjermingsverdig informasjon og objekt. Barrierene skal helst forhindre, eller i hvert fall redusere muligheten for, at trusselaktører kan utnytte våre sårbarheter. Det er vesentlig at de ulike tiltakene er samstemt og utgjør en helhetlig sikring av informasjonen og objekter.

De ulike tiltakene kan videre deles inn i ulike underkategorier. Dette kan være:

- **fysiske** - som f eks gjerder, vegger/dører/vinduer, oppbevaringsenheter, alarmsystemer
- **psykologiske** - som f eks normer, sanksjoner og informasjon

- **personellmessige** – som f eks sikkerhetsklarering og autorisasjon
- **elektroniske** - som f eks strålingshindring, systemtekniske krav
- **logiske** – som f eks kryptologi
- **administrative** – som f eks organisering, rapportering, adgangskontroll og håndteringsprosedyrer, plan- og regelverk, revisjoner og risikohåndtering

Barrierene fastsettes mer spesifikt innenfor de ulike fagområdene innen forebyggende sikkerhet.

5.1.2 Deteksjon

Deteksjon er her å forstå som virksomhetenes fysiske eller elektroniske evne til å avdekke sikkerhetstruende hendelser. Dette kan være egenforskyldt kompromittering av informasjon eller sikkerhetstruende aktivitet fra en trusselaktør. Dette kan eksempelvis omhandle hvilke personer eller metoder en trusselaktør nyttiggjør seg for å forberede eller gjennomføre et anslag.

Dersom et forhold er detektert, vil det gjerne være viktig med en rask og tilpasset reaksjon. Rutiner og prosedyrer for deteksjon reguleres i de ulike forskriftene til sikkerhetsloven.

5.1.3 Reaksjon

Reaksjon er her å forstå som virksomhetens handlemåte etter at kompromittering eller annen sikkerhetstruende virksomhet er avdekket. Reaksjonen kan være av elektronisk, fysisk eller administrativ karakter.

Reaksjonstiltak vil normalt først bli implementert dersom en forhåndsdefinert situasjon oppstår, for eksempel når en trusselaktør forsøker å bryte gjennom fysiske eller elektroniske barrierer, når essensielle funksjoner av betydning for sikkerheten ikke fungerer, eller når det ut fra egen etterretningsinformasjon sannsynliggjøres at et anslag er nært forestående. Reaksjonstiltak må likevel planlegges så godt det lar seg gjøre og øves jevnlig, slik at reaksjonstiden blir så liten som mulig og uforutsette problemer blir avklart.

Reaksjonstiltakene kan for det første innebære at ytterligere barrierer eller skjerpede avdekkingstiltak iverksettes som følge av forsøk på trusselutløsning. Tiltakene kan gå ut på å skjerpe sikkerheten der forsøket ble detektert, eller de kan distribueres ut også i andre virksomheter som kan føles truet. Slike ytterligere tiltak omtales gjerne som beredskapstiltak.

Et vesentlig tiltak under overskriften reaksjon vil være å få oversikt over skaden som har skjedd eller kan ha skjedd i forhold til de verdier som ønskes sikret. Hvor omfattende er skaden, og hvilken karakter har den? Dette vil ofte være vesentlig i forhold til beslutninger om hvilke øvrige tiltak som skal iverksettes.

Rutiner og prosedyrer for reaksjon reguleres i de ulike fagforskriftene til sikkerhetsloven, særlig i Forskrift om sikkerhetsadministrasjon.

6 Særlig om IKT-sikkerhet

Store deler av samfunnet er i økende grad avhengig av informasjons- og kommunikasjonsteknologi (IKT). IKT betegner en bred kategori av teknologier som anvendes for innhenting, lagring, behandling, presentasjon og overføring av informasjon. Utviklingen i de underliggende teknologiene muliggjør stadig nye anvendelser som reiser nye problemstillinger. De sikkerhetsmessige utfordringene knyttes gjerne til begreper som autentisitet, konfidensialitet, integritet, ansvarlighet, tilgjengelighet, pålitelighet, robusthet og styrbarhet.

De fleste samfunnssektorer har gjort seg avhengig av den samme kritiske infrastruktur som igjen er avhengig av IKT-systemer. Med kritisk infrastruktur forstås her eksempelvis kraftforsyning, telekommunikasjon, olje og gass, transport og vannforsyning. Dagens kritiske infrastruktur

kjennetegnes gjennom stor grad av gjensidig avhengighet. Svikt innen kraftforsyningen vil eksempelvis medføre svikt i andre deler av den kritiske infrastrukturen. Dette har igjen medført at samfunnets totale sårbarhet er økt. Disse problemstillingene er mer grundig utredet eksempelvis gjennom "Beskyttelse av samfunnet (BAS)" – prosjektene ved Forsvarets Forskningsinstitutt og Sårbarhetsutvalgets rapport.

Det fremstår som et stadig viktigere strategisk mål å sikre våre IKT-systemer. Nasjonal integritet og konstitusjonell handlefrihet kan ikke lenger bare defineres innenfor rammen av et konvensjonelt territorielt forsvar. Våre politiske og militære beslutningsprosesser integreres stadig tettere inn i regionale og globale informasjons- og kommunikasjonsnettverk. Tilgang på kritisk, relevant og tidsriktig informasjon utgjør således en stadig viktigere strategisk ressurs for et utall statlige så vel som ikke-statlige aktører.

På bakgrunn av dette får begrepet statlig suverenitet en bredere innholdsmessig betydning som går utover tradisjonell territorial integritet. Nasjonal integritet og konstitusjonell handlefrihet berører i økende grad også vår nasjonale evne til å fatte egne beslutninger på et selvstendig, korrekt og tidsriktig informasjonsgrunnlag. IKT-systemene er en kritisk faktor i dette bildet.

For å sikre fremtidig nasjonal integritet og konstitusjonell handlefrihet er det helt vesentlig at vi har evne til å sikre de kritiske IKT-systemene. Dette innbefatter sikring mot både spionasje, sabotasje, terrorisme og kriminalitet. Denne sikringen må igjen omfatte hele spennet fra fred til krise og krig.

Det fremstår derfor som en strategisk utfordring at IKT-sikkerheten nedfelles i nasjonale strategi- og doktrinedokumenter. Strategi- og doktrinedokumenter må igjen følges opp med organisatoriske og teknologiske løsninger som samsvarer med fastlagte mål. Slike løsninger må innebære komplette sikkerhetsløsninger som er underlagt effektiv styring, hvor det er etablerte overvåkings- og responssentre, som er under kontinuerlig sikkerhetstesting og hvor prosess og organisasjon er tilpasset sikkerhetsbehovene.

6.1 Den forebyggende sikkerhetstjenestens rolle

Den forebyggende sikkerhetstjenesten spiller en vesentlig rolle i det nasjonale arbeidet med å sikre IKT-systemer. En viktig oppgave for sikkerhetstjenesten er å beskytte skjermingsverdig informasjon overalt der slik informasjon måtte befinne seg. IKT-systemene hvor gradert informasjon behandles, fremstår derfor som særlig sentrale. De store konsentrasjonene av sikkerhetsgradert informasjon befinner seg i økende grad i IKT-systemer. Graderte IKT-systemer finnes igjen i de fleste virksomheter som har en rolle innen Totalforsvaret.

