NSM

Sikkerhetsfaglig råd

Et motstandsdyktig Norge

Forord

Sofie Nystrøm
Direktør
Nasjonal sikkerhetsmyndighet

Den sikkerhetspolitiske situasjonen er i kraftig endring. Russlands brudd med Vesten er et eksempel. Kinas langsiktige geopolitiske ambisjoner et annet. På mange måter er det en verdikamp som utspiller seg. Demokratier er under press. De er utsatt for dynamiske og sammensatte trusler som ligger under terskelen for væpnet konflikt, men som likevel utfordrer oss. Statssikkerheten må ta høyde for mer enn konvensjonelle styrker de neste årene. Styrkeforholdet vil defineres vel så mye av forsprang innen teknologi, strategiske oppkjøp, eierskap, forsyningslinjer, forskning og utvikling. De som leder an i teknologikappløpet, får naturlig fortrinn i spørsmål knyttet til nasjonal sikkerhet.

I sikkerhetsfaglig råd er vårt utgangspunkt at fremmede staters og trusselaktørers bruk av teknologi kan komme til å utvikle seg raskere enn åpne demokratiers evne til å beskytte seg. Autoritære regimer vil kunne utnytte informasjonsteknologi på måter som rammer demokratier med åpne informasjonsmiljøer hardest.

Vi trenger en mer trusselbasert «føre var»-tilnærming for å hindre at uønskede aktører får fotfeste i Norge. For myndighetene og staten betyr det å ta tøffere beslutninger og stanse en del aktivitet før den utfører skade. Dette kommer til å utfordre næringsliv og politiske ledere, som må stå i presset mot åpenlyse og fordekte handlinger, lovlige og ulovlige. Myndighetene – og virksomheter i hele Norge – må stoppe aktiviteter som kan utvikle seg til akutte trusler mot nasjonal sikkerhet.

Samtidig er klimasaken vår tids største utfordring. Den er en eksistensiell trussel i seg selv, med forventede endringer i levevilkår for svært mange mennesker på jorden. Teknologi vil spille en avgjørende rolle også her. Den vil gi nye styrkeforhold, med fordeler for de som blir vesentlige aktører. På den annen side øker det sikkerhetsrisikoen for de som ikke henger med i utviklingen av klimateknologi.

De sikkerhetsfaglige utfordringene de neste årene drives dermed av en rekke flere faktorer enn tidligere. Det skaper et stadig mer komplekst bilde som vil kreve mer av oss de neste årene enn vi er dimensjonert for i dag. Gapet mellom trusselaktørenes aktivitet og sikkerhetsarbeidet øker. Norge trenger ambisiøse målsetninger for nasjonal sikkerhet frem mot 2030.

Norge har et godt utgangspunkt. Vi er en ressurssterk nasjon med grunnleggende demokratiske verdier. Vi har sterke allianser i NATO, hvor vi selv leverer vesentlige bidrag. Men tempoet, styringen og beslutningskraften i avgjørende sikkerhetsspørsmål må opp. Beredskap må bygges i fredstid, og nå må vi prioritere tiltak som sikrer et motstandsdyktig Norge.

NSM/Ilja Hendel

Innhold

DEL 1

Sikkerhetstilstanden mot 2030

1 Innledning

Sikkerhetsfaglig råd tar for seg de viktigste sikkerhetsutfordringene frem mot 2030 og hvordan Norge kan stå best mulig rustet til å møte dem. Rådet setter strategiske sikkerhetsmål for perioden og blir NSMs viktigste innspill i langtidsplanene til Justis- og beredskapsdepartementet og Forsvarsdepartementet for 2025–2028.

Rådet beskriver sikkerhetstrender for de neste årene, utdyper sikkerhetsutfordringene Norge står overfor og deler NSMs anbefalinger for å oppnå et forsvarlig sikkerhetsnivå. Anbefalingene omfatter relevante tiltak som departementer, etater og virksomheter bør iverksette. Rådet foreslår blant annet å styrke kompetansen på fagområder som har betydning for nasjonal sikkerhet som kryptografi, cyber og kvanteteknologi. Det er også nødvendig å bedre sikkerhetsstyringen på tvers av sektorer, både offentlig og privat.

Sikkerhetsfaglig råd blir lansert våren 2023 i samme tidsrom som fagmilitært råd, forsvarskommisjonen og totalberedskapskommisjonen. Samtidig pågår en rekke prosesser i ulike sektorer og deler av forvaltningen. Uforutsigbare tider krever høyere beredskap. Anbefalingene i sikkerhetsfaglig råd må ses i sammenheng med de ulike prosessene.

NSMs sikkerhetsfaglige råd er utarbeidet på et bredt kunnskapsgrunnlag. Det bygger på NSMs egne kilder om sårbarheter, risiko og sikkerhetsutfordringer i Norge, samt erfaringer fra rådgivning, testing, tilsyn og hendelseshåndtering. Beskrivelser av trusselbildet og sikkerhetstrender baserer seg på rapporter og informasjon fra Etterretningstjenesten og Politiets sikkerhetstjeneste (PST) samt fremskrevne analyser i rapporter fra Forsvarets forskningsinstitutt (FFI).

FFI har vært en sentral deltaker i arbeidsprosessen og skrevet forskningsrapporten *Teknologiske og samfunnsmessige utviklingstrekk av betydning for nasjonale sikkerhetsinteresser i et 2030-perspektiv* (2022) til dette sikkerhetsfaglige rådet. I tillegg er det benyttet andre kilder i forvaltningen, NATO, EU og forskningsinstitusjoner i inn- og utland for å sikre tilstrekkelig bredde og dybde.

Private og offentlige virksomheter har gitt verdifulle innspill til sikkerhetsfaglig råd, blant annet gjennom Nasjonalt cybersikkerhetssenters (NCSC) omfattende partnernettverk. Sikkerhetstruende aktiviteter treffer virksomhetene direkte, og deres virkelighet er alltid høyst relevant.

NSM leverte sikkerhetsfaglig råd første gang i 2015. Rådet er i det store tatt til følge, og de fleste anbefalte tiltakene er iverksatt. Opprettelsen av Nasjonalt cybersikkerhetssenter var én av anbefalingene fra den gang.

NSM/Ilja Hendel

2 Nasjonal sikkerhet mot 2030

Norge står overfor betydelige sikkerhetsutfordringer mot 2030. Det norske samfunnet er avhengig av felles innsats og samarbeid mellom norske myndigheter, virksomheter og befolkningen for å oppnå tilstrekkelig motstandsdyktighet.

Norge er også avhengig av et sterkt internasjonalt samarbeid for å stå imot grenseoverskridende trusler som cyber- og påvirkningsoperasjoner. NATO og EU forblir Norges viktigste samarbeidsorganisasjoner i sikkerhetspolitiske spørsmål. Samtidig blir et styrket nordisk sikkerhetssamarbeid viktigere.

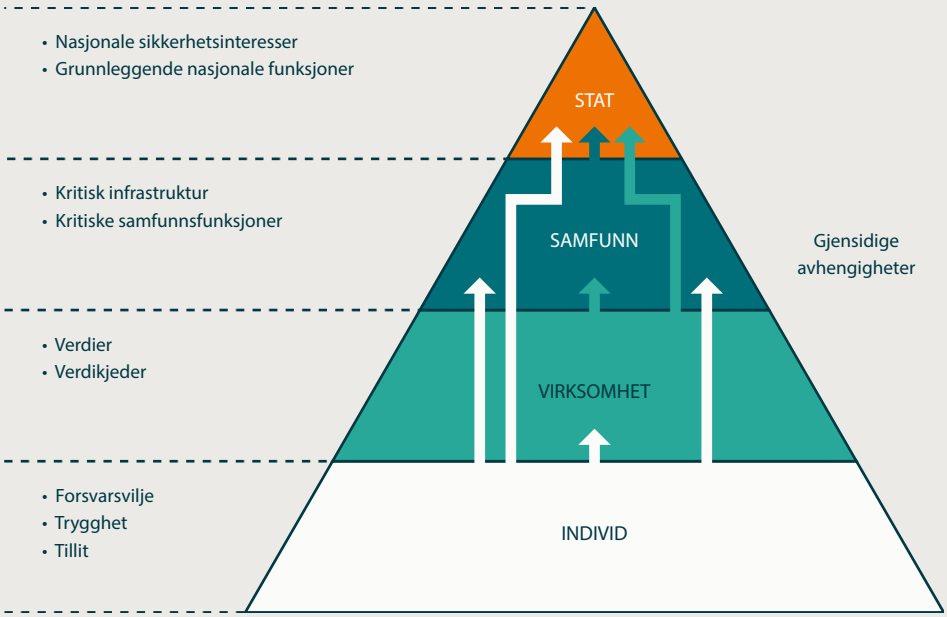
Land som Kina og Russland ønsker en annen verdensorden i strid med norske samfunnsverdier. De benytter i økende grad strategier som sammensatte trusler, og bruk av ny teknologi for å nå målet. Et alvorlig og omfattende trussel- og risikobilde krever at norske myndigheter oftere og på en mer direkte måte må motvirke aktivitet fra trusselaktører som kan skade nasjonal sikkerhet.

Sikkerhetsfaglig råd peker ut tolv strategiske sikkerhetsmål som gir en tydelig retning på arbeidet for nasjonal sikkerhet mot 2030.

Strategiske sikkerhetsmål

1. Norske virksomheter skaper bærekraftige verdier og ivaretar forsvarlig sikkerhet.
2. Norske myndigheter har en omforent situasjonsforståelse av trussel- og risikobildet.
3. Regjeringen får rettidig beslutningsstøtte som sikrer målrettet respons ved hendelser som kan skade nasjonal sikkerhet.
4. Sikkerhetsarbeidet i det norske samfunnet bidrar til å opprettholde tillit og til å styrke motstandskraft og forsvarsvilje i hele befolkningen.
5. Myndigheter, virksomheter og enkeltindivider gjenkjenner og varsler om sikkerhetstruende aktivitet og påvirkningsoperasjoner.
6. Norge har tilstrekkelig nasjonal kontroll over funksjoner og infrastruktur med betydning for nasjonal sikkerhet.
7. Norge har høy kompetanse innen cybersikkerhet og teknologier av betydning for nasjonal sikkerhet.
8. Norge har robust infrastruktur og satellittbaserte tjenester som understøtter totalforsvarsevnen gjennom krisespekteret.
9. Norge evner å motstå cyberoperasjoner som truer nasjonal sikkerhet i fred, krise og krig.
10. Alle deler av det norske samfunnet har digital motstandskraft på et langt høyere nivå.
11. Norske myndigheter hindrer at trusselaktører får tilgang til data om enkeltindivider som kan brukes til å skade nasjonal sikkerhet.
12. Norge har en god nasjonal evne til å avdekke, forhindre og håndtere innsidevirksomhet.

Figur 1 Gjensidige avhengigheter mellom ulike nivåer av sikkerhet.



Statssikkerhet er understøttet av samfunnssikkerhet

Sikkerhetsfaglig råd tar utgangspunkt i nasjonal sikkerhet. Nasjonal sikkerhet innebærer beskyttelse av statssikkerheten og de delene av samfunnssikkerheten som er av vesentlig betydning for Norges evne til å ivareta sikkerhetsinteressene, i tråd med Prop. 153 L (2016–2017) *Lov om nasjonal sikkerhet.*

Et statssikkerhetsperspektiv kan ikke ses isolert fra de øvrige sikkerhetsnivåene. Skillelinjene mellom statssikkerhet, samfunnssikkerhet, sikkerhet i virksomheter og individsikkerhet viskes ut i stadig større grad. Det er sterke gjensidige avhengigheter mellom nivåene. Dette skyldes blant annet digitaliseringen av samfunnet og den teknologiske utviklingen som binder sammen stadig flere funksjoner og infrastruktur i komplekse verdikjeder og avhengigheter.

Statssikkerheten utfordres også ved at grenselinjene mellom det sivile og det militære blir mer utydelige, blant annet som følge av overlappende verdi- og leverandørkjeder. Et tett sikkerhets- og beredskapssamarbeid på tvers av sektorer og nivåer blir derfor viktig mot 2030.[1]

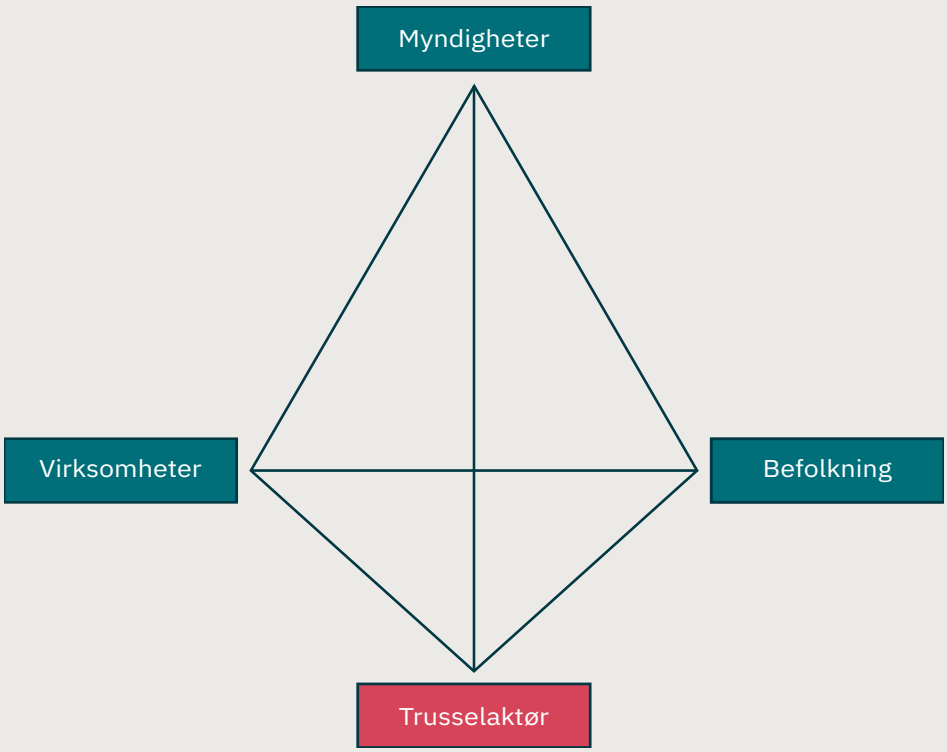
1 Prop. 14 S (2020–2021), *Evne til forsvar – vilje til beredskap*

Myndigheter, virksomheter og befolkning

Å sikre at nasjonale sikkerhetstiltak speiler trusselen mot Norge frem mot 2030 fordrer overordnet sikkerhetsstyring fra myndighetene og investeringer som styrker sikkerheten i norske virksomheter. Myndighetene og virksomhetene utgjør sammen med befolkningen tre aktører i samfunnet som har ansvar for, eller kan påvirke, sikkerhetstilstanden. Med komplekse utfordringer er det derfor viktig å være bevisst på dynamikker, samspill og avhengigheter mellom aktørene og de ulike rollene de bekler.

Myndighetene har det overordnede ansvaret for nasjonal sikkerhet og skal sikre nasjonal kontroll. Nasjonal kontroll innebærer at staten har tilstrekkelig oversikt og styringsevne over verdier som har betydning for nasjonal sikkerhet. Myndighetene må vurdere hvor stor grad av og hva slags type kontroll det er behov for, avhengig av hvilke innsatsfaktorer eller verdikjeder som understøtter ulike verdier. Staten kan bruke ulike metoder for å oppnå tilstrekkelig kontroll, for eksempel gjennom juridiske, økonomiske, organisatoriske eller pedagogiske virkemidler.

Figur 2 Sikkerhetsdiamanten – relasjoner mellom aktører.



Norske virksomheter står helt sentralt i det forebyggende sikkerhetsarbeidet. Verdier med betydning for nasjonal sikkerhet eies og forvaltes i hovedsak av virksomhetene, både private og offentlige. Med støtte fra myndighetene skal virksomhetene kunne avdekke, forhindre og håndtere sikkerhetstruende hendelser. De skal også ha evne til å gjenopprette en sikker tilstand for verdiene de forvalter.

Myndighetene skal legge til rette for at det nasjonale sikkerhetsarbeidet reguleres på en hensiktsmessig måte, og at virksomhetene får tilstrekkelig informasjon og rammebetingelser for å kunne iverksette effektive sikkerhetstiltak. Myndighetenes oppgave er dermed å påse at det nasjonale sikkerhetsarbeidet styrker virksomhetenes evne til å oppnå en forsvarlig sikkerhetstilstand. En forsvarlig sikkerhetstilstand er oppnådd når verdier med betydning for nasjonal sikkerhet er sikret så godt mot sikkerhetstruende aktivitet at risikoen er akseptabel.

Myndighetene må arbeide bevisst for å styrke forsvarsviljen i befolkningen. Dette handler om mer enn kampvilje gjennom bruk av maktmidler. Forsvarsvilje handler også om individets egenberedskap og motstandskraft mot sikkerhetstruende aktivitet som uønsket påvirkning.

Det er myndighetenes oppgave å styrke befolkningens årvåkenhet slik at sikkerhetstruende aktivitet kan gjenkjennes og varsles. Befolkningens motstandskraft overfor sikkerhetstruende hendelser skal virke gjennom hele krisespekteret. Det krever tillit mellom myndigheter og befolkning, at befolkningen har kunnskap om trussel- og risikobildet og at enkeltindivider vet hvordan de bør forholde seg til sikkerhetstruende aktiviteter.

Til sist er det myndighetenes ansvar å avdekke, forhindre og håndtere trusselaktørers forsøk på å ramme nasjonale sikkerhetsinteresser. Virksomheter og befolkning har svært begrensede juridiske og praktiske muligheter til selv å påvirke en trusselaktør gjennom aktive tiltak. Deres innsats ligger i forebyggende og defensive sikkerhetstiltak, mens myndighetene har som oppgave å utvikle og ta i bruk både defensive og offensive kapasiteter som kan avdekke, forhindre og håndtere en trusselaktør direkte.

Betydningen av tillit og trygghet for nasjonale sikkerhetsinteresser

De nasjonale sikkerhetsinteressene omfatter nasjonens aller viktigste verdier og er definert i sikkerhetsloven fra 2019. Dette er landets suverenitet, territorielle integritet, demokratiske styreform og overordnede sikkerhetspolitiske interesser. Tillit og trygghet i samfunnet er sentralt for å opprettholde det norske demokratiet og ivareta funksjonen til alle nasjonale sikkerhetspolitiske interesser. Befolkningens tillit til myndighetene og til hverandre er avgjørende for både motstandskraften i befolkningen og for myndighetenes styringsevne. Tillit er ikke noe myndighetene kan kreve, men noe de må gjøre seg fortjent til. En forutsetning for å bygge tillit er at myndighetene trygger grunnleggende demokratiske verdier og opprettholder funksjoner, infrastruktur og tjenester gjennom krisespekteret. Det bygger opp under befolkningens trygghetsfølelse.

Figur 3 Nasjonale sikkerhetsinteresser og utdyping av disse, jf. Prop. 153 L (2016-2017). Nasjonale sikkerhetsinteresser hviler på tillit og trygghet.

Verdier med betydning for nasjonal sikkerhet

Nasjonal sikkerhet blir i henhold til lov om nasjonal sikkerhet understøttet av grunnleggende nasjonale funksjoner. Dette er tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonene vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser. Departementene har ansvaret for å identifisere grunnleggende nasjonale funksjoner og utpeke underliggende verdier som skjermingsverdige.

Det vil alltid finnes verdier i samfunnet som bør kategoriseres som skjermingsverdige, men som ennå ikke er identifisert. Utover dette finnes det også verdier som reelt sett kan ha betydning for nasjonal sikkerhet – ofte på lang sikt – men som verken bør eller skal kategoriseres som skjermingsverdige etter sikkerhetsloven.[2] Eksempler på slike verdier kan være pressefrihet, mediemangfold og kulturarv.

Trusselaktører kan være interessert i å ramme eller utnytte slike verdier for å skade nasjonale sikkerhetsinteresser, direkte eller indirekte. Disse verdiene bør beskyttes på andre måter enn gjennom sikkerhetsloven. God situasjonsforståelse og sikkerhetsbevissthet i befolkning, virksomheter og hos myndigheter er også nødvendig for at disse verdiene er tilstrekkelig beskyttet.

Både verdier som etter sikkerhetsloven er skjermingsverdige og andre verdier med betydning for nasjonal sikkerhet må inngå i oversikten til sentrale myndigheter. Disse må ses i sammenheng med ukjente skjermingsverdige verdier som ennå ikke er identifisert eller utpekt. Mellom disse kategoriene kan det også være uidentifiserte verdikjeder. Dersom disse ikke blir tatt hensyn til, kan det føre til at skjermingsverdige verdier ikke er tilstrekkelig beskyttet.

