NASJONAL
SIKKERHETSMYNDIGHET

# RISIKO 2020

**Nasjonal sikkerhetsmyndighet (NSM)** er fagmyndighet for forebyggende sikkerhet. NSM gir blant annet råd om og fører tilsyn med sikring av informasjon, informasjonssystemer, objekter og infrastruktur av nasjonal betydning. Videre er NSM nasjonalt fagmiljø for digital sikkerhet og har et ansvar for på nasjonalt nivå å oppdage, varsle og koordinere håndtering av alvorlige digitale angrep. I rapporten «Risiko 2020» vurderer NSM risikoen for at samfunnet skal rammes av tilsiktede handlinger som direkte eller indirekte kan skade viktige samfunnsinteresser. Vurderingen utgis i første kvartal.

**Politiets sikkerhetstjeneste (PST)** er Norges nasjonale innenlands etterretnings- og sikkerhetstjeneste. PSTs hovedoppgave er å forebygge og etterforske alvorlig kriminalitet mot nasjonens sikkerhet. PSTs årlige trusselvurdering er en analyse av forventet utvikling innenfor PSTs ansvarsområder.

**Etterretningstjenesten (E-tjenesten)** er Norges utenlandsetterretningstjeneste. E-tjenestens hovedoppgave er å varsle om ytre trusler mot Norge og norske interesser og støtte utformingen av norsk sikkerhets-, utenriks- og forsvarspolitikk. Tjenesten utgir en årlig vurdering av forhold i utlandet og utenlandske trusler som har betydning for Norge og norske interesser. Årets vurdering, «Fokus 2020», beskriver aktuelle forhold og sikkerhetstrusler innen ulike land, regioner og temaer. Analysen har en tidshorisont på ett år, men peker også på utviklingstrekk som kan få sikkerhetsmessig betydning innenfor en horisont på fem til ti år.

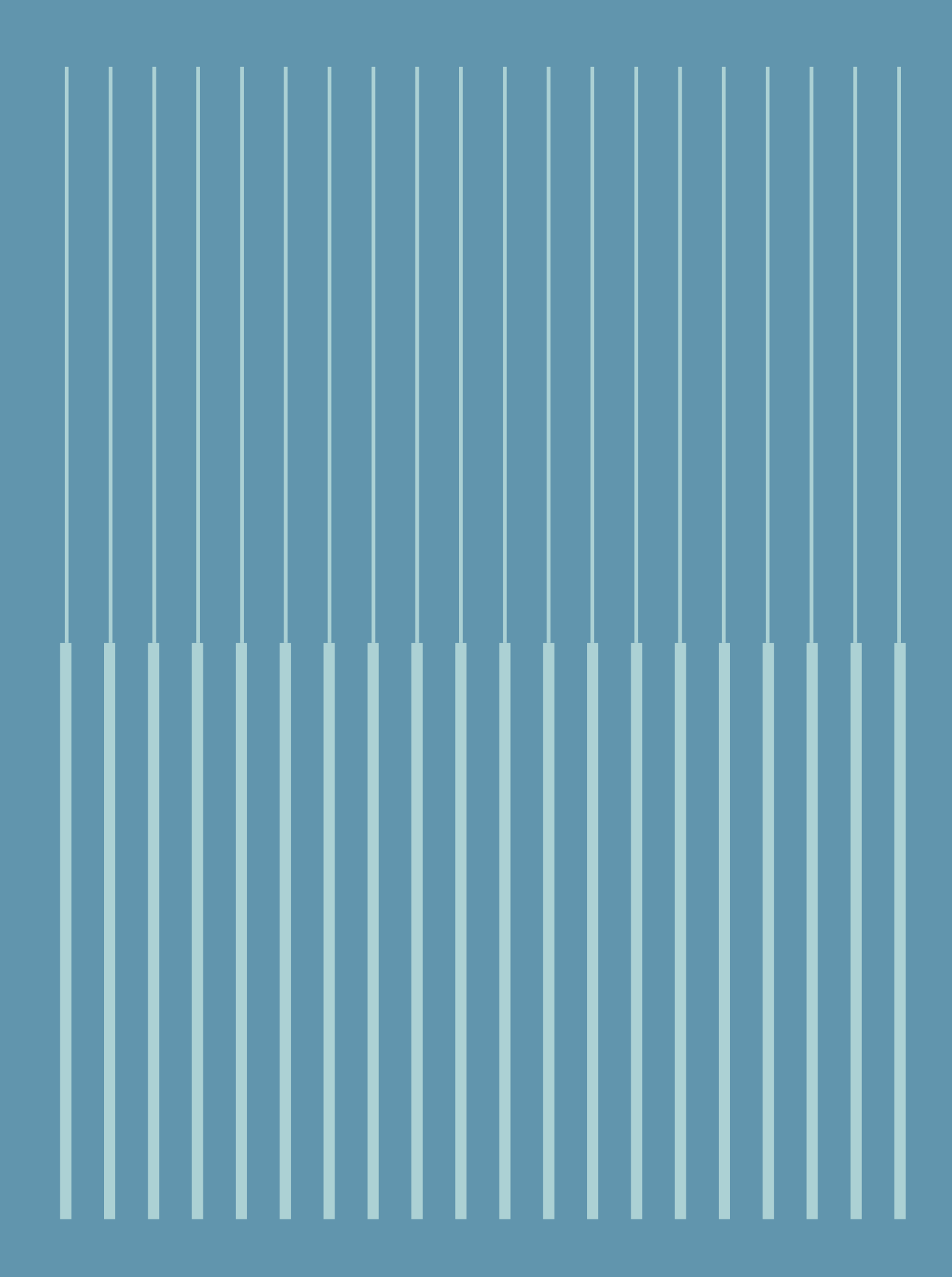
**Direktoratet for samfunnssikkerhet og beredskap (DSB)** skal ha oversikt over risiko og sårbarhet i samfunnet. DSB har utgitt scenarioanalyser siden 2011*. Analysene omhandler risiko knyttet til katastrofale hendelser som kan ramme det norske samfunnet og som det bør være forberedt på å møte. Analysene omfatter både naturhendelser, store ulykker og tilsiktede handlinger. De har en lengre tidshorisont enn de årlige vurderingene til de øvrige tre etatene og utgis på høsten.

* DSBs scenarioanalyser het t.o.m. 2015 «Nasjonalt risikobilde». F.o.m. 2017 er navnet på publikasjonen endret til «Analyse av krisescenarioer».

# Innhold




**RISIKO 2020** | **Design:** HyperRedink **Trykk og distribusjon:** RK grafisk



# Forord

Året 2020 vil preges av covid-19-pandemien. Norge står sammen med resten av verden i en uoversiktlig og vanskelig situasjon. På alle områder må behovet for å opprettholde samfunnsfunksjoner veies opp mot risikoen knyttet til økt smittespredning. Helsevesenets kapasitet til å behandle smittede med alvorlige symptomer må ikke overskrides. Her har vi alle et viktig ansvar.

Situasjonen gjør oss sårbare, og vi må ta høyde for at trusselaktører ser sitt snitt til å utnytte seg av den økte sårbarheten som oppstår.

Norge har gjennom mange år tronet på toppen av FNs levekårsindeks, som rangerer land basert på forventet levealder, levestandard, utdanning og kunnskapsnivå i befolkningen. Vi forvalter verdier som er attraktive for andre stater og aktører, i form av blant annet viktige og verdifulle naturressurser, teknologiutvikling og vår geografiske beliggenhet, som er av stor strategisk betydning for mange andre land.

Stadig flere av våre verdier digitaliseres. Innen de fleste samfunnssektorer er funksjoner og tjenester del av digitale verdikjeder, og avhengighetene på tvers er store og mange. En stor del av trusselaktiviteten mot Norge skjer i det digitale rom.

Hos oss i NSM er håndtering av cyberhendelser mot norske virksomheter en stor del av hverdagen. For å styrke dette arbeidet ble Nasjonalt cybersikkerhetssenter (NCSC) åpnet i november 2019. Senteret er en del av NSM.

Samtidig er det viktig å huske at nasjonal sikkerhet ikke bare bygges i det digitale rom. Fremmede stater forsøker å påvirke norske beslutninger. Etterretningstjenester søker innpass i miljøer som driver med forskning og teknologiutvikling, og kartlegger installasjoner og infrastruktur. Vi står overfor profesjonelle aktører med et stort arsenal av metoder. Fysiske innbrudd, oppkjøp og investeringer og forsøk på å rekruttere nordmenn for å få tilgang til sensitiv informasjon og bedriftshemmeligheter er bare noen.

En av NSMs hovedoppgaver er å se til at våre viktigste virksomheter og samfunnsfunksjoner er trygt ivaretatt. Vi tester og kartlegger sikkerheten i norske virksomheter, og gjennom ulike rapporter, råd og veiledere deler vi våre funn og anbefaler tiltak som vil heve nasjonal sikkerhet.

I årets rapport vil jeg fremheve tre risikofaktorer for nasjonal sikkerhet:

1) Samfunnets økende avhengighet av elektronisk kommunikasjon og satellittbaserte tjenester og den fundamentale avhengigheten av kraft.
2) Økende avhengighet av digitale infrastrukturer og verdikjeder som strekker seg utover våre grenser.
3) Sammensatt virkemiddelbruk i form av blant annet strategiske oppkjøp, investeringer og påvirkning.

Det er bra å se hvordan befolkningen, virksomhetene og myndighetene står sammen når krisehåndteringen nå settes på prøve. Med en slik nasjonal dugnadsånd er jeg trygg på at vi skal klare å dra lasset sammen fremover – også for å opprettholde nasjonal sikkerhet.

Foto: Cicilie S. Andersen

**Kjetil Nilsen**
**Direktør NSM**

# Risikobildet

*Risiko 2020* beskriver sårbarheter i virksomheter og på nasjonalt plan, hvordan trusselaktørene kan utnytte dem og hvilken risiko dette medfører. Rapporten omtaler også hvordan virksomhetene og myndighetene bør redusere sårbarheter for å gjøre trusselaktørenes jobb vanskeligere.

*Risiko 2020* henvender seg til ledere og personell med sikkerhetsoppgaver i alle sektorer. Målet med rapporten er å gi virksomhetene mulighet til å sette sikkerhetsarbeidet i en bredere kontekst. Dette er spesielt viktig for virksomheter underlagt sikkerhetsloven, men også for andre virksomheter.

Vårt nasjonale risikobilde er i kontinuerlig endring. Risikoen endrer seg blant annet når verdiene endrer seg, eksempelvis som følge av teknologisk utvikling eller andre globale, regionale eller nasjonale utviklingstrekk som påvirker samfunnet og funksjonene våre.

Den krevende situasjonen vi nå opplever med covid-19-pandemien, viser hvor raskt hendelser ett sted på kloden kan få enorme ringvirkninger. Drastiske tiltak iverksettes i mange land, og hele samfunn stenges ned for å begrense smitten. Det nasjonale risikobildet påvirkes også av denne situasjonen.

Krisesituasjoner av dette omfanget utfordrer myndigheters styringsevne og bringer med seg et uoversiktlig nyhetsbilde. Slike situasjoner kan utnyttes av trusselaktører som vil undergrave tilliten til myndighetene eller skape splid for å oppnå egne mål. Dette krever ekstra årvåkenhet mot falske nyheter og uønsket påvirkning. I tillegg påvirkes det digitale sårbarhetsbildet blant annet av at mange i disse dager arbeider på hjemmekontor. Slike omfattende endringer kan innebære uforutsette sårbarheter og økt risiko for virksomhetene. Når store deler av Norge jobber hjemmefra, påvirkes også belastningen på ekom-infrastrukturen.

Vi er som nasjon utsatt for et dynamisk trusselbilde, der fremmede staters interesse i norske verdier og deres kapasitet til å drive etterretning, påvirke eller sabotere også endrer seg.

Politiets sikkerhetstjeneste (PST) og Etterretningstjenesten forteller oss hvilken intensjon og kapasitet fremmede stater og trusselaktører har til å ramme norske verdier og hva de ønsker å påvirke i det norske samfunnet. Trusselaktører leter systematisk etter sårbarheter i norske virksomheter og norsk infrastruktur på jakt etter våre verdier, som kan være teknologi, naturressurser, forretningshemmeligheter eller sensitiv informasjon om vår forsvars- og beredskapsevne.