De graderte systemene er underkastet ulike systemtekniske og administrative sikkerhetskrav. Disse sikkerhetskravene er utarbeidet av NSM og er nedfelt i forskriftene til sikkerhetsloven. Egne veiledninger for gjennomføringen av kravene er laget for å utfylle forskriftene. Enhver virksomhet som har et sikkerhetsgradert IKT-system vil, gjennom å følge de pålagte kravene, oppnå en viktig grunnsikring for sine systemer. I tillegg må den enkelte virksomhet gjennom utøvelse av risikohåndtering løpende vurdere behovet for å implementere ytterligere sikkerhetstiltak utover minimumskravene i forskriftene.

Sikkerhetsstandardene for de graderte IKT-systemene gir ringvirkninger videre utover i samfunnet. De strenge standardene blir ofte helt eller delvis adoptert av virksomheter som ønsker en bedre sikring av ikke-graderte systemer, hvilket bidrar til et sikrere IKT-avhengig samfunn.

Et ytterligere forhold som kan øke den forebyggende sikkerhetstjenestens rolle i det nasjonale IKT-sikkerhetsarbeidet er implementeringen av fagområdet objektsikkerhet. Objektsikkerheten vil trolig omfavne objekter innenfor eksempelvis kritisk infrastruktur med tilhørende IKT-systemer. Dette er ofte systemer som ikke behandler sikkerhetsgradert informasjon, men som er

funksjonskritiske for objektet. Det må her antas at sikkerhetsstandardene som skal sikre systemene som understøtter samfunnskritiske systemer i enkelte tilfeller vil bli skjerpet.

Summen av dette bidrar til at den forebyggende sikkerhetstjenesten gir et vesentlig bidrag for å sikre det digitale Norge.

Det finnes ulike andre ordninger som utfyller NSMs bidrag til IKT-sikkerhetsarbeidet. Ordningen for sertifisering av IT-sikkerhet i produkter og systemer, SERTIT, er et konkret eksempel. Hensikten med denne ordningen er å dekke myndighetenes og industriens behov for en kostnadseffektiv og rasjonell sikkerhetsmessig evaluering og sertifisering av IT-produkter og systemer. IT-produktene og systemer skal evalueres og sertifiseres i henhold til de internasjonale evalueringskriteriene Common Criteria. SERTIT er en del av Nasjonal sikkerhetsmyndighet. Mer informasjon om ordningen finnes på www.sertit.no.

Et annet viktig bidrag i IKT-sikkerhetsarbeidet er prøveordningen Senter for informasjonssikring (SIS) i Trondheim. SIS mottar hendelsesrapporter fra offentlige og private virksomheter og arbeider med å kartlegge trusselbilde mot norske IKT-systemer. (www.norsis.no)

6.2 IKT-sikkerhet – som en del av helhetlig sikkerhetstjeneste

De systemtekniske sikkerhetstiltakene som kreves for IKT-systemene må ses i sammenheng med andre sikkerhetstiltak. En helhetlig sikring av IKT-systemene må derfor innbefatte nødvendige fysiske sikringstiltak som sikrer de rom og bygninger hvor systemene befinner seg. Videre må IKT-systemene omfattes av sikkerhetsadministrative krav. Dette omfatter mellom annet sikkerhetsorganisatoriske krav, krav til kompetanse, krav til rapportering ved sikkerhetsbrudd og/eller sikkerhetstruende hendelser.

Personellsikkerhet inngår som en viktig del også av IKT-sikkerheten. Personellet som har autorisert tilgang til et gradert IKT-system utgjør en sikkerhetsmessig kritisk faktor. Gjennomføring av nødvendig sikkerhetsklarering, gode rutiner for autorisasjon og fastsettelse av tilgangsrettigheter er her viktig.

Sikring mot andre trusler som elektromagnetisk puls, mikrobølgevåpen og tempest-stråling er andre områder som er viktig for IKT-sikkerheten.

6.3 Trusler mot IKT-systemene

Tre ulike trusselkategorier kan nevnes i forhold til IKT-systemer. Dette er ikke en uttømmende beskrivelse av trusselkategoriene. Beskrivelsen gir en ide om noe av særpreget som gjelder for IKT-området. De tre kategoriene betegnes som ondsinnede aktører, ikke-ondsinnede aktører og trusselen fra naturkatastrofer og ulykker.

6.3.1 Ondsinnede aktører

Med ondsinnede aktører menes her individer, grupper, organisasjoner og nasjoner som besitter en intensjon og kapasitet til å utnytte sårbarheter tilliggende IKT-systemer for å oppnå sine målsetninger. Aktiviteter gjennomført av fremmede stater (eks. etterretningstjenesten) vil gjerne være godt forberedt og utføres profesjonelt. I fredstid vil målet helst være å tilegne seg informasjon uten å etterlate spor. I krise/krig kan tilegnet kunnskap om våre IKT-systemer brukes til å manipulere informasjonen og systemenes funksjonalitet, eller påvirke IKT-systemenes tilgjengelighet.

Andre operasjoner kan tenkes utført av terrororganisasjoner. En målsetning vil også her være å skaffe informasjon om våre sårbarheter. Denne informasjonen vil igjen kunne bli brukt i både elektroniske og konvensjonelle terrorangrep. Det er kjent at enkelte terrorgrupper har betydelig IKT-kompetanse og kan allerede ha kapasitet til å gjennomføre angrep mot kritiske IKT-systemer.

Også kriminelle vil kunne angripe våre IKT-systemer. Dette kan resultere i at informasjon kompromitteres eller manipuleres samt at kriminelle kan påvirke systemenes funksjonalitet.

6.3.1.1 Interne trusler

Tradisjonelt har det vært fokusert mye på angrep utenfra, men i praksis viser det seg at angrep gjerne skjer innenfra – og som oftest av legitime brukere. Trusselen går på at brukere forsøker å tilegne seg informasjon de ikke har et tjenestemessig behov for, at de endrer informasjon på en uautorisert måte, påvirker funksjonaliteten til IKT-systemene eller også sletter informasjon. Dette kan være ansatte som av ulike grunner ønsker å skade virksomheten, det kan være nysgjerrige ansatte uten noe egentlig ønske om å forårsake skade, eller det kan være brukere som er blitt vervet av noen av de eksterne trusselaktørene, eller som sympatiserer med dem og handler på eget initiativ. Det vil alltid være et mål for fremmed etterretning å verve folk på innsiden av en virksomhet. Gjennomføring av større, systematiske kompromitteringer lettes, dersom det helt eller delvis gjennomføres av internt personell.

Problemet med interne trusler er bekymringsverdig i lys av hvor hyppig dagens IKT-systemer vokser, den store mengden informasjon som lagres elektronisk og hvor mange nye brukere som daglig kommer til.

6.3.2 Egeneksponering

Sikkerheten i IKT-systemene svekkes også dersom eget sikkerhetsarbeid ikke gjennomføres i henhold til de foreliggende krav. Dette kan dels skyldes at de systemtekniske krav ikke blir implementert, eller at de administrative rutiner ikke blir fulgt. Mangelfull kompetanse og manglende internkontroll er to forhold som bidrar til at IKT-sikkerheten svekkes.