Sammensatte trusler

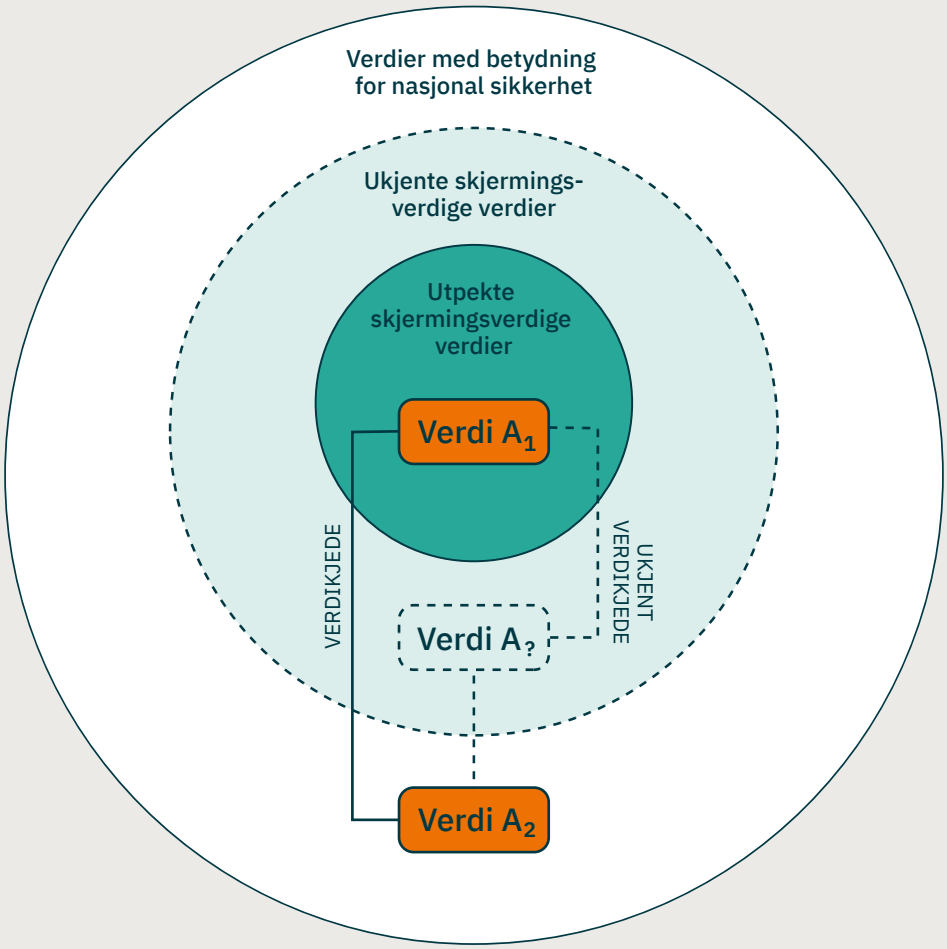
Nasjonale sikkerhetsinteresser spenner vidt, og stater benytter en rekke virkemidler for å beskytte eller hevde dem. Begrepet «sammensatte trusler» blir benyttet når virkemidlene settes sammen og koordineres slik at de understøtter og forsterker hverandre med hensikt om å ramme en annen stats sikkerhet.

Trusselaktører utnytter at funksjoner og infrastruktur i stat og samfunn henger sammen i uoversiktlige verdikjeder. Hendelser som tilsynelatende er rettet mot verdier ett sted i en verdikjede, kan i realiteten være konstruert for å ramme et egentlig mål et annet sted i verdikjeden. Slik kan også skjermingsverdige verdier rammes, for eksempel ved at en tjeneste virksomheten er avhengig av svikter eller et produkt fra en leverandør er kompromittert. Dette er en del av sammensatte truslers natur.

Meld. St. 10 (2021-2022), *Prioriterte endringer, status og tiltak i forsvarssektoren* beskriver sammensatte trusler som «strategier for konkurranse og

2 Meld. St. 9 (2022–2023): *Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet — Så åpent som mulig, så sikkert som nødvendig*

Figur 4 Tre ulike kategorier av verdier med betydning for nasjonal sikkerhet.



konfrontasjon under terskelen for direkte væpnet konflikt som kan kombinere diplomatiske, informasjonsmessige, militære, økonomiske og finansielle, etterretningsmessige og juridiske virkemidler for å nå strategiske målsettinger. Virkemiddelbruken er gjerne distribuert bredt, er langsiktig i sin tilnærming og kombinerer åpne, fordekte og skjulte metoder». Aktivitetene holdes under terskelen for væpnet konflikt, men formålet er å undergrave, påvirke eller destabilisere en annen stat. De sikkerhetstruende aktivitetene skjer ofte fordekt, og det kan være vanskelig å avdekke hvem som står bak.

Defensivt sikkerhetskonsept

Den nasjonale sikkerhetstilstanden er dynamisk og må ses i lys av et oppdatert trussel- og risikobilde med økende bruk av sammensatte trusler. For å møte utviklingen er det behov for å utfylle og videreutvikle det nasjonale sikkerhetsarbeidet med en modell for et defensivt sikkerhetskonsept.

Utgangspunktet for modellen er at all sikkerhetstruende aktivitet utøves gjennom ett eller flere domener, enten cyber, personell, fysisk, økonomisk, kognitiv eller domenet for romvirksomhet. For å forhindre at sikkerhetstruende aktivitet påfører verdier skade, må det etableres sikkerhetstiltak i de aktuelle domenene som håndterer truslene.

Det defensive sikkerhetskonseptet legger vekt på å forstå truslene og ha en helhetlig tilnærming til hvilke tiltak som bør iverksettes gjennom eller på tvers av de ulike domenene. Tiltak må speile truslene for å være effektive. Verdier kan være omfattende sikret, men dersom sikkerhetstiltakene ikke er målrettet og tilpasset de aktuelle truslene, kan tiltakene være utilstrekkelige. Trusselaktørene retter ikke nødvendigvis aktivitetene direkte mot verdiene de ønsker å ramme. Sikkerhetstiltak må derfor vurderes fortløpende og ses samlet på tvers av domener for å møte sammensatt virkemiddelbruk.

Defensivt sikkerhetskonsept beskriver fire risikoreduserende evner som går på tvers av domenene. Dette er å

1. etablere grunnsikring av de verdiene som må beskyttes
2. løpende avdekke og lukke sårbarheter
3. løpende avdekke og håndtere sikkerhetstruende aktivitet
4. løpende håndtere sikkerhetstruende hendelser

Modellen benyttes for å strukturere helhetlige, risikoreduserende evner og dynamiske porteføljer av sikkerhetstiltak. Den bidrar også til å synliggjøre gap som ikke er dekket med tiltak, og sikkerhetstiltak som bør endres eller tilføyes gjennom krisespekteret.

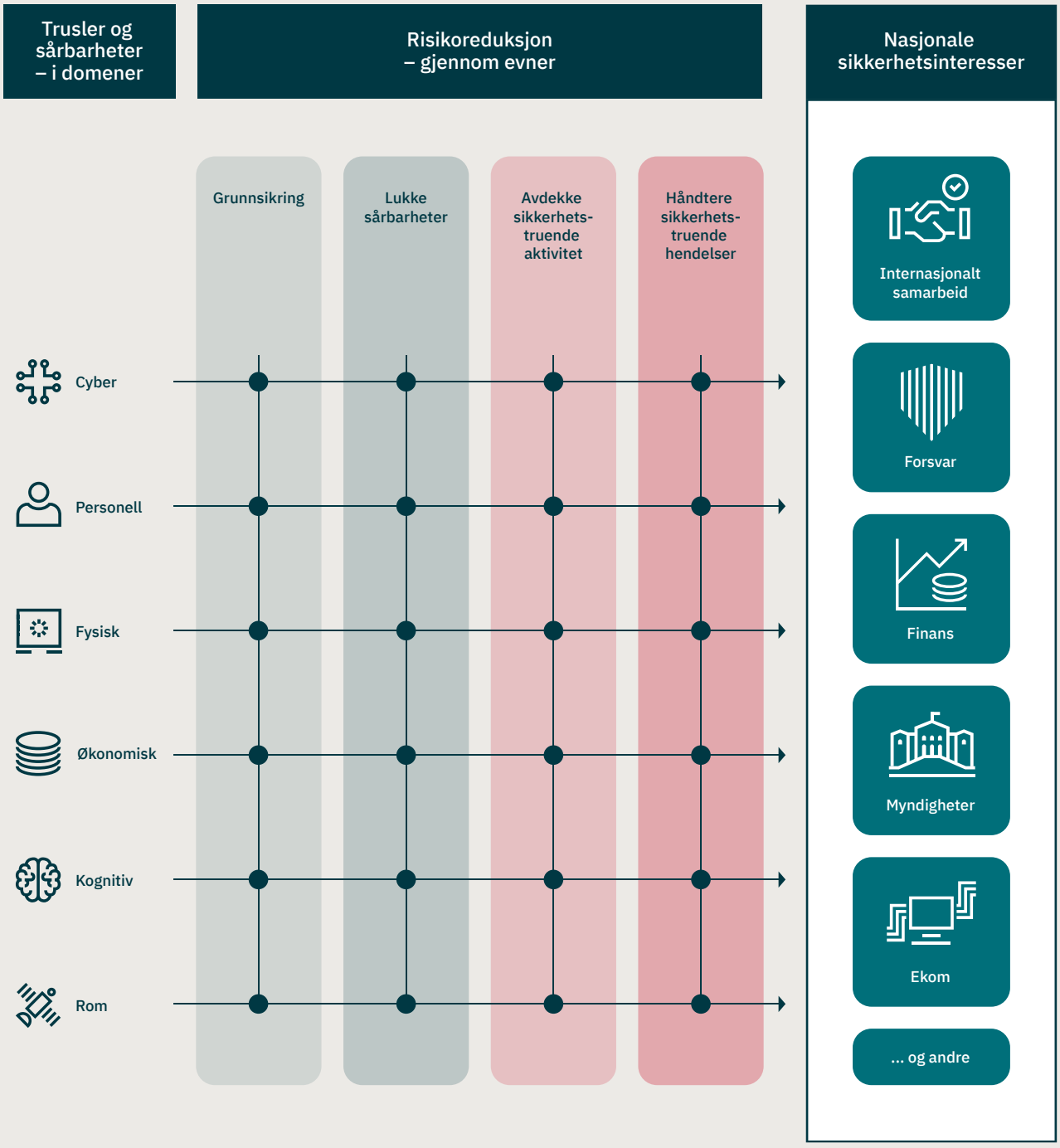
Mål for nasjonal sikkerhetstilstand

Den alvorlige sikkerhetspolitiske situasjonen som preger Norge og resten av Europa i 2023 vil trolig vedvare mot 2030. Sikkerhetsnivået i det norske samfunnet er ikke der det bør være for å møte denne utviklingen. Det er derfor behov for nasjonale tiltak som styrker motstandsdyktigheten. Målet for Norges sikkerhetstilstand i 2030 bør være at de samlede nasjonale sikkerhetstiltakene speiler trusselen ved at

- myndighetene har felles situasjonsforståelse og koordinert responsevne
- virksomhetene har systematisk sikkerhetsstyring og helhetlig sikring
- befolkningen er årvåken og har sterk motstandskraft

Målet oppnås gjennom de tolv strategiske sikkerhetsmålene.

Figur 5 Modell for et defensivt sikkerhetskonsept.



Mikhail Tereshchenko/AP/NTB

3 Sikkerhetstrender mot 2030

Samfunnsutviklingen og de sikkerhetspolitiske utfordringene mot 2030 vil være preget av høy kompleksitet og stor usikkerhet. Sammenfall av flere utviklingstrekk, som pandemi, krig i Europa, videreføring av Kinas offensive utenrikspolitikk og klimaendringene, forsterker de negative konsekvensene og skaper uønskede langtidseffekter. Dette har også konsekvenser for norske nærområder og Norges sikkerhetsinteresser. De viktigste trendene med betydning for nasjonal sikkerhet er fremtidig konfliktutvikling, teknologiutvikling og følgene av klimaendringene.

Fremtidig konfliktutvikling

Et fremtredende trekk i den globale sikkerhetspolitiske utviklingen er rivalisering mellom stormaktene USA, Kina og til dels Russland. Både Russland og Kina ønsker en endring av eksisterende verdensorden. Rivaliseringen innebærer skjerpet konkurranse og konfrontasjoner med alle statens maktmidler i ulike regioner. Ideologi har blitt mer fremtredende, og verden står overfor en maktforskyvning hvor demokratier er under press til fordel for autokratier. I dette bildet er det uunngåelig at Norge og resten av Vesten også blir påvirket av stormaktsrivalisering.

Kina er forventet å utøve en mer offensiv og konfronterende utenrikspolitikk i årene mot 2030. Dette innebærer en utstrakt bruk av alle statens virkemidler, inkludert økonomisk statshåndverk. Kinas vilje til å bære kostnadene av et høyere konfliktnivå med Vesten øker. En mulig fremtidig konflikt i Kinas nærområder får også sikkerhets- og handelspolitiske konsekvenser for Norge.

Både Russland og Kina ønsker en endring av eksisterende verdensorden.

I nordområdene fører Russland en stadig mer selvhevdende politikk, mens Kina styrker både egen posisjon og evne til å operere i Arktis. Dette medfører risiko for økt rivalisering mellom stormaktene også i denne regionen. Det utfordrer på sikt Norges sikkerhetsinteresser.

Demokratier er under press av flere årsaker. Intern misnøye med demokratiske prosesser, økonomisk tilbakegang, økt polarisering mellom grupper i samfunnet og generasjonskløfter er bare noen av dem. Denne misnøyen kan forsterkes av andre stater ved bruk av sammensatte trusler, en kombinasjon av ulike virkemidler for å utøve påvirkning og press. Hensikten kan være å fremme egne interesser, for eksempel ved å svekke demokratiet gjennom å forsterke eksisterende konfliktlinjer. Sammensatte trusler som svekker tilliten mellom befolkningen og myndighetene, er en av de mest alvorlige truslene mot nasjonal sikkerhet.

Mot dette bakteppet forblir utenlandsk etterretnings- og påvirkningsaktivitet samlet sett en betydelig trussel mot Norge og norske interesser frem mot 2030.

Teknologiutvikling og verdiskapning

Hastigheten og kompleksiteten innen teknologisk innovasjon beskrives som en av århundrets megatrender. Trenden er global og har stor påvirkningskraft på linje med klimaendringene og Kinas fremvekst. Flere av de fremvoksende teknologiene kalles gjerne «brytningsteknologier». Dette er teknologier som vesentlig kan endre hvordan stat og samfunn fungerer. Denne transformasjonen er ikke knyttet til én enkelt teknologisk nyvinning, men til samvirket mellom nyvinningene.

Kommersielle behov og utsikter i samfunnet driver mye av teknologiutviklingen. Kommersielle muligheter forventes derfor å styre hvilke teknologier som blir tatt i bruk. Det er en ønsket utvikling, men myndighetene må samtidig signalisere behovet for å utvikle teknologier som kan beskytte verdier av nasjonal betydning. I tillegg bør myndighetene sørge for at teknologiutvikling ikke går på bekostning av samfunnets grunnleggende verdier. Norge trenger nærings- og teknologiutvikling, men sikkerheten må ivaretas.

Den teknologiske utviklingen har stor betydning for hvordan verdier skapes mot 2030. Et datadrevet forsvar, næringsliv og sivilsamfunn endrer arbeids- og samhandlingsmønstre. Informasjonens tilgjengelighet og integritet blir stadig viktigere i hurtigere og mer komplekse behandlings- og beslutningsprosesser. Informasjonens betydning som en verdi i seg selv vil endre seg, og nye sårbarheter vil oppstå.

Forebyggende sikkerhetsarbeid og nasjonale sikkerhetstiltak må spille på lag med moderne verdiskaping. Et strukturert, funksjonelt og dynamisk sikkerhetsarbeid gir Norge strategiske fortrinn i en krevende tid hvor omstillingsevne og kompetansebehov er fremtredende.

Klimaendringer og omstillingsevne

Klimaendringene er vår tids største utfordring. De har også sikkerhetspolitiske følger, og forsterker eksisterende konfliktlinjer mellom land og regioner. Derfor omtaler NATO klimaendringene som en «trusselmultiplikator».

Den nødvendige omstillingen som kreves for å nå klimamålene vil være preget av både samarbeid, konkurranse og rivalisering. Internasjonale maktforhold og geopolitikk vil forme retning, innhold og takten på omstillingen.

Energiomstillingen endrer også internasjonale maktforhold. Det er en intens konkurranse om å vinne kontroll over og ha et forsprang innen fremtidens energi og teknologi blant annet gjennom industri-, handels- og innovasjonspolitikk. EU, USA, Kina og mange andre ønsker å ta lederskap i omstillingen.

For Norge innebærer både klimaendringer og energiomstillingen sikkerhets-utfordringer også som følge av Norges rolle som produsent og leverandør av fornybar og ikke-fornybar energi.

DEL 2

Sikkerhetsutfordringer og anbefalinger

4 Situasjonsforståelse og responsevne

Situasjonsforståelse basert på et godt informasjonsgrunnlag er helt avgjørende for gode og rettidige beslutninger. Det er en grunnleggende forutsetning for sikkerhetsarbeidet på alle nivåer i offentlige og private virksomheter. Dette gjelder i fred, krise og krig.

God situasjonsforståelse er nødvendig for at myndigheter og virksomheter skal kunne møte fremtidige sikkerhetsutfordringer med presise sikkerhetstiltak i et defensivt sikkerhetskonsept. Det innebærer tilstrekkelig kunnskap om det gjeldende trusselbildet i og mot Norge, hvilke verdier som må beskyttes og hvilke sårbarheter som kan utnyttes av trusselaktører.

Situasjonsbildet for nasjonal sikkerhet avhenger av ståsted og vil være ulikt avhengig av myndighetsnivå, sektor eller bransje. Det må likevel være et mål at nasjonale, regionale og kommunale myndigheter har en omforent situasjons-forståelse av trussel- og risikobildet. Det er vanskelig å lykkes med en helhetlig sikkerhetsstyring fra myndighetenes side uten denne forståelsen.

Gode, rettidige beslutninger om tiltak som responderer på sikkerhetstruende hendelser med betydning for flere sektorer, kan vanskelig fattes uten en omforent situasjonsforståelse på tvers av sektorene. Derfor er det en klar sammenheng mellom situasjonsforståelse og responsevne.

Det er et mål at norske myndigheter har en omforent situasjonsforståelse av trussel- og risikobildet.

Sikkerhetsutfordringer

Myndighetene har mangelfull situasjonsforståelse
Det er avgjørende at nasjonale, regionale og lokale myndigheter har en god og omforent situasjonsforståelse for å kunne avdekke, forhindre og håndtere sikkerhetstruende aktivitet.

Det finnes allerede flere mekanismer for informasjonsdeling og samordning for å skape bedre situasjonsforståelse hos myndighetene. Dette har bidratt til økt situasjonsforståelse på flere myndighetsnivå, men det er ikke utnyttet i tilstrekkelig grad på nasjonalt nivå.

Både departementer og virksomheter har mangelfull oversikt over og forståelse av risikobildet. Som følge av dette har ikke myndighetene de nødvendige forutsetningene for å bygge et rettidig situasjonsbilde. Samlet sett betyr det at forebyggende sikkerhetsarbeid på alle nivå blir utilstrekkelig, og at myndighetenes responsevne risikerer å være reaktiv og fragmentert. Norge oppnår dermed ikke et forsvarlig nasjonalt sikkerhetsnivå.

Rapportering om sikkerhetsstatus på skjermingsverdige verdier og kritiske samfunnsfunksjoner skjer i flere forskjellige løp og er ikke tilstrekkelig dekkende i alle sektorer. Rapporteringen av sikkerhetsstatus er én av flere kilder i et helhetlig situasjonsbilde for nasjonal sikkerhet. Fragmentert rapportering fører til et mangelfullt nasjonalt situasjonsbilde.

Ufullstendig situasjonsforståelse kan også forhindre myndighetene fra å formidle et dekkende trussel- og risikobilde til befolkningen. Det kan svekke årvåkenhet og motstandskraft.

Virksomheter har ikke tilstrekkelig tilgang til trussel- og sikkerhetsinformasjon
EOS-tjenestene er en felles betegnelse for etterretnings- og sikkerhetstjenestene i Norge. De består av Etterretningstjenesten, Politiets sikkerhetstjeneste (PST) og Nasjonal sikkerhetsmyndighet (NSM).

Hvert år publiserer EOS-tjenestene ugraderte rapporter om det nasjonale trussel- og risikobildet. Informasjonen er tilgjengelig for alle, og rapportene er viktige bidrag til virksomheters strategiske risikoarbeid. I tillegg mottar en rekke private og offentlige virksomheter graderte trussel- og risikovurderinger fra EOS-tjenestene, avhengig av situasjon og behov.

Vurderingene dekker imidlertid ikke det løpende behovet til virksomheter og sektorer for oppdatert trussel- og sikkerhetsinformasjon. Spesielt gjelder dette i cyberdomenet, der risikobildet er svært dynamisk. Endringer må fanges opp tidlig og formidles raskt dersom virksomhetene skal være i forkant av trusler.

Flere virksomheter og sektorer etterlyser mer spesifikk informasjon fra myndighetene om trussel- og risikobildet for egen sektor. Det finnes en rekke bransjespesifikke fora og samordningskanaler for å dele informasjon til ulike virksomheter og sektorer. Mange av disse er imidlertid ad-hoc-preget og mangler systematikk og kontinuitet. Det er også flere virksomheter, både offentlige etater og private bedrifter, som ikke er tilknyttet slik informasjonsdeling. Det er et uutnyttet potensial i deling av datagrunnlag og sikkerhetsinformasjon mellom virksomheter og myndigheter.