NSM avdekker sårbarheter i virksomheter som forvalter landets mest sentrale verdier. Vi stiller krav og gir råd til virksomhetene slik at de kan iverksette tiltak som sikrer verdiene de forvalter på samfunnets vegne. Risikovurderinger er kjernen i dette arbeidet. NSM foretar risikovurderinger av samfunnets viktigste verdier og gir anbefalinger til departementene om hvilke tiltak de bør iverksette på strategisk nivå. Samspillet mellom NSM, PST og Etterretningstjenesten danner grunnlaget for å forstå risikobildet og skape nasjonal sikkerhet.

Gjennom rapporten presenteres en rekke anbefalinger og tiltak. Vi presiserer ikke hvilket departement eller myndighet tiltakene retter seg mot. Det er en dialog NSM fører med våre styrende departementer. NSM utarbeider også en årlig gradert risikorapport. Denne danner grunnlag for anbefalinger til departementene i deres prioritering av tiltak for bedre nasjonal sikkerhet.

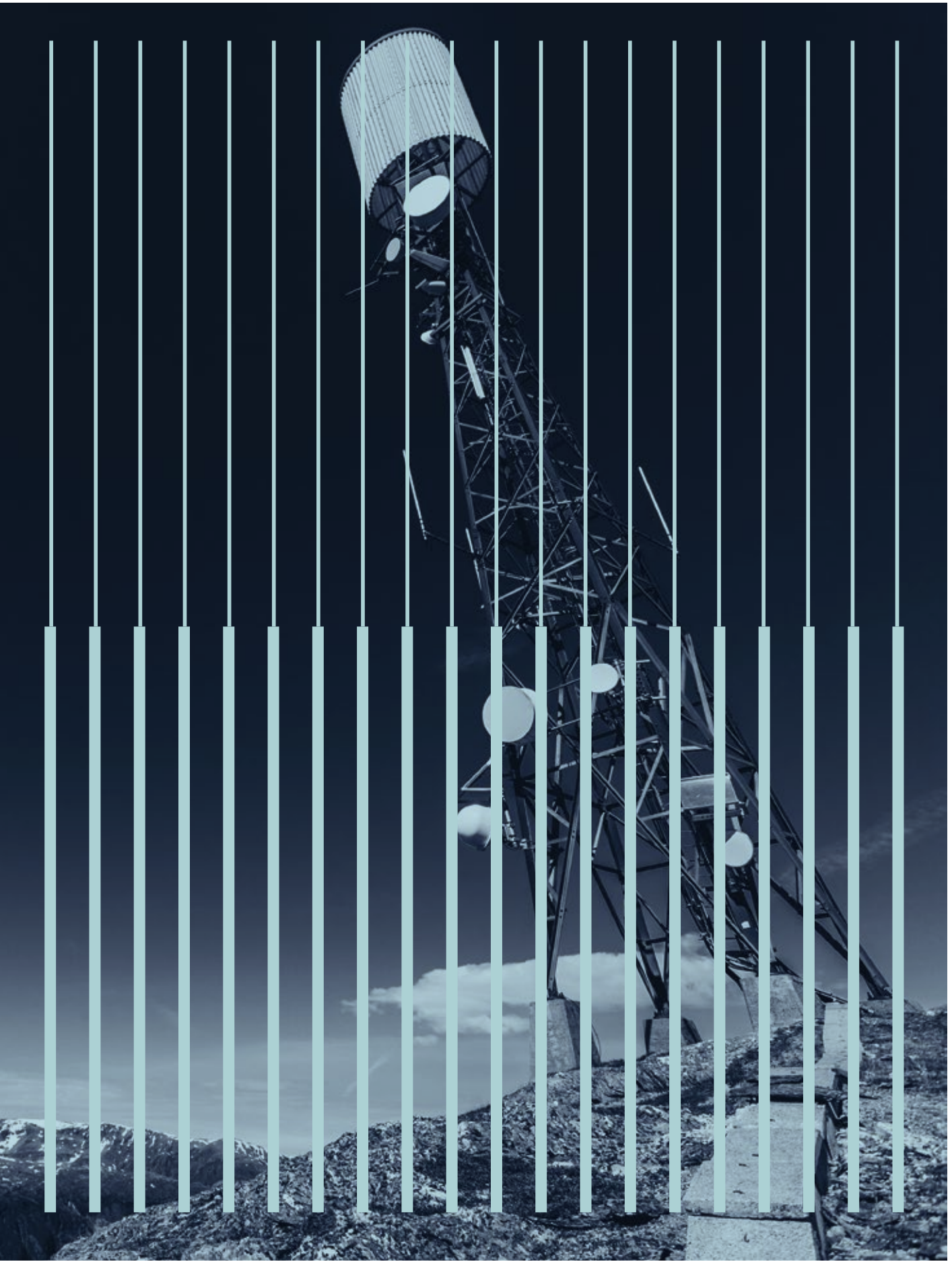
Avhengigheter mellom samfunnsfunksjoner skaper effektivitet og bedre tjenesteleveranser, men kan også gi sårbarheter ved at feil som oppstår ett sted i en verdikjede, kan forplante seg.

### Våre grunnleggende nasjonale funksjoner er sårbare

Vi lever i et åpent, velfungerende og moderne demokrati. Nordmenn har høy tillit til myndighetene og offentlige institusjoner og forventer at offentlige tjenester og viktige samfunnsfunksjoner fungerer til enhver tid. Landet forvalter store og verdifulle naturressurser, norsk forskning og teknologi er langt fremme på flere områder, og vi har en geografisk posisjon som er av stor strategisk betydning for mange land.

For mange er landets suverenitet, territorielle integritet og demokratiske styreform verdier vi i dag tar for gitt. Sikkerhetsloven skal hegne om disse og *andre nasjonale sikkerhetsinteresser*, samt våre *grunnleggende nasjonale funksjoner*. Det disse verdiene hviler på, er norske offentlige og private virksomheter som forvalter viktig informasjon, informasjonssystemer, objekter eller infrastruktur. Dette omtaler vi som skjermingsverdige verdier.

Departementene gjennomgår i disse



dager hvilke samfunnsverdier som må beskyttes. De identifiserer grunnleggende nasjonale funksjoner og virksomheter som understøtter disse funksjonene. Dette er vår nasjonale verdivurdering og utgangspunktet for sikkerhetstiltak på nasjonalt og strategisk nivå. Sikkerhetsloven er vårt viktigste verktøy for å sikre nasjonale verdier. Gjennom denne loven kan viktige tiltak iverksettes for å sikre verdiene som samfunnet er avhengig av. Alle virksomheter underlagt sikkerhetsloven skal kartlegge sine verdier slik at de kan sikres forsvarlig. Øvrige virksomheter anbefales også å gjøre dette.

## Avhengigheter mellom samfunnsfunksjoner

Samfunnsutviklingen preges av stadig sterkere avhengigheter mellom samfunnsfunksjoner. Disse avhengighetene skaper effektivitet og bedre tjenesteleveranser. Samtidig gir avhengigheter ofte sårbarheter ved at feil som oppstår ett sted i en verdikjede, kan forplante seg.

De fleste samfunnsfunksjoner er avhengige av kraft og elektronisk kommunikasjon (ekom). Videre blir vi stadig mer avhengige av satellittbaserte tjenester. NSM vil derfor utdype disse tre funksjonene nedenfor.

De stadig sterkere avhengighetene mellom ulike samfunnsfunksjoner er i stor grad drevet og gjort mulig av den raske utviklingen innen digitalisering. Denne utviklingen fortsetter og gjør de digitale verdikjedene enda mer komplekse og uoversiktlige. **Virksomhetene anbefales å kartlegge egne sårbarheter som følge av avhengigheter til andre virksomheter.** Virksomhetene underlagt sikkerhetsloven er pålagt å kartlegge slike avhengigheter. **Enhver virksomhet bør legge planer for bortfall av kraft og ekom.**

Fra et samfunnsperspektiv er det viktig å vurdere og forstå hvilken risiko et eventuelt utfall av henholdsvis kraft, ekom eller satellittbaserte tjenester utgjør for andre verdikjeder i samfunnet. Dersom kraftforsyningen faller ut, vil store deler av samfunnet stoppe opp. Utfall av ekom vil ha umiddelbar konsekvens for mobiltjenester, nettilgang, informasjons- og nyhetsformidling og digital samhandling over internett. Utfall av satellittbaserte tjenester vil få konsekvenser for blant annet Forsvaret, redningstjenester, skips- og luftfart, deler av finansnæringen, så vel som kraft og ekom.

**Stabile kraftleveranser og verdikjeder**

Dagens kraftleveranser er svært stabile, og Norge har hittil vært skånet for større bortfall av kraft. Det har medført at mange virksomheter tar stabil tilgang til kraft for gitt. Imidlertid er det en risiko knyttet til at virksomhetene i liten grad kjenner til de faktiske konsekvensene av vesentlig ustabilitet eller bortfall av kraftleveransene. I tillegg til de direkte konsekvensene for virksomhetene vil bortfall av kraft kunne ha store konsekvenser

Femte generasjon mobilnett (5G) bygges ut og vil bli fundamentet i det digitaliserte samfunnet i årene fremover.

som følge av komplekse verdikjeder. Følgelig kan en virksomhet rammes av bortfall av kraft som skjer helt andre steder.

Som følge av sårbarhetene som knytter seg til digitalisering og de sterke tverrsektorielle avhengighetene forbundet med kraft, er dette en sektor som er risikoutsatt. Risikoen øker gjennom krisespennet og forplanter seg til alle funksjoner i samfunnet som er avhengige av kraft. Avhengigheten til kraft og kraft-infrastruktur utnyttes som maktmiddel i sikkerhetspolitiske kriser og konflikter.[1 2]

**Elektronisk kommunikasjon**

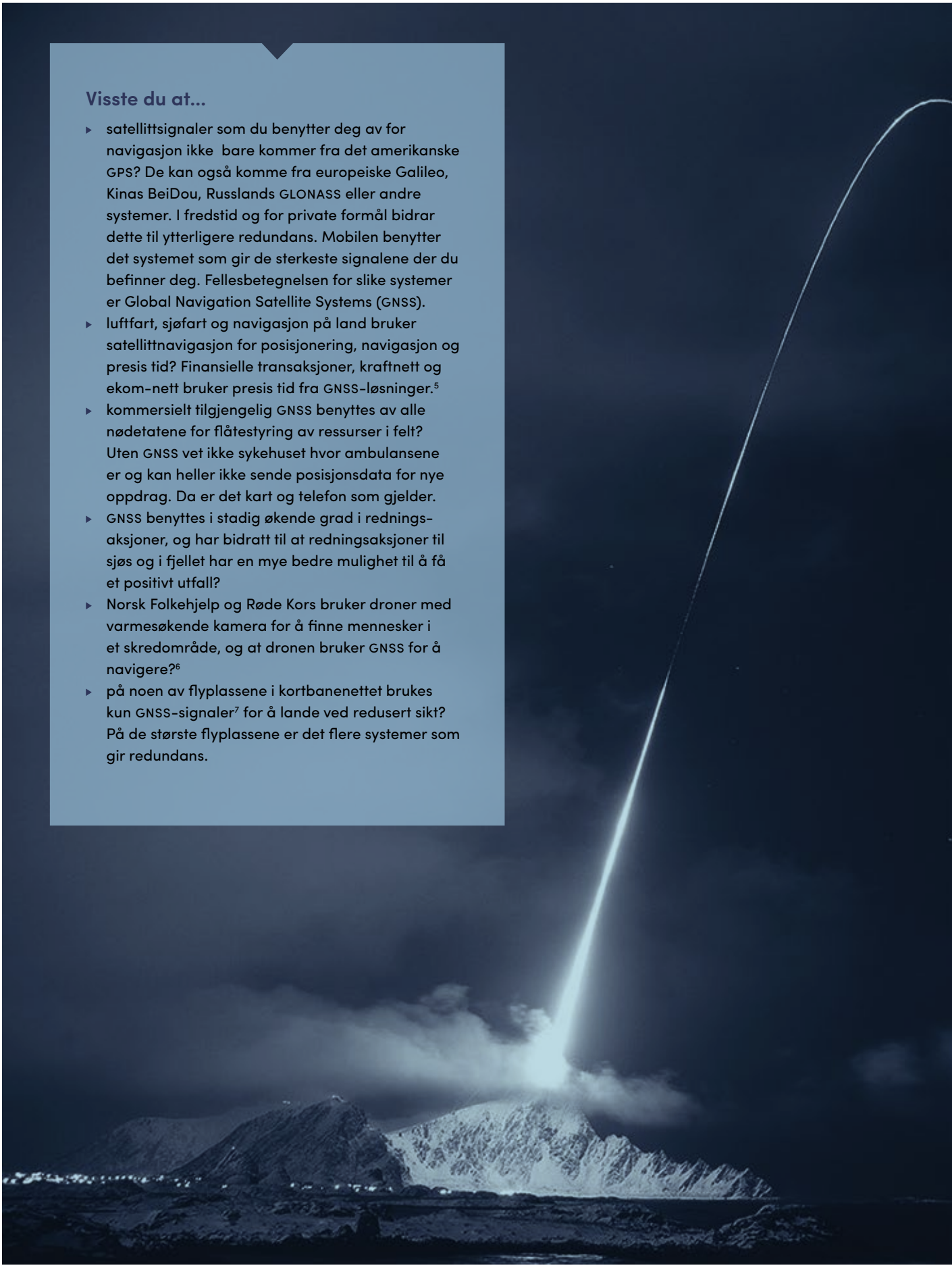
Femte generasjon mobilnett (5G) bygges ut og vil bli fundamentet i det digitaliserte samfunnet i årene fremover. Utviklingen av 5G vil gi et mobilnett med høyere hastighet, lavere forsinkelse, økt pålitelighet og større kapasitet enn dagens mobilnett (4G). Nye produkter og tjenester vil kunne tas i bruk i de fleste samfunnsområder, deriblant forsvar, samferdsel, forvaltning, helse, industri, varehandel og finans. Som del av 5G-utbyggingen vil tjenestetilbyderne også kunne tilby distribuerte sky-løsninger[3] for lagring av store mengder data. Teknologiutviklingen vil rasjonalisere og forbedre tjenester til kundene, men samtidig medføre lengre og mer komplekse verdikjeder med stadig flere involverte aktører.[4]