6.3.3 Ulykker og katastrofer

Fysiske og miljømessige belastninger kan påvirke eksistensen og den fysiske tilstanden til IKT-utstyr. Det tenkes her mellom annet på naturkatastrofer, brann, teknisk svikt i utstyr eller menneskelig svikt. På samme måte som for bevisste handlinger kan ulykkeshendelser resultere i kompromitteringer, modifisering eller ødeleggelse av informasjon, eller forstyrrelse eller ødeleggelse av prosesseringen. Generelt er naturkatastrofer eller teknologiske ulykker tilfeldige hendelser som til en viss grad kan bli forutsett gjennom å analysere historiske data av hyppighet og geologiske forhold. Ulykker kan også være iscenesatt med vilje fra en trusselaktør.

Selv om den forebyggende sikkerhetstjenesten hovedsakelig skal forebygge villede hendelser, er det også viktig at trusselen fra ulykker og katastrofer tas hensyn til i det totale sikkerhetsarbeidet.

6.4 Angrepsmåter mot IKT-systemer

Det finnes et utall angrepsmåter som kan påføre våre IKT-systemer skade eller kompromittere informasjonen som sirkulerer inne i systemene. Metoder og verktøy som nyttes i slike angrep prøver gjerne å utnytte foreliggende sårbarheter.

Det er ikke lenger nødvendig med høy kompetanse for å utføre angrep mot IKT-systemer. Detaljerte fremgangsmåter og verktøy kan lastes ned fritt fra Internett. Dette gjør at mulige trusselaktører er mange. Attraktiviteten vil i utgangspunktet kunne øke dersom trusselaktøren avdekker at sikkerhetstiltakene ikke er tilfredsstillende eller at man enkelt kan tilegne seg mye informasjon om et mål. Utnyttelse av foreliggende sårbarheter til informasjonssystemer vil kunne gi rask og gjerne fordekt tilgang til store mengder informasjon. Tilgang til systemene vil, foruten selve innsynet i informasjonen, åpne muligheten til å endre eller gjøre informasjonen utilgjengelig for brukerne. Angriperen vil også prøve å slette flest mulige spor av sine handlinger for å skjule skadeomfanget og forhindre en effektiv etterforskning.

Nedenfor listes et utvalg av aktuelle angrepsmåter, uten at opplistingen er utfyllende.

6.4.1 Tjenestenekt

Gjennom bruk av tjenestenekt-programmer (Denial of Service) vil tilgjengeligheten til informasjon og IKT-systemer forhindres. Programmene kan bruke opp ressursene (linjekapasitet, prosessorkraft, minne etc.) til et system eller sørge for at brukerne av systemet ikke oppnår kontakt (ruting/DNS-manipulering). Slike angrep kan være meget vanskelig å beskytte seg mot uten at legitime brukere av systemet påvirkes.

Det finnes også distribuerte versjoner av dette angrepet (DDoS) hvor angrepet utføres fra mange forskjellige datamaskiner rundt om i verden, uten at informasjonssystemenes eiere er klar over det. Måten dette kan gjøres på er at angriperen i forkant av angrepet installerer ondsinnet kode på et utall maskiner (vha. virus e.l.), og så kommanderer de infiserte maskinene til å starte angrep mot et gitt system på et bestemt tidspunkt. Det var et slikt angrep de 13 DNS root serverne (som kontrollerer Internett) ble utsatt for i oktober 2002. Da var det hundrevis av infiserte PC'er rundt om i verden som i en time bombarderte serverne med så mye data at kun fire av dem var i stand til å utføre jobben sin. Dette var altså et angrep mot Internett.

Typisk har tjenestenekt-angrepene hatt til hensikt å sørge for at den som er under angrep mister tilgangen til Internett (eMail, Web etc.). I tillegg kan slike angrep tenkes utført mot systemer som støtter opp om kritiske nasjonale infrastrukturer; systemer som ikke er designet for å være nede over lengre tid. Tap av strømforsyning vil eksempelvis kunne ha katastrofal innvirkning på medisinske eller andre kritiske tjenester. Angrep kan også komme mot andre IKT-systemer innen kritisk infrastruktur.

6.4.2 Misbruk av andres IKT-utstyr

Ulike IKT-ressurser kan misbrukes uten at brukerne er klar over det. Dette kan omfatte misbruk av andres telefonlinjer. Ved å angripe IKT-systemer via andres utstyr er sjansen for å bli tatt liten ettersom egne spor lettere kan skjules. Misbruk av andres IKT-ressurser kan også ha som motiv å utnytte andres prosessorkraft til knekking av kryptokoder.

Det er særlig informasjonssystemer som enten er koblet på Internett ved hjelp av bredbånd, eller som står i et online-nettverk, som misbrukes.

Det kan tenkes at trusselaktører etter hvert forsøker å rette seg mot andre typer IKT-ressurser, også sikkerhetsgraderte.

6.4.3 Avlytting av datatrafikk og bruk

Dette er en angrepsform hvor brukerens aktiviteter og kommunikasjon overvåkes av utenforstående. Det mest vanlige er å installere små programmer på de systemene som ønskes avlyttet. Dette kan være programmer som i utgangspunktet er lovlige og som er ment brukt av systemadministratorer, eller det kan være programmer som er utviklet med den hensikt å drive ulovlig aktivitet. Fysiske komponenter som for eksempel lytter på tastaturledningen eller på nettverket kan også installeres.

6.4.4 Virus/ormer

Dette er en kategori ondsinnet programvare som er velkjent. Dersom IKT-systemer infiseres av virus eller ormer vil dette kunne medføre sletting av store mengder data. Videre kan infiserte informasjonssystemer bli instruert til å utføre definerte operasjoner som for eksempel videresending av epost til alle i adresseboken, eller åpning av en bakdør som trusselaktører senere kan benytte til innbrudd. Viruset eller ormer er svært ofte i stand til å spre seg videre til andre maskiner i et informasjonssystem.

Stadig utvikling av nye typer virus eller ormer gjør det utfordrende å bekjempe disse ondsinnede programmene.

6.5 Sårbarheter innen IKT

Kjennskap til aktuelle og fremtidige trusler er avgjørende for å utforme forebyggende tiltak samt planlegge mottiltak dersom trusselen materialiserer seg. Dessverre er det i praksis umulig å forutse alle tenkelige trusler. Derfor bør det heller fokuseres på sårbarheter. Nedenfor er det omtalt noen sårbarheter som er fremtredende i eksisterende IKT-systemer som håndterer sikkerhetsgradert informasjon.

6.5.1 Totalløsninger

Enterprise-teknologi som sikter mot helhetlige og tett integrerte totalløsninger for virksomhetenes IKT-systemer blir stadig mer utbredt. Dagens situasjon er at eksisterende systemer har hatt en begrenset fokus på enterprise-sikkerhet som følge av rask teknologisk utvikling, hyppig utrullingstakt, kraftig vekst i omfang samt stadige organisasjonsendringer. Kostnadsspørsmålet har også vært viktig, for det er til dels vanskelig å begrunne satsning på sikkerhet i et kortsiktig økonomisk perspektiv. Sikkerhet har dermed blitt noe man ofte har implementert til slutt i systemutviklingsprosjektene – og helst på de områder hvor det ikke har medført for mye kompleksitet eller tatt for mye tid.