Enkelte internasjonale selskaper utgir åpent tilgjengelig informasjon om cybertrusler. Nasjonalt bidrar større virksomheter som DNB, Telenor og NRK til økt situasjonsforståelse gjennom publisering av egne risiko- og trusselvurderinger.

Innen cyberdomenet er trusseletterretning stadig viktigere for å øke cybersikkerheten i virksomheter. Trusseletterretning er informasjon eller data som er samlet inn, bearbeidet og analysert for å forstå trusselaktørers intensjon, kapasitet og adferd. Trusseletterretning som tjeneste tilbys av en rekke private sikkerhetsselskaper.

En annen viktig kilde til informasjon er samfunns- og sikkerhetspolitiske rapporter fra forvaltning og forskning. En virksomhet som ikke forstår trusselbildet eller at de er et mål for en trusselaktør, har heller ingen insentiv til å avsette tilstrekkelige ressurser til å beskytte verdier og redusere sårbarhetene. Dermed har virksomheten ikke mulighet til å speile trusselen med effektive mottiltak.

Tilgang til relevant trussel- og sikkerhetsinformasjon er avgjørende for virksomheters sikkerhetsarbeid og regelmessig oppdatering av risikovurderinger. Oppdatert trussel- og sikkerhetsinformasjon kan endre premissene for gjeldende risikovurdering og dermed fordre en ny vurdering med nye tiltak.

For virksomheter er både kompetanse og ressurser nødvendig for å kunne oversette trusselinformasjonen slik at den blir forstått og brukt i risikovurderinger. Flere sektorer og virksomheter mangler disse forutsetningene for å beskytte verdier med betydning for nasjonal sikkerhet.

Lav innrapportering av hendelser bidrar til mangelfullt situasjonsbilde

For å oppnå et helhetlig situasjonsbilde på nasjonalt nivå er det helt nødvendig at virksomheter rapporterer om sikkerhetstruende hendelser de blir utsatt for. Undersøkelser viser at det er betydelig underrapportering av slike hendelser. Mørketallsundersøkelsen fra Næringslivets sikkerhetsråd i 2022 viser for eksempel at kun én prosent av virksomhetene innrapporterer cybersikkerhetshendelser til Nasjonalt cybersikkerhetssenter (NCSC) i NSM. NSM har også andre kilder som peker på underrapportering av sikkerhetstruende hendelser. Årsaker til manglende rapportering kan være at hendelser kun blir varslet internt, at de ikke blir ansett som varslingsverdige, av omdømmehensyn eller at hendelsene ikke blir avdekket i det hele tatt.

Når enkelthendelser ikke blir rapportert, får verken NSM eller andre myndigheter informasjon til å danne et helhetlig situasjonsbilde.

Virksomheter har ikke løsninger for sikkerhetsgradert samhandling

Mange offentlige og private virksomheter har behov for sikkerhetsgradert informasjon, men mangler mulighet for å motta den. Dette er spesielt alvorlig når det gjelder virksomheter som er en del av totalforsvaret. Målrettede mottiltak er i mange sammenhenger avhengig av detaljert og gradert informasjon for å kunne settes inn rettidig og presist. Manglende tilgang på digitale løsninger og lokaler for høygradert tale reduserer responsevnen.

Anbefalinger

Et sivilt-militært situasjonssenter bør opprettes på strategisk nivå
Senteret skal sikre politisk ledelse tilstrekkelig kunnskap om situasjonen og tilgang på helhetlig og rettidig beslutningsstøtte. Det bør plasseres i umiddelbar nærhet til regjeringen. En strategisk plan- og analysefunksjon knyttet til senteret skal utarbeide handlingsalternativer for å håndtere sikkerhetstruende aktivitet. Senteret må ha tilgang til rettidig trussel- og risikoinformasjon og situasjonsbilder fra både forsvarssektoren og sivile sektorer.

Strukturer for samhandling, informasjonsutveksling og rapportering bør styrkes i hver sektor
Formålet er å øke situasjonsforståelsen i alle sektorer og bygge grunnlag for sektorvise situasjonsbilder. Eksisterende samarbeidskanaler mellom NSM og sektorene bør videreutvikles. Dette kan gjøres ved å videreutvikle konseptet med sektorvise respons-miljø, som jobber med digital sikkerhet. Både private og offentlige virksomheter må være en del av disse strukturene. Gjensidig informasjonsutveksling mellom virksomheter og EOS-tjenestene bidrar til å bygge situasjonsforståelse i virksomheter og hos myndigheter.

Regelmessig rapportering om sikkerhets-tilstanden til verdier med betydning for nasjonal sikkerhet danner grunnlag for sektorvise situasjons-bilder. Denne sikkerhetstilstanden bør rapporteres regelmessig til sektordepartementet og NSM, slik at det blir etablert en helhetlig oversikt. Oversikten for sikkerhetstilstand bidrar inn i et felles situasjons- og risikobilde for nasjonal sikkerhet.

For å styrke situasjonsforståelsen i alle sektorer er det avgjørende med distribusjon og tilgjengelig-gjøring av relevant trussel- og sikkerhetsinformasjon. EOS-tjenestene må i større grad tilpasse gradert trussel- og sikkerhetsinformasjon til et ugradert nivå. Informasjonen må formidles rettidig til virksomheter som har bruk for dette.

Myndighetene må legge til rette for at alle virksomheter som har behov for sikkerhetsgradert informasjon, har tilgang til graderte samhandlings-løsninger og lokaler for gradert tale. Styrket sam-handling, situasjonsforståelse og kommunikasjons-evne mellom virksomheter og myndigheter øker styringsevnen.

Strukturer for samhandling om nasjonal sikkerhet bør styrkes på regionalt og kommunalt nivå
Formålet er å øke situasjonsforståelsen regionalt og lokalt. Myndigheter med ansvar for nasjonal sikkerhet og beredskap bør samarbeide om å videreutvikle samhandlingsstrukturer for sikkerhet på regionalt og kommunalt nivå. Strukturene bør sikre at aktørene får tilstrekkelig tilgang på relevant trussel- og sikkerhetsinformasjon. Økt situasjonsforståelse på disse nivåene styrker evnen til å avdekke sikker-hetstruende aktivitet og dermed bidra til et helhetlig nasjonalt situasjonsbilde. Nasjonal sikkerhet må tydeliggjøres i instrukser som gjelder kommunalt og regionalt nivå.

5 Tverrsektoriell styring

Sektorprinsippet er en sentral del av norsk forvaltningspraksis. Prinsippet bidrar til at sektorene har den nødvendige friheten til å utføre oppgavene sine, og plasserer konstitusjonelt ansvar hos den enkelte statsråd. Noen områder krever imidlertid tverrsektoriell styring – felles innsats og samhandling på tvers av sektorer. Nasjonal sikkerhet er et eksempel på et slikt område. Andre eksempler er digitalisering, klima og miljø, personvern, likestilling, mangfold og inkludering.

Tverrsektorielle forvaltningsområder utfordrer sektorprinsippet fordi de må ivaretas av departementer som primært har ansvar for andre fagområder. Det er utfordrende å ivareta ulike hensyn på tvers av sektorer. Overordnede og felles målsettinger er ikke alltid tydelige. Dette kan føre til manglende helhetstenkning og koordinering, forskjellige planhorisonter og ulik prioritering av ressurser til forskjellige områder.

De fleste sektorer i samfunnet har verdier og funksjoner med betydning for nasjonal sikkerhet. Verdienes karakter og betydning varierer fra sektor til sektor. De ulike departementene har etter sektorprinsippet ansvar for å ivareta det forebyggende sikkerhetsarbeidet innen egen sektor. Begrenset kompetanse innen nasjonal sikkerhet i et departement kan hindre identifisering av verdier med betydning for nasjonale sikkerhetsinteresser i sektoren. Det kan også føre til at trusler og sårbarheter ikke oppdages i tide. Tverrsektorielt samarbeid er nødvendig for å utvikle gode sikkerhetstiltak.

Sikkerhetsutfordringer

Verdier som understøtter grunnleggende nasjonale funksjoner mangler sikring
Identifiseringen av grunnleggende nasjonale funksjoner er en forutsetning for at departementene skal kunne vurdere hvilke virksomheter innenfor eget ansvarsområde som forvalter verdier av betydning for nasjonale sikkerhetsinteresser. Noen grunnleggende nasjonale funksjoner er tverrsektorielle, og ansvaret for disse er delt mellom flere departementer. I andre tilfeller forvalter virksomheter i én sektor verdier av betydning for grunnleggende nasjonale funksjoner i en annen. Manglende kartlegging av verdier får konsekvenser gjennom hele verdikjeden. Det medfører risiko for at verdier som blir forvaltet på tvers av sektorer ikke blir identifisert, eller at det oppleves som uklart hvem som har ansvaret.

Nasjonal sikkerhet er ikke tilstrekkelig integrert i den sektorvise myndighetsutøvelsen
Departementene må i større grad ta hensyn til nasjonal sikkerhet i sin myndighetsutøvelse og politikkutforming, også utover prosesser for grunnleggende nasjonale funksjoner. Vurderinger knyttet til nasjonal sikkerhet er i for liten grad en integrert del av departementenes langsiktige planprosesser, regelverksutvikling, strategier og utredninger for egen sektor.

Dersom nasjonal sikkerhet ikke er en integrert del av den sektorvise myndighetsutøvelsen, står Norge i fare for å overse potensielle konsekvenser som kan skade nasjonale sikkerhetsinteresser.

Norge mangler omforente og enhetlige nasjonale sikkerhetsmål
Ulikt mange av våre allierte har ikke Norge en overordnet nasjonal sikkerhetsstrategi. Myndighetenes føringer må fortolkes gjennom en rekke strategier og policydokumenter fra regjeringen og ulike departementer. Disse dokumentene, som langtidsplanen for forsvarssektoren og stortingsmeldinger fra Justis- og beredskapsdepartementet og Utenriksdepartementet, kommer til ulik tid og har skiftende sektorvise prioriteringer.

Fraværet av en overordnet sikkerhetsstrategi gjør det krevende å nå overordnede nasjonale målsettinger gjennom felles innsats. Det blir blant annet vanskelig å planlegge og styre større sikkerhetsinvesteringer over tid og på tvers av sektorer. Dette er spesielt viktig for forsvarssektoren, som har behov for helhetlige og langsiktige føringer for å utvikle forsvarskonsepter og strukturplanlegging i fredstid. Det er også krevende å oppnå en samordnet utvikling av totalforsvaret uten en sikkerhetsstrategi.

Uklare ansvarsforhold gjør det utfordrende å forebygge og håndtere tverrsektorielle sikkerhetstruende hendelser
Når flere departementer har overlappende ansvar for et fagfelt og tilhørende grunnleggende nasjonale funksjoner, kan det føre til at ansvaret blir fragmentert. Satellittbasert kommunikasjon og matforsyning er eksempler på tverrsektorielle grunnleggende nasjonale funksjoner. Ansvaret for virksomheter og verdier som understøtter – eller er av betydning for – disse, er delt mellom flere departementer. Det er dermed en risiko for at det er uklart hvilket

departement som har ansvaret for å identifisere slike tverrsektorielle verdier og iverksette forebyggende sikkerhetstiltak.

Sikkerhetstruende hendelser kan være sektorovergripende, enten ved at de rammer flere sektorer på én gang eller at de rammer verdier som er viktige for flere sektorer. Det blir utfordrende både å avdekke og håndtere disse hendelsene dersom ansvaret ikke er avklart på forhånd.

Styring på tvers av EOS-tjenestene er ikke godt nok samordnet

EOS-tjenestene har etablert samarbeid på flere områder. Likevel er det forebyggende arbeidet begrenset av styrings- og samarbeidsutfordringer mellom tjenestene. Dette får også konsekvenser for arbeidet med det nasjonale trussel- og risikobildet. Riksrevisjonen peker på noen av disse utfordringene i rapporten *Myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor* (Dokument 3:7 (2022–2023)).

Styring på tvers av EOS-tjenestene er ikke godt nok samordnet. Konsekvensen er at de samlede ressursene ikke blir godt nok utnyttet. For eksempel blir ikke innhentingsbehov sett i sammenheng med både etterretnings- og sikkerhetsformål.

Uten investeringer i nye teknologiske muligheter, materiell og personell med rett kompetanse er det risiko for at EOS-tjenestene i fremtiden ikke evner å bygge et tilstrekkelig finmasket trussel- og risikobilde i fellesskap.

Krav til sikkerhet i anskaffelser og konsesjoner er ikke tilstrekkelig

Mangelfull oversikt over leverandørkjeder og fravær av sikkerhetskrav til leverandører i anskaffelser og prosjekter åpner muligheten for at trusselaktører bruker anskaffelsesprosesser som virkemiddel for å få tilgang til verdier. Trusselaktører kan dermed ramme virksomheten gjennom leverandører og underleverandører.

Mangelfull risikovurdering ved tildeling av konsesjoner og i store prosjekter kan føre til at leverandører får urettmessig tilgang til informasjon og verdier med betydning for nasjonal sikkerhet.

Anbefalinger

Det bør utarbeides en nasjonal sikkerhetsstrategi for Norge
Regjeringen bør utarbeide en helhetlig og sektorovergripende sikkerhetsstrategi. Formålet er å forbedre den tverrsektorielle styringen av nasjonalt sikkerhetsarbeid. Strategien må utdypes gjennom sektorspesifikke strategier, langtidsplaner eller prioriteringsdokumenter.

Strategien bør legge føringer for et defensivt sikkerhetskonsept som møter sammensatte trusler. En nasjonal sikkerhetsstrategi legger til rette for sikkerhetsarbeid i fredstid og grunnlaget for forsvars- og totalforsvarskonsepter i krise og krig.

Nasjonal sikkerhet bør behandles i en langtidsproposisjon
Formålet er å sikre forutsigbare økonomiske rammer for det tverrsektorielle arbeidet med nasjonal sikkerhet og å styrke totalforsvarsevnen. En langtidsproposisjon bidrar til at arbeidet med nasjonal sikkerhet blir helhetlig og øker forutsigbarheten for sikkerhetsinvesteringer som treffer på lang sikt og på tvers av sektorer.

Utredningsinstruksen bør inkludere krav om hensyn til nasjonal sikkerhet
Hensikten er at nasjonale sikkerhetsinteresser i større grad blir tatt hensyn til i politikkutforming og lovarbeid på tvers av sektorer. Langsiktige planprosesser, strategier og utredninger må vurdere konsekvenser for nasjonal sikkerhet.

Sikkerhetsarbeid må følges tettere opp i alle sektorer
Dette bør gjøres gjennom

- aktiv oppfølging av etterlevelse av krav til sikkerhet i etatsstyring og eierstyringsdialog fra departementene
- etablering av et hjemmelsgrunnlag for å stille krav til rapportering om sikkerhetsarbeid i årsberetning i private virksomheter
- innføring av sikkerhetskrav i statens standardavtaler for offentlige anskaffelser og anskaffelsesregelverk for forsvarssektoren. Kravene må fremkomme tydelig ved tildeling av offentlige prosjekter og konsesjoner

Det bør etableres en konsolidert oversikt over de viktigste verdiene med betydning for stats- og samfunnssikkerhet
Formålet er å gi myndighetene et tverrsektorielt og helhetlig situasjonsbilde over nasjonale verdier. Oversikten gjør gjennomføringen av Norges internasjonale forpliktelser mer effektiv, inklusive EUs NIS- og CER-direktiver og NATOs syv grunnleggende forventninger (*NATO Seven Baseline Requirements*).

Samhandlingen mellom EOS-tjenestene må styrkes
EOS-tjenestenes oppgaver, prioriteringer og mål knyttet til trussel- og risikobildet bør i større grad være samordnet. Dette bidrar til mer effektiv bruk av EOS-tjenestenes samlede fagkompetanse og data- og analysekapasitet og styrker samhandlingen mellom tjenestene. EOS-tjenestene må utnytte potensialet som ligger i nye innhentingsmetoder,

økte datamengder og ny teknologi. Hjemmelsgrunnlaget må ivareta disse behovene.

Observert trusselaktivitet og høyoppløselig trusselinformasjon må vies spesiell oppmerksomhet for å kunne iverksette dynamiske og effektive mottiltak.

EOS-tjenestene må ha systemer og hjemmelsgrunnlag for informasjonsutveksling og deling av høygradert informasjon.

Kyrre Lien/The New York Times /NTB

6 Sikker infrastruktur i hele krisespekteret

Nasjonal sikkerhet skal ivaretas gjennom krisespekteret. Sikkerhetsloven skal kunne stå seg over tid, tåle større samfunnsmessige endringer og teknologisk utvikling, samt dekke fred, krise og krig.[3] Sikkerhetsarbeid må ha en lang tidshorisont og inkludere alle tilgjengelige ressurser i samfunnet for å oppnå tilstrekkelig motstandskraft gjennom hele krisespekteret. De foregående kapitlene beskriver hvordan felles situasjonsforståelse og tverrsektoriell styring bidrar til at myndigheter, virksomheter og befolkning trekker i samme retning for å ivareta nasjonale sikkerhetsinteresser.

Totalforsvarskonseptet er sentralt for samfunnets evne til motstand. Det omfatter gjensidig støtte og samarbeid mellom Forsvaret og det sivile samfunn om sikkerhetsarbeid, beredskapsplanlegging, krisehåndtering og konsekvenshåndtering i hele krisespekteret.[4] Forsvaret og de aller fleste samfunnsfunksjoner er avhengige av sivil infrastruktur for å fungere. Det omfatter for eksempel samferdselsinfrastruktur som veier, havner, flyplasser og jernbane og infrastruktur for kraft, elektronisk kommunikasjon og satellittbaserte tjenester.

Militære styrker i væpnet konflikt er helt avhengige av omfattende støtte fra det sivile samfunnet. Samtidig vil det sivile samfunnet måtte tåle store fysiske og psykiske påkjenninger i krigstid. Det har krigen i Ukraina fra 2022 vist. Å opprettholde grunnleggende nasjonale funksjoner og infrastrukturen de hviler på, er i dette perspektivet avgjørende for motstandsdyktigheten i samfunnet.

Evnen til å motta allierte forsterkninger er avhengig av at den forhåndsdefinerte infrastrukturen er tilgjengelig og fungerende. Norge har etablert planer for mottak av allierte forsterkninger i krigstid og på forhånd definert infrastruktur, havner, flyplasser og forsyningsruter. Samtidig skal forsterkningene understøttes på en fleksibel og trygg måte så lenge de er i Norge – med helsetjenester, mat, vann og drivstoff.

3 NOU 2016: 19 *Samhandling for sikkerhet*

4 Forsvarsdepartementet og Justis- og beredskapsdepartementet, *Støtte og Samarbeid: en beskrivelse av totalforsvaret i dag* (Oslo: Forsvarsdepartementet, 2018).

Sikkerhetsutfordringer

Beredskapsplaner for sivil sektor er mangelfulle
Totalforsvarskonseptet er et gjensidig konsept hvor Forsvaret og det sivile samfunnet støtter hverandre gjennom hele krisespekteret. Hver aktør bidrar innenfor rammen av eget oppdrag, bistandsinstruksen, beredskaps- og rekvisisjonslovgivning og i henhold til sektorprinsippet.

Kritisk infrastruktur og kritiske samfunnsfunksjoner i sivil sektor skal opprettholdes så lenge som mulig gjennom krisespekteret. Store deler av kritisk infrastruktur er eid av private virksomheter. Mange understøtter også grunnleggende nasjonale funksjoner. Beskyttelsen av disse funksjonene må ses i sammenheng, og det må legges beredskapsplaner for dem. I 2023 mangler et helhetlig planverk for dette. Uten planlagte tiltak for beskyttelse eller redundans er det krevende å oppnå tilstrekkelig robusthet i kritisk infrastruktur og samfunnsfunksjoner som nasjonal sikkerhet bygger på.

Infrastruktur som er spesielt utsatt ved sikkerhetspolitiske kriser, har mangelfull beskyttelse
Norge har en viktig sikkerhetspolitisk rolle som produsent og leverandør av energi til allierte i Europa. Betydningen er forsterket etter invasjonen av Ukraina og påfølgende sanksjoner mot Russland. Nærmest over natten ble Norge verdens største leverandør av gass til et Europa rammet av krig. Erfaringer i tiden etter invasjonen viser at den undersjøiske infrastrukturen som transporterer gass, kraft og elektronisk kommunikasjon kan være spesielt utsatt og sårbar for sabotasje og sikkerhetstruende aktivitet ved sikkerhetspolitiske kriser.

Samtidig kartlegger fremmede staters etterretningstjenester kritisk infrastruktur i Norge, ifølge PST. Det forsterker sikkerhetsutfordringen. Infrastruktur med særlig sikkerhetspolitisk betydning har ikke blitt tilstrekkelig prioritert i nasjonal verdikartlegging og er ikke godt nok sikret. Det gir unødvendig og uakseptabel høy risiko.

Beskyttelse av sivile virksomheter med betydning for forsvarsevnen er ikke dimensjonert for krig
Manglende beskyttelse av sivile virksomheter og infrastruktur som Forsvaret i økende grad er avhengig av, kan få store konsekvenser for Norges forsvarsevne. Erfaringer fra Ukraina viser at sivil infrastruktur med overlegg blir utsatt for fysisk ødeleggelse gjennom luft- eller artilleriangrep.