Den enkeltes, virksomheters og samfunnets avhengighet til ekom-infrastrukturen vil øke i takt med innføringen av nye produkter og tjenester, og mengden av informasjon som flyter i ekom-nettene vil øke dramatisk. Denne informasjonen vil ha stor etterretningsverdi. Samtidig vil bortfall eller redusert funksjon i ekom få betydelige konsekvenser. **Myndighetene må sikre at vi kan ha tillit til utstyrsleverandører, tjenestetilbydere og andre aktører som kan få tilgang til denne informasjonen eller kontrollerer funksjoner i den nasjonale ekom-infrastrukturen.**

Nasjonale ekom-tjenester og -nett er tett knyttet til infrastruktur utenfor Norges grenser, og hendelser i andre land kan derfor påvirke vår digitale infrastruktur. Nasjonal kommunikasjonsmyndighet (Nkom) anbefaler at eiere av norske mobilnett og landsdekkende transportnett blir pålagt å drifte nettene sine autonomt i Norge. De anbefaler at disse kravene gjelder for situasjoner der det er særlig viktig å sikre nasjonal styringsevne og kommunikasjon. NSM støtter disse anbefalingene. **Myndighetene må fortløpende vurdere behov for tiltak relatert til innføring og bruk av 5G spesielt og ekom generelt.**

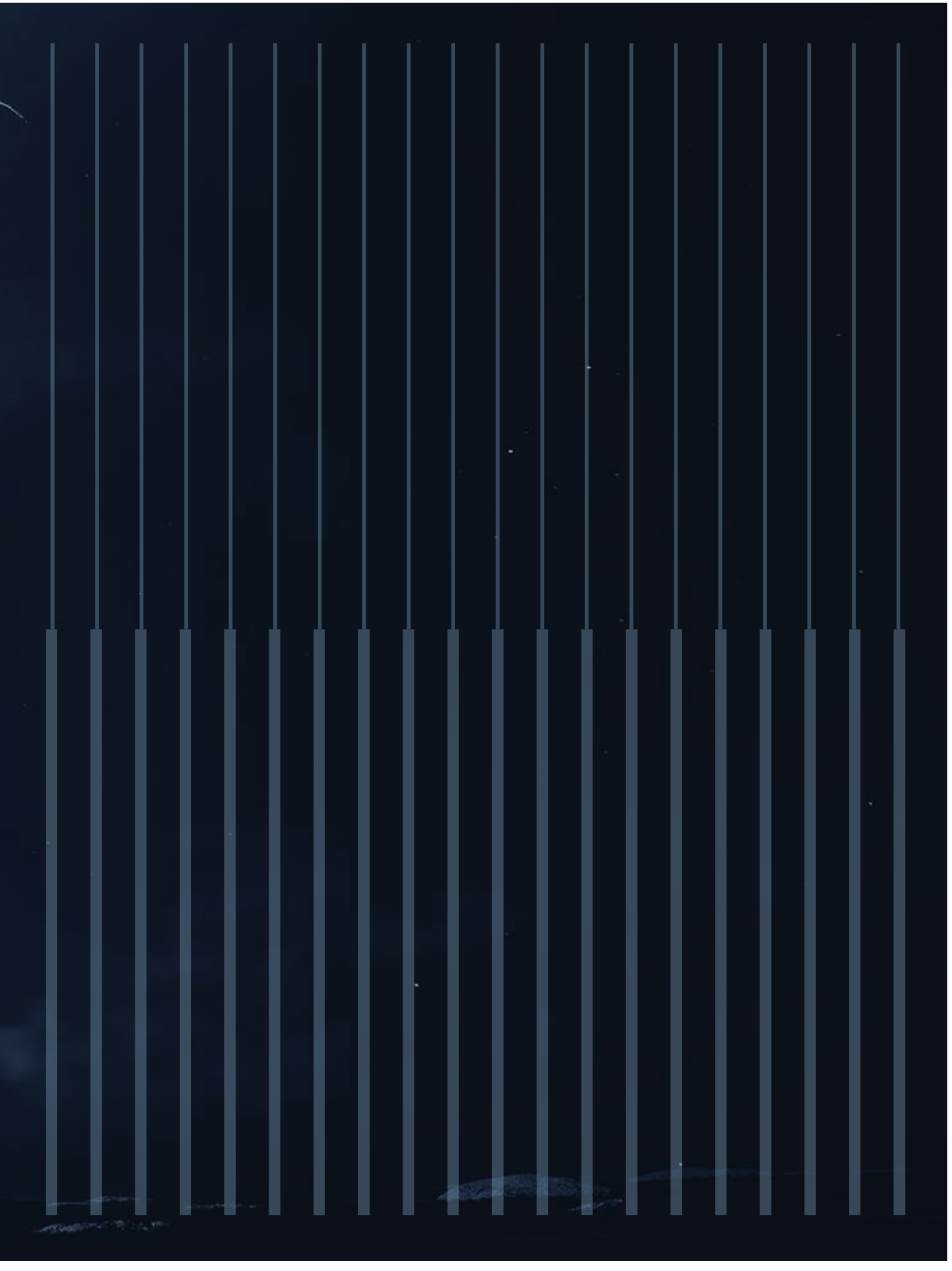
**Satellittbaserte tjenester**

Satellittbaserte tjenester som posisjons-bestemmelse, navigasjon og tids-bestemmelse (PNT), jordobservasjon og kommunikasjon bidrar til betydelig effektivisering og bedre sikkerhet på mange områder. Som følge av dette har mange funksjoner i samfunnet i dag gjort



## Visste du at...

- satellittsignaler som du benytter deg av for navigasjon ikke bare kommer fra det amerikanske GPS? De kan også komme fra europeiske Galileo, Kinas BeiDou, Russlands GLONASS eller andre systemer. I fredstid og for private formål bidrar dette til ytterligere redundans. Mobilen benytter det systemet som gir de sterkeste signalene der du befinner deg. Fellesbetegnelsen for slike systemer er Global Navigation Satellite Systems (GNSS).
- luftfart, sjøfart og navigasjon på land bruker satellittnavigasjon for posisjonering, navigasjon og presis tid? Finansielle transaksjoner, kraftnett og ekom-nett bruker presis tid fra GNSS-løsninger.[5]
- kommersielt tilgjengelig GNSS benyttes av alle nødetatene for flåtestyring av ressurser i felt? Uten GNSS vet ikke sykehuset hvor ambulansene er og kan heller ikke sende posisjonsdata for nye oppdrag. Da er det kart og telefon som gjelder.
- GNSS benyttes i stadig økende grad i redningsaksjoner, og har bidratt til at redningsaksjoner til sjøs og i fjellet har en mye bedre mulighet til å få et positivt utfall?
- Norsk Folkehjelp og Røde Kors bruker droner med varmesøkende kamera for å finne mennesker i et skredområde, og at dronen bruker GNSS for å navigere?[6]
- på noen av flyplassene i kortbanenettet brukes kun GNSS-signaler[7] for å lande ved redusert sikt? På de største flyplassene er det flere systemer som gir redundans.




Gjennom Nasjonalt cybersikkerhetssenter følger NSM med på hendelser i det digitale rom som kan ramme viktige samfunnsfunksjoner.

seg avhengige av satellittbaserte tjenester.

Satellittbaserte tjenester er av stor betydning for sivil og militær luftfart, navigasjon til sjøs, helsetjenester, politi, rednings- og nødetater samt andre samfunnsfunksjoner. Dette viser viktigheten av å kunne ha tillit til slike satellittbaserte tjenester.

Opprettholdelse og drift av satellittbaserte tjenester krever store investeringer og ressurser. Likevel er det stadig store prosjekter for å etablere nye globale satellittnavigasjonssystemer (GNSS[8]). I tillegg til det amerikanske Global Positioning System (GPS) har EU etablert Galileo-systemet, som er i drift og vil være fullt operativt i løpet av 2020. Galileo vil tilby tjenester med bedre presisjon, sikkerhet og tilleggstjenester for myndigheter og er det eneste globale satellittnavigasjonssystemet som er utviklet for sivile formål. Dette gir både større uavhengighet og kontroll, samtidig som det har gitt økt redundans. Som konsekvens av at Storbritannia nå er utenfor EU, utreder britene om de skal utvikle et eget satellittnavigasjonssystem.[9] For Norge vil dette i så fall resultere i at viktige samfunnsfunksjoner trolig vil kunne benytte flere satellittnavigasjonssystemer

Vi må forstå hva trusselaktørene er ute etter og hvordan de kan utnytte sårbarhetene i samfunnet vårt, systemene våre og hos enkeltpersoner.

som vi kan ha høy grad av tillit til.

Sårbarheter og forstyrrelser av satellittbaserte tjenester er nærmere omtalt på side 28.

## Trusselaktører utnytter sårbarhetene våre

For å sikre verdiene våre godt nok må vi forstå hva trusselaktørene er ute etter og hvordan de kan utnytte sårbarhetene i samfunnet vårt, systemene våre og hos enkeltpersoner. Trusselbildet mot norske myndigheter og offentlige og private virksomheter spenner fra opportunistisk kriminalitet på nett til målrettede forsøk på rekruttering av personer i sentrale posisjoner og nettverksoperasjoner fra statlige eller statstilknyttede aktører. Etterretningstjenesten og PST beskriver i sine åpne vurderinger et trusselbilde i endring.[10] Stadig mer av aktiviteten foregår i det digitale rom, og stater bruker ikke-militære virkemidler som økonomisk maktbruk, desinformasjonskampanjer, overvåkingsaktivitet og nettverksoperasjoner for å oppnå sine mål. Det benyttes et bredt spekter av metoder og virkemidler for å utnytte våre sårbarheter. Når slike virkemidler kombineres, omtales det som sammensatt virkemiddelbruk, og dette kan utgjøre såkalte hybride trusler. Nedenfor beskriver vi noen av metodene trusselaktører bruker for å utnytte ulike sårbarheter.

**Etterretning, spionasje og påvirkning**

Forsvars- og sikkerhetsforhold, politiske

### Mistenkelige gaver og etterretningsoppmerksomhet på utenlandsreiser

Norske delegasjoner og myndighetspersoner på reise til enkelte risikoland utsettes for ulike former for etterretningsaktivitet fra lokale etterretnings- og sikkerhetstjenester. NSMs eget personell har opplevd dette ved flere anledninger, blant annet i form av åpenlys aktivitet for å vise at man holdes under oppsikt. Det kan dreie seg om at noen har vært inne på hotellrommet og lagt igjen synlige spor, bagasje som har blitt undersøkt og åpenlys overvåking på gaten. Vårt personell har også avdekket at de har vært utsatt for fordekt aktivitet.