Det har ikke vært prioritert å tenke sikkerhet gjennom hele livssyklusen til prosjektet. Dette har ført til at anerkjente prinsipper for sikkerhetsdesign (overvåking, konfigurasjonsstyring, administrasjon, nettverks- og perimetersikring og sikkerhetstesting) bare i liten grad følges av prosjektene når systemene designes, og de organisasjons- og prosessrelaterte forbedringene det ofte er behov for har vært vanskelig å få gjennomslag for. Dermed har det også vært begrenset hva man har vært i stand til å implementere av sikkerhet i etterkant, og sikkerhetsmessig drift av systemet har fått kompliserte forhold å fungere under. Systemets operative data har også blitt strukturert og organisert på en måte som ikke understøtter sikker administrasjon og drift. Det finnes heller ingen gode rutiner for en sikkerhetsmessig forsvarlig måte å avvikle systemet på når det skal erstattes eller fjernes. Bare en omfattende og strukturert risikovurdering av de faktiske systemer vil kunne gi nødvendig oversikt over og innsikt i sårbarhetene.

6.5.2 Kosteffektivisering

Skjerpede økonomiske krav til kostnadseffektivitet har ført til utstrakt bruk av sikkerhetsprodukter som fås kjøpt i butikken (hyllevare). Dette er produkter man har sterkt varierende kontroll med, og hvor bruken derfor medfører en viss grad av risiko. Risikoen kommer i form av muligheter for skjulte feil, manglende forståelse for hvordan produktet skal brukes eller ved at det med viten og vilje er lagt inn sikkerhetshull (bakdører) beregnet for angrep.

Den raske teknologiutviklingen gjør at produsentene går på akkord med kvaliteten på programvareproduktene sine og derfor oppdages det også stadig vekk nye sikkerhetshull. Det er en kontinuerlig konkurranse mellom hackere og programvareprodusenter om først å oppdage disse feilene for så å utnytte versus reparere dem. Enkelte av produktene gjennomgår en selvpålagt eller offentlig pålagt sertifisering – noe som gir god gevinst – men mange produkter faller også utenfor.

6.5.3 Hjemmeløsninger

Flere og flere gis i dag muligheten til å jobbe hjemmefra ved av man tillater oppkobling av hjemme-PC mot virksomhetenes informasjonssystemer. Dette er hjemme-PC'er som ofte er langt mindre sikre enn datamaskiner i virksomhetenes nettverk – og som svært ofte også kobles opp mot Internett. Når virksomheten velger å stole på brukeren av denne PC'en, og gi tilgang til kritiske deler av IKT-systemet, har man introdusert en bakdør. En såkalt VPN-forbindelse (kryptering av data) mellom hjemme-PC'en og virksomhetenes datanettverk vil ikke gi noen

beskyttelse mot at en trusselaktør kan kompromittere hjemme-PC'en og benytte denne for å få tilgang til virksomhetens IKT-systemer, og få samme tilgangsrettigheter som en intern bruker.

6.5.4 Mobile enheter

Økende bruk av mobile enheter (PDA'er, bærbare PC'er, mobiltelefoner etc.) har introdusert nye sårbarheter i form av økt distribusjon av store mengder informasjon utenfor virksomhetenes kontroll, og lagring av informasjon på enheter som lett kommer på avveie i form av tap eller at de blir stjålet. Kopier av kalender på mobiltelefonen eller på PDA'en, kan innholde informasjon av interesse for en trusselaktør.

Et annet moment er at slike mobile enheter ofte ikke beskyttes med brannmurer, krypteringsprogramvare, antivirusprodukter og lignende sikkerhetsprogramvare slik som stasjonært utstyr. Det gjør at disse enhetene er mye enklere å kompromittere og at de er perfekte overføringsmekanismer for ondsinnet programvare. Disse enhetene blir også i økende grad koblet direkte mot virksomhetenes nettverk, og dette foregår ofte trådløst noe som gjør det vanskelige å kontrollere. Dermed har man introdusert ytterligere nye svake ledd i IKT-systemet.

6.6 Sikkerhetsmessige utfordringer tilknyttet IKT

6.6.1 Generelle utfordringer

Rask teknologisk utvikling, stor spredning av IKT-systemer, økt tilgjengelighet av sofistikerte redskaper, samt mangel på utviklede og implementerte sikkerhetsmekanismer, gjør at både graderte informasjonssystemer og støttesystemer er sårbare.

6.6.2 Særlige utfordringer for den forebyggende sikkerhetstjenesten

Den forebyggende sikkerhetstjenesten står overfor en viktig utfordring for å finne frem til sikre løsninger for graderte IKT-systemer, og systemer som understøtter samfunnskritiske objekter. Denne prosessen vil innebære et samarbeid mellom sentrale aktører samt utvikling av strategier og sikkerhetstiltak med fokus på elementer som autentisitet, konfidensialitet, integritet, ansvarlighet, tilgjengelighet, pålitelighet, robusthet og styrbarhet. Det er altså ikke lenger bare tradisjonell konfidensialitetssikring som er av betydning. Nedenfor listes det opp de viktigste tiltakene for at de nevnte elementene skal falle på plass.

6.6.2.1 Krypto

Krypto har tradisjonelt vært benyttet for å sikre konfidensialiteten til informasjon under transmisjon. Dagens krypto beskytter i tillegg informasjonens integritet. Krypto blir tatt i bruk på en rekke nye områder, herunder sikring av lagret informasjon, etablering av need-to-know prinsippet, autentisering, integritet, samt sikring av drift og vedlikeholdsinformasjon.

Norge har i dag en fremtredende posisjon når det gjelder utvikling av krypteringsalgoritmer og utstyr for konfidensialitetssikring av kommunikasjon. Ved fortsatt å utvikle egne krypto-produkter trenger vi ikke benytte og stole på produkter fra andre nasjoner. Om det skulle komme til en internasjonal konflikt ville det vært vanskelig å fortsatt benytte for eksempel krypteringsalgoritmer fra ikke-vennlige nasjoner. Vi har i dag derfor full kontroll med egen konfidensialitet.

Samtidig blir kryptering i dag stadig med utbredt i IKT-systemer, og ikke lenger bare for kommunikasjonssikring. Dette gir nye utfordringer som må møtes om Norge skal opprettholde sin posisjon. Kryptoutstyr vil, på linje med andre IKT-komponenter, være utsatt for angrep. Det kan være mot kryptoalgoritmen og kan bestå i å utnytte svakheter ved beskyttelse av nøkkelmateriell, eller ved å omgå kryptomekanismene. Programvarekryptering blir stadig mer vanlig. Det fører til at nøkkelmateriell, i en eller annen form, vil være tilgjengelig på IKT-systemene. Det vil derfor være attraktivt å angripe IKT-systemene med det formål å tilegne seg nøkkelmateriell, for så å kunne dekryptere transmittert eller lagret informasjon.

6.6.2.2 PKI (public key infrastructure)

Etablering av elektronisk identifisering, signering og kryptering av IKT-kommunikasjon vil være avgjørende for å kunne ha tillit til informasjonen i IKT-systemene, samt sikre at informasjonen kun er tilgjengelig for autorisert personell. PKI er en fundamental teknikk for sikker tilgangskontroll i store nettverk med tildels uoversiktlig brukermasse og sikrer elektronisk informasjon samme juridiske gyldighet som tradisjonelle dokumenter, samt nøkkelutveksling for tradisjonelt kryptoutstyr.