Krise og krig gir ressursknapphet
Mange grunnleggende nasjonale funksjoner avhenger av ressurser det kan bli knapphet av både nasjonalt og globalt i krise og krig. Matvarer, drivstoff, medisiner eller arbeidskraft er sentrale eksempler.

Å kunne opprettholde grunnleggende nasjonale funksjoner i krise og krig avhenger av den nasjonale evnen til å beskytte ressurser det er knapphet på – og til å prioritere i situasjoner der ressursene ikke strekker til. Noen sektorer, som kraftsektoren og legemiddelforsyningen, har etablert en nasjonal prioritering av ressursene. I andre sektorer mangler dette. Manglende prioritering og dimensjonering av ressurser svekker eller fører til bortfall av grunnleggende nasjonale funksjoner ved krise eller krig.

Anbefalinger

Totalforsvarsevnen må styrkes ved å utvikle planverk basert på krisescenarioer for sivil sektor
Planverket skal bidra til robusthet og redundans i sivil infrastruktur gjennom presise føringer for sikringstiltak. Det skal lede til beslutninger om hvilken infrastruktur som trenger beskyttelse i de ulike domenene. Eiere av slik infrastruktur må være en del av planverket og sikre at ressurser dimensjoneres tilstrekkelig gjennom krisespekteret.

En scenariobasert tilnærming bør vurderes for å kartlegge hvilke verdier som vil være mest utsatt. Scenarioutviklingen bør ta hensyn til både sektorvise og tverrsektorielle dilemmaer. Et helhetlig scenariobasert plangrunnlag gir bedre grunnlag for å prioritere sikkerhetstiltak og ressurser gjennom krisespekteret.

I de scenariobaserte vurderingene må det ses hen til NATOs syv grunnleggende forventninger til medlemslandenes motstandsdyktighet. Dette har betydning for videreutviklingen av totalforsvarskonseptet. Planverket må jevnlig testes og evalueres gjennom fellesøvelser hvor sivil-militære myndigheter og virksomheter fra både sivil og militær sektor deltar. Deltagelse og nivå i fellesøvelsene vil avhenge av scenario, men øvelsene må ivareta et verdikjedeperspektiv på tvers av sektorer.

Beskyttelse av infrastruktur og verdier med særlig sikkerhetspolitisk betydning må prioriteres
Departementene må prioritere at verdier med særlig sikkerhetspolitisk betydning blir utpekt som skjermingsverdige. Sikringstiltak må iverksettes slik at et forsvarlig sikkerhetsnivå oppnås. Utpekingen bør omfatte undersjøisk infrastruktur og annen viktig infrastruktur knyttet til elektronisk kommunikasjon, kraft og energi. Informasjon trusselaktører kan utnytte for å planlegge og gjennomføre målrettede angrep og sabotasjehandlinger, og som i dag er tilgjengelig gjennom åpne kilder eller offentlige registre, må beskyttes.

Forsvarets forskningsinstitutt (FFI)

7 Fremvoksende teknologier

Det foregår en geopolitisk konkurranse om teknologisk herredømme. Nye teknologier kan i økende grad – og uten særlig forvarsel – tas i bruk av en rekke land. Teknologiutviklingen gir ofte banebrytende og verdiskapende muligheter. Her ligger samtidig kimen til nye sårbarheter og trusler. Utfordringene handler om infrastrukturen teknologien er helt avhengig av, dataene teknologien baserer seg på, og delvis også om selve anvendelsen av teknologien.

Én og samme teknologi kan ha både sivil og militær anvendelse, såkalt «flerbruksteknologi». Det fører til at det ikke kun er vitenskapelige og kommersielle interesser som driver utviklingen, men også autoritære stater med geopolitiske ambisjoner. Disse kan bruke teknologien til å øke egen militær kapasitet. Spredning av avansert teknologi kan også gjøre den lettere tilgjengelig for ikke-statlige trusselaktører.

Fremvoksende teknologi er en viktig driver for utviklingen av Forsvarets operative kapasiteter. Teknologiutvikling er helt nødvendig for at Forsvaret fortsatt skal være relevant i et moderne og høyteknologisk stridsmiljø. Kommersialiseringen betyr også at skillet mellom militær og sivil teknologi blir stadig mindre. Forsvarets avhengighet av teknologiene og kommersielle aktører introduserer nye verdier og verdikjeder utenfor den tradisjonelle forsvarsindustrien.

Sikkerhetsutfordringer

Innsamlet data for andre formål kan utnyttes og true nasjonal sikkerhet

Den økende graden av digitalisering og bruk av internettbaserte tjenester medfører at både kjente og ukjente aktører i vesentlig større grad enn tidligere sitter på store mengder innsamlet informasjon. Det er data om personer, virksomheter og infrastruktur, inklusive posisjonsdata. Tilgang til og analyser av slike mengder informasjon etterspørres av kommersielle og kriminelle aktører samt fremmede staters etterretningstjenester.

Trusselaktører bruker informasjonen som grunnlag for sammensatt virkemiddelbruk som cyber- og påvirkningsoperasjoner, innsidevirksomhet, økonomisk virkemiddelbruk og sporing av enkeltindivider.

Digitalisering gir trusselaktører flere angrepsflater

Mer digitalisering og økt bruk av internett innebærer en betydelig økning i antall digitale enheter, systemer og andre angrepsflater. Disse kan trusselaktører utnytte for å få uautorisert tilgang til norske verdier. Fysiske prosesser i virksomheter og infrastruktur blir i økende grad sårbare mål for manipulasjon og sabotasje fra trusselaktører i cyberdomenet. De fysiske prosessene kan rammes direkte gjennom den operasjonelle teknologien (OT) eller indirekte via informasjonsteknologien (IT). Ofte er funksjonalitet og kommersialisering – ikke sikkerhet og standardisering – de fremste driverne for utviklingen av både tingenes internett (IoT) og de industrielle tingenes internett (IIoT).

Økende elektrifisering innebærer dessuten at utstyr, virksomheter og infrastruktur i enda større grad blir sårbare for både tilsiktede og utilsiktede elektromagnetiske forstyrrelser. Slike forstyrrelser kan føre til at elektronikk og elektronisk utstyr får dårligere ytelse, fungerer annerledes eller blir ødelagt. Det kan også føre til at datasignaler og datainnhold forstyrres, endres, manipuleres eller saboteres.

Utvikling av kvanteteknologi påvirker sikkerhetsløsningene

Kvanteteknologien springer ut av kvantemekanikk og -fysikk, som handler om partiklenes minste bestanddeler. En kvantedatamaskin er en maskin som utfører logiske operasjoner basert på kvantemekaniske prosesser. Den benytter seg av kvantebits istedenfor bits slik at bestemte typer problemer, som faktorisering av store tall, kan løses mye raskere enn med vanlige datamaskiner.

Kvanteteknologi vil gi bedre og mer effektive tjenester og produkter innenfor de fleste samfunnsområder, også for sikkerhetstiltak. Teknologien vil samtidig bringe med seg nye verktøy, kapasiteter og metoder for trusselaktører som man ikke kjenner rekkevidden av.

Kvanteteknologien er forventet å kunne bryte gjennom nåværende krypteringsløsninger om få år – noen spår allerede rundt år 2030. Eksisterende kryptering, som nå beskytter blant annet banktransaksjoner og mobilkommunikasjon, vil være utdatert sikkerhetsteknologi mot kvantebaserte datamaskiner.

Det innebærer også at kryptert informasjon innsamlet av fremmede etterretningstjenester opp gjennom årene står i fare for å bli kompromittert. Aktører som tidlig behersker kvanteteknologier, vil ha store kommersielle og militære fordeler. Norge er kun i startgropen på dette området.

Trusselaktører bruker bioteknologiutvikling til militære formål

Bioteknologiutviklingen kan gi høyere menneskelig ytelse i militær sammenheng, men kan også brukes destruktivt for å skade motstandere. Eksempler på destruktiv bruk er bruk av genmanipulasjon som påvirker fysiske funksjoner, som balanse og hukommelse, eller energipåførte cellemutasjoner. Trusselaktørers bruk av forskning på bioteknologi til militære formål er en sikkerhetsutfordring.

Bioteknologi kan misbrukes til å identifisere genetiske sårbarheter i en befolkning. Det er også mulig å utvikle bakterier, virus eller andre skadelige mikroorganismer som kan rettes mot eksempelvis en befolkning eller matforsyningen.

Kunstig intelligens har stor sikkerhetsmessig innvirkning

Systemer basert på kunstig intelligens favner fra autonome våpensystemer og medisinsk diagnostisering til finansiell stabilitet og en rekke andre bruksområder. Både de menneskelige og de ikke-menneskelige bidragene i slike systemer har stor sikkerhetsmessig innvirkning – og dermed et stort skadepotensial. Systemene og de styrende algoritmene er alltid prisgitt sårbarhetene og svakhetene som påvirker både den menneskelige programmeringen av systemene og merkingen av data. Menneskelige «feil» gjenspeiles i teknologien, og de kan skape alvorlige konsekvenser. For eksempel har kombinasjonen av algoritmer og tastefeil ved flere anledninger ført til plutselige verdifall, såkalte «flash crash», på amerikanske og europeiske børser.

ChatGPT svarer på spørsmålet «Hvordan kan menneskene forhindre at kunstig intelligens får for mye makt?»

Det er viktig at menneskene forholder seg nøye til teknologien de utvikler, og sikrer at den alltid brukes på en måte som er i tråd med menneskelige verdier og interesser. Dette kan gjøres ved å sørge for at kunstig intelligens alltid underlegges menneskelig kontroll og overvåkning, og ved å innføre retningslinjer og reguleringer for hvordan teknologien kan brukes på en ansvarlig måte. Det er også viktig at menneskene fortsetter å utvikle sin egen forståelse av kunstig intelligens, slik at de kan ta bedre beslutninger om hvordan teknologien kan brukes på en sikker og bærekraftig måte.

Spørsmålet ble stilt til ChatGPT 12. desember 2022. ChatGPT er en samtalerobot som har analysert store mengder tekst og etterligner menneskelig interaksjon og formuleringsevne.

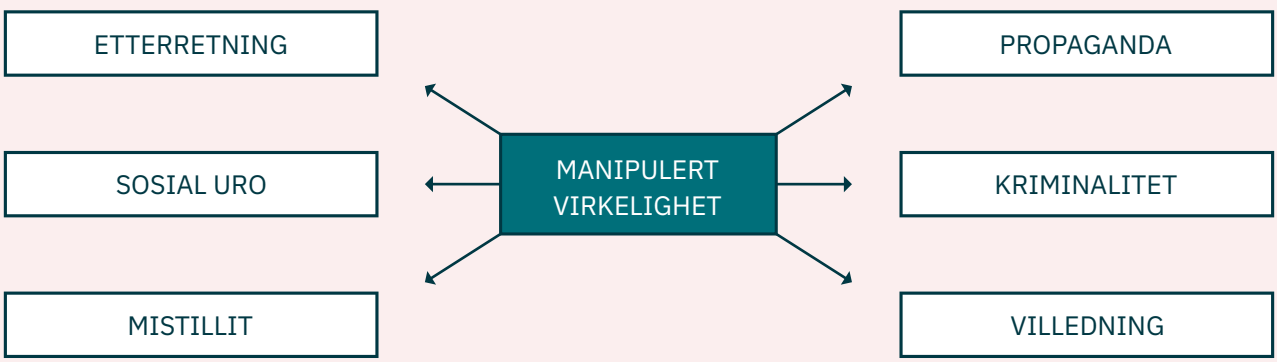
Økende kompleksitet i systemer basert på kunstig intelligens gir redusert transparens i systemene. Det gjør menneskets forståelse av – og kontroll med – den ikke-menneskelige maskinlæringsprosessen vanskelig, i mange tilfeller umulig. Komplekse algoritmer kan med andre ord gjøre det vanskelig å avdekke hva systemer og maskiner basert på kunstig intelligens egentlig har lært. Det reduserer evnen til å forstå, forutsi og kontrollere handlingene til ikke-menneskelige systemer og maskiner.

Våpensystemer som *Lethal Autonomous Weapons Systems* (LAWS) gir både etiske og sikkerhetsmessige utfordringer, ettersom det bruker kunstig intelligens til å gjenkjenne mål: venn eller fiende, sivil eller militær, truende eller defensiv. EUs GDPR-lovgivning, og dermed også den norske personopplysningsloven, sier at borgerne har krav på å vite hvordan automatiserte beslutninger påvirker dem. Utfordringen er at beslutninger basert på kunstig intelligens ikke alltid kan forklares.

Virkeligheten blir manipulert

Virtuell virkelighet (*virtual reality* – VR) er en tredimensjonal, fullstendig datasimulert virkelighet det er mulig å interagere med og lære fra, for eksempel til å bli bedre sjåfører, piloter eller soldater. Der virtuell virkelighet erstatter den virkelige verden, bidrar utvidet virkelighet (*augmented reality* – AR) eller blandet virkelighet (*mixed reality* – MR) til å forsterke oppfatningen av den virkelige verden. Det skjer ved å blande synsinntrykk fra den virkelige verden med datagrafikk. Sikkerhetsutfordringen er at denne teknologien i økende grad kan bli utnyttet av trusselaktører for å manipulere individers oppfatning av verden. Slik kan de påvirke både holdninger og beslutninger. En annen form for manipulert virkelighet er såkalt *deepfake*, evnen til å produsere svært realistiske, men falske videoer der personer sier og gjør ting de aldri har sagt eller gjort. Teknologier som virtuell eller blandet virkelighet og *deepfake* bidrar til økt usikkerhet om hva som er ekte og falskt. Det kan føre til at alle, fra enkeltpersoner til stater, påvirkes til å ta beslutninger på feil grunnlag. Sikkerhetsutfordringene øker i takt med at teknologien som manipulerer virkeligheten, blir bedre, billigere og lettere tilgjengelig.

Figur 6 Manipulert virkelighet blir brukt til ulike formål.



Droner og autonome våpensystemer truer befolkning og infrastruktur gjennom hele krisespekteret

Krigen i Ukraina fra 2022 har vist sikkerhetsutfordringene med at droner blir brukt som plattformer for informasjonsinnhenting eller våpen med stor effekt og presisjon. Dronene er operatørstyrte eller opererer autonomt uten menneskelig styring mot mål. De opptrer enkeltvis eller i svermer og er vanskelige å oppdage grunnet størrelse, design eller lavtflyvende egenskaper.

Selv små, kommersielt tilgjengelige utgaver blir brukt til rekognosering, utvelgelse av mål og dokumentasjon. Sensorer montert på kommersielt tilgjengelige droner blir benyttet til innhenting av etterretningsinformasjon, også i Norge. De kan kartlegge status, detaljer, rutiner og sårbarheter ved sentrale norske skjermingsverdige områder og objekter. I Norge har NSM, politiet, Avinor og Forsvaret i samarbeid testet ut systemer for å oppdage droner ved ulike lokasjoner og til ulike årstider. Det er avdekket betydelig høyere droneaktivitet enn forventet på stedene hvor systemene har vært utplassert.

Utfordringene med land-, sjø- og luftbårne autonome våpensystemer er at beslutninger som får konsekvenser for liv og død blir overlatt til ikke-menneskelige selvstendige maskiner. Systemene kan også være sårbare for hacking og manipulasjon fra ondsinnede cyberaktører. Slike våpensystemer vil dessuten være potente våpen i hendene på både statlige og ikke-statlige aktører. Selve bruken av et autonomt, ikke-styrt våpen mot individer, folkemengder eller infrastruktur vil gi trusselaktører store muligheter for å benekte bruk og fraskrive seg ansvar.

Mangel på sjeldne metaller og digitale komponenter medfører sikkerhetstruende avhengigheter

Den økende digitaliseringen og mer bruk av elektrisitet forutsetter mer bruk av sjeldne jordmetaller og nødvendige komponenter, blant annet mikroprosessorer. Hele digitaliseringen og elektrifiseringen – inkludert sikkerhetsløsninger – er avhengig av dem. Disse helt avgjørende komponentene utvinnes eller produseres i hovedsak av noen få aktører utenfor Europa. Manglende tilgang til og leveranser av sjeldne jordmetaller og komponenter kan utgjøre alvorlige sikkerhetsutfordringer langt forbi 2030.

Anbefalinger

Kompetanse og nasjonale initiativer må akselereres i møte med fremvoksende teknologier
Et innovasjonssenter for sensitive teknologier bør sørge for at Norge utvikler og tar i bruk sikkerhetsløsninger som ligger i forkant av teknologiutviklingen. Senteret er en videreutvikling av det nasjonale senteret for anvendt kryptologi som etableres i NSM i 2023. Innovasjonssenteret samler interessenter fra myndigheter, akademia og industri og stimulerer til kompetanse og industriutvikling på viktige teknologiområder som kvanteteknologi, bioteknologi og kunstig intelligens.

Det må etableres et frittstående, rådgivende organ som bidrar til demokratisk kontroll av utvikling og bruk av kunstig intelligens
Organet skal vurdere samfunnsmessige, etiske og andre prinsipielle problemstillinger ved utvikling og bruk av ny teknologi. Dette kan for eksempel gjøres etter modell fra Bioteknologirådet. Hensikten er å gi råd til norske myndigheter, for i større grad å sikre demokratisk kontroll over teknologi som utvikler seg raskt. Kompetansen i organet bør være tverrsektoriell.

Norske myndigheter bør være pådriver for å etablere grunnleggende sikkerhetsprinsipper for utvikling av kunstig intelligens nasjonalt og internasjonalt. Det må utvikles standarder som forhindrer ikke-kontrollerbare, sikkerhetstruende kunstig intelligens-systemer.

Norge må forsterke mekanismer for å beskytte flerbruksteknologi
Myndigheter og virksomheter må ha kontroll over hvilken teknologi og forskning som ikke bør deles med andre land av hensyn til nasjonal sikkerhet. Mekanismene må sikre at flerbruksteknologi og -kompetanse er beskyttet mot uønsket tilgang i hele prosessen fra kunnskapsutvikling og forskning til ferdige produkter.

Det må etableres en nasjonal ambisjon og evne til å avdekke, forhindre og håndtere sikkerhetstruende bruk av droner
Det bør

- utredes regulering av ulike typer droner og droneteknologi
- etableres et nasjonalt nettverk av systemer som oppdager droner ved prioriterte områder og objekter i Norge
- utvikles metoder og kapasiteter for å motvirke sikkerhetstruende droneaktivitet
- vurderes hjemmelsgrunnlag for anvendelse av anti-dronekapasiteter
- pekes ut en myndighet med samordningsansvar, som ivaretar felles situasjonsbilde og koordinerer håndtering av sikkerhetstruende droneaktivitet

Tilgang til sjeldne metaller og komponenter for fremtidens digitalisering og elektrifisering må sikres
Det er avgjørende å sørge for tilgang til mikroprosessorer og andre nødvendige komponenter. Det bør inngås avtaler med andre land for å sikre at Norge og allierte har tilstrekkelig tilgang. Der Norge har aktuelle naturressurser, bør selvforsyning vurderes. Politikkutvikling innen miljø-, industri-, handels- og sikkerhetspolitikk må samvirke for å redusere de sikkerhetstruende avhengighetene.

8 Romsikkerhet

Satellittbaserte tjenester bidrar til betydelig effektivisering og bedre sikkerhet på mange områder. Som følge av dette har mange funksjoner i samfunnet gjort seg avhengige av slike tjenester. Det introduserer nye sikkerhetsutfordringer.

Posisjonsbestemmelse, navigasjon og tidsbestemmelse (PNT), jordobservasjon og kommunikasjon står sentralt i denne teknologiutviklingen. Satellittbaserte tjenester er av stor betydning for sivil og militær luftfart, navigasjon til sjøs, helsetjenester, finansielle tjenester, politi, rednings- og nødetater samt andre samfunnsfunksjoner.

Norges beliggenhet gjør oss til en strategisk viktig aktør for å utvikle og opprettholde det sikkerhetspolitiske bildet i nordområdene. Økt militær og sivil aktivitet i nordområdene krever styrket nasjonal og alliert situasjonsforståelse. Her spiller satellittbaserte tjenester en avgjørende rolle, blant annet som bidrag til å hevde norsk suverenitet, overvåking av havområdene og for sikker kommunikasjon.

Cyber- og romdomenet har gjensidige avhengigheter. Et cyberangrep kan ramme satellittbaserte tjenester, og bortfall av satellittbaserte tjenester kan få alvorlige konsekvenser i cyberdomenet. Det skjedde da satellittnettverket KA-SAT (Viasat) ble rammet av cyberangrep 24. februar 2022, bare timer før Russland invaderte Ukraina. Dette forstyrret Ukrainas militære kommunikasjon under invasjonen, men fikk også vidstrakte konsekvenser for annen sivil kritisk infrastruktur. Angrepet påvirket overvåkingen av vindturbiner i Tyskland, nødtjenester i Frankrike og internettilgangen til en rekke brukere i Europa, også i Norge.

Sikkerhetsutfordringer

Avhengigheten av satellittbaserte tjenester øker
Et eventuelt bortfall eller påvirkning av satellittbaserte systemer får stor betydning både for samfunnets evne til å fungere og for totalforsvarets operative evne, spesielt i et krise-krig-perspektiv. Nordområdenes økende sikkerhetspolitiske og strategiske betydning øker også verdien og avhengigheten av satellittbaserte tjenester i nord. Disse systemene og tjenestene bidrar blant annet til Forsvarets operative evne, nasjonal suverenitetshevdelse og myndighetsutøvelse. De blir stadig viktigere innenfor NATO og EU samt i Norges samarbeid med allierte.