PST beskriver i sin åpne trusselvurdering at etterretnings- og sikkerhetstjenester i land med autoritære regimer benytter metoder som avlytting av hotell- og møterom, avlytting av elektronisk kommunikasjon, infisering av telefoner, minnepinner og datamaskiner med skadevare.

NSM mottar et økende antall forespørsler om bistand til å analysere sluttbrukerutstyr, eksempelvis mobiltelefoner, nettbrett, bærbare PC-er og annet, som det er mistanke om at har blitt kompromittert, modifisert eller tappet for informasjon i utlandet. Vi mottar også henvendelser fra virksomheter som har mottatt gaver i form av mobiltelefoner, minnepinner og annet elektronisk utstyr fra utenlandske firmaer eller gjester.

Det anbefales å følge NSMs reisevettregler for digital sikkerhet: **nsm.stat.no/aktuelt/reiserad-fra-nsm**

NSM gjennomfører tekniske sikkerhetsundersøkelser av bygg og lokaler som inneholder norske skjermingsverdige verdier i inn- og utland. Vi avdekker stadig hull i sikkerheten – både som følge av egne sårbarheter og trusselaktørers omfattende og oppfinnsomme metodebruk. Her er det boret hull i etasjeskillet, trolig klargjort for avlytting.

beslutninger, norske naturressurser og norsk forskning og teknologi innen ulike fagfelt er av interesse for andre stater. Samtidig kartlegges viktig infrastruktur og sentral funksjonalitet som kan benyttes for å øve press på norske beslutningstakere i en eventuell konfliktsituasjon. Etterretningstrusselen mot Norge er omfattende og har et bredt nedslagsfelt. Fremmede stater samler informasjon om norske forhold og standpunkter og forsøker å påvirke beslutninger i sin favør. Det foregår også omfattende industrispionasje, blant annet ved at etterretningstjenester bistår eget næringsliv.

Mange land vil bruke store ressurser og avanserte metoder for å skaffe informasjon eller fortrinn som er viktig for å ivareta sine nasjonale interesser. Blant disse metodene er nettverksoperasjoner, fysisk og digital kartlegging, påvirkningsoperasjoner, rekruttering av personer, strategiske investeringer, avlytting av rom og telefontrafikk og avlesing av digitale signaler fra annet sluttbrukerutstyr.

**Kartlegging gjennom fysisk og teknisk innhenting**

Fremmed etterretning kartlegger norsk sivil og militær infrastruktur i fredstid som et ledd i å planlegge for fremtidig sabotasje i en eventuell konfliktsituasjon eller for å identifisere nye mål for innhenting. Mye informasjon kan innhentes gjennom åpne kilder. Eksempler på slik informasjon er ulike offentlige registre, kart, detaljer om infrastruktur, statlige og kommunale beslutningsprosesser og offentlige postjournaler. Andre eksempler er virksomheters hjemmesider og virksomheter og privatpersoners bruk av ulike sosiale medier. Volumet av tilgjengelig åpen informasjon er stort og

NSM avdekker jevnlig svakheter som gjør det mulig for uvedkommende å avlytte akustiske og elektromagnetiske signaler og avlese kommunikasjons- og informasjonssystemer.

forventes å øke fremover. Sammenstilling av åpent tilgjengelig informasjon kan tegne et tilstrekkelig bilde til å ramme verdifull infrastruktur og andre funksjoner.

Andre informasjonsbrikker innhentes ved hjelp av andre etterretningsmetoder, og både virksomheter og enkeltpersoner kan bli utsatt for kartlegging. Nettverksoperasjoner[11] benyttes både for å kartlegge virksomheter og infrastruktur og identifisere nye mål. Trusselaktører kan følge med på reiseaktivitet og offisielle besøk. Tilreisende etterretningspersonell driver fysisk kartlegging av infrastruktur og installasjoner, og det benyttes mange ulike type sensorer plassert på kjøretøy, fly, maritime fartøy og andre mobile plattformer.

Høyttalere og mobiltelefoner kan brukes som avlyttingsutstyr, uten at eieren av utstyret er klar over det. Dataskjermer kan avleses på avstand gjennom vegger og fra utsiden av bygg. Usikrede Wifi-rutere og andre IoT-enheter[12] kan hackes på lang avstand via trådløs tilgang.[13]

NSM gjennomfører undersøkelser for

å se om uvedkommende kan skaffe seg tilgang til sikkerhetsgradert informasjon ved avlytting, innsyn eller avlesning av signaler.[14] Det avdekkes jevnlig svakheter som gjør det mulig for uvedkommende å avlytte akustiske og elektromagnetiske signaler og avlese kommunikasjons- og informasjonssystemer. Det finnes mange avanserte angrepsmetoder, og mulighetene for kompromittering øker i takt med at teknologi og sensorer tilknyttet nettverk bringes inn i kontorer, møterom og styrerom. De samme metodene kan benyttes for å få tak i eller endre annen sensitiv informasjon. **Virksomheter som skal etablere systemer for håndtering av sikkerhetsgradert informasjon, kan finne tekniske veiledninger, råd og anbefalinger på NSMs nettside.**

I virksomheter hvor de ansatte har mangelfull situasjonsforståelse eller sikkerhetskompetanse, er NSMs erfaring at bruk av avanserte avlyttingsmetoder vil være overflødig.

**Sammensatt virkemiddelbruk og påvirkning**

Hybride trusler og sammensatt virkemiddelbruk benyttes for å fremme et lands interesser på bekostning av et annet lands interesser. Dette er et fenomen som det er krevende å utvikle gode tiltak mot. Ved sammensatt virkemiddelbruk utnyttes sårbarheter ved de mest fundamentale verdiene i et liberalt demokrati. Påvirkningsoperasjoner er en viktig del av hybride trusler og sammensatt virkemiddelbruk. I den lavere delen av krisespennet kan påvirkningsoperasjoner bli brukt uten at annen virkemiddelbruk er tydelig. Slike operasjoner er det flere eksempler på internasjonalt gjennom de senere årene.

Som et åpent samfunn er vi sårbare. Den informasjonen vi ser i det offentlige rom, sosiale medier eller på nyhetssider kan lett bli endret av forfalsking, halvsannheter og lignende, og det kan være vanskelig å ivareta tilstrekkelig kildekritikk. Risikoen for misbruk av åpen informasjon vil være vanskelig å redusere tilstrekkelig uten å svekke våre demokratiske verdier. Det er derfor viktig å ivareta og bygge opp under den åpne samfunnsdebatten.

Viktige demokratiske prosesser som Brexit-avstemmingen og presidentvalget i USA i 2016 ble utsatt for omfattende påvirkningsoperasjoner.[15] Både sosiale og redaksjonelle medier ble utnyttet i begge disse sakene. Vi har eksempler på at store konferanser, folkemøter og demonstrasjoner arrangeres med en bakenforliggende intensjon om å påvirke meningsdannelse, og slik sett berører norske sikkerhetsinteresser.

Fremmede stater forsøker å påvirke norske beslutninger for å nå sine sikkerhetspolitiske og strategiske målsettinger. Slik påvirkning skjer både åpent og i det skjulte. Påvirkningsoperasjoner kan blant annet brukes for å svekke befolkningens

Enkeltpersoner kan bli utnyttet på en kynisk måte der personvern og rettssikkerhet er satt fullstendig til side.

### Hva er en innsider?

En innsider er 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.

Risikoen for en innsidehandling påvirkes av personens
- *intensjon*, eller motivasjon for å gjennomføre en tilsiktet uønsket handling
- *kapasitet*, det vil si personens kunnskap, erfaring, tilganger og egnethet
- *mulighet*, den faktiske anledningen en person har for å utøve innsidevirksomhet

En bevisst innsider har intensjon om å begå handlinger som strider mot virksomhetens interesser, enten selvmotivert eller utløst av press eller annen påvirkning. Slik påvirkning kan for eksempel innebære at man blir kultivert av fremmed etterretningspersonell og dermed villig til å gi fra seg informasjon over en lengre periode.

En ubevisst innsider påfører virksomheten skade eller tap uten overlegg, for eksempel som følge av manglende kunnskap, naivitet, uoppmerksomhet eller sviktende kjennskap til sikkerhetsregler og rutiner.

tillit til myndigheter, valg og politiske prosesser. Slike operasjoner kan også ha som mål å påvirke opinionen i enkeltsaker eller styre samfunnsdebatten i en bestemt retning.

Påvirkningsaktivitet tar stadig nye former og kan være vanskelig å avdekke. Tiltak mot falske nyheter har gitt effekt. Samtidig ser man at aktører har endret sin bruk av påvirkningsaktivitet gjennom sosiale medier, blant annet ved at polariserende temaer eller saker som løfter spesifikke budskap fra etablerte nyhetsplattformer, videreformidles.

Det kan være vanskelig for befolkningen å skille mellom oppkonstruerte saker, saker som fremstilles på en tendensiøs måte og faktiske opplysninger. Det hviler derfor et stort ansvar på redaksjonelle medier for å fremstille saker balansert og være tydelige på bruk av kilder og kildehenvisninger. **For myndighetene vil det være viktig å etablere og opprettholde et godt situasjonsbilde for å kunne identifisere og håndtere slike trusler.** I dette arbeidet må også media og andre relevante sivile aktører involveres. **Virksomheter underlagt sikkerhetsloven skal varsle NSM ved begrunnet mistanke om sikkerhetstruende virksomhet.**[16]

**Innsiderisiko**

Fremmede etterretningstjenester bruker store ressurser på å rekruttere både egne og norske borgere med tilgang til informasjon eller andre verdier som er

## Tidligere etterretningsoffiser dømt for spionasjeforsøk

Ron Rockwell Hansen, en tidligere ansatt i amerikanske Defense Intelligence Agency (DIA), ble i september 2019 dømt til 10 års fengsel for å ha forsøkt å kommunisere, overlevere og overføre sikkerhetsgradert informasjon om det amerikanske forsvaret til Kina i perioden 2016-2018.[17] Før Hansen begynte hos DIA som sivilt ansatt i 2006, hadde han en over 20 år lang karriere bak seg i det amerikanske forsvaret.[18]

Hansen hadde store økonomiske problemer. I 2012 hadde han mer enn 200 000 USD i privat gjeld, samtidig som han hadde et privatforetak som tapte mer enn 1 000 000 USD rundt 2014. I 2014 ble Hansen kontaktet og rekruttert av kinesisk etterretning, og som innsider mottok han flere hundre tusen dollar.

## Vi lar oss lure

NSM bruker ofte e-post som angrepsvektor i våre inntrengingstester og erfarer at tilstrekkelig mange lar seg lure til å kjøre skadevare (det kan være nok med én). Når trusselaktøren først har fått en fot innenfor virksomhetens nettverk, starter jobben med å utvide tilgangen.

**Sikkerheten kan ikke alene overlates til den enkelte medarbeider. Virksomheten må ha tiltak som hindrer kompromittering selv om den ansatte kommer i skade for å gjøre feil.**

**Vi viser til *NSMs grunnprinsipper for IKT-sikkerhet* og *Grunnleggende tiltak for sikring av e-post*.**

Strategiske investeringer og oppkjøp brukes som metode for å skaffe innpass i prosesser og beslutninger og tilgang til sensitiv informasjon, teknologi og kompetanse.

### Nøkkelpersonell

Nøkkelpersoner har spesielle oppgaver eller kunnskap som gjør dem ekstra viktige for virksomhetens leveranser eller som kan være avgjørende for viktige samfunnsfunksjoner som virksomheten ivaretar.

Fremmede etterretningstjenester kan ha interesse av å tilnærme seg og kultivere personer i norske virksomheter med viktig kompetanse, tilganger og talenter. I etterretningsutsatte virksomheter vil nøkkelpersonell være av stor interesse, da de har mulighet til å kompromittere, sabotere eller ødelegge viktige eller skjermingsverdige verdier.