6.6.2.3 Konfigurasjonsstyring

Den raske teknologiske utviklingen, samt behov for hyppige endringer, krever en effektiv kontroll med utrulling, oppdateringer og avvikling av systemkomponenter for å sikre kontrollen over systemene. Konfigurasjonsstyringen vil også gi verdifull input til systemovervåkingen.

6.6.2.4 Katalogtjeneste og systemadministrasjon

Per i dag struktureres systemenes "operative" data (brukerkonti, brukergrupper, andre systemdata) på en måte som ikke understøtter sikker administrasjon og drift. Kvaliteten på disse dataene er kritisk for styrbarheten til systemet.

6.6.2.5 Perimeter- og nettverkssikkerhet

Det må etableres sikkerhetsbarrierer som hindrer inntrengning og som kontrollerer informasjonsflyt i ytre soner mot NATO og i interne sikkerhetssoner. En effektiv sektor/soneinndeling for å etablere forsvar i dybden, inklusive mekanismer for kommunikasjon på tvers av ulike sikkerhetsgraderingeringer, blir viktig. Hva som gjelder av sikkerhetstiltak overfor eksterne brukere må også gjelde for interne brukere. Som tidligere nevnt kommer de fleste angrepene fra innsiden og perimetersikring alene vil derfor ikke være nok. Inntregningsforsøk og ulovlig bruk av nettverkstjenester må oppdages og det må etableres et robust stamnett.

6.6.2.6 Sikkerhetstesting

For å kunne avdekke svakheter i eksisterende IKT-systemer må det etableres både sikkerhetsverifikasjon og inntrengningstesting. Sikkerhetsverifikasjonen må gjøres på kontinuerlig basis og skal vurdere om sikkerheten er ivaretatt i forhold til gitte profiler. Inntrengningstestingen vil utføres mer ad-hoc og vil søke etter svakheter i produkter eller løsninger som kan gi ikke-autorisert tilgang til systemet. Det er like viktig å teste ut IKT-systemer under for eksempel øvelser, som det er å teste personell, materiell og rutiner.

6.6.2.7 Sertifisering

For å holde kontroll med kritiske IKT-systemer som utvikles både i det sivile og i Forsvaret er det behov for en uhildet evaluering av systemsikkerheten utført av en nøytral faginstans som tar sikte på å avdekke eventuelle feil og mangler. Evalueringen bør lede frem til en sertifisering - helst basert på internasjonale kriterier (Common Criteria). Det bør nevnes at kryptoutstyr innholder funksjoner som ikke på en tilfredsstillende måte er dekket av Common Criteria-sertifisering, og må derfor gjennomgå tilleggsevaluering og testing. NSM forestår i dag sertifisering av kryptoutstyr som skal beskytte informasjon gradert etter sikkerhetsloven. I dagens samfunn der produktivitet og lønnsomhet står sentralt og representerer et være eller ikke være for virksomhetene, er det en nødvendighet å kunne velge blant tillitvekkende løsninger. Sertifisering gir tillit. En sertifisering vil lette beslutningsprosessen for anskaffer, redusere behovet for egne evalueringer og gi trygghet om at løsningen holder et gitt tillitsnivå.

6.6.2.8 Bruk av hyllevareprodukter

En annen viktig sikkerhetsmessig utfordring er den økte bruken av hyllevareprodukter. Økt bruk av hyllevareprodukter gjør det nødvendig å bygge opp kompetanse omkring de

sikkerhetsmessige løsningene for disse produktene. Kompetansen er viktig både når det gjelder evaluering av produktene og når det gjelder implementasjon, enten det er som frittstående komponenter eller om de er integrert med andre produkter. Ikke minst er dette viktig i store innformasjonssystemer. På grunn av den raske videreutviklingen av disse hyllevareproduktene må kompetansen oppdateres kontinuerlig. Evaluering, bruk og integrasjon av hyllevareprodukter må derfor ses på som en viktig FoU-aktivitet.

6.6.2.9 Hjemmekontor

Økt bruk av hjemmekontor hvor man kobler seg opp via Internett, eller gjennom direkte oppringt forbindelse, vil tvinge seg frem på mange arbeidsplasser. Utfordringen blir å sørge for at hjemme PC'en ikke kan kompromitteres slik at den blir en bakdør inn i virksomhetenes IKT-systemer, samtidig som implementasjon av sikkerheten ikke skal være noe brukeren trenger å forholde seg til. Helst bør det være usynlig for brukeren. En slik tilnærming vil stille store krav til både systemarkitekter, programleverandører og tjenestetilbydere.

7 Ulike fagområder innen forebyggende sikkerhetstjeneste

Den forebyggende sikkerhetstjenesten er inndelt i ulike fagområder. I dette kapitlet gis det en presentasjon av de aktuelle fagområdene.

7.1 Sikkerhetsadministrasjon

Gjennom utøvelse av forebyggende sikkerhetstjeneste skal skjermingsverdig informasjon gis beskyttelse gjennom hele livssyklusen. Beskyttelsestiltakene tar utgangspunkt i de ulike fagområdene. For å sikre en helhetlig utøvelse av sikkerhetstjenesten er det imidlertid viktig med en overordnet tilnærming som ser de fagspesifikke tiltakene i sammenheng. Sikkerheten må med andre ord bli koordinert på tvers av de respektive fagområdene. Dette sikres gjennom utøvelse av sikkerhetsadministrasjon. Hvordan sikkerhetsadministrasjonen skal utøves, er fastlagt gjennom en egen forskrift til sikkerhetsloven.

NSM anser utøvelse av en systematisk sikkerhetsadministrasjon som helt nødvendig for å kunne gjennomføre en tilfredsstillende sikkerhetstjeneste. På mange måter er utøvelse av sikkerhetsadministrasjon ledelsens mulighet til å ha oversikt over og styring med egen sikkerhetstjeneste. Gjennom utøvelse av sikkerhetsadministrasjon skal ledelsen mellom annet sørge for at det etableres en lokal, koordinerende og tilsynsførende sikkerhetsorganisasjon innen virksomheten.

Forskrift om sikkerhetsadministrasjon underbygger lovens bestemmelser om ansvarsforhold. Mellom annet slås det fast at det er virksomhetens leder som har det overordnede ansvar for alle sider av sikkerheten innen sin virksomhet, herunder ansvar for at det avsettes tilstrekkelig med ressurser til sikkerhetsarbeidet.

7.2 Dokumentsikkerhet

Innen den forebyggende sikkerhetstjenesten forstås et dokument som en logisk avgrenset informasjonsmengde som er lagret på et medium for senere lesing, lytting, fremføring eller overføring. Med andre ord medregnes her både elektroniske lagringsmedia, papirdokumenter, film, lydbånd, bilder og tegninger. Alle disse ulike typene av dokumenter skal sikkerhetsgraderes dersom de inneholder informasjon som er av betydning for rikets sikkerhet eller andre vitale, nasjonale sikkerhetsinteresser.

Gjennom fagområdet dokumentsikkerhet, fastsettes ulike rutiner og prosedyrer for hvordan de ulike dokumentene skal håndteres. Kategorier av rutiner og prosedyrer innen dokumentsikkerhet er merking av sikkerhetsgrad, journalføring, forsendelse, intern ombringelse, medbringelse på reise, utlån, mangfoldiggjøring, spredning, tilintetgjøring, evakuering og rekonstruksjon. Regelverket er til for å sikre en mest mulig forsvarlig håndtering av sikkerhetsgradert

informasjon. Brudd på regelverket kan føre til eksponering av informasjonen, som igjen kan resultere i at informasjon kompromitteres, altså at den blir kjent for uautorisert personell.