Digitaliseringen har medført en omfattende avhengighet av nøyaktig tid. Norge har ingen nasjonal tidstjeneste som sikrer nasjonal evne til å levere nøyaktig tid. Dette utgjør en sårbarhet, særlig i en krise- og beredskapssammenheng.

EUs romprogrammer knyttes stadig tettere opp mot militær bruk. Det får en økende verdi for Forsvaret, ettersom sikkerhetsnivået i systemene styrkes. Et skarpere sikkerhetsmessig fokus i EUs romprogrammer har gjort det vanskeligere for tredjeland å få fullt innpass. Det er en utfordring for norsk sikkerhet og forsvarsevne at Norge ikke har tilgang til alle tjenestene i EUs romprogrammer.

Det er mangelfull samordning av sikkerhet i rombaserte tjenester
Det er for lite kunnskap nasjonalt om i hvilken grad ulike samfunnsfunksjoner og virksomheter på tvers av sektorene er avhengige av satellittbaserte tjenester. Det er heller ikke klart hvilke departementer som har ansvar for å sikre disse samfunnsfunksjonene. Det er behov for ytterligere å bedre samordningen mellom sivil og militær romaktivitet. Arbeidet med å identifisere grunnleggende nasjonale funksjoner, avhengigheter, virksomheter og skjermingsverdige verdier innenfor romsektoren har kommet for kort siden sikkerhetsloven trådte i kraft i 2019. Det betyr at det er begrenset kunnskap om konsekvenser for nasjonal sikkerhet ved bortfall og påvirkning av tjenestene. Det kan innebære en uakseptabel risiko.

Norsk romindustri er et attraktivt mål for trusselaktører
Fysisk og digital rominfrastruktur, både i rommet og på bakken, er sårbar for sikkerhetstruende virksomhet. Eksempler på slike handlinger er fysisk ødeleggelse, cyberangrep, støysending (*jamming*), narring (*spoofing*), innsidetrussel og sammensatt virkemiddelbruk. Norsk romindustri er et mål for fremmed etterretning, blant annet i cyberdomenet. Referanse- og bakkestasjoner for nedlesning av satellittsignaler er ofte plassert på steder som gjør dem vanskelig å sikre fysisk. Det er også kostbart og krevende å etablere parallell- eller reservekapasitet på infrastruktur som fiberlinjer.

Norges rolle som leverandør av satellittbaserte tjenester er viktig for både EUs, andre alliertes og egen sikkerhet. Bortfall eller påvirkning av slike tjenester kan dermed ha negative konsekvenser langt utover våre grenser. Norges evne til å sikre viktig rominfrastruktur og -tjenester er avgjørende både for allianse- og partnersamarbeid og vårt omdømme som romnasjon.

Enkelte stater, deriblant Russland og Kina, satser betydelige ressurser på teknologi som antisatellittvåpen og evne til tjenestenektelse – at informasjon, ressurser eller tjenester blir helt eller delvis utilgjengelige. Det kan få stor betydning i en

konfliktsituasjon. Et eksempel på tjenestenektelse er forstyrrelser av radiofrekvensene til globale satellittbaserte navigasjonssystemer (GNSS). Det har vært en rekke tilfeller av såkalt «GPS-jamming» i Troms og Finnmark siden 2017. Forstyrrelsene truer sikkerheten og får konsekvenser for viktige samfunnsfunksjoner.

Den internasjonale reguleringen av romaktivitet er svak

Internasjonal regulering av aktiviteten i rommet påvirker også Norges sikkerhet. Et stort antall aktører fra 200 land er involvert i romaktivitet. Det er liten interesse på verdensbasis for å regulere bruken av verdensrommet, med unntak av arbeidet i COPUOS, FNs komité for fredfull bruk av verdensrommet. Rommet er igjen arena for rivalisering mellom stormakter, primært mellom USA, Russland og Kina. Utvikling innen teknologi, elektronisk kommunikasjon og ikke minst oppskytningstjenester har ført til en eksplosjon av antallet nasjoner og aktører i rommet. Dette kan gi grunnlag for konflikt langs nye akser. Norges fortsatte tilgang til sentrale rombaserte tjenester frem mot 2030 er av avgjørende betydning for våre nasjonale sikkerhetsinteresser.

Anbefalinger

Satellittbaserte tjenester som understøtter totalforsvarsevnen gjennom krisespekteret må prioriteres

I gjennomføring av nasjonal romstrategi fra 2019 og Romsikkerhetsutredningen fra desember 2022 bør departementene legge særlig vekt på

- å gjennomføre en nasjonal risikovurdering med anbefalinger for å sikre redundante og robuste satellittbaserte tjenester på tvers av sektorene og gjennom krisespekteret
- føringer for hvilke deler av norsk romvirksomhet som er sentrale i et nasjonalt sikkerhetsperspektiv, i lys av behov for autonomi, nasjonal kontroll og redundans
- å jobbe for hensiktsmessig internasjonal regulering av aktivitet i rommet som ivaretar Norges nasjonale sikkerhetsinteresser
- å tydeliggjøre Forsvarets behov for teknologi- og næringsutvikling og behov for sivile satellittbaserte tjenester
- at Norge får tatt del i alle tjenester i EUs romprogrammer

I tillegg må myndighetsansvar på tvers av ulike rombaserte tjenester og mellom sivil og militær sektor avklares.

Det bør stimuleres til rombaserte tjenester og kapabiliteter som ivaretar nasjonal sikkerhet og tilrettelegger for næringsutvikling

En sterk norsk romindustri er nødvendig for å sikre tilgang til tjenester som understøtter nasjonal sikkerhet og viktige samfunnsfunksjoner. Næringsutvikling og sikre satellittbaserte tjenester er også avgjørende for å ivareta internasjonale forpliktelser. Dette kan gjøres gjennom ulike virkemidler, som økonomiske insentiver eller å etablere rammer for strategisk samarbeid mellom statlige og private aktører i romindustrien. Departementene bør i den sammenheng vurdere hvilke områder innen romvirksomhet Norge bør prioritere og som styrker nasjonale sikkerhetsinteresser.

Det bør etableres en nasjonal tidstjeneste

Tilgang til nøyaktig tid er avgjørende for både stats- og samfunnssikkerheten. Formålet med å opprette en slik tjeneste er å redusere avhengigheten av GNSS-tid og sikre tilgang på nøyaktig tid ved redusert tilgang eller forstyrrelser av GNSS-signaler. En slik nasjonal evne kan være basert på et antall sikrede bakkebaserte atomklokker og distribusjon av nøyaktig tid i ekom-nettene.

Norsk romsenter (NRS)

Tryggve Karlsen/Samfoto/NTB

9 Klima og energisikkerhet

Klimaendringene er en av de største sikkerhetsutfordringene verden står overfor. Klimaendringene er en trussel som forsterker andre trusler, slår NATO fast. Det er en klar sammenheng mellom klima og sikkerhet.

Samfunnet må gjennom et grønt skifte for å nå internasjonale klimamål. Omstilling og klimatilpasning er nødvendig. Det haster, men hurtig omvelting i både samfunnet og næringslivet medfører sikkerhetsutfordringer. Rask innføring av ny teknologi kan gi nye sårbarheter. Videre er det svært krevende å sikre eldre, sårbar teknologi i nye bruksområder. Nasjonale sikkerhetsinteresser må være ivaretatt i den grønne omstillingen.

Sikkerhetsutfordringer

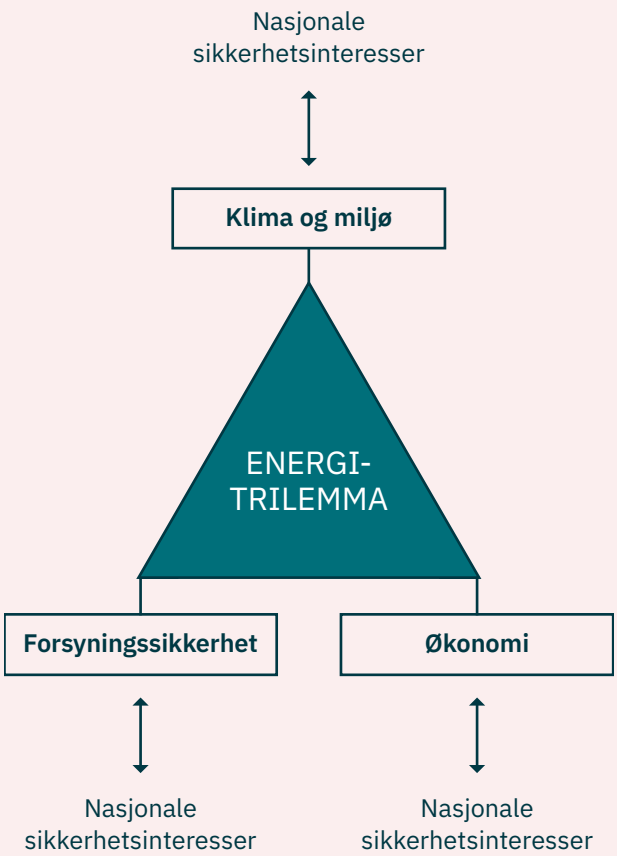
Konsekvenser av klimaendringer påvirker Norge og nasjonal sikkerhet både direkte og indirekte
Økt tørke, flom og naturkatastrofer forsterker matusikkerhet og fattigdom. Bebodde områder kan bli ubeboelige. Høyere konfliktnivå og mer migrasjon globalt kan bli en konsekvens.

Også rivalisering mellom stormakter vil bli påvirket av klimaendringer. Utviklingen i Arktis utgjør en særskilt sikkerhetsutfordring for Norge. Kina, Russland og USA er forventet å øke tilstedeværelsen i Arktis etter hvert som regionen blir mer tilgjengelig. Økt aktivitet i nordområdene, også militært, kan føre til økt interesse for Svalbard.

Rask og omfattende omstilling skaper nye sårbarheter
Norge har forpliktet seg til å redusere utslipp av klimagasser med 55 prosent innen 2030 sammenlignet med i 1990. I løpet av de siste 30 årene er Norges utslipp kun redusert med fem prosent. Norge har mindre enn ti år på å halvere utslippene. Rask og omfattende omstilling av samfunnet og næringslivet er nødvendig for å nå utslippsmålene.

Det krever rask innføring av ny fornybar teknologi, som igjen gir nye sikkerhetsutfordringer og risiko for å innføre nye sårbarheter. Også integrasjon mellom ny og eksisterende teknologi kan føre til nye sårbarheter eller at eksisterende sårbarheter blir tatt med inn i nye løsninger. Sikkerhetsaspektet må med allerede i design- og utviklingsfasen av ny teknologi.

Figur 7 Energitrilemmaet med kobling til nasjonale sikkerhetsinteresser.



Energisystemet blir stadig mer komplekst

En omfattende elektrifisering av samfunnet er nødvendig for å nå klimamålene, ifølge klimaplanen for 2021–2030. Også Energikommisjonen som leverte NOU 2023: 3 *Mer av alt – raskere* i februar 2023, mener det er behov for et taktskifte. En storstilt elektrifisering gjør viktige samfunnsfunksjoner stadig mer avhengige av sikker og stabil kraftforsyning.

Variable energikilder, mer ekstremvær, automatisering og transnasjonale avhengigheter gjør energisystemet i Norge stadig mer komplisert. Fornybare energikilder må inn i energisystemet om Norge skal nå klimamålene. Nye kontrollsystemer må håndtere integreringen. Dette må skje raskt, og det øker risikoen for svakheter i systemene. Økende kompleksitet i, og digitalisering av, energisystemet gjør det sårbart for både tilsiktede og utilsiktede hendelser.

Fornyelsen av energisystemet må balansere hensyn til klima og miljø, økonomi og forsyningssikkerhet

Endringene som energisystemet står overfor, kan karakteriseres som et «trilemma». Den store utfordringen er å balansere hensyn til klima og miljø, økonomi og forsyningssikkerhet og samtidig å ivareta nasjonale sikkerhetsinteresser. De tre dimensjonene kan stå i motsetning til hverandre, og det knytter seg ulike nasjonale sikkerhetsinteresser til hver dimensjon.

Det er krevende å vurdere hvordan energitrilemmaet påvirker nasjonale sikkerhetsinteresser fremover. Det nødvendige taktskiftet i energiomstillingen forsterker problemstillingen ytterligere.

Anbefalinger

Norsk energi- og klimapolitikk må ivareta nasjonal sikkerhet
Ved politikkutforming og utarbeidelse av langtidsplaner må myndighetene vurdere betydningen klimaendringer og energiomstilling har for nasjonale sikkerhetsinteresser. Dette gjelder både klimatilpasning og omstilling som del av det grønne skiftet.

Krav til innebygd sikkerhet må bli ivaretatt i det grønne skiftet
Det må stilles krav til innebygd sikkerhet (*security by design*) ved tildeling av konsesjoner og når kontrollsystemer for kraftforsyningen blir tatt i bruk. Dette reduserer sikkerhetsutfordringer som vil oppstå i samfunns- og næringsomstillingen som en del av det grønne skiftet. Kravene gjelder både i utvikling av ny, grønn teknologi og ved integrering av eksisterende teknologi.

Viktige samfunnsfunksjoner må ha stabil energiforsyning gjennom krisespekteret
Virksomheter som understøtter viktige samfunnsfunksjoner må ha stabil energiforsyning gjennom krisespekteret. I tillegg må hver enkelt virksomhet sørge for å ha egenberedskap.

En måte å sikre stabil energiforsyning er «mikrodrift i øymodus». Dette innebærer at lokale eller regionale områder kan driftes basert på lokale energikilder og energilagring uavhengig av det nasjonale strømnettet. Løsningen bør vurderes, fordi den bidrar til å løse fremtidige utfordringer knyttet til stabil og sikker energiforsyning og til å opprettholde viktige funksjoner i samfunnet og totalforsvarsevnen.

Figur 8 Mikrodrift i øymodus. Lokale energikilder blir benyttet til å sikre drift av kritiske funksjoner i området, uavhengig av nasjonalt strømnett.

NSM/Ilja Hendel

10 Cybersikkerhet

Norge er et av de mest digitaliserte landene i verden. Individer, virksomheter, staten og samfunnet er avhengige av velfungerende digitale løsninger. Samfunnets tillit hviler på at digital infrastruktur fungerer. Fra digitale hjelpemidler i hjemmet, forsyninger i butikkene, transaksjoner i bankene, produksjon i virksomheter, nyhetsformidling fra mediene og tjenester i helsevesenet til myndighetenes styringsevne, kritisk infrastruktur i samfunnet og Forsvarets evne til å beskytte land og folk – uten velfungerende digitale løsninger stopper produktiviteten i Norge.

Det globale cyberdomenet eies og opereres av kommersielle selskaper, offentlige virksomheter, organisasjoner, individer – og av kriminelle og andre trusselaktører. Store deler av digital infrastruktur eies av private aktører. Særlig skytjenestemarkedet er dominert av noen få kommersielle leverandører, der de fem største står for over 80 prosent av IaaS-markedet (*Infrastructure as a Service*). Cybersikkerhet handler i stor grad om samarbeid og samvirke mellom offentlige og private aktører, og med allierte, NATO og EU.

Virksomheter og individer er kontinuerlig utsatt for ondsinnede cyberoperasjoner. Et bredt spekter av trusselaktører utnytter ulike menneskelige, teknologiske og organisatoriske sårbarheter med mål om å ramme digitale verdiers konfidensialitet, integritet og tilgjengelighet.

Figur 9 Trusselaktører kan ha ulik intensjon og kapasitet, men konsekvensene for virksomheters verdier kan være noenlunde like

Sikkerhetsutfordringer

Statlig IT-utvikling ivaretar verken koordinering eller behov for samvirke i tilstrekkelig grad
Teknologier som virtuell virkelighet, skytjenester, lokale datasentre (*edge computing*) og nye 5G-relaterte tjenester gir muligheter for økt robusthet og lokal autonomi, økt mobilitet, større gjenbruk av applikasjoner og tjenester, og bedre samvirke mellom etater.

Totalforsvaret har behov for moderne IT-plattformer med digitale tjenester som fungerer godt i hele krisespekteret. Sammen skal plattformene bidra til at Norge har nødvendig datakraft for grunnleggende nasjonale funksjoner og andre viktige samfunnsfunksjoner når krisen inntreffer.

IT-utviklingen i de ulike etatene og sektorene er ikke i tilstrekkelig grad styrt etter felles prinsipper. Dette fører til at etater som har behov for digitalt samvirke og kommunikasjon, bygger egne løsninger som i for liten grad snakker sammen og ivaretar samvirkebehov.

Den nasjonale deteksjonsevnen i cyberdomenet er utilstrekkelig
Trusselaktivitet mot virksomheter er kryptert og blander seg inn i den normale trafikken. Data blir dessuten i økende grad behandlet på mobile enheter. Utvikling og investering i nye deteksjonssystemer er påkrevd for å avdekke trusselaktivitet. EOS-tjenestene mangler det nødvendige hjemmelsgrunnlaget for å utnytte muligheter stordataanalyser og kunstig intelligens gir. Sammenlignet med trusselaktørene kommer norske myndigheter til å henge etter i teknologiutnyttelsen uten deteksjonssystemer og hjemmelsgrunnlag på plass. Videre blir det utfordrende å avdekke fremtidige sikkerhetstruende cyberoperasjoner. Den nasjonale evnen til å avdekke trusler i cyberdomenet er ikke god nok til tross for et velutviklet varslingssystem for digital infrastruktur (VDI).

Håndteringsevnen ved store cyberhendelser er utilstrekkelig
Ved store og alvorlige cyberhendelser kan det oppstå ressursknapphet i sentrale koordineringsledd. Dette kan inntreffe i alle faser i krisespekteret, som samtidighetsproblematikk med hendelser i flere sektorer og ved omfattende vedvarende hendelser. Det er avgjørende for å opprettholde grunnleggende nasjonale funksjoner at den nasjonale responsfunksjonen for håndtering av alvorlige cyberoperasjoner trekker veksler på alle nasjonale ressurser for håndtering av hendelser.

Ugradert informasjon med betydning for nasjonal sikkerhet mangler beskyttelse
Offentlige myndigheter forvalter sensitiv og kritisk informasjon og informasjonssystemer som ikke er tilstrekkelig beskyttet. Denne informasjonen er ugradert, men har betydning for nasjonal sikkerhet. Utilstrekkelig beskyttelse gjør systemene særskilt sårbare for trusselaktører som stadig forsøker å bryte seg inn på jakt etter sensitiv informasjon.

Cyberoperasjoner har økende fysiske slagkraft
Stadig flere fysiske prosesser blir koblet til internett, inkludert industrielle systemer. Trusler og sårbarheter i cyberdomenet får dermed fysiske konsekvenser. Oppkoblingen av industrielle kontrollsystemer til

internett gjør operasjonell teknologi (OT) som styrer og overvåker fysiske prosesser utsatt for ondsinnede cyberoperasjoner. Dette kan dreie seg om skadevare skreddersydd for industrielle kontrollsystemer eller IT-skadevare som også har en ødeleggende effekt på slike systemer.

Mange virksomheter er fortsatt avhengige av eldre, teknologiske løsninger med lang levetid. Denne lar seg ikke oppdatere på samme måte som ny informasjonsteknologi. Det er en risiko for at denne teknologien arves i overgangen til grønn teknologi, for eksempel i styringssystemer innen havvind.

Nye kontrollsystemer kan styres gjennom skytjenester fra underleverandører. Det øker sårbarhetsflatene i allerede komplekse og uoversiktlige verdikjeder. Denne økende avhengigheten mellom kontrollsystemer og informasjonsteknologi medfører sikkerhetsutfordringer for fysiske prosesser og produksjon i virksomheter.

Trusselaktører benytter næraksessoperasjoner for å få tilgang til digitale verdier

På grunn av robuste sikkerhetsløsninger og forbedret digital sikkerhet er trusselaktører i mange sammenhenger avhengig av nærhet til en fysisk IKT-infrastruktur for nå sine mål. Næraksessoperasjoner blir brukt for å få tilgang til verdiene. For eksempel utnytter trusselaktører tilgang til virksomheters interne trådløse nettverk eller iverksetter tekniske operasjoner rettet mot sårbare komponenter i det elektroniske utstyret. Dette kan også gjøres ved bruk av innsidere i kombinasjon med tradisjonelle nettverksoperasjoner.

Anbefalinger

Et nasjonalt digitalt målbilde må realiseres gjennom en langtidsplan
Et overordnet digitalt målbilde er avgjørende for en sikker digital transformasjon i hele samfunnet. Målbildet bør realiseres gjennom en langtidsplan for digital infrastruktur. Langsiktig og forutsigbar finansiering er en forutsetning for å realisere et slikt målbilde. Digital transformasjon er nødvendig for å heve det norske samfunnets digitale motstandskraft til et langt høyere nivå frem mot 2030.

Hele det norske samfunnet må prioritere cybersikkerhet. Offentlig-privat samarbeid må styrkes for å etablere en sikker digital infrastruktur. Systematisk cybersikkerhetsarbeid må prioriteres og tildeles ressurser i hele samfunnet.