**Det kan være nødvendig å implementere virksomhetsspesifikke tiltak for å redusere denne sårbarheten og dermed også risikoen knyttet til nøkkelpersonell til et akseptabelt nivå. Første skritt vil være å vurdere hva som utgjør virksomhetens mest sentrale funksjoner og hvem som er avgjørende for å utføre dem.**

### Trusselaktører velger sine mål

I tillegg til personer virksomheten er avhengig av på grunn av spesiell kompetanse, kan nøkkelpersonell – sett fra en trusselaktørs perspektiv – også være

- personer med beslutningsmyndighet
- personer som har tilgang til spesielt sensitiv informasjon
- personell som har eller gir tilgang til viktig infrastruktur og IT-systemer (administratorrettigheter)

viktige for deres nasjonale interesser. For å oppnå sine mål leter trusselaktører systematisk etter personer som kan utnyttes eller er villige til å gi dem tilgang til de verdiene de jakter på. Fremmed etterretning har personell som er spesialtrent for å utnytte og forlede personer. De vil også kunne manipulere utnyttede eller rekrutterte personer til å tro at det er for sent å trekke seg. I dette spillet kan enkeltpersoners skjebne ha liten betydning for fremmed etterretning opp imot deres nasjonale målsettinger, og enkeltpersoner kan bli utnyttet på en kynisk måte der personvern og rettssikkerhet er satt fullstendig til side. **NSM vil understreke at det aldri er for sent å trekke seg. Personer som utsettes**

**for tilnærming eller blir utnyttet av trusselaktører, må ta kontakt med PST.**

Ved å utnytte menneskelige sårbarheter hos personer med de rette tilgangene vil en trusselaktør kunne skaffe seg urettmessig tilgang til informasjon, informasjonssystemer eller andre verdier det er viktig å beskytte. For en virksomhet vil en potensiell innsider være en betydelig risikofaktor. Medarbeidere eller andre som kjenner interne systemer og rutiner ved virksomheten, vil kunne omgå både digitale og fysiske sikkerhetsbarrierer eller sette slike tiltak ut av spill. Dersom virksomheten ivaretar viktige samfunnsfunksjoner, vil innsidevirksomhet kunne ha alvorlige konsekvenser for våre nasjonale sikkerhetsinteresser.

Innsidevirksomhet oppstår i de fleste tilfeller  noen år etter at en person ble ansatt.[19] **Det er derfor svært viktig at alle virksomheter følger opp sitt personell gjennom hele ansettelsesforholdet, slik at omstendigheter som kan benyttes som pressmiddel med tanke på rekruttering, kan avdekkes og håndteres fortløpende. I tillegg må virksomhetene iverksette andre sikkerhetstiltak som reduserer risiko for innsidevirksomhet. Dette gjelder for eksempel soneinndeling/ autorisasjonsskiller både i fysiske domener og informasjonssystemer, i tillegg til logging av aktivitet i systemer så vel som i virksomhetens lokaler.**

Les mer om innsidere i NSMs tema-rapport *Innsiderisiko*.[20]

### Personellsikkerhet

Virksomheten bør skape et helhetlig system for å styrke personellsikkerheten, uavhengig av om den omfattes av sikkerhetsloven eller ikke. Forankring hos ledelsen, tydeliggjøring av ansvar samt utvikling av rutiner og prosedyrer er tiltak som kan bidra til å styrke personellsikkerheten i virksomheten.

- Det er viktig at virksomhetene ivaretar personell-sikkerheten før, under og etter ansettelsesforholdet ved å sikre at risikoreduserende tiltak er iverksatt.[21] For personell som er sikkerhetsklarert for tilgang til sikkerhetsgradert informasjon, understrekes behovet for jevnlige autorisasjonssamtaler.
- Virksomhetene må ha tilstrekkelig kompetanse og ressurser til å beskytte virksomhetens verdier mot innsidevirksomhet.
- Virksomheten må legge til rette for en god sikkerhetskultur gjennom å øke de ansattes forståelse av sikkerhetsregler og rutiner samt legge til rette for oppfølging av de ansatte.
- De ansatte må være bevisst på verdiene de skal være med på å beskytte både på arbeidsplassen og på reise.

**Strategiske investeringer og oppkjøp**

Norge er en del av en åpen, global økonomi og er avhengig av utenlandske investeringer og kompetanse. En nylig NUPI-undersøkelse viser at Norge og de andre nordiske landene er generelt positivt innstilt til utenlandske investeringer. Det er en klart positiv

NSM ser et jevnt trykk av nettverks-operasjoner mot mål i Norge.

### Løsepengevirus

Løsepengevirus er en type skadevare som brukes til å kryptere filer hos virksomheter, og deretter kreve penger for å dekryptere dem. De siste årene har man sett en økning av løsepengevirus rettet mot bedrifter og virksomheter med større betalingsevne enn enkeltpersoner. Sammen med Kripos har NSM utarbeidet en temarapport[22] om løsepengevirus. Temarapporten beskriver hva løsepengevirus er og hvordan man kan beskytte seg mot slike angrep, blant annet råd[23] om hvordan man kan hindre skadevaren i å kjøre og begrense konsekvensene skadevaren kan påføre.

holdning til utenlandske investeringer fra EU-land. Samtidig er det utbredt skepsis til investeringer fra Russland og Kina. Dette gjelder særlig investeringer i sektorer som forvalter naturressurser, teknologi og infrastruktur.[24]

Strategiske investeringer og oppkjøp brukes som metode for blant annet å skaffe innpass i prosesser og beslutninger og tilgang til sensitiv informasjon, teknologi og kompetanse.[25] [26] [27] Det kan for eksempel dreie seg om oppkjøp av eller investeringer i virksomheter som utvikler teknologi eller forvalter naturressurser eller kjøp av eiendom.

Dette kan være en gunstig måte å drive innhenting på eller å oppnå påvirkningsmuligheter. Det kan gi legitim tilgang til informasjon og teknologi som kan benyttes for illegitime formål. Slike oppkjøp kan også bidra til å posisjonere egne selskaper i et strategisk viktig marked. Denne typen aktivitet kan skje gjennom stråselskaper og komplekse selskapsstrukturer og kan dermed være vanskelig å avdekke. Det kan være vanskelig å skille strategiske oppkjøp med illegitime hensikter fra ordinær porteføljeforvaltning foretatt ut fra rene kommersielle hensyn.

For virksomheter som omfattes av sikkerhetsloven, kan slike utfordringer håndteres gjennom bestemmelsene om eierskapskontroll. Bestemmelsene gir regjeringen mulighet til å stanse eller sette vilkår for erverv av virksomheter som er underlagt loven, dersom ervervet «kan medføre en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet».[28]

Strategiske investeringer og oppkjøp vil imidlertid kunne representere en betydelig nasjonal risiko selv om investeringene som gjøres og virksomhetene som kjøpes opp, ikke er omfattet av sikkerhetsloven. Regjeringen har også mulighet til å stanse slik aktivitet i henhold til § 2-5 i sikkerhetsloven.[29] I slike tilfeller vil det imidlertid være utfordrende for myndighetene å holde oversikt og oppdage aktiviteten i tide. **Ved mistanke om at utenlandske aktører forsøker å kjøpe opp eller investere i norske virksomheter eller eiendom med hensikt om å gjennomføre sikkerhetstruende virksomhet, skal det varsles til NSM.**

**Nettverksoperasjoner**[30]
Nettverksoperasjoner utgjør en alvorlig risiko for norske virksomheter og samfunnsfunksjoner, og NSM ser et jevnt trykk av slike operasjoner mot mål i Norge. I tillegg blir de vanskeligere å oppdage, og metodene er sammensatte.

Fremmede stater søker blant annet etter høyteknologi og forretnings-hemmeligheter, i tillegg til stats-hemmeligheter, når de gjennomfører digitale etterretningsoperasjoner mot norske virksomheter. Disse aktørene har store ressurser og jobber med langsiktige målsettinger. Operasjonene er i mange tilfeller sofistikerte, og det anvendes høy teknologisk kompetanse. Nettverksoperasjoner med etterretningsformål kan gjennomføres på måter som gjør dem vanskelig å oppdage.

Trusselaktører utfører rekognosering og informasjonsinnhenting mot mål i Norge. NSM vurderer at statsforvaltningen og virksomheter innen sektorene forsvar, rom, maritim, petroleum og kraft er risiko-utsatt. I tillegg er det risiko for nettverks-operasjoner mot virksomheter som driver ulike former for forskning. Kartlegging av sårbarheter i kritisk infrastruktur kan i tillegg utgjøre forberedelse til fremtidige sabotasjehandlinger ved en eventuell eskalering i krisespennet.

Norske virksomheter er også mål for andre typer nettverksoperasjoner. Virksomheter utsettes for eksempel for utpressingsforsøk ved bruk av

## Nasjonalt cybersikkerhetssenter

Nasjonalt cybersikkerhetssenter (NCSC) ble etablert som del av NSM i november 2019 og skal bidra til å beskytte grunnleggende nasjonale funksjoner, offentlig forvaltning og næringsliv mot digitale angrep. NCSC legger til rette for tettere samarbeid internt i offentlig sektor og med næringsliv, akademia og internasjonale partnere. Allerede har 41 virksomheter inngått partnerskap med senteret. Det er et behov for at alle disse aktørene arbeider sammen, med utgangspunkt i et felles risikobilde og med samme situasjonsforståelse.

NCSC vil støtte sikkerhetsarbeidet i norske virksomheter gjennom tre hovedfunksjoner:

1. utvikle og tilgjengeliggjøre tiltak og anbefalinger samt drive rådgivning
2. ivareta nasjonal responsfunksjon og avdekke alvorlige digitale hendelser
3. tilby tjenester innen teknisk sikkerhet

Senteret skal være en driver for digital sikkerhet i Norge.

## Allvis NOR

Allvis NOR er en tjeneste NSM tilbyr for å kartlegge og avdekke sårbarheter på internetteksponerte IKT-systemer. Kartleggingen foregår kontinuerlig og dekker alle TCP-porter på oppgitte IP-adresser. Virksomheter underlagt sikkerhetsloven kan abonnere på denne tjenesten. Her er noen nøkkeltall:

- Antall virksomheter: 205
- Antall innmeldte IP-adresser: 1 140 886
- Antall IP-adresser med minst en eksponert tjeneste: 13 140

Tilsiktet jamming og andre former for forstyrrelse av satellittsignaler benyttes aktivt for militære formål.

### Erfaringer fra Nasjonalt cybersikkerhetssenter i 2019:

De digitale hendelsene NCSC registrerte og håndterte i 2019, er i tråd med trendene man har sett i det digitale domenet de siste årene. Metodene som brukes for å komme inn i norske virksomheter utvikler seg fra år til år, men er i stor grad gjenkjennbare fra tidligere. Trusselaktørene benytter kjente sårbarheter for å trenge inn i systemer og nettverk, ofte via internetteksponerte tjenester hos virksomheten. Bred kartlegging av sårbarheter og innsamling av åpen informasjon om en virksomhet kan benyttes for å skreddersy e-poster som brukes i målrettede operasjoner mot virksomheten. Denne informasjonen kan benyttes for å skaffe påloggingsdetaljer via målrettede e-post-kampanjer som deretter utnyttes til å få tilgang til systemene.

I tillegg ser vi at:

- Løsepengevirus (ransomware) er et vedvarende problem.
- Internetteksponerte tjenester kan gjøre virksomheten sårbar for angrep.
- Tjenesteutsetting av IT-drift uten god kravstilling kan eksponere data.
- Løsninger for fjernaksess er en vedvarende sårbarhet.
- Norske virksomheter blir mer sikkerhetsbevisste – de identifiserer tiltak og iverksetter disse i større grad.

løsepengevirus, der trusselaktørene lammer digitale systemer og krever løsepenger for å låse opp krypteringen. Et nylig og alvorlig eksempel på løsepengevirus mot norske virsomheter er Hydro-saken fra i fjor vår, som stoppet deler av Hydros aktivitet. Svindelforsøk i form av direktørsvindel, digitale innbrudd og misbruk av infrastruktur til utvinning av kryptovaluta rammer også mange norske virksomheter.

Trusselaktører bryter seg inn i virksomheters nettverk blant annet for å hente ut informasjon fra systemene. Slik systemtilgang gjør det også mulig å endre informasjon. Aktørene kan også etablere funksjonalitet slik at systemene kan benyttes for illegale formål rettet mot andre virksomheter. Trusselaktørers utnyttelse av legitime virksomheters digitale infrastruktur utgjør en alvorlig risiko.