7.3 Fysisk sikkerhet

Sikkerhetsgradert informasjon skal alltid være omsluttet av fysiske sikkerhetstiltak. Dette innebærer at fysiske sikringstiltak skal være implementert overalt der sikkerhetsgradert informasjon befinner seg. Slik sett utfyller de fysiske sikkerhetstiltakene de øvrige sikkerhetsfagene, idet skjermingsverdige dokumenter, skjermingsverdig IKT-utstyr, lokaler godkjent for gradert muntlig kommunikasjon skal gis beskyttelse gjennom fysiske tiltak. Med andre ord skal bygninger eller områder der det manuelt eller elektronisk behandles sikkerhetsgradert informasjon i materiell eller immateriell form være fysisk sikret.

Den fysiske sikkerheten inndeles i administrative, mekaniske og elektroniske tiltak. Det er samspillet mellom tiltak fra disse kategoriene som igjen utgjør den samlede fysiske sikringen.

De administrative tiltakene kan eksemplifiseres gjennom definering av kontrollert, beskyttet eller sperret området, og påfølgende autorisering av tilgangsrettigheter for personell. Et annet viktig administrativt tiltak er nøkkeladministrasjon.

De mekaniske tiltakene er eksempelvis tradisjonelle låser, gjerder og oppbevaringsenheter for informasjon.

De elektroniske sikringstiltakene kan eksemplifiseres gjennom overvåkingskameraer, alarmsystemer og elektronisk innpasseringsportaler.

Fysisk sikkerhet er også særlig viktig i sikringen av ulikt materiell som eksempelvis våpen og annet farlig materiell. Videre utgjør fysisk sikkerhet et viktig fagområde innen objektsikkerhet.

7.4 Administrativ kryptosikkerhet

Kryptografi er beskyttelse av informasjon ved å gjøre den ugjenkjennelig for andre enn adressaten. I dag blir dette som oftest gjort elektronisk ved at man i et kryptoapparat blander klartekst med en kryptonøkkel. En forutsetning for tilgang til informasjonen er at man har samme nøkkel og maskin.

All elektronisk overføring av sikkerhetsgradert informasjon skal beskyttes av godkjente kryptosystemer. Denne godkjenningen er det NSM som foretar. Administrativ kryptosikkerhet er de rammene en har rundt kryptosystemet for å sikre at kryptomaskiner og nøkkel materiell ikke kommer uvedkommende i hende. Disse rammene er i korte trekk kvalifisert personell, kontroll, instrukser, rutiner og fysisk sikring.

7.5 Tekniske sikkerhetsundersøkelser

Steder hvor sikkerhetsgradert informasjon kommuniseres, utgjør uten etablerte sikringstiltak en betydelig sårbarhet. Gjennom tekniske sikkerhetsundersøkelser (TSU) er målsetningen å avsløre illegalt avlyttings- eller avtittingsutstyr. Videre er målsetningen å påvise svakheter i bygningskonstruksjoner, installasjoner og fysisk sikring som bidrar til å øke faren for avtitting eller avlytting av tale eller avlesing av elektroniske signaler.

Gjennom avdekking av svakheter kan så nødvendige forholdsregler iverksettes. Selve gjennomføringen av TSU skal i henhold til sikkerhetsloven foretas av NSM, eller den NSM bemyndiger.

Det finnes et antall permanent sikrede rom både i Forsvaret og den sivile del av statsforvaltningen. Dette er rom der det er foretatt akustiske og kontrollmessige tiltak. Disse rommene blir jevnlig undersøkt av TSU-personell. Videre avholdes det ofte graderte møter utenfor kontrollert område. Ved møter hvor informasjonen som skal diskuteres er

KONFIDENSIELT eller høyere, skal møtelokale og dets omgivelser på forhånd godkjennes av TSU-personell.

I forbindelse med prosjektering av nybygg hvor sikkerhetsgradert informasjon skal kommuniseres, er det viktig at TSU-personell ved NSM rådspørres i en så tidlig fase av prosjektet som mulig.

7.6 Elektromagnetisk stråling – tempest

Aktører med ressurser og kompetanse vil kunne få tilgang til sikkerhetsgradert informasjon ved analyse av elektromagnetisk stråling fra et informasjonssystem. Muligheten for en slik analyse vil være avhengig av hvor nært og hvor lenge en avlytter kan etablere seg ved en installasjon. Avhengig av type signaler som kan analyseres, kan deler av eller hele den sikkerhetsgraderte informasjonen gjenskapes.

Sikkerhetsfaget som skal forebygge kompromittering av skjermingsverdig informasjon gjennom avlesning av elektromagnetisk stråling, kalles TEMPEST. Sårbarhet kan reduseres ved å fastsette tiltak som bidrar til å redusere utstyrets eller systemets utstråling. Et eksempel på tiltak kan være at utstyret gjennomgår en TEMPEST-risikovurdering.

7.7 Informasjonssystemsikkerhet

Etablering av sikre informasjonssystemer fremstår som en betydelig utfordring for den forebyggende sikkerhetstjenesten. Årsaken til dette er at sikkerhetsgradert informasjon som utstedes, lagres og behandles hovedsakelig skjer elektronisk i informasjonssystemer. De store konsentrasjonene av gradert informasjon gir økt sårbarhet gjennom at skadepotensialet ved kompromitteringer er svært stort.

Et informasjonssystem defineres i sikkerhetsloven som *en organisert samling av periferutrustning, programvare, datamaskiner og kommunikasjonsnett som knytter dem sammen.* Periferutrustning innbefatter alle tilkoplede komponenter så som kopimaskiner, skrivere og skannere. Datamaskiner er servere, arbeidsstasjoner, bærbare PCer, og CD-rom og PDAer (Personell Digital Assistent)/lomme-PC-er som koples til nettet. I selve kommunikasjonsnettet inngår komponenter som switcher, rutere, brannmurer, linjer og fibernett. Programvare er gjerne kommersiell hyllevare.

Systemene blir stadig mer komplekse og kobles ofte sammen i større nettverk, noe som medfører at man kan få tilgang til svært mye informasjon fra en enkelt arbeidsstasjon. Når det gjelder sikkerhetsgradert informasjon er det derfor vesentlig å sørge for mekanismer og rutiner som sikrer at den enkelte kun får adgang til den informasjonen vedkommende er sikkerhetsklarert og autorisert for.

Forskrift om informasjonssikkerhet stiller krav til informasjonssystemene for å sikre tilgjengelighet, integritet og konfidensialitet til skjermingsverdig informasjon. En obligatorisk godkjenningsprosess skal sikre at alle relevante forhold for sikkerheten i og rundt et informasjonssystem blir gjennomgått og vurdert individuelt. Godkjenningen gjennomføres av den enkelte virksomhet, NSM, eller den NSM utpeker. Hvem som tillegges godkjenningsmyndighet i det enkelte tilfellet, bestemmes av systemets sikkerhetsgrad og kompleksitet. Kravene til sikkerhetsdokumentasjon vil være de samme uavhengig av hvem som er godkjenningsmyndighet.