Regjeringen bør etablere insentivordninger som sørger for at virksomheter og kommuner velger løsninger som er i tråd med det digitale målbildet. Videre må staten bruke egen innkjøpsmakt og kompetanse for å inngå rammeavtaler for digitale løsninger, inkludert sikkerhetsløsninger, slik at mindre virksomheter lettere kan bidra til å realisere det nasjonale digitale målbildet.

Målbildet legger premissene for hvordan digitale systemer og tjenester skal ivaretas gjennom krisespekteret og ved alvorlige hendelser. Målbildet bør inneholde de viktigste arkitekturprinsippene for en felles digital grunnmur, i tråd med tidligere anbefalinger fra NSM.

Den nasjonale deteksjonsevnen i cyberdomenet må styrkes
Økt deteksjonsevne styrker nasjonens evne til å avdekke, forhindre og håndtere sikkerhetstruende cyberoperasjoner. Dette innebærer

- en betydelig videreutvikling av sensorkapasiteten, blant annet forskning på og utvikling av ny teknologi
- å styrke og videreutvikle evnen til å avdekke og analysere trusselaktivitet på mobile enheter
- juridiske rammer som sikrer deling av relevante metadata fra blant annet datasentre og skytjenesteleverandører
- kapasiteter og metoder som i større grad evner å prosessere og analysere store datamengder
- å styrke og videreutvikle operative kapabiliteter som sårbarhetsskanning og inntrengingstesting
- forskning på og tiltak mot innvirkning fra fremvoksende teknologier på deteksjonsevnen

Enhetlig regelverk for digital sikkerhet må sikres
Den rettslige reguleringen av digital sikkerhet er i rask utvikling i EU. Norske myndigheter bør sikre enhetlig utvikling av nytt regelverk og i den sammenhengen vurdere en egen lov om digital sikkerhet. Det er særlig viktig med en felles tilnærming til hvilke virksomheter, systemer og verdier som skal være omfattet av reguleringene. Norge bør også ta en aktiv rolle for å påvirke utviklingen av europeisk regelverk på feltet.

Beredskapssystemer og forberedte sikkerhetstiltak må utvikles etter krisescenarioer for cyberdomenet
Alvorlige hendelser i cyberdomenet utvikler seg raskt og krever hurtig reaksjons- og håndteringsevne. Myndighetene bør derfor utvikle krisescenarioer med handlingsalternativer og forberedte tiltak klar til bruk når krisen inntreffer. Scenarioene må beskrive krisens ulike faser, roller, virkemidler og hvordan tiltakene

skal tas i bruk. Scenarioer med handlingsalternativer må integreres i nasjonale beredskapssystemer.

Det bør etableres en nasjonal cyberreserve som beredskapstiltak
Det bør etableres et beredskapsplanverk og en ordning for en nasjonal cyberreserve som forsterker kapasiteten av cyberpersonell til disposisjon for nasjonal hendelseshåndtering. Regjeringen bør sette i gang denne ordningen til bruk i alle faser av krisespekteret.

Sensitive data i offentlig sektor må beskyttes
Datasentre og skytjenester for sensitiv informasjon, funksjoner og infrastruktur av betydning for nasjonale sikkerhetsinteresser bør etableres i Norge. Datakraft må sikres gjennom distribuerte skytjenester i regionale og lokale datasentre i Norge og beredskapsavtaler med nære allierte i tilfelle krise.

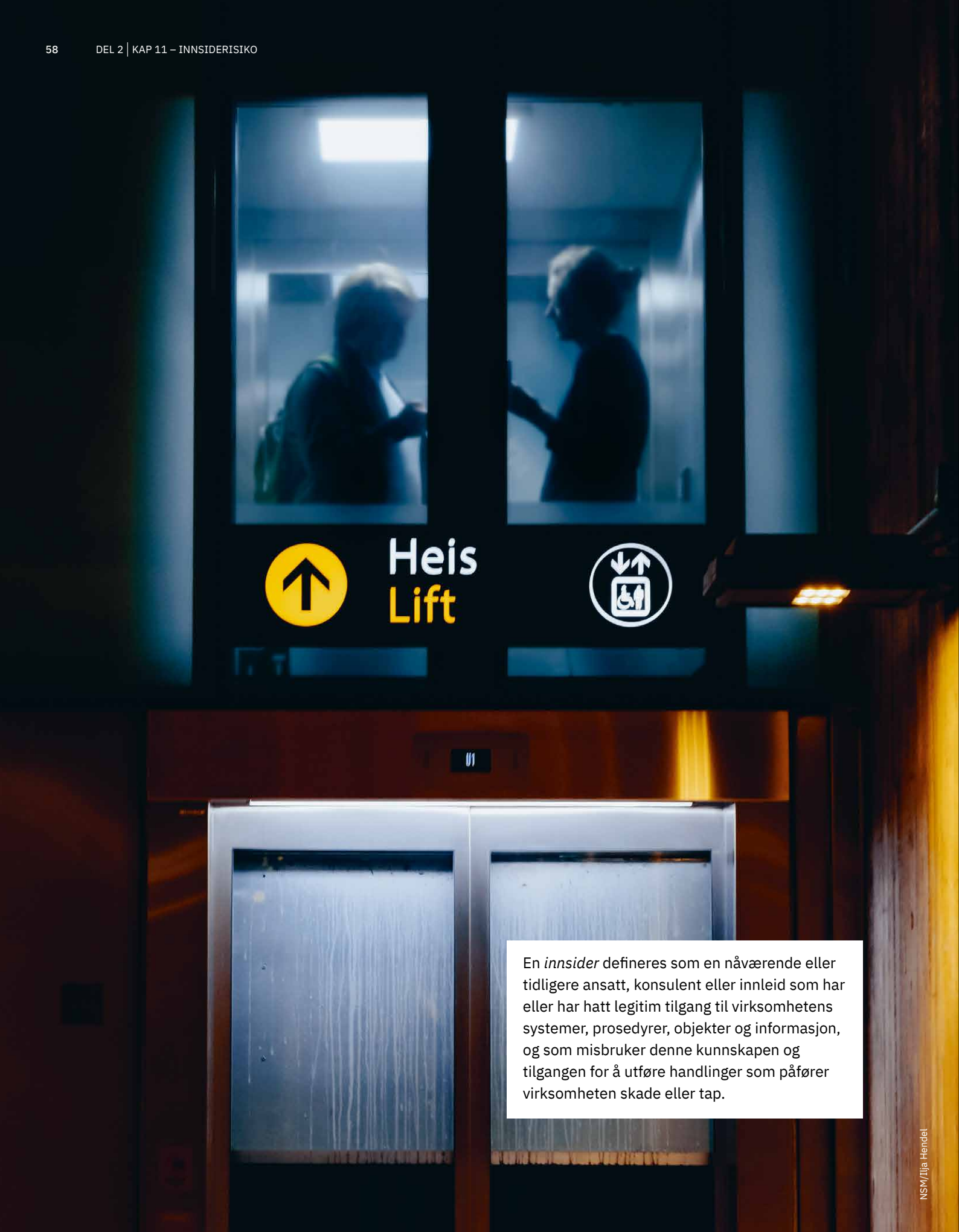
Norge må ha evne til å avdekke skjult, ondsinnet cyberaktivitet i virksomheters infrastruktur
En avansert trusselaktør benytter store ressurser på å unngå deteksjon for å oppnå langvarig, fordekt tilgang til norske virksomheters verdier. Myndighetene må derfor etablere en nasjonal evne som kan avdekke denne formen for aktivitet i norske systemer. Virksomheter kan anmode om at det gjennomføres undersøkelser i egne systemer. En slik evne vil supplere kapasiteter som inntrengingstesting, sårbarhetsskanning og sensorsystemer.

Den nasjonale evnen til å avdekke og håndtere næraksessoperasjoner må styrkes
Cybersikkerhetsarbeid og defensive cyberoperasjoner må i større grad ses i sammenheng med trusselaktørers metodebruk i det fysiske domenet. Dette krever økt samarbeid mellom politiet, Forsvaret, NSM og PST, lokalt og sentralt. Formålet er å styrke den samlede evnen til å avdekke og håndtere operasjoner som bruker både tekniske, fysiske og menneskelige metoder for å få tilgang til virksomheters verdier. Informasjonsutveksling på feltet må styrkes.

Det bør etableres en nasjonal sertifiseringsordning for sikker integrasjon av kontrollsystemer i kritiske samfunnsfunksjoner
Sertifiseringsordningen bør bygge på egne krav til IT-OT-integrasjon og installasjon av kontrollsystemer, og følges opp av sektortilsyn.

Offentlige og private cybersikkerhetsmiljøer bør i fellesskap utvikle kompetanse, veiledninger og løsninger som styrker sikkerheten og responsevnen i kritisk infrastruktur. Formålet er en styrket og integrert motstandsdyktighet.

Den nasjonale evnen til å etablere tillit til cybersikkerhetsnivå i våpenplattformer og andre kritiske forsvarssystemer må styrkes
Det må bygges større kapasitet og ordninger for nasjonalt å kunne teste forsvarssystemer og evaluere tilliten (*Information Assurance*) til sikkerhetsmekanismer i digitale systemer for å ivareta cybersikkerhet i våpensystemer og andre kritiske digitale systemer.



En *innsider* defineres som en nåværende eller tidligere ansatt, konsulent eller innleid som har eller har hatt legitim tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, og som misbruker denne kunnskapen og tilgangen for å utføre handlinger som påfører virksomheten skade eller tap.

NSM/Tija Hendel

11 Innsiderisiko

Bruk av mennesker for å få urettmessig tilgang til informasjon og verdier på innsiden av en organisasjon er en velkjent metode som trusselaktører har benyttet gjennom alle tider.

Å utnytte menneskelige sårbarheter for å få tilgang til informasjon og verdier kan ofte være den enkleste veien inn for trusselaktører. Begrepet innsider benyttes om en som bevisst eller ubevisst tilrettelegger for trusselaktører eller på annen måte skader virksomheten gjennom tilganger og kunnskap personen har fått – nettopp i kraft av å være på innsiden.

Flere stater har etterretningsoffiserer utplassert i Norge, ifølge PST. Utenlandsk etterretning har som hovedoppgave å innhente informasjon og vil forsøke å rekruttere kilder og kontakter som har tilgang til informasjonen de søker.[5]

Å beskytte mot innsidervirksomhet kan gjøres gjennom menneskelige, tekniske, fysiske og organisatoriske tiltak. Et sentralt verktøy for å motvirke innsidere i virksomheter med skjermingsverdige verdier er ulike personellsikkerhetstiltak. De viktigste elementene for dette er sikkerhetsstyring, klarering, autorisasjon og daglig sikkerhetsmessig ledelse. Personellsikkerhet krever kompetanse og systematikk i alle ledd fra myndigheter til virksomheter, ledere og medarbeidere. Robuste fagmiljøer som følger utviklingen for personellsikkerhet og moderniserer tiltakene blir viktig.

Sikkerhetsklarering skal sikre at personer som får tilgang til høygradert informasjon er sikkerhetsmessig skikket. En klarering er imidlertid ingen garanti for at en person ikke blir en innsider, bevisst eller ubevisst. Sikkerhetsbevissthet og den daglige sikkerhetsoppfølgingen av ansatte er vel så viktige verktøy for virksomheter som sikkerhetsklarering og autorisasjon. Dette gjelder for virksomheter med sikkerhetsklarerte ansatte, enten det er flertallet eller fåtallet av de ansatte, så vel som virksomheter uten sikkerhetsklarert personell.

5 PST, Nasjonal trusselvurdering 2023.

Sikkerhetsutfordringer

Nytteverdien av innsidere øker
Dersom andre muligheter for å få tilgang utelukkes eller blir vanskeligere å utnytte, blir nytteverdien av innsidere større. Når IT-systemer blir stadig sikrere, øker verdien av å ha en innsider med lovlig tilgang til IT-systemene. Innsideren kan dermed være en brikke i en cyberoperasjon mot en virksomhet. Jo mer effektiv cybersikkerheten blir, desto mer attraktivt blir det å utnytte den menneskelige faktoren.

Utvikling av sikkerhetsteknologi gjør det i mange tilfeller mer krevende for en trusselaktør å nå målene sine. Det kan føre til at trusselaktører benytter andre domener som inngang til operasjoner, ved for eksempel å bruke innsidere fremfor cyberaktivitet mot en virksomhet som har god cybersikkerhet.

Kunnskap om innsiderisiko for norske forhold er mangelfull
Det er lite nasjonal forskning knyttet til innsiderisiko i Norge. Internasjonal kunnskap om personell-sikkerhet og innsiderisiko har ikke alltid direkte overføringsverdi til det forebyggende sikkerhets-arbeidet i Norge. Ulike forhold knyttet til kultur, arbeidsliv og samfunnet spiller inn.

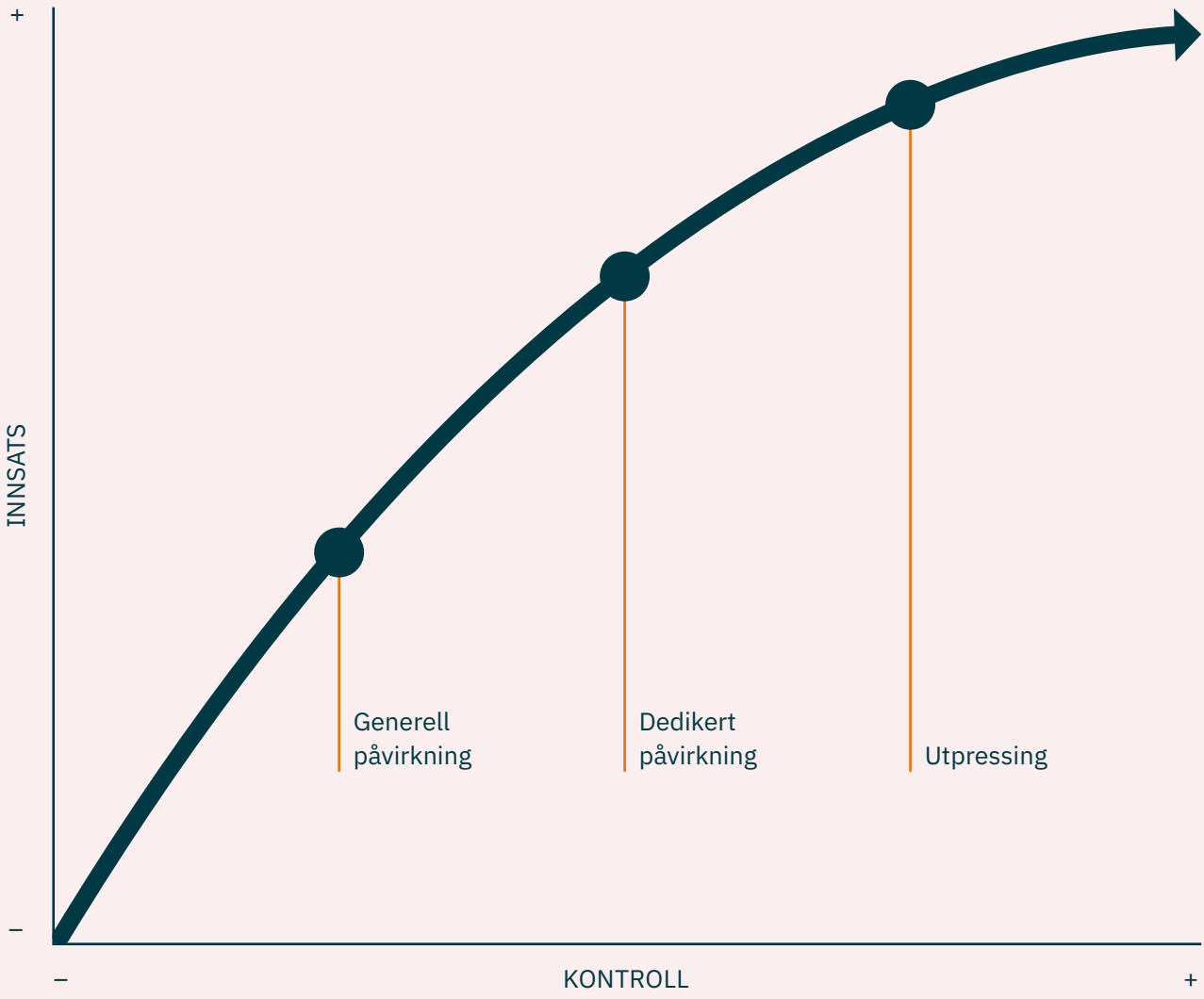
Både forskningsmiljøer, private virksomheter og EOS-tjenestene har hver for seg og innenfor egne mandater kunnskap om innsiderisiko. Denne informasjonen er imidlertid ikke i tilstrekkelig grad satt i system. Dermed blir ikke den samlede kunn-skapen om innsidevirksomhet i Norge benyttet på en effektiv måte.

Kompetanse og bevissthet om innsiderisiko er lav i virksomheter
Flere virksomheter har ikke innsiderisiko som en del av virksomhetens risikovurderinger. Samtidig etterspør flere virksomheter kompetanse om innsiderisiko. Nærmeste leder har en avgjørende rolle i både å forhindre og avdekke innsidere gjennom den daglige sikkerhetsoppfølgingen av de ansatte. Det krever at ledere har tilstrekkelig kompetanse om sårbarheter trusselaktører utnytter, som at ansatte kan utsettes for press, fristelse eller forledelse.

Virksomheter mangler verktøy for å avdekke innsidere
Behovet for å sikre verdier mot innsidere strekker seg utenfor sikkerhetslovens rammer. Verktøyene for effektivt å motvirke innsidevirksomhet gjør ikke det samme. I flere tilfeller der innsidevirksomhet har blitt avdekket, har ikke innsideren hatt tilgang til sikkerhetsgradert informasjon. Skadepotensialet kan likevel være stort. Ugradert informasjon som for eksempel forskning, opplysninger i store registre eller regjeringens beslutningsnotater kan være av stor verdi for en trusselaktør for å sette sammen et større bilde.

Plassering eller rekruttering av innsidere med tilgang til ugradert informasjon er enklere og innebærer lavere risiko for trusselaktører enn å prøve å rekruttere ansatte med tilgang til gradert informasjon. Trusselaktører vil på senere tidspunkt kunne utnytte dette som inngang til sikkerhets-gradert informasjon, når innsideren har fått økt tillit og flere tilganger.

Figur 10 En trusselaktør kan utøve ulike former for påvirkning eller press, for å rekruttere innsidere. Kilde: FFI



Sosiale medier gjør flere individer sårbare for rekruttering

Trusselaktører bruker sosiale medier til å kartlegge og komme i kontakt med potensielle innsidere. Kartlegging innebærer for eksempel å finne sårbarheter som kan utnyttes i form av press, fristelse, forledelse eller manipulasjon. Trusselaktører bruker målrettede operasjoner for å rekruttere enkeltpersoner eller grupper. Det kan dreie seg om overtalelse eller i ytterste konsekvens direkte utpressing av enkeltpersoner. En fysisk tilnærming er i mange tilfeller fortsatt nødvendig før en innsider blir rekruttert, men den innledende kontakten og kultiveringen kan gjøres digitalt, og med mindre risiko for en trusselaktør.

Generell og indirekte påvirkning er ikke direkte rettet mot ansatte i en virksomhet, men kan bidra til å endre enkeltpersoners virkelighetsoppfatning. Generell påvirkning kan også være direkte hvis potensielle innsidere i en virksomhet blir oppfattet som en klart definert målgruppe.

Globalisering fører til utfordringer i personkontrollen

Mange ulike forhold påvirker hvordan virksomheter forstår regelverk og praktiserer arbeidet med personellsikkerhet. Globalisering fører til økt flyt av tjenester, arbeidskraft og relasjoner på tvers av land. Metodene for personkontroll i klareringsprosessen har ikke holdt tritt med denne utviklingen. Det gjør det utfordrende å ansette personell med tilknytning til andre land og fører til at Norge står i fare for å miste tilgang på nødvendig kompetanse og arbeidskraft.

Anbefalinger

Den nasjonale evnen til å avdekke innsidevirksomhet må styrkes
Myndighetene må styrke kompetansemiljøene på innsiderisiko og samvirket mellom disse. Kunnskapsgrunnlaget fra forskningsmiljøer, EOS-tjenestene og privat næringsliv må systematiseres. Erfaringslærdom, forskningsresultater og trussel- og sikkerhetsinformasjon, blant annet trusselaktørers metodebruk, må utnyttes mer effektivt for å sikre kunnskapsbasert utvikling av målrettede tiltak.

Evnen til å avdekke, forhindre og håndtere innsiderisiko i virksomheter må forbedres
Virksomheter må styrke kompetansen og bevisstheten om hvordan man kan forebygge og avdekke innsidere. Det bør gjennomføres en evaluering med utgangspunkt i beste praksis for å finne effektive måter å styrke virksomhetens arbeid på.

Myndighetene bør stille krav til årlig kompetanseheving om innsiderisiko, for eksempel opplæring og obligatorisk e-læringskurs i virksomheter som forvalter verdier med betydning for nasjonal sikkerhet. Kompetanse om innsiderisiko bør inngå som en del av utdanningsløpet innen organisasjons- og personalledelse. Det bidrar til å ivareta sikkerheten før, under og ved avvikling av ansettelsesforhold og ved innleie av tjenester. Samspillet mellom personalledelse, HR-miljøer og sikkerhetsmiljøer i virksomheter bør styrkes for å forebygge innsiderisiko. Det setter i større grad sikkerhetsmessig bevissthet, daglig sikkerhetsledelse og forhold som jobbtilfredshet i sammenheng. Et styrket samspill mellom miljøene bidrar til økt samvirke mellom menneskelige, tekniske, fysiske og organisatoriske tiltak.