Kriminelle og statlige aktører benytter leid infrastruktur og digitale vertstjenester med infrastruktur i Norge til ondsinnet aktivitet. Fremleie av vertstjenester kan skje i flere ledd, noe som gjør det vanskelig å forebygge, etterforske og stoppe slik aktivitet.

**NSM anbefaler alle virksomheter å implementere NSMs grunnprinsipper for IKT-sikkerhet for å redusere risikoen for nettverksoperasjoner. Virksomheter underlagt sikkerhetsloven bør abonnere på sårbarhetsskanning av sine internett-eksponerte systemer gjennom NSMs tjeneste Allvis NOR. Departementene må innenfor sitt ansvarsområde vurdere hvilke virksomheter som bør tilknyttes NSMs**

# Digital sikkerhet – effektive råd

NSM anbefaler fire enkle, men effektive tekniske tiltak som virksomheter bør benytte for å beskytte sine systemer mot internett-relaterte nettverksoperasjoner.

De mest vanlige nettverksoperasjonene skjer via infiserte e-poster, nettsider eller USB-minnepinner. De fleste av disse er teknisk og kostnadsmessig sett relativt enkle å stoppe.

1

### Oppgrader program- og maskinvare.

Nyere produktversjoner har tettet flere sikkerhetshull enn eldre versjoner, og de har ofte flere og bedre sikkerhetsfunksjoner. Dette gjelder både program- og maskinvare.

2

### Installer sikkerhetsoppdateringer så fort som mulig.

Selv de beste produktene har feil og sårbarheter som kan bli utnyttet av angripere. Virksomheter bør etablere et sentralt styrt regime for oppdatering av applikasjoner og operativsystemer. Dette er viktig fordi kunnskap om nyoppdagede sårbarheter spres raskt. Derfor bør virksomheter være tilsvarende raske med å installere sikkerhetsoppdateringer som fjerner eller motvirker sårbarhetene.

3

### Ikke tildel administrator-rettigheter til sluttbrukere.

De fleste sluttbrukere har ikke behov for administrator-rettigheter. Dessverre gir altfor mange virksomheter brukerne (og angriperne) skriverettigheter til systemområder. Dette er unødvendig, og man lar i så fall datamaskinen være ganske åpen for angriperne. Man bør derfor fjerne administrator-rettigheter fra vanlige kontorbrukere og distribuere virksomhetsgodkjent programvare fra et felles distribusjonspunkt.

4

### Tillat kun kjøring av autoriserte programmer («hvitelisting»).

Bruk egnede verktøy for å kontrollere at sluttbrukere kun får kjøre godkjente applikasjoner. Blokker spesielt programmer utenfor godkjente mapper og på flyttbare media, for eksempel på CD-er og minnepinner.

Alle brukere av satellittbaserte tjenester bør vurdere behovet for reserveløsninger, inkludert rutiner og alternative prosedyrer.

**varslingssystem for digital infrastruktur (VDI).**

Rammeverk for digital hendelseshåndtering ble etablert i 2016. Dette er under stadig utvikling. **Departementene må etablere og videreutvikle de sektorvise responsmiljøene for å sikre god implementering av rammeverket.**

**Forstyrrelse av satellittbaserte systemer**

Tilsiktet jamming og andre former for forstyrrelse av satellittsignaler benyttes aktivt for militære formål. Forstyrrelser av satellittbaserte navigasjonssystemer som GPS har ved flere anledninger påvirket signaler i norsk luftrom. Russisk øvingsaktivitet i grenseområdene mot Øst-Finnmark har flere ganger skapt problemer for sivil lufttrafikk. Slike forstyrrelser og utfall kan få alvorlige konsekvenser for militær og sivil luft- og sjøtrafikk, i tillegg til viktige nød- og beredskapsfunksjoner.

Hovedtypene forstyrrelser av satellittsignaler er jamming og narring (spoofing). Jamming betyr å sende støysignaler i det aktuelle frekvensområdet for å forstyrre mottaket av signaler, mens spoofing går ut på å sende falske signaler som manipulerer tidsinformasjon og posisjon.

Hensikten med jammingen kan være å demonstrere makt eller sette kapasiteter ut av funksjon. Forstyrrelse av satellittsignaler vil få konsekvenser for både sivile og militære kapabiliteter. I 2019 har det vært flere hendelser der sivil luftfart har vært rammet av støysignaler. Bortfall av sivile og militære satellittbaserte tjenester må påregnes, både som følge av tilsiktede og utilsiktede hendelser og naturfenomen.

Samfunnets avhengighet av PNT og trusselsituasjonen gjør det viktig å sikre infrastruktur for PNT-tjenester mot forstyrrelser, fysiske anslag og nettverksoperasjoner. Slike hendelser kan ha konsekvenser for samfunnssikkerhet og nasjonal sikkerhet. Satellittbaserte tjenester preges av et betydelig offentlig-privat samarbeid, og dette samarbeidet

### Digital svindel (KRISINO 2019[31])

Av de 2500 private og offentlige virksomhetene som ble undersøkt i Næringslivets sikkerhetsråds undersøkelse KRISINO 2019, hadde 15 prosent av respondentene vært utsatt for løsepengevirus de siste 12 månedene. 13 prosent hadde vært utsatt for direktørsvindel, det vil si at direktørens e-postadresse eller telefonnummer er brukt for å lure økonomiansatte til å overføre penger. Et interessant funn i NSRs undersøkelse er at blant private virksomheter med mer enn 100 ansatte var hele 50 prosent utsatt for direktørsvindel.

Undersøkelsen tyder på at private virksomheter er mer utsatt enn offentlige for slik kriminalitet. Det er også verdt å merke seg at 81 prosent av respondentene som hadde vært utsatt for løsepengesvindel, direktørsvindel eller to andre former for svindelforsøk, ikke hadde politianmeldt hendelsene.

Digital svindel og svindelforsøk bør politianmeldes.

er sentralt også i et sikkerhetsperspektiv.

Forstyrrelser eller bortfall av PNT-tjenester utgjør en stor risiko. **Alle brukere av satellittbaserte tjenester bør vurdere behovet for reserveløsninger, inkludert rutiner og alternative prosedyrer.** Dette vil særlig gjelde for samfunnsfunksjoner som er avhengige av presis navigasjon og posisjonering. Både virksomheter og myndigheter må vurdere mulige løsninger. Sektormyndigheter og deres overordnede departementer har et særlig ansvar.

**Droner**

Økt dronebruk skaper utfordringer for nasjonal sikkerhet. Det er observert flere tilfeller av uautorisert droneaktivitet i forbindelse med militære øvelser og ved forbudsområder, hvor det er forbud mot fotografering, filming og bruk av andre sensorer fra luften.

Utstrakt droneaktivitet innebærer at det tas enorme mengder bilder av landskap, bygninger og mennesker. Flere leverandører tilbyr lagring av data i en sky-løsning. Som følge av dette samles store mengder av ulike type geotagget data (bilder, film og så videre) som en trusselaktør kan utnytte dersom den får tilgang. Dette gjelder alt fra informasjon om enkeltpersoner til detaljert kartlegging av områder der data fra flere droner i samme område kan sammenstilles. På denne måten kan etterretningstjenester få hjelp av intetanende personer over hele verden til innhenting av store mengder verdifull informasjon. Tilsvarende problemstilling gjelder for data aggregert fra blant annet andre mobile og autonome enheter. Trusselaktører kan få tilgang til store mengder data dersom sikkerheten i leverandørens løsning eller i datasenteret der slik informasjon lagres, ikke er tilstrekkelig god. Statlige etterretningsorganisasjoner har i noen land tilgang på informasjon som er lagret i private datasentre som er lokalisert innenfor landets grenser eller som driftes av selskaper registrert i landet.

For å unngå uønsket innhenting fra droner er det etablert forbudsområder i henhold til *forskrift om kontroll med informasjon innhentet ved bruk av luftbårne sensorsystemer.* På NSMs

### GPS-jamming i Troms og Finnmark

Ved flere anledninger gjennom 2018 og 2019 ble GPS-signalene i Troms og Finnmark slått ut. Etterretningstjenesten avdekket at det var russisk aktivitet som førte til forstyrrelsene. Forstyrrelsene har til en viss grad påvirket sivil luftfart og skipstrafikk, men har heldigvis ikke fått alvorlige konsekvenser. Det er imidlertid et stort potensial for å ramme flere sentrale samfunnsfunksjoner. Ettersom aktiviteten blant annet var stor ved NATO-øvelsen Trident Juncture, er det ifølge Etterretningstjenesten grunn til å tro at noen av tilfellene var tilsiktede forstyrrelser fra russisk side, mens andre tilfeller kan ha vært utilsiktede effekter i Norge som følge av russisk øvingsaktivitet.

# Droner som verktøy

Bruk av droner har økt i omfang i de siste ti årene. Utviklingen har medført at droner har blitt allemannseie. Dronene er blitt mindre og mer portable, enklere å styre samt billigere å kjøpe. Mange opererer droner uten å sette seg inn i regelverk eller luftromsstruktur. Som arbeidsverktøy har dronene stor nytteverdi og et bredt anvendelsesområde. For eksempel har de forenklet arbeid som tidligere var risikofylt og vanskelig, slik som inspeksjon av luftspenn. Slik bruk er et gode og reduserer fare for liv og helse.

Autonome droner er i dag fullt mulig – dronene kan navigere selv og unngå hindringer. Det er også mulig for privatpersoner og statlige aktører å koble avanserte sensorer på relativt små, ubemannede luftfartøyer.

Trusselaktørene kan bruke droner for å oppnå samme resultat som tidligere krevde langt mer ressurser. Data fra luftbårne sensorer kan kombineres med annen tilgjengelig informasjon og bearbeides i lett tilgjengelig programvare for blant annet å lage 3D-modeller av objekter og terreng. Kombinasjon av forskjellige typer sensorer, eksempelvis laserskanner (LIDAR) og fotokamera, er økende. En slik kombinasjon gir gode muligheter for å lage detaljerte, virkelighetsnære og skalerte 3D-modeller som kan bli brukt blant annet til å planlegge innbrudd, sabotasje, eller inneholde etterretningsinformasjon.

## Regulering av droner og andre luftbårne sensorer

I 2017 ble det vedtatt en ny lov om informasjon i bestemte områder.[32] Forskriften som regulerer bruken av droner og andre luftbårne sensorer i nærheten av skjermingsverdige objekter trådte i kraft i 2018.[33] Det nye regelverket søker å balansere samfunnets behov for tilgang til informasjon med nødvendig grad av beskyttelse av skjermingsverdig informasjon. På bakgrunn av dette har NSM offentliggjort og holder vedlike en oversikt over hvor det er forbudt å benytte sensorsystemer fra luften.

## Dronehendelse ved Haakonsvern

I oktober 2019 ble to utenlandske personer anholdt og mistenkt for brudd på flyforbud i området over marinebasen Haakonsvern i Bergen. Personene hadde flydd droner over området. De erkjente straffskyld, ble bøtelagt og løslatt. Dronene ble inndratt. Det aktuelle området er i tillegg til å være flyforbudsområde også forbudsområde for bruk av luftbårne sensorsystemer, jf. *forskrift om kontroll med informasjon innhentet med luftbårne sensorsystemer*. Filming av forbudsområder kan være sikkerhetstruende virksomhet, som for eksempel spionasje. Opptaksmateriell fra filming av forbudsområder anses som sikkerhetsgradert informasjon.

Virksomheter og myndigheter må veie risikoen åpen informasjon representerer opp mot fordelene det gir.

nettsider ligger en oppdatert oversikt over forbudsområder. **Observasjoner innenfor eller i nærheten av sensor-forbudsområder må varsles til NSM og andre relevante myndigheter. Dersom droneoperatøren lokaliseres, må politiet involveres.** For øvrig er utfordringer knyttet til skylagring omtalt på side 34.

I andre deler av verden øker bruken av droner som våpen. Droner med eksplosiver har blant annet vært benyttet i Syria, i et påstått attentatforsøk mot president Maduro i Venezuela og i angrep på to viktige oljeinstallasjoner i Saudi-Arabia. En drone med eksplosiver kan gjøre store ødeleggelser til en lav kostnad.