7.8 Sikkerhetsgraderte anskaffelser

Sikkerhetsgradert informasjon, som utleveres til leverandører, skal beskyttes gjennom hele livssyklusen. For å ivareta sikkerheten hos leverandørene, har en fastsatt tiltak gjennom en egen forskrift i sikkerhetsloven. Denne forskriften er tilpasset private virksomheter, men det er viktig

å poengtere at leverandørene i tillegg er underlagt de andre forskriftene i sikkerhetsloven. Grunnprinsippet for å beskytte sikkerhetsgradert informasjon er likt for alle.

Før en leverandør kan motta sikkerhetsgradert informasjon (KONFIDENSIELT eller høyere) skal en leverandørklarering foreligge og sikkerhetsavtale skal være inngått mellom anskaffende myndighet og leverandør. På BEGRENSET nivå skal sikkerhetsavtale være inngått.

Inspeksjon, minst hver 18. måned hos leverandør med leverandørklarering, avdekker ulike mangler knyttet til etterlevelse av bestemmelsene i sikkerhetsloven med forskrifter.

7.9 Personellsikkerhet

En forsvarlig og troverdig personellsikkerhetstjeneste må ligge til grunn i alle prosesser hvor skjermingsverdig informasjon blir behandlet. Personellsikkerhetstjenestens oppgave er å hindre at personer som utgjør eller vil kunne utgjøre en sikkerhetsrisiko, plasseres slik at risikoen aktualiseres. Denne oppgaven søkes løst gjennom forskjellige tiltak, og da særlig tiltak rettet mot personer som skal gis lovlig tilgang til skjermingsverdig informasjon. De personellsikkerhetsmessige tiltak er gjenstand for relativt detaljert regulering i sikkerhetsloven og personellsikkerhetsforskriften.

Sikkerhetsklarering og autorisasjon er i denne sammenheng sentrale tiltak. Alt personell som skal gis tilgang til skjermingsverdig informasjon må på forhånd autoriseres etter bestemte regler. For personell som skal ha tilgang til skjermingsverdige opplysninger med høyere gradering enn BEGRENSET kreves i tillegg sikkerhetsklarering. Sikkerhetsklarering gis for forskjellige sikkerhetsgrader, og er basert på undersøkelser omkring den enkelte, såkalt personkontroll.

Tatt i betraktning at det er rikets eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser som står på spill, og at store skadevirkninger kan oppstå som følge av sikkerhets- og taushetsbrudd, må det legges stor vekt på den grunnleggende forutsetning at det bare er personer man fullt ut kan stole på, som kan gis sikkerhetsklarering. Sikkerhetsklarering kan bare gis eller opprettholdes dersom det ikke er rimelig tvil om vedkommendes sikkerhetsmessige skikkethet. Ingen har krav på sikkerhetsklarering, og sikkerhetsklarering kan nektes før det foreligger en formodning om at vedkommende representer en aktuell sikkerhetsrisiko. Her kommer personellsikkerhetstjenestens forebyggende karakter klart frem.

Ved vurdering av en persons sikkerhetsmessige skikkethet skal det bare legges vekt på forhold som er relevante for å vurdere vedkommendes pålitelighet, lojalitet og sunne dømmekraft i forhold til behandling av skjermingsverdig informasjon. Forhold som kan tillegges betydning i denne sammenheng fremgår av sikkerhetsloven § 21, og omfatter bl.a. straffbare handlinger, rusmisbruk, økonomiske forhold og forbindelse med organisasjoner som anser vold eller terrorhandlinger som akseptabelt. Klareringsavgjørelsen skal baseres på en konkret og individuell helhetsvurdering av de foreliggende opplysninger.

Den generelle utviklingen innenfor fagområdet, hvor bl.a. kravet til individuell behandling er fremtredende, har medført at vurderingskriteriene har blitt mindre håndfaste og mer skjønnsmessige. Dette forholdet aktualiserer behovet for en god sikkerhetsmessig oppfølging av den som klareres og et kompetent sikkerhetsmiljø ved både de autoriserende myndigheter og ved klareringsmyndighetene.

Mange av de sikkerhetstiltakene bedrifter, organisasjoner eller offentlige etater iverksetter er rettet mot en ekstern trussel. Den interne trussel, som personellsikkerheten forsøker å motvirke, er ikke like opplagt og blir ofte ikke prioritert i nødvendig grad.

8 Avslutning

I denne risikovurderingen har NSM forsøkt å beskrive sentrale forhold innen det nasjonale sikkerhetsbilde. Dette er gjort innenfor rammen av NSM sitt ansvarsområde. Forebyggende sikkerhetstjeneste omfatter i Norge alle tiltak som iverksettes for å sikre skjermingsverdig informasjon og skjermingsverdige objekter mot sikkerhetstruende virksomhet (spionasje, sabotasje og terrorhandlinger). Den samlede nasjonale forebyggende sikkerhetstjenesten omfatter fagmyndigheten NSM i tillegg til alle virksomheter i den offentlige forvaltning og Forsvaret som håndterer skjermingsverdig informasjon eller eier, eventuelt kontrollerer, skjermingsverdige objekter. Næringslivet er også en del av den samlede nasjonale forebyggende sikkerhetstjenesten for eksempel som leverandører av varer eller tjenester til det offentlige i forbindelse med sikkerhetsgraderte anskaffelser, eller dersom private virksomheter eier, eventuelt kontrollerer, skjermingsverdige objekter eller håndterer sikkerhetsgradert informasjon.

Denne risikovurderingen er den første som er utformet av NSM. Ambisjonsnivået for vurderingen har vært å se sammenhengen mellom trusselen, sårbarhets- og verdivurderingsaspektet. Denne tilnærmingen er nødvendig for å dekke det brede fokuset den forebyggende sikkerhetstjenesten må ha i sitt arbeid.

Nasjonal sikkerhetsmyndighet har, gjennom inspeksjoner, dialog med virksomheter og på andre måter, avdekket ulike former for sikkerhetsmangler. Det er grunn til å påpeke at dersom reglene i sikkerhetsloven følges, gir dette en grunnsikring mot sikkerhetstruende hendelser som terrorisme, spionasje og sabotasje. Dagens trusselbilde er både diffust og skiftende slik at det er viktig å rette fokus mot en god grunnsikring, idet en innser at det sjelden vil være mulig å ha en fullstendig oversikt over trusselbildet. NSMs anbefaling er derfor at sikkerhetslovens regler følges opp i større grad enn det som synes å ha vært tilfelle hittil.

9 Begrep og definisjoner

Anskaffelsesmyndighet

-Et forvaltningsorgan som har til hensikt å anskaffe, eller har anskaffet, varer eller tjenester fra rettssubjekt som ikke er forvaltningsorgan. (Sikkerhetsloven §3 pkt. 13)

Asymmetrisk aktør

-Utviklingen i verdenssamfunnet har ført til at store, konvensjonelt utrustede, militære avdelinger stort sett ikke kriger mot hverandre lenger. Trusselen kommer i dag i større grad fra enheter og organisasjoner som ikke kan utfordre den militære styrken til statsmaktene. Det er altså et asymmetrisk forhold mellom statsmaktene og slike enheter og organisasjoner. På bakgrunn av dette tar de asymmetriske aktørene andre midler i bruk for å kjempe for sin sak (f eks bruk av terrorhandlinger).