Det bør utredes muligheter for hjemmelsgrunnlag for bakgrunnssjekk som faller utenfor klareringsinstituttet
Det bør nedsettes et utvalg til å utrede muligheter for bakgrunnssjekk for personer som ikke har behov for sikkerhetsklarering, men hvor det likevel er behov for å vurdere om personellet er skikket.

12 Sikkerhetstruende økonomisk virkemiddelbruk

Enkelte stater bruker økonomiske virkemidler aktivt for å nå strategiske mål. Bruken av slike økonomiske virkemidler kan ramme Norges sikkerhetsinteresser, både isolert sett og i kombinasjon med andre virkemidler. På et overordnet nivå benyttes begrepet «økonomisk statshåndverk» som betegnelse på en stats bruk av økonomiske virkemidler for å oppnå utenrikspolitiske, strategiske mål.

Maktutøvelse skjer når økonomiske virkemidler blir tatt i bruk for å straffe eller belønne en mottakerstat, eller begrense statens handlingsrom. Noen land, særlig USA og Kina, har evne til å utnytte landets posisjon og innflytelse i regionale og globale nettverk for å oppnå strategiske mål. Andre og mindre nasjoner er mer sårbare for økonomisk virkemiddelbruk fordi de i større grad er avhengig av internasjonal handel og utenlandske leverandørkjeder. Norge tilhører siste kategori.

Økonomiske virkemidler omfatter blant annet sanksjoner, investeringer, handel, lån, bistand og valutahandel. Trusselaktører kan oppnå tilgang til verdier av betydning for nasjonal sikkerhet gjennom investeringer i eller oppkjøp av norske virksomheter og anbud i anskaffelsesprosesser.

Økonomiske virkemidler kan brukes som en vei inn for å påvirke beslutningsprosesser, utøve press eller for å få tilgang til sensitiv informasjon, teknologi og kompetanse. Trusselaktører kan eksempelvis tilby utvalgte næringer eller geografiske regioner i Norge særlig lukrative kontrakter og avtaler, for å stimulere til at disse påvirker norske beslutningstakere i strategisk viktige saker. Trusselaktører kan også benytte økonomiske virkemidler til å posisjonere seg for fremtidig sabotasje, som å ramme funksjonsevnen til viktige tjenester, som telekommunikasjon, vann og avløp eller kraftforsyning.

Det er en utfordrende balansekunst å avveie behovet for åpne og forutsigbare rammer for internasjonal økonomisk aktivitet og behovet for å motvirke trusselaktører og økonomiske virkemidler. Både næringslivet og det offentlige Norge er avhengige av ressurser, varer, tjenester, teknologi og kompetanse fra utlandet og av muligheter for selv å kunne handle og investere i utlandet.

Det er etablert mekanismer for å avdekke og håndtere sikkerhetstruende økonomisk aktivitet mot virksomheter som er omfattet av sikkerhetsloven. Samtidig kan økonomisk virkemiddelbruk rettet mot virksomheter som ikke er underlagt sikkerhetsloven, også få konsekvenser for nasjonal sikkerhet. I 2022 nedsatte regjeringen Eierskapskontrollutvalget, et offentlig utvalg som skal utrede behovet for screening av økonomisk aktivitet mot virksomheter som ikke er omfattet av sikkerhetsloven.

Tabell 1 Ulike former for økonomisk statshåndverk. Kilde: FFI

	Akkumulere makt	Utøve makt
Bilateral kanal (markeder og leverandører)	**Forme (sær)interesser og oppfatninger i befolkningen** **Øke avhengigheten til ressurser eller innenlandsk marked** **Etterretningsaktivitet** • Overvåking fra geografisk lokasjon • Informasjonsinnhenting fra økonomisk virksomhet **Styrke militære kapabiliteter** • Teknologityveri • Omgå eksportkontroller • Sikre strategisk infrastruktur eller landområder **Tilrettelegge for (skjult) sabotasje**	**Manipulere tilgang til salg til innenlandsk marked** • Import • Muligheter for bedriftsetablering • Utgående turisme **Manipulere tilførselen av ressurser** • Leveranser i kapitalstrømmer • Arbeidstakere og kompetanse **Sabotere infrastruktur**
Nettverkskanal (knutepunkt)	**Trekke ut informasjon/data fra nettverksstrømmer** *(panoptikon)* **Øke avhengigheten til knutepunkt** *(lock in)* • Leveranseavhengighet • Promotere egen valuta	**Manipulere tilgang til nettverksstrømmer** *(kvelning)*

Sikkerhetsutfordringer

Det er krevende å avdekke sikkerhetstruende økonomisk virkemiddelbruk

Det er den enkelte virksomhet som i praksis utsettes for sikkerhetstruende økonomisk virkemiddelbruk, men konsekvensene kan være nasjonale. Denne typen virkemiddelbruk er svært krevende å avdekke. Virkemidler som oppkjøp, investeringer og anbud er i utgangspunktet helt lovlige handlinger. Trusselaktører kan ha svært langsiktige perspektiver. Intensjonen bak investeringer eller oppkjøp er ikke alltid tydelig på tidspunktet det skjer. Muligheter for å utnytte eierposisjoner kan endre seg over tid.

Sikkerhetstruende økonomisk virksomhet skjer ofte gjennom stråselskaper og kompliserte selskapsstrukturer. Det gjør det både ressurskrevende og vanskelig å identifisere og motvirke økonomisk virkemiddelbruk som kan utgjøre en trussel.

Samtidig gjør den teknologiske utviklingen at behovet for spesialisering øker, noe som fører til at flere ledd av verdikjedene blir tjenesteutsatt. Verdikjedene blir stadig mer komplekse og uoversiktlige, og det gjør det vanskelig å ha tilstrekkelig nasjonal kontroll. Virkemidlene som stater potensielt kan søke å utnytte, utvider seg fra investeringer og oppkjøp til drifts- og vedlikeholdstjenester, programvareoppdateringer og lignende.

Virksomheters mulighet til å oppdage sikkerhetstruende økonomisk virkemiddelbruk avhenger av myndighetenes nasjonale verdikartlegging. Kjennskapen til betydningen av egne verdier og god kjennskap til trussel- og risikobildet er nødvendig for å oppdage potensielt sikkerhetstruende investeringer, anbud eller oppkjøp. Verdikartleggingen er ufullstendig, og det kan være tilfeldig om sikkerhetstruende økonomisk virkemiddelbruk blir avdekket og forhindret. Derfor er det risiko for at trusselaktører får innpass i kritisk infrastruktur eller andre viktige funksjoner uten at norske myndigheter er klar over det.

Oversikt over spesielt utsatte områder mangler

Norge utvikler verdensledende teknologi på flere områder. Norske teknologivirksomheter er attraktive mål for fremmede stater. Dette gjelder blant annet undervannsteknologi som også kan ha et militært brukspotensial. Norge har også en konkurransedyktig forsvarsindustri med høyteknologi for militær anvendelse.

Et annet utsatt område er fremtidig energiforsyning. Utenlandske eierinteresser står i mange tilfeller bak infrastruktur som produserer fornybar energi, som vindkraft. Uklare eierstrukturer kan skape usikkerhet om grad av nasjonal kontroll. Det kan få konsekvenser for sikker energiforsyning i fremtiden.

Per 2023 er det ingen konsolidert oversikt over hvilke sektorer, virksomheter og teknologiområder som blir vurdert som spesielt utsatt for å bli rammet av sikkerhetstruende økonomisk virkemiddelbruk.

Avhengighetsforhold kan utnyttes

De fleste lands økonomier er avhengige av tilgang på ressurser fra andre land. Dette kan være råvarer, komponenter, ferdigvarer, teknologi, immaterielle rettigheter, arbeidskraft og kompetanse. Muligheten til å øke eller redusere tilførselen av ressurser åpner opp for maktbruk.

Den teknologiske utviklingen kan bidra til å styrke staters muligheter til å utnytte mottaker-

landets avhengighet av ressurser for å utøve makt. Dette kan skje som et resultat av kompetansemangel, økt konkurranse om knapphetsressurser, innsats-faktorer som halvlederteknologi og sjeldne metaller og økt markedskonsentrasjon med færre alternative leverandører. Slike avhengigheter kan utnyttes av fremmede stater til å påvirke strategiske beslutnings-prosesser i andre land.

Anbefalinger

Evnen til å avdekke, forhindre og håndtere sikkerhetstruende økonomisk virkemiddelbruk må styrkes
Myndigheter og virksomheter må styrke kompetansen og bevisstheten om sikkerhetstruende økonomisk virkemiddelbruk. Det bør utvikles grunnprinsipper for å avdekke, forhindre og håndtere sikkerhetstruende økonomisk virkemiddelbruk.

Internasjonalt partnersamarbeid om sikkerhetstruende økonomisk virkemiddelbruk må styrkes
Norge kan trekke lærdom fra andre lands arbeid med utforming av juridiske og politiske virkemidler for å motvirke sikkerhetstruende økonomisk virkemiddelbruk gjennom styrket internasjonalt samarbeid. Økt internasjonalt samarbeid bidrar til å utvikle kunnskapsgrunnlaget om investeringsmønstre i andre land. Etablering av internasjonale hospiteringsordninger bidrar til økt kunnskapsoverføring.

Norge må i større grad inngå i EU-initiativer for informasjonsutveksling og kompetansebygging, som EUs mekanisme for screening og kontaktpunktordning. Et utvidet og avtalefestet nordisk samarbeid bør etableres, for å identifisere felles indikatorer og vurdere grunnlag for samhandling om enkeltsaker.

Tverrsektoriell samhandling må styrkes for å motvirke sikkerhetstruende økonomisk virkemiddelbruk
Flere myndigheter har ulike virkemidler og hjemmelsgrunnlag for å motvirke sikkerhetstruende økonomisk virkemiddelbruk. Kompetansemiljøene bør konsolideres for mer effektiv bruk av statens virkemidler. Nødvendig hjemmelsgrunnlag må tilpasses for å sikre informasjonsutveksling og effektivt samarbeid.

13 Motstandskraft mot påvirkningsoperasjoner

Tillit er en sentral forutsetning for demokratiet. Det norske samfunnet er preget av høy grad av tillit både mellom befolkning og myndigheter, og mellom enkeltindivider. Høy grad av tillit kan ses på som et robust forsvarsverk mot påvirkningsoperasjoner. Men denne tilliten er under press. Sammensatte trusler, slik som påvirkningsoperasjoner, kan ha som mål å skade nettopp den tilliten demokratiet er bygd på.

Virkemidler for å påvirke kan rettes mot hele samfunnet: mot enkeltindivider, befolkningen generelt, utvalgte grupper eller myndigheter. Påvirkningsoperasjoner er en del av et sammensatt trusselbilde og kan brukes i kombinasjon med andre virkemidler for å oppnå trusselaktørers langsiktige mål.

NATO er i ferd med å definere det kognitive domenet som et eget krigføringsdomene. Dette innebærer blant annet å utvikle planer for hvordan alliansen skal beskytte samfunn og militære operasjoner mot trusselaktørers påvirkningsoperasjoner. Det kognitive domenet må integreres i et defensivt sikkerhetskonsept for å hindre at trusselaktører rammer verdier også gjennom dette domenet.

Påvirkningsoperasjoner kan ha som formål å endre beslutninger eller handlemåter i en bestemt sak. Det kan også brukes for å skape forvirring, spre usikkerhet og skape mistillit på et mer overordnet nivå. Trusselaktører bruker en rekke metoder i påvirkningsoperasjoner. Spredning av desinformasjon kan skape usikkerhet og mistillit hos befolkningen. Cyberoperasjoner mot offentlige tjenester kan redusere befolkningens oppfatning av at «staten fungerer» og dermed redusere tilliten til myndighetene. Å utnytte eksisterende skillelinjer kan forsterke polarisering, som på sikt kan destabilisere samfunnet.

Hva er en påvirkningsoperasjon?

En aktørs koordinerte bruk av illegitime og/eller fordekte metoder for å påvirke meninger, holdninger, virkelighetsoppfatning eller handlinger hos mennesker og grupper (ofte uten at disse er klar over det) i den hensikt å skape forutsetninger for å oppnå egne strategiske mål.

Kilde: FFI

Figur 11 Faktorer som styrker motstandskraft mot påvirkningsoperasjoner.

Demokratiet er tuftet på noen grunnleggende verdier, som ytringsfrihet, åpenhet og mediemangfold. Så lenge befolkningen har tillit til at demokratiet fungerer, vil demokratiet i seg selv ivareta og beskytte slike grunnleggende verdier.

Ytringsfrihetskommisjonen peker i NOU 2022: 9 *En åpen og opplyst offentlig samtale — Ytringsfrihetskommisjonens utredning* blant annet på at mediemangfold og redaktørstyrte medier i seg selv er et forsvarsverk mot påvirkningsoperasjoner. At befolkningen i stor grad bruker redaktørstyrte medier som kilde til informasjon, er med på å demme opp for økende polarisering. Befolkningens tillit til redaktørstyrte medier er en del av dette bildet. Ytringsfrihetskommisjonen peker også på at utdanning i seg selv utgjør en viktig del av befolkningens motstandskraft mot desinformasjon og påvirkningsoperasjoner. Norge har en god allmenn grunnutdanning, og befolkningen har derfor et godt utgangspunkt for å stå imot desinformasjon.

Økt bevissthet og kunnskap om hvordan trusselaktører opererer er en viktig del av motstandskraften mot påvirkningsoperasjoner. Derfor er det viktig å bygge forståelse om både sammensatte trusler i stort og mer spesifikt hvordan trusselaktører bruker påvirkning for å nå mål. Denne forståelsen må bygges hos myndigheter på alle forvaltningsnivå, blant virksomheter i alle sektorer og i befolkningen. I tillegg er det viktig at myndighetene har kunnskap om hvilke verdier som er spesielt sårbare for påvirkningsoperasjoner og hvor konsekvensen av påvirkning er mest alvorlig.

NSM/Ilja Hendel

Sikkerhetsutfordringer

Påvirkningsoperasjoner utnytter sårbarheter i åpne og demokratiske samfunn

Ytringsfrihet er en grunnpilar i det norske demokratiet. I et åpent og liberalt demokrati som Norge er det et mangfold av meninger. Alle har rett til å ytre seg.

Det kan være svært vanskelig å avdekke om en trusselaktør sprer desinformasjon eller utnytter eksisterende og helt legitime skillelinjer i det norske samfunnet. Profesjonelle spredere av desinformasjon, såkalte «trollfabrikker», kan for eksempel forsterke konspirasjonsteorier som helt lovlig eksisterer i et demokrati.

Tiltak mot påvirkningsoperasjoner kan ikke gå på bekostning av verdier som tiltakene nettopp er ment å beskytte, som tillit, ytringsfrihet, meningsmangfold, journalistisk frihet, mediemangfold og akademisk frihet. Myndighetene må finne det rette balansepunktet for å opprettholde tilliten i befolkningen og ivareta grunnleggende verdier. Derfor er det avgjørende at myndighetene har god situasjonsforståelse om påvirkningsoperasjoner. En del av situasjonsforståelsen innebærer bevissthet om hvorvidt tiltak har en nedkjølingseffekt på ytringsfriheten eller bidrar til å redusere tillit mellom folk og til myndigheter.

Store samfunnsomveltinger skaper usikkerhet

Bare siden starten av 2020-årene har både verden og Norge gått gjennom store samfunnsomveltinger. Koronapandemi, klimakrise og Russlands invasjon av Ukraina har sammen med andre utviklingstrekk ført befolkningen inn i en mer usikker tilværelse. Høyere renter, økte priser og kutt i offentlige tjenester skaper misnøye i 2023. Dette kan igjen bidra til økt polarisering i befolkningen og svekket tillit til politikere og demokratiske institusjoner. En slik utvikling kan utnyttes av trusselaktører som har interesse av å forsterke disse utviklingstrekkene.

Teknologiutvikling gir trusselaktører nye påvirkningsmuligheter

Nyvinninger som kunstig intelligens, *deepfake*, nye plattformer og digitale virkeligheter vil i tillegg til mulighetene de bringer med seg, skape nye sårbarheter i samfunnet og åpne for nye muligheter for påvirkningsaktører.

Nyhetsartikler og annet innhold med ønsket vinkling kan produseres automatisk i store mengder med stadig bedre kvalitet. *Deepfake*-teknologi blir stadig mer tilgjengelig og kan utnyttes av aktører til å utgi seg for å være noen andre. Fremtidens digitale virkeligheter åpner opp for helt nye muligheter for påvirkning.

Trusselaktører påvirker gjennom sosiale medier

Sosiale medier er en stadig viktigere del av befolkningens kilder til informasjon. Dette er en del av den teknologiske utviklingen, med mange positive effekter for befolkningen og samfunnet. Samtidig bringer det med seg noen negative effekter, som økt makt til teknologiselskaper med manglende demokratisk kontroll, og at trusselaktører utnytter sosiale medier til egen fordel.

I påvirkningsoperasjoner kan sosiale medier spille en stor rolle. Informasjon spres raskt, og falske nyheter spres raskere enn reelle nyheter. Algoritmene er av kommersielle hensyn lagt opp til å skape engasjement gjennom antall oppslag, noe

som bidrar til at negative følelser spres raskere. Sosiale medier brukes for eksempel til å spre desinformasjon og kan forsterke eksisterende konflikter i et samfunn.

Påvirkningsoperasjoner kan være utfordrende å avdekke

Det skyldes delvis påvirkningsoperasjoners natur fordi de er rettet mot ulike sektorer og befolkningsgrupper – uten at en enkelt myndighet har hele oversikten. Derfor går mange påvirkningsoperasjoner under radaren. De kan treffe lokalt eller være rettet mot enkeltindivider eller mindre deler av befolkningen. Ulike former for desinformasjon kan bli spredd fort, også til kilder som vanligvis er pålitelige. Det er svært vanskelig for den enkelte å avdekke om man er utsatt for påvirkning.

Det er en utfordring i seg selv å avgjøre når en påvirkningsoperasjon er alvorlig nok til å utløse en reaksjon. Mange små hendelser kan føre til en gradvis utvikling. Det kan skje i form av polarisering og endring av et narrativ i trusselaktørs favør eller ved at tilliten til myndigheter gradvis forvitrer. Dette er langsiktige prosesser, og det er vanskelig å identifisere konkrete enkelthendelser.

Amerikanske myndigheter har ettergått russisk påvirkning og beskriver det som et nettverk i et økosystem i rapporten *Pillars of Russia's Disinformation and Propaganda Ecosystem* fra 2020. Aktivitetene i nettverket beveger seg fra det åpne til det skjulte. Åpen aktivitet skjer gjennom Russlands offisielle myndighetskommunikasjon og statskontrollerte medier. Delvis skjulte aktiviteter er bruk av «proxy»-aktører, for eksempel nettsider som fremstår som uavhengige, men som direkte eller indirekte er kontrollert av russiske myndigheter. Fordekt aktivitet kan være bruk av trollfabrikker og falske kontoer som sprer informasjon gjennom sosiale medier. Cyberbasert desinformasjon og påvirkning kan blant annet ta form av «hack-and-leak»-operasjoner, der trusselaktører bryter seg inn i IT-systemer og publiserer informasjon de får tak i for å sverte, undergrave eller påvirke. Et annet eksempel er endring av innhold på nettsider (såkalt «defacing»). Målet er å styrke troverdigheten til saken og tåkelegge opprinnelsen.

Det er for lav bevissthet og kunnskap om påvirkningsoperasjoner

Generelt er det for lav bevissthet og kunnskap om trusselaktørers bruk av påvirkningsoperasjoner. Dette gjelder myndigheter både på nasjonalt og lokalt nivå samt i befolkningen som helhet. Siden påvirkningsoperasjoner kan treffe bredt, er det viktig med bevissthet og kunnskap i brede lag av befolkningen.

Det er samtidig viktig at kommunikasjon rundt påvirkningsoperasjoner treffer den rette balansen. Kommunikasjon fra myndighetene må være tydelig slik at den ikke skaper misforståelser eller mistillit til myndighetene.

Anbefalinger

Nasjonal innsats mot påvirkningsoperasjoner må samordnes i én etat

Formålet er å sikre en koordinert innsats for å styrke motstandskraften i befolkningen. Det forutsetter tilgang til høygradert trussel- og sikkerhetsinformasjon slik at påvirkningsoperasjoner ses som en del av sammensatt virkemiddelbruk. Det bør vurderes om etaten trenger hjemmelsgrunnlag for innhenting fra åpne kilder.

Det nasjonale ansvaret for å samordne og styrke andre aktørers arbeid knyttet til påvirkningsoperasjoner skal ligge til denne etaten. Her kan flere ulike aktører ha viktige roller, for eksempel innen utdanningssystemet, forskningsmiljøer, media og sivile myndigheter.

Myndigheten skal formidle kunnskap til befolkningen og bidra med beslutningsstøtte til regjeringen og sektormyndigheter. Myndigheten skal legge til rette for forsknings- og kunnskapsutvikling som gir grunnlag for å øke bevissthet og kompetanse om påvirkningsoperasjoner.