## Sårbarheter i et digitalt samfunn i rask utvikling

Den teknologiske utviklingen går i et rivende tempo og gjør at fremtiden inneholder muligheter som vi i dag ikke kan forestille oss. Ny teknologi tas i bruk hver eneste dag, både i det offentlige og det private, og muligheter for effektivisering og tilrettelegging både for samfunnet og den enkelte privatperson er store. Samtidig er digitalisering og automatisering et tveegget sverd. På den ene siden er det en helt nødvendig samfunnsutvikling for å optimalisere ressursbruk og skape konkurransedyktighet og forsvarsevne i et globalt perspektiv. På den andre siden kan utviklingen føre med seg sårbarheter som vi ikke ønsker, dersom vi ikke er bevisste på hvordan vi som privatpersoner, virksomheter og nasjon skal sikre oss mot å havne i situasjoner der vi lar det være opp til andre land eller private multinasjonale selskaper å ha full kontroll over den teknologien som vi har blitt helt avhengig av.

### Åpenhetens dilemma

Daglig omgir vi oss med produkter som har sensorer som samler informasjon om oss og våre bevegelser. Antallet sensorer øker raskt. Denne informasjonen har bred kommersiell anvendelse, og nye tjenester basert på blant annet stordataanalyse og datasyn (computer vision) er i utvikling. Eksempler på sensorer er mobiltelefoner, smartklokker, strømmålere, elektroniske dørlåser og alarmsystemer, satellitt- og flybilder, action-kameraer, droner, overvåknings- og trafikkameraer og nye avanserte kjøretøy. Felles for disse sensorene og teknologiene er at de gjør hverdagen vår enklere. De bidrar til effektivisering av tid og ressurser. Samtidig kan de ha konsekvenser vi ikke er bevisst, noe som gjør det vanskelig å identifisere tiltak og medfører at sikkerhetsarbeidet blir hengende etter.

Åpen informasjon er informasjon som ved lovlig fremgangsmåte er tilgjengelig for alle som ønsker å finne den. Verdien av enkeltbiter av åpen informasjon trenger ikke isolert sett å være stor. Aggregert kan imidlertid informasjonen være av en slik kvalitet eller verdi at den burde vært sikkerhetsgradert. En av årsakene til at verdien av informasjonen

Utstrakt bruk av teknologi har skapt et overvåkingssamfunn som vi ikke forstår omfanget av.

øker, er at kapasiteten for automatisert dataanalyse øker eksponentielt og prosesser automatiseres. Dette muliggjør sammenstilling og nye former for analyse av det enorme volumet av åpen informasjon.

Mengden åpen informasjon og muligheten til å sammenstille informasjon digitalt innebærer en betydelig risiko for at trusselaktører får innsikt i forhold vi ønsker å skjerme eller burde skjerme. Slik sett er trusselaktørenes kostnad og risiko knyttet til innhenting betydelig redusert i forhold til for 10–20 år siden.

## Mangelfulle risikovurderinger

Ved NSMs tilsyn hadde en stor andel mangler knyttet til gjennomføringen av skade- eller risikovurderinger. Risikovurdering var ofte ikke foretatt for alle relevante områder, og vurderingene ble ikke vedlikeholdt over tid. Konsekvensene av dette kan bli å implementere tiltak på feil grunnlag og dermed med potensielt manglende effekt. NSM erfarer at tiltak ofte rettes mot fysiske forhold i stedet for digitale eller menneskelige.

Mangelfull kunnskap om risikovurdering gjør dermed at virksomhetene ikke blir i stand til avgjøre hva som utgjør et forsvarlig sikkerhetsnivå for egne skjermingsverdige verdier og deres betydning for grunnleggende nasjonale funksjoner. **NSM anbefaler derfor at virksomheter gjør jevnlige og grundige risikovurderinger.**

Åpen informasjon misbrukes til blant annet å planlegge uønsket aktivitet og kriminalitet mot enkeltpersoner og virksomheter. Den kan også benyttes for å planlegge og gjennomføre sikkerhetstruende virksomhet mot Norge og norske interesser, jf. side 16 og 19. **Virksomheter og myndigheter må veie risikoen åpen informasjon representerer opp mot fordelene det gir. Myndighetene må vurdere hvilken informasjon som bør skjermes for å unngå tilgang for trusselaktører, samt hvordan denne informasjonen kan gjøres lett tilgjengelig for virksomheter med legitime behov.**

**Din nettaktivitet påvirker virksomhetens risiko**

Har du oversikt over hvilke apper på telefonen din som samler inn informasjon om dine bevegelser? Hvor bevisst er du på hva du deler av personlig informasjon i sosiale medier? Har du telefon, nettbrett eller PC gjennom jobben som også kobles til privat nettverk hjemme eller på flyet, toget eller et hotell i utlandet?

I vårt gjennomdigitaliserte samfunn deler vi bevisst og ubevisst informasjon til enhver tid om våre bevegelser, handlinger, synspunkter og følelser. Dette kan innebære at vi lar aktører med ulike hensikter se oss i kortene – både i form av kommersielle selskaper som selger data om oss i markedsføringsøyemed og fremmede stater som samler informasjon til andre formål. Utstrakt bruk av teknologi har således skapt et overvåkingssamfunn

som vi ikke forstår omfanget av.

Når data om hvor mobilen er, hvem vi ringer til, hva vi surfer på og hva vi kjøper blir koblet sammen, kan det ha sikkerhetsmessige konsekvenser. Informasjonen du deler om deg selv og virksomheten du jobber i, eller mobiltelefonen du bærer med deg overalt, kan brukes som inngangsportal for en trusselaktør. **Vær derfor bevisst på hvilken informasjon du deler, ikke minst gjennom sosiale medier og ulike digitale plattformer. Alle virksomheter bør gi de ansatte klare retningslinjer og anbefalinger om hvordan de bør oppføre seg i det digitale rom.**

**Digitale verdikjeder og «grenseløse» avhengigheter**

Digitalisering legger til rette for verdiskapning og er et gode for samfunnet. Fordi systemene integreres med hverandre, kan imidlertid en hendelse som oppstår i ett system forplante seg på tvers av systemer og samfunnssektorer og slik utløse en uforutsett og negativ dominoeffekt.

Digitale verdikjeder etableres primært ut fra hva som er kostnadseffektivt for virksomhetene, og hvor det finnes markedsmuligheter. Verdikjeder vil i de fleste tilfeller strekke seg utover landets grenser. Utviklingen i digitale tjenestetilbud skjer raskt, noe som gjør verdikjedene svært dynamiske.

Kompleksiteten gjør det utfordrende å få oversikt over de totale sårbarhetene.

### «The Wild West» – lokasjonsdata som Big Business[34]

I desember hadde New York Times en sak om lokasjonsdataindustrien hvor de interaktivt viste lokasjonen til 12 millioner amerikanere – på børsen i New York, i velstående nabolag langs stranda i Los Angeles, i sikre bygninger som Pentagon, i Det hvite hus og på president Trumps Mar-a-Lago i Palm Beach. Ved hjelp av datasettet The Times Privacy Project fikk tak i, kombinert med offentlig tilgjengelig informasjon, kunne de finne lokasjonen og følge bevegelsen til enkeltpersoner.[35]

I USA sendes presis lokasjon fra mobiltelefoner til selskaper som samler slike data og gjør dem om til «Big Data».[36] Dette skjer ved at apper på mobiltelefonene bruker programvare som samler lokasjonsdata som selges videre til andre selskaper. Disse bruker dataene blant annet til analyser, målrettede markedsføringsformål og i programvare som brukes ved utvikling av nye apper (Software Development Kit, SDK). Det kan være nesten umulig å vite hvilke selskaper som mottar din lokasjonsinformasjon eller hva de bruker den til. Samling av lokasjonsdata er i varierende grad regulert internasjonalt. Denne type informasjon har høy kommersiell verdi og samtidig stor etterretningsmessig verdi.

For å redusere risikoen ved tjeneste-utsetting må virksomhetene sørge for ikke å bli låst til én leverandør.

## Huskeliste på vei ut i skyen

Virksomhetene må sørge for at nødvendige ressurser og applikasjoner ikke blir låst til spesifikke produkter, leverandører eller skyer, men til enhver tid er tilgjengelige ved at de fleksibelt kan flyttes mellom ulike tjenestetilbydere.

a. **Migrer til cloud native-paradigmet.** Cloud native-plattformer og -applikasjoner er mer åpne og interoperable enn tradisjonelle plattformer og applikasjoner. Selv om eksisterende applikasjoner kan straks-virtualiseres ved hjelp av relativt enkel lift-and-shift, er dette ikke en like god løsning sett på lengre sikt.

b. **Velg åpne produkter basert på åpne standarder.** Unngå leverandørlåsing, ikke velg leverandørspesifikke løsninger. Se for eksempel til Cloud Native Computing Foundation (CNCF).

c. **Ikke implementer løsningen på en proprietær måte.** Bevar produktenes interoperabilitet og evne til å flytte applikasjoner mellom ulike applikasjonsplattformer.

d. **Ikke bind løsningen til en spesifikk fysisk lokasjon.** Datasenter er en modell, ikke et sted. Ha nødvendig smidighet til å kunne flytte løsningen mellom ulike fysiske datasentre og kanskje til og med til ulike offentlige skyer – alltid i henhold til behov gitt i systemets sikkerhetskonsept.

Virksomhetene vil arve sårbarhetene til virksomheter som ligger tidligere i verdikjeden. En trusselaktør kan derfor utnytte virksomheter og produkter ett sted i verdikjeden for å få tilgang til informasjon og funksjonalitet andre steder i verdikjeden. Samfunnsviktige funksjoner kan bli rammet ved at sårbarheter utenfor nasjonal kontroll blir utnyttet.

Ved bruk av tjenester i utlandet eller lagring av informasjon i andre land vil det være avgjørende at vi kan ha tillit til at dataene beskyttes, at det er stabile og trygge forhold i landet data lagres i så vel som i transittland, og at forbindelsene er oppe slik at tjenester og data er tilgjengelig når vi trenger dem. I tilfelle krise og krig må vi forvente at dette kan falle bort.

**Alle virksomheter som skal ta beslutninger om eventuell tjeneste-utsetting eller bruk av skytjenester må gjennomføre risikovurderinger. Risikovurderingene må ta hensyn til risiko og sårbarheter knyttet til verdikjeder virksomheten er en del av.**

### Skytjenester og tjenesteutsetting

Virksomhetene benytter tjenesteutsetting, inkludert skytjenester, som ett av virkemidlene for å holde følge med teknologiutviklingen og digitaliseringen. De aller fleste av skytjenestetilbyderne har ikke installasjoner på norsk jord og må derfor tilby sine tjenester fra utlandet. Dette innebærer en betydelig risiko.

Tjenesteutsetting og bruk av

skytjenester kan imidlertid bidra til bedre sikkerhet som følge av at IKT-driften skjer i store, profesjonelle miljøer. Mange av utfordringene NSM ser knyttet til dårlig IKT-sikkerhet, skyldes små driftsmiljøer og mangel på kompetanse og ressurser. På denne bakgrunn anbefaler NSM at det etableres færre og større IKT-miljøer. Da kan tjenesteutsetting være én løsning.