Autorisasjon

-Avgjørelse, foretatt av autorisasjonsansvarlig, om at en person etter forutgående sikkerhetsklarering (med unntak for tilgang til informasjon sikkerhetsgradert BEGRENSET), bedømmelse av kunnskap om sikkerhetsbestemmelser, tjenstlig behov samt avlagt skriftlig taushetsløfte, gis tilgang til informasjon med angitt sikkerhetsgrad. (Sikkerhetsloven §3 pkt. 17)

Dokument

-En logisk avgrenset informasjonsmengde som er lagret på et medium for senere lesing, lytting, fremføring eller overføring. (Forskrift om informasjonssikkerhet §1-2 pkt. 1)

Grunnsikring

-De forebyggende sikkerhetstiltak som, i henhold til sikkerhetsloven, skal være implementert hos de ulike virksomheter.

Informasjon

- Enhver form for opplysninger i materiell eller immateriell form. (Sikkerhetsloven §3 pkt. 7)

Informasjonssystem

- En organisert samling av periferutrustning, programvare, datamaskiner og kommunikasjonsnett som knytter dem sammen. (Sikkerhetsloven §3 pkt. 10)

Integritet	-Informasjon og objekters nøyaktighet og fullstendighet, samt pålitelighet av transaksjoner.
Intensjon	-Personers eller organisasjoners vilje og motivasjon til å realisere en trussel.
Kapasitet	-De ressurser og den kompetanse som er nødvendig for å realisere en trussel.
Kompromittering	-Tap eller mistanke om tap av konfidensialitet, integritet eller tilgjengelighet for skjermingsverdig informasjon, herunder uønsket avhending, modifisering eller ødeleggelse. (Forskrift om sikkerhetsadministrasjon §1-2 pkt. 3)
Konfidensialitet	-Det forhold at informasjon ikke er tilgjengelig for uautoriserte personer eller ikke-godkjente systemer.
Kryptering	-Forvrenging av informasjon slik at den underliggende klartekstinformasjonen ikke lenger kan rekonstrueres av uvedkommende.
Kryptonøkkel	-Manuell eller automatisk enhet i enhver form som benyttes til kryptering eller dekryptering. (Forskrift om informasjonssikkerhet §1-2 pkt. 9)
Personellsikkerhet	-Tiltak, handlinger og vurderinger for å hindre at personer som vil kunne utgjøre en sikkerhetsrisiko, plasseres eller er plassert slik at risikoen aktualiseres. (Forskrift om personellsikkerhet §1-2 pkt. 1)
Personkontroll	-Innhenting av relevante opplysninger til vurdering av sikkerhetsklarering. (Sikkerhetsloven §3 pkt. 15)
Risiko	-Uttrykk for den fare som uønskede hendelser representerer for informasjon/objekter av skjermingsverdig karakter. Risikoen uttrykkes ved sannsynligheten for og konsekvensene av de uønskede hendelsene.
Sabotasje	-Tilsiktet ødeleggelse, lammelse eller driftsstopp av utstyr, materiell, anlegg eller aktivitet, eller tilsiktet

	uskadeliggjøring av personer, utført av eller for en fremmed stat, organisasjon eller gruppering. (Sikkerhetsloven §3 pkt. 4)
Sikkerhetsadministrasjon	- Internkontroll ved gjennomføring av systematiske tiltak for å sikre at virksomhetens aktiviteter planlegges, organiseres, utføres og revideres i samsvar med krav fastsatt i og i medhold av sikkerhetsloven. (Forskrift om sikkerhetsadministrasjon §1-2 pkt. 1)
Sikkerhetsbrudd	- Brudd på bestemmelse om sikkerhetstiltak gitt i sikkerhetsloven eller forskrifter til sikkerhetsloven. (Forskrift om sikkerhetsadministrasjon §1-2 pkt. 4)
Sikkerhetsgradert anskaffelse	-Anskaffelse, foretatt av anskaffelsesmyndighet, som innebærer at leverandøren av varen eller tjenesten vil kunne få tilgang til skjermingsverdig informasjon eller objekt, eller som innebærer at anskaffelsen må sikkerhetsgraderes av andre årsaker. (Sikkerhetsloven §3 pkt. 14)
Sikkerhetsklarering	-Avgjørelse, foretatt av klareringsmyndighet og bygget på personkontroll, om en persons antatte sikkerhetsmessige skikkethet for angitt sikkerhetsgrad. (Sikkerhetsloven §3 pkt. 16)
Sikkerhetstruende hendelse	- Sikkerhetstruende virksomhet, kompromittering av skjermingsverdig informasjon og grove sikkerhetsbrudd.
Sikkerhetstruende virksomhet	-Forberedelse til, forsøk på og gjennomføring av spionasje, sabotasje eller terrorhandlinger, samt medvirkning til slik virksomhet. (Sikkerhetsloven §3 pkt. 2)
Skjermingsverdig informasjon	-Informasjon som skal merkes med sikkerhetsgrad i henhold til sikkerhetslovens §11. Det skilles mellom sikkerhetsgradene Strengt Hemmelig, Hemmelig, Konfidensielt og Begrenset. Vurderingen av hvilken sikkerhetsgradering informasjonen skal få, er basert på en vurdering av hvilken skade på rikets sikkerhet og andre vitale sikkerhetsinteresser som ville oppstå, dersom informasjonen ble kompromittert. (Sikkerhetsloven §3 pkt. 8)

Skjermingsverdig objekt	-Eiendom som må beskyttes mot sikkerhetstruende virksomhet av hensyn til rikets eller alliertes sikkerhet eller andre vitale, nasjonale sikkerhetsinteresser. Sikkerhetsloven §3 pkt. 12)
Spionasje	-Innsamling av informasjon ved hjelp av fordekte midler i etterretningsmessig hensikt. (Sikkerhetsloven §3 pkt. 3)
Sårbarhet	-En svakhet som reduserer eller begrenser samfunnets eller systemets evne til å motstå en uønsket, negativ hendelse, eller til å gjenopprette en ny, stabil tilstand etter at hendelsen har inntruffet.
Terrorhandlinger	-Ulovlig bruk av, eller trussel om bruk av, makt eller vold mot personer eller eiendom, i et forsøk på å legge press på landets myndigheter eller befolkning eller samfunnet for øvrig for å oppnå politiske, religiøse eller ideologiske mål. (Sikkerhetsloven §3 pkt. 5)
Tilgjengelighet	-Tilgang til objekter, tjenester og informasjon ved behov og uten unødvendig forsinkelse.
Trussel	-Ethvert forhold eller enhver enhet med potensiale til å forårsake en uønsket, negativ hendelse.
Trusselaktør	-En person, organisasjon eller et objekt som ønsker og er i stand til/evner å utløse en uønsket, negativ hendelse. ”Ønsket” kan relateres til intensjon, ”evne” kan relateres til kapasitet.
Verdivurdering	-Vurdering som har til hensikt å klarlegge hvilken informasjon og hvilke objekter som må anses skjermingsverdige, og i hvilken grad informasjonen og objektene er skjermingsverdige, sett i forhold til konsekvenser for rikets sikkerhet og andre vitale, nasjonale sikkerhetsinteresser, dersom informasjonen kompromitteres og objektene rammes av tilsiktede handlinger.
Virksomhet	-Et forvaltningsorgan eller annet rettssubjekt som sikkerhetsloven gjelder for, jfr. sikkerhetslovens §2.