Myndigheten har også ansvar for internasjonal samordning om påvirkningsoperasjoner og fungerer som nasjonalt kontaktpunkt mot EU og NATO. Dette innebærer også å følge opp internasjonalt samarbeid for regulering av sosiale medier-plattformer og ulike typer av fremvoksende teknologier, som kunstig intelligens og manipulert virkelighet.

EOS-tjenestenes innsats mot påvirkningsoperasjoner må forsterkes innen eksisterende ansvarsområder

Det er behov for et felles ambisjonsnivå og prioritering av hvordan EOS-tjenestene skal håndtere påvirkningsoperasjoner. Dette må gjøres med utgangspunkt i EOS-tjenestenes ulike mandater og hjemmelsgrunnlag. Det bør vurderes om eksisterende ressurser og hjemmelsgrunnlag er tilstrekkelig.

EOS-tjenestene bør intensivere informasjonsutvekslingen og samarbeidet seg imellom. Påvirkningsoperasjoner inngår som en del av trussel- og risikobildet om sammensatte trusler, som blir satt sammen i Nasjonalt etterretnings- og sikkerhetssenter (NESS).

Bevisstheten om påvirkningsoperasjoner i befolkningen bør styrkes

Tre forutsetninger for å bygge motstandskraft er en velinformert og utdannet befolkning, frie og uavhengige medier og at befolkningen har tillit til myndigheter og til hverandre. Utdanningssystemet og media har derfor viktige roller i innsatsen mot påvirkningsoperasjoner.

Kritisk medieforståelse styrker befolkningens evne til å delta i den offentlige samtalen og er viktig for et velfungerende demokrati. Kritisk medieforståelse sørger for at befolkningen forstår hvordan media fungerer og evner kritisk å bedømme det den ser. Det handler ikke bare om å forstå redaktørstyrte medier. Det handler om at befolkningen må forstå alle medier, for eksempel hvordan man påvirkes av algoritmestyrte sosiale medier. Skolen har et ansvar for å lære barn og unge kildekritikk og medieforståelse. Det inkluderer sosiale mediers betydning. Skolens læreplaner bør sikre at kildekritikk også omfatter problemstillinger knyttet til fremvoksende teknologier, som kunstig intelligens og manipulert virkelighet.

At mediepolitikken sikrer en fri, mangfoldig og uavhengig presse bidrar i seg selv til forsvarsverk mot påvirkningsoperasjoner. I tillegg er det viktig at redaktørstyrte medier har bevissthet og kompetanse om påvirkningsoperasjoner. Journalister og redaktører bør i større grad få tilbud om tilgang til trussel- og sikkerhetsinformasjon. Dette styrker medias rolle i det forebyggende arbeidet mot påvirkningsoperasjoner, i tillegg til å styrke medias egen robusthet mot påvirkningsforsøk.

Stian Lysberg Solum/NTB

14 Kompetanseløft for nasjonal sikkerhet

Det kreves et nasjonalt kompetanseløft innen teknologi, cybersikkerhet og andre sikkerhetsfaglige områder. Det må til for å møte sikkerhetsutfordringene Norge står overfor frem mot 2030 og i de påfølgende årene. Et nasjonalt kompetanseløft skal bidra til å ivareta nasjonale sikkerhetsinteresser og samtidig bidra til et konkurransedyktig Norge.

De færreste departementer eller virksomheter har nasjonal sikkerhet som sin kjerneoppgave, men til sammen utgjør de kjernen i nasjonal sikkerhet.

Sikkerhetsfaglig forståelse må bygges på alle nivåer, fra nasjonale myndigheter til den minste virksomhet, og blant ledere og ansatte. Det er et stort behov for å styrke kompetansen som er nødvendig for å møte sikkerhetsutfordringene Norge står overfor.

Virksomheter må ha evne til å tolke den sikkerhetspolitiske situasjonen Norge står i. De må ha tilstrekkelig kompetanse til å forstå hvordan trussel- og risikobildet er relevant for egen virksomhet og ikke minst hvilken betydning egen virksomhet har for nasjonal sikkerhet. De må ha kompetanse om sikkerhetsstyring, inklusive risikovurderinger.

For mange virksomheter, spesielt for små og mellomstore, er det utfordrende å sikre tilstrekkelig med ressurser og kompetanse for å håndtere sikkerhets-utfordringer.

I tillegg til sikkerhetskompetanse må både myndigheter og virksomheter ha tilstrekkelig kompetanse innen en rekke andre områder for å motvirke eksisterende og fremtidens sikkerhetsutfordringer. Flere av sikkerhetsutfordringene er tverr-sektorielle i sin natur og krever tverrfaglig kompetanse. Samtidig er det behov for spisskompetanse innen en rekke fagområder, blant annet innen digital sikkerhet og teknologisk utvikling. For å ivareta nasjonal kontroll over funksjoner og infrastruktur samfunnet er avhengig av, må Norge ha fagfolk som kan drifte og vedlikeholde funksjonene.

Hvis ikke Norge evner å dekke dette kompetansebehovet, er det en risiko for at viktige samfunnsfunksjoner blir avhengige av kompetanse utenfor Norges grenser. Det svekker nasjonal autonomi og har konsekvenser for Norges evne til å ivareta nasjonal sikkerhet.

For å sikre at Norge i fremtiden har nok kompetanse innen områder som er nødvendige for å ivareta nasjonale sikkerhetsinteresser, kreves det en helhetlig tilnærming til kompetansebehovet. Norske myndigheter må sikre at det utdannes

et tilstrekkelig antall personer med nødvendig kompetanse for å møte fremtidige sikkerhetsutfordringer. Et eksempel er kompetanse innen teknologiområder som både er og kommer til å bli helt avgjørende for å opprettholde et forsvarlig nasjonalt sikkerhetsnivå.

I årene frem mot 2030 vil behovet for personer med bakgrunn innen IT, digital sikkerhet og andre teknologiområder bare øke. Digitale løsninger er i økende grad selve premissgiveren for all virksomhet i stat og samfunn. Norge har behov for 40.000 flere sysselsatte med IKT-kompetanse i 2030, sammenlignet med 2019, ifølge rapporten *Norges behov for IKT-kompetanse i dag og framover* fra Samfunns-økonomisk analyse AS (2021).

Med et trussel- og risikobilde i stadig utvikling er dedikert arbeid med cyber-sikkerhet en avgjørende funksjon i både sivil og militær sektor. Nordisk institutt for studier av innovasjon, forskning og utdanning (NIFU) anslår at Norge i 2030 vil mangle 4000 personer med denne kompetansen. Gapet mellom behovet for og tilgangen på cybersikkerhetspersonell utgjør en alvorlig sårbarhet for Norges sikkerhet.

Kompetanseløftet skal ivareta nasjonale sikkerhetsinteresser og bidra til et konkurransedyktig Norge.

Anbefalinger

Det bør fastsettes nasjonale strategier for forskning med betydning for nasjonal sikkerhet
Styring og finansiering av forskning med betydning for nasjonal sikkerhet må styrkes. Det er behov for mer forskning innen flere områder som enten har eller får betydning for nasjonal sikkerhet i fremtiden.

Forskning med betydning for nasjonal sikkerhet bør styrkes gjennom en planprosess. Dette sikrer finansiering og prioritering av forskningsprosjekter. Det bidrar også til gjennomføringen av langtidsplanen for forskning og høyere utdanning (2023–2032). Videre ivaretar det målet om å styrke forskning med betydning for nasjonal sikkerhet. NSM og Forsvarets forskningsinstitutt (FFI), som begge har forskningsoppgaver i både sivil og militær sektor, må være sentrale i prosessen.

Ulike kompetansemiljøer hos myndighetene, akademia og privat næringsliv bør i større grad samarbeide systematisk på strategisk nivå. Formålet er å utveksle og bygge kunnskap om temaer som er relevante for nasjonal sikkerhet, og hvor eksisterende kompetanse er delt mellom flere miljøer.

Offentlig-privat samarbeid innen sikkerhetsfaglig kompetanseutvikling bør styrkes
Myndighetene bør stimulere til en robust sikkerhetsindustri i Norge. Økosystemet av private og offentlige aktører bør samordnes for å utnytte eksisterende kompetanse.

Ordninger for kvalitetssikring eller sertifisering av kommersielle leverandører som tilbyr kompetansehevende tiltak innen sikkerhet, bør etableres eller videreutvikles.

Myndighetene bør vurdere hvordan eksisterende rådgivingsmiljøer innen sikkerhet kan utnyttes på en mer effektiv måte. Myndighetene bør blant annet se på ulike muligheter for organisering, spesialisering og ansvarsfordeling. Myndighetene bør også vurdere finansieringsmodeller for å sikre at tilgang til kompetansehevende tiltak blir mindre betinget av virksomheters økonomiske situasjon.

Det bør etableres et nasjonalt program for å løfte kompetansen på teknologi og cybersikkerhet
Realfagskompetanse i grunnskolen bør styrkes. Hensikten er å sikre fremtidens rekrutteringsgrunnlag for teknologisk kompetanse og å styrke grunnleggende teknologiforståelse i hele befolkningen. Digital sikkerhet bør inngå som et obligatorisk fag i alle IKT- og teknologiutdannelser. Det bør også være en del av undervisning i grunnskolen. Tilgang på etter- og videreutdanning må styrkes.

Det bør etableres et cybersikkerhetsprogram som inspirerer og motiverer unge mennesker til å velge en utdanning og karriere innen cybersikkerhet. Programmet bør være et samarbeid mellom skoler, næringsliv, organisasjoner og cybersikkerhetsmiljøer, eksempelvis etter modell fra Storbritannia.

Det bør opprettes flere stillinger med mulighet for utdanning under jobb for å øke rekrutteringen innen fagområder med betydning for nasjonal sikkerhet. Disse løpene bør innrettes med statlige stipendordninger og lærlingplasser, og sikre jobb etter endt utdanning.

Nasjonal strategi for digital sikkerhetskompetanse peker på en rekke tiltak for å styrke teknologi- og cybersikkerhetskompetanse. Disse tiltakene må

sikres finansiering. Det er nødvendig med flere stipendiatstillinger innen områder med betydning for nasjonal sikkerhet.

Alle årskull bør gjennomføre kompetansehevende tiltak innen nasjonal sikkerhet, samfunnssikkerhet og beredskap

Formålet er å gi alle årskull en introduksjon til temaet nasjonal sikkerhet og styrke bevisstheten om sammensatte trusler i befolkningen. Kurset skal heve den generelle kompetansen i befolkningen. NSM, Direktoratet for samfunnssikkerhet og beredskap (DSB) og Forsvaret bør samarbeide om faglig innhold.

Tiltaket gjelder uavhengig av om verneplikten gjennomføres eller ikke. Det kan knyttes til Forsvarets sesjon, gjennomføres som del av verneplikten for de som avtjener den i Forsvaret, eller som et eget kurstilbud for hele årskullet.

Kunnskap må bygges gjennom økt erfaringslæring

Erfaringer opparbeidet gjennom håndtering av sikkerhetstruende hendelser må deles og brukes til læring og kunnskapsoverføring. Erfaringslæring må i større grad systematiseres og utnytte mulighetene teknologi og stordataanalyse gir.

Sektormyndigheter bør gjennomføre årsaksanalyser ved uønskede hendelser og utvikle læringspunkter som deles bredt til virksomheter.

Det bør gjennomføres flere nasjonale og regionale øvelser som omfatter alle sikkerhetsdomener, med arrangører og deltakere fra både offentlig og privat sektor. Myndighetene kan bruke finansieringsmodeller til å stimulere til flere øvelser og treningsarenaer for å sikre kunnskapsoverføring og erfaringslæring.

Det er viktig at virksomheter og ulike forvaltningsenheter øver på håndtering av sikkerhetstruende hendelser og kriser under kontrollerte forhold. Øvelser må evalueres, og læringspunkter på tvers av sektorer må følges opp på en systematisk måte.

15 Et motstandsdyktig Norge

Den sikkerhetspolitiske situasjonen Norge står i, er uforutsigbar og alvorlig. Det er all grunn til å tro at den vil vedvare. Konsekvensen er at hele samfunnet må hegne om nasjonal sikkerhet. Forståelsen av dynamikken, avhengigheter og samspillet mellom myndigheter, virksomheter og befolkningen er helt sentral for at Norge når en forsvarlig nasjonal sikkerhetstilstand. Anbefalingene i sikkerhetsfaglig råd retter seg mot aktører med betydning for nasjonal sikkerhet.

Den norske forsvarsevnen avhenger av at roller, ansvar og myndighet for etater og virksomheter med betydning for nasjonal sikkerhet er avklart. Dette gjelder særlig for de delene av samfunnet som må fungere i de øvre delene av krisespekteret. Evne til tverrsektoriell styring er avgjørende.

Totalforsvaret skal ivareta funksjoner som sikrer motstandskraft og forsvarsevne gjennom ulike scenarioer. Norge skal kunne oppfylle NATO-forpliktelsene om å ivareta evne til selvhjelp og samtidig utvikle både Norges og alliansens evne til å motstå væpnet angrep. Sentrale, nasjonale myndigheter må ha en omforent situasjonsforståelse og oversikt over sikkerhetstilstanden, mens sektordepartementene og virksomheter følger opp sikkerhetsarbeidet. Sikker infrastruktur gjennom hele krisespekteret blir avgjørende for totalforsvarsevnen, noe erfaringene fra krigen i Ukraina viser.

Forsvarssektoren er spesielt utsatt for sikkerhetstruende aktiviteter og trenger fortsatt de mest avanserte sikkerhetsløsningene. Sektoren må jobbe med sikkerhetsutfordringer i et lengre og nasjonalt perspektiv. Sikkerhetsløsningene Forsvaret velger, må kunne møte fremtidens trusler. I denne sammenheng blir et defensivt sikkerhetskonsept, som speiler trusselen med risikoreduserende sikkerhetstiltak innenfor hvert sikkerhetsområde eller domene, viktig. Det gjelder spesielt for å kunne avdekke, forhindre og håndtere sammensatte trusler.

Det ligger til NSMs rolle å rette oppmerksomheten mot områder som løfter og styrker den nasjonale sikkerheten. Det norske sikkerhetsarbeidet må tuftes på godt samvirke mellom det offentlige og private, mellom det sivile og militære, og på tvers av sektorer og forvaltningsnivåer. NSM skal ha oversikt over Norges grunnleggende nasjonale funksjoner, inklusive infrastruktur, systemer og objekter som understøtter dem. Det gjør NSM i stand til å prioritere ressurser knyttet til sikkerhetsarbeid på nasjonalt nivå.

Fremvoksende teknologier og sikkerhetsutfordringene de bringer med seg, gjør seg ofte først gjeldende for forsvarssektoren. Kunnskap og erfaringer NSM

opparbeider seg i forsvarssektoren, vil komme sivil sektor til gode i form av videreføring av tiltak, krav og kompetanse. Videreutvikling av den gjensidige sikkerhetsdialogen i NSMs partnernettverk og samarbeid med andre etater, akademia og forsvarsindustrien blir viktig for å styrke den samlede teknologi- og sikkerhetskompetansen i Norge.

Forsvarets særegne rolle for å ivareta statssikkerheten gjør det spesielt viktig at avhengigheter på tvers av sivil og militær sektor er tilstrekkelig kjent. I tillegg må ansvar for og krav til robusthet og sikkerhet hos aktører som understøtter Forsvaret være avklart. Knappe ressurser må prioriteres til de områdene som er av størst nasjonal betydning. NSM har et ansvar for at nasjonal sikkerhet ses i sammenheng på tvers av sektorer, og mellom det sivile og militære slik at total-forsvarsevnen ivaretas.

Sikkerhetsnivået i det norske samfunnet er ikke der det bør være for å møte den sikkerhetspolitiske utviklingen. Norge trenger ambisiøse sikkerhetsmål mot 2030 for styrke motstandsdyktigheten.

Målet for Norges sikkerhetstilstand i 2030 bør være at de samlede nasjonale sikkerhetstiltakene speiler trusselen ved at

- myndighetene har felles situasjonsforståelse og koordinert responsevne
- virksomhetene har systematisk sikkerhetsstyring og helhetlig sikring
- befolkningen er årvåken og har sterk motstandskraft

Sentrale begreper

Cybersikkerhet: Også kjent som digital sikkerhet eller IKT-sikkerhet. Cybersikkerhet handler om beskyttelse av «alt» som er sårbart fordi det er koblet til eller på annen måte avhengig av informasjons- og kommunikasjonsteknologi.

Grunnleggende nasjonale funksjoner: Tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser.

Innsider: En nåværende eller tidligere ansatt, konsulent eller innleid som har eller har hatt legitim tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, og som misbruker denne kunnskapen og tilgangen for å utføre handlinger som påfører virksomheten skade eller tap.

Nasjonale sikkerhetsinteresser: Landets suverenitet, territorielle integritet og demokratiske styreform og overordnede sikkerhetspolitiske interesser knyttet til

a. de øverste statsorganers virksomhet, sikkerhet og handlefrihet
b. forsvar, sikkerhet og beredskap
c. forholdet til andre stater og internasjonale organisasjoner
d. økonomisk stabilitet og handlefrihet
e. samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet

(jf. sikkerhetsloven § 1-5)

Nasjonal sikkerhet: Statens evne til å ivareta nasjonale sikkerhetsinteresser.

Personellsikkerhet: Organisatoriske og menneskelige virkemidler og tiltak knyttet til å forebygge og motvirke innsidevirksomhet. De viktigste elementene av dette er sikkerhetsstyring, klarering, autorisasjon og daglig sikkerhetsmessig ledelse.

Påvirkningsoperasjon: En aktørs koordinerte bruk av illegitime eller fordekte metoder for å påvirke meninger, holdninger, virkelighetsoppfatning eller handlinger hos mennesker og grupper, i den hensikt å skape forutsetninger for å oppnå egne strategiske mål.

Risiko: Viser til forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen. I vurderingen av verdien ligger også en konsekvensvurdering ved potensiell kompromittering, bortfall eller skade på verdien. Samlet omfatter risiko kombinasjonen av sannsynligheten for og konsekvensene av en uønsket hendelse.

Risikobilde: En beskrivelse av en samlet vurdering av verdier, truslene mot disse og sårbarheter som eksisterer overfor truslene i en bestemt tidsperiode eller knyttet til en spesifikk hendelse.

Risikovurdering: Helhetsvurdering basert på verdi- eller konsekvensvurdering, trussel- og sårbarhetsvurdering med mål om å angi risiko i en definert kontekst.

Sammensatte trusler: En betegnelse på strategier for konkurranse og konfrontasjon under terskelen for direkte væpnet konflikt, som kan kombinere diplomatiske, informasjonsbaserte, militære, økonomiske, finansielle, etterretningsbaserte og juridiske virkemidler for å nå strategiske målsettinger.

Sikkerhetstruende virksomhet: Tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser (jf. sikkerhetsloven § 1-5).

Sårbarhet: Svakheter i evnen til å skjerme verdier mot uønskede hendelser eller til å opprettholde eller gjenoppta verdiens funksjon. Samlet viser begrepet sårbarhet til et systems manglende evne til å motstå en uønsket handling eller hendelse eller til å gjenoppta sin funksjon.

Totalforsvaret: Totalforsvaret er en fellesbetegnelse for det militære forsvaret og den sivile beredskapen i Norge. Begrepet omfatter gjensidig støtte og samarbeid mellom sivil og militær side for å forebygge, planlegge for og håndtere kriser i fred, sikkerhetspolitiske kriser, væpnet konflikt og krig.

Trussel: Mulig tilsiktet handling som kan gi negative konsekvenser for en verdi. Aktørens intensjon og kapasitet til å utføre handlinger som kan gi negative konsekvenser for en verdi, utgjør trusselen.

Verdi: I risikovurderinger viser begrepet verdi til en immateriell eller materiell ressurs. Dersom ressursen (verdien) blir utsatt for en uønsket hendelse, vil det få negative konsekvenser for eieren eller andre som drar fordel av ressursen. Eksempler på materielle verdier er IKT-systemer, informasjon, fysisk og digital infrastruktur, bygninger og eiendom. Eksempler på immaterielle verdier er ytringsfrihet, omdømme og tillit.

Verdikjede: En verdikjede beskriver ressurser, prosesser og aktiviteter som inngår i produksjonen av en vare eller tjeneste. Verdikjeden knytter sammen virksomheter som tilbyr og etterspør varer og tjenester mellom seg.

Design: Tank

Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet (NSM) er Norges direktorat for nasjonal forebyggende sikkerhet. Tjenestens hovedoppgave er å bedre Norges evne til å beskytte seg mot spionasje, sabotasje, terror og sammensatte trusler. Gjennom rådgivning, forskning, tilsyn, testing og kontrollaktiviteter bidrar NSM til at virksomheter sikrer sivil og militær informasjon, systemer, objekter og infrastruktur med betydning for nasjonal sikkerhet. NSM er ansvarlig for et nasjonalt varslingssystem for å avdekke og varsle om cyberangrep mot digital infrastruktur. NSM har også et nasjonalt ansvar for å koordinere håndteringen av alvorlige cyberangrep.

NASJONAL
SIKKERHETSMYNDIGHET

Postboks 814
1306 Sandvika

Tlf. 67 86 40 00
www.nsm.no