Tjenesteutsetting innebærer imidlertid også utfordringer som virksomhetene må ta hensyn til. De viktigste utfordringene er at informasjon og funksjonalitet er basert på infrastruktur på fysiske lokasjoner langt unna, ofte i andre land (som beskrevet i kapittelet over); eierskapsstrukturer og uautorisert tilgang til informasjon kan være vanskelig å kontrollere; ved avtaleinngåelse benyttes standardkontrakter der tjenesteleverandørens premisser er styrende; virksomheten står i fare for å bli låst til én leverandør som følge av praktiske utfordringer ved å flytte informasjon og funksjonalitet til andre leverandører; det krever at virksomheten etablerer god bestillerkompetanse. **Virksomheter som vurderer tjenesteutsetting, bør følge anbefalingene NSM gir i temaheftet *Sikkerhetsfaglige anbefalinger ved tjenesteutsetting*.** [37]

**NSMs temarapport *Anbefaling om landvurdering ved tjenesteutsetting* bør benyttes av virksomheter som vurderer leverandører av digitale tjenester fra andre land.**

**For å redusere risikoen ved tjenesteutsetting må virksomhetene sørge for ikke å bli låst til én leverandør. Virksomheten må unngå å bli låst til spesifikke produkter, leverandører eller skyer. NSM har utarbeidet en rekke IKT-tekniske sikkerhetsråd som virksomheter som har eller skal etablere skjermingsverdige informasjonssystemer bør følge.**

**NSM anbefaler at myndighetene stimulerer til etablering av skytjenester basert på infrastruktur i Norge. I tiden fremover vil det være viktig å etablere skytjenester med et forsvarlig sikkerhetsnivå for virksomheter som understøtter grunnleggende nasjonale funksjoner. Myndighetene må se på muligheter for sterkere nasjonal regulering av skytjenester og liknende tjenesteutsetting. Myndighetene må arbeide for bedre internasjonal regulering av slike tjenester.**

**Redundansutfordringer**

Redundans innebærer at man har flere tilgjengelige systemer som utfører samme type oppgave, slik at funksjonen ivaretas i tilfelle et eller flere av de parallelle systemene skulle falle bort. Selv med flere alternativer er det imidlertid ikke gitt at vi har effektiv redundans. De ulike systemene kan være avhengige av en felles ressurs eller funksjon slik at bortfall av denne rammer alle de parallelle systemene. **Både virksomheter og myndigheter bør kartlegge verdikjedene de er avhengige av og vurdere hvilke sårbarheter som eksisterer der.**

Ved at flere produkter blir «smarte» og knyttet til internett, vil også sårbarheter og angrepsflater øke.

### Systemisk sårbarhet i eldre versjoner av Windows

Fra og med 14. januar 2020 har Microsoft avsluttet kundestøtte for Windows 7, Windows Server 2008 og Windows Server 2008 R2 og lager derfor ikke lenger programvareoppdateringer. Et operativsystem som ikke oppdateres, kan lettere utnyttes dersom det finnes eller utvikles sikkerhetshull eller nulldagers-sårbarheter.

Det anbefales fra Microsofts side å bytte operativsystem for å ivareta sikkerheten i PCen.

**Virksomheter underlagt sikkerhetsloven er pålagt å kartlegge slike avhengigheter. For viktige samfunnsfunksjoner og styringssystemer må det være reserve-løsninger. Manuelle rutiner bør være forberedt.**

**«Smarte byer» og tingenes internett**

Begrepet «smarte byer» brukes om urbane områder hvor data fra sensorer i IoT-enheter sammenstilles og analyseres for å effektivisere og forbedre ressurser og tjenester. Ved å utnytte store datamengder fra nettilkoblede sensorer vil man bedre kunne styre trafikkavvikling, kraftforsyning, vann- og avløpsfunksjoner, avfallshåndtering, helsetjenester og andre funksjoner i samfunnet. Slike prosesser kan også benyttes for å effektivisere nød- og beredskapsfunksjoner og bekjempelse av kriminalitet. Digitalisering og utvikling av «smarte byer» er ment å gjøre fremtidens byer mer bærekraftige, effektive og trygge. Ulike tjenesteområder, teknologier og datakilder vil integreres, slik at data kan deles av offentlige organer, private bedrifter, FoU-aktører og organisasjoner i sivilsamfunnet. Slik integrasjon vil foregå raskere, i større omfang og mye mer effektivt enn i dag.

Dataene som samles inn gjennom «smart by»-løsninger, vil kunne få stor kommersiell verdi og vil kunne brukes for å skape et bredt spekter av nye tjenester. Vi som individer vil imidlertid i liten grad kunne begrense hvilke data som samles inn om oss og hvilke «smarte» enheter som kan brukes som kilder. I et sikkerhetsperspektiv vil det være risiko for at store mengder informasjon blir tilgjengelig for trusselaktører. Det er også risiko for at trusselaktører etablerer kapasitet til å påvirke samfunnsfunksjoner gjennom «smart by»-løsninger. Tjenester vi etter hvert blir avhengige av, vil kunne manipuleres eller falle bort.

Mange «smarte» enheter for forbruker-markedet, inkludert IoT-enheter, har liten eller ingen sikkerhet og vil være sårbare for misbruk. Mange enheter vil samle og dele informasjon om innbyggere og være avhengig av kommunikasjon med skytjenester og eventuelt leverandøren for å fungere som forutsatt. Det meste av teknologien i «smarte byer» utvikles i utlandet, og det er risiko for at enkelte

# Erfaringer fra inntrengingstesting

- **E-post fungerer fortsatt som angrepsvektor.** NSMs erfaring er at tilstrekkelig mange fortsatt lar seg lure til å åpne vedlegg eller klikke på lenker og slik kjøre skadevare som virus, ormer, trojaner eller lignende.

- **Virksomhetene sliter med å holde IKT-infrastrukturen oppdatert.** NSM utnytter kjente sårbarheter i applikasjoner og operativsystemer i sine inntrengingstester. I halvparten av testene sist år fant NSM enkeltkomponenter i virksomhetens infrastruktur som ikke lar seg oppdatere fordi supporten på produktet for lengst har opphørt. Mangelfull sikkerhetsoppdatering er en gjenganger.

- **Passord utgjør fortsatt en betydelig sårbarhet.**
  - Virksomhetene glemmer ofte å bytte standardpassord på produkter.
  - Passordene er for enkle og forutsigbare, noe som muliggjør passordgjetting.
  - Passord gjenbrukes mellom personlige administrative konti og sluttbrukerkonti, mellom ulike tjenester og mellom forskjellige systemer, både interne og eksterne. Ett passord kan dermed gi tilgang til flere systemer.

- **Virksomheter benytter adgangskort basert på sårbar teknologi.** NSM ser fortsatt utstrakt bruk av kort som er forholdsvis enkel å kopiere. Test-teamet produserer egne kort og verifiserer at disse kan benyttes til å ta seg inn i virksomhetens lokaler.

- **Sosial manipulasjon og tailgating fungerer.** Det er bare et spørsmål om tid.

- **Sensorer plassert utenfor kontrollert område kan benyttes som veien inn i virksomhetens infrastruktur.** Test-teamet har fått tilgang til sensitive data på det interne nettet via tilgang fra adgangskontrollsystem og sensorer utendørs.

Når sikkerhetstiltak implementeres utelukkende på bakgrunn av erfaring, kjører man baklengs inn i fremtiden.

### Varsling av uønskede hendelser

Varsler om uønskede hendelser er viktig for å sikre et oppdatert situasjonsbilde og raskt identifisere eventuelle tiltak på overordnet nivå. Varslene er også viktige for å avdekke liknende sårbarheter i andre virksomheter.

Virksomheter plikter å varsle NSM og andre tilsynsmyndigheter, jf. sikkerhetsloven § 4-5, dersom:

a) Den har blitt rammet av sikkerhetstruende virksomhet
b) Det er begrunnet mistanke om at sikkerhetstruende virksomhet har rammet eller vil kunne ramme virksomheten eller andre virksomheter.
c) Det har skjedd alvorlige brudd på krav til sikkerhet etter sikkerhetslovens bestemmelser om informasjonssikkerhet, informasjonssystemsikkerhet og objekt- og infrastruktursikkerhet.

Ved datainnbrudd kan også Nasjonalt cybersikkerhetssenter varsles. Du finner nettsiden for både varsling av uønskede hendelser og datainnbrudd på **https://www.nsm.stat.no/om-nsm/varsling/.**

utenlandske teknologiselskaper vil kunne få svært dominerende posisjoner regionalt eller nasjonalt. Tilsvarende problemstillinger er knyttet til skytjenester. Økt kompleksitet og antall sammenkoblinger, ukjente avhengigheter, begrensinger i kompetanse og evne til effektiv hendelseshåndtering vil kunne gi store utfordringer for sikkerhet i «smarte byer».

En annen sikkerhetsutfordring er mulighetsrommet for økt digital kriminalitet. Ved at flere produkter blir «smarte» og knyttet til internett, vil også sårbarheter og angrepsflater øke. Når vi blir mer avhengige av «smarte» enheter og flere produkter kan misbrukes, øker også incentivene for kriminelle til å utnytte sårbarhetene ved bruk av for eksempel bruk av løsepengevirus.

5G-teknologien legger til rette for økt bruk av IoT og overføring av store datamengder i IoT-økosystemer. Dette er en viktig forutsetning for videre utvikling av «smart by»-prosjekter.

**Myndighetene bør kartlegge alle påbegynte og planlagte «smart by»-prosjekter, og det må stilles krav om risikovurdering når «smart by»-prosjekter etableres for å ivareta sikkerheten i kritiske funksjoner og verdier for samfunnet.**

**Myndighetene må følge med på hvilke data som samles inn, hvordan disse lagres og sammenstilles samt hvem som har tilgang til dataene for å ivareta personvern og nasjonal sikkerhet.**

**Myndighetene bør sette krav til sikker-**

**het i produkter og datakilder som benyttes i offentlige «smart by»-prosjekter.**

**Myndighetene må vurdere om det skal innføres sertifisering eller merkeordninger for sikkerhet i IoT-produkter slik at forbrukerne får hjelp til å velge trygge produkter.**

**Sikkerhetshull kan avdekkes**

En del av NSMs arbeid med forebyggende sikkerhet er å teste sikkerhetsfunksjonalitet og -tiltak. Dette gjøres blant annet ved inntrengingstesting av objekter og informasjonssystemer av nasjonal viktighet. Formålet er å teste om sikkerhetstiltakene en virksomhet har implementert er effektive, for eksempel fysiske barrierer rundt og i objektet, adgangskontroll, sensorer, tilgangsstyring av virksomhetens IKT-infrastruktur og sikring av tjenester publisert på internett. **Virksomheter underlagt sikkerhetsloven kan anmode NSM om inntrengingstesting av digitale og fysiske sikkerhetstiltak.** For øvrige virksomheter tar NSM sikte på å etablere en kvalitetsordning for tilbydere av inntrengingstester.

Innhenting av informasjon fra åpne kilder, om virksomheten, objektet eller informasjonssystemet virksomheten ivaretar, inngår som en del av forberedelsene til inntrengingstester. Når test-teamet får et fotfeste i virksomhetens infrastruktur, fortsetter informasjonsinnhentingen. NSMs erfaring tilsier at virksomhetene skjermer systemteknisk informasjon for dårlig, og at det er for lite forståelse for hvorfor denne typen informasjon bør begrenses til personell med tjenstlig behov.

**NSM anbefaler virksomhetene å være varsomme med å eksponere informasjon som kan utnyttes av trusselaktører til å forberede og utvikle et angrep.** Dette kan for eksempel være:

- Informasjon om virksomheten, ansatte, funksjoner og brukerroller som kan utnyttes til å målrette angrep
- Informasjon om hvilke produkter og versjoner som benyttes, hvordan produktene brukes og hvilke sikkerhetstiltak som er iverksatt, gjør det mulig å studere produktenes sårbarheter og slik kunne finne den mest hensiktsmessige måten å utnytte disse på i forkant
- Informasjon om hvilke produsenter, leverandører og distribusjonsnettverk virksomheten benytter, kan utnyttes til å kompromittere produkter før de når frem

### Forsvarlig sikkerhetsnivå

Sikkerhetsloven gir fleksibilitet i hvordan virksomheter kan oppnå et forsvarlig sikkerhetsnivå. NSM forventer at virksomhetene innfører kombinasjoner av tiltak i de ulike sikkerhetsdisiplinene (menneskelige, elektroniske, fysiske og organisatoriske) for å oppnå en helhetlig og balansert sikring.

Økt fleksibilitet innebærer at det stilles høyere krav til sikkerhetsfaglig kompetanse i virksomhetene.

### Informasjon og kompetanse i forebyggende sikkerhetsarbeid

Når sikkerhetstiltak implementeres utelukkende på bakgrunn av erfaring, kjører man baklengs inn i fremtiden. Da vil vi alltid ha et etterslep på iverksetting av nødvendige tiltak. Utvikling av sikkerhetsmekanismer basert på hendelser og erfaring er nødvendig for å tette kjente sårbarheter, men er ikke tilstrekkelig for å tette alle sikkerhetshull. Mange sårbarheter ved eksisterende produkter er ennå ikke oppdaget, men vil like fullt kunne utnyttes dersom trusselaktører avdekker dem. Trusselaktører utnytter de svakhetene de finner, uavhengig av om de er menneskelige, organisatoriske, digitale eller fysiske. Noen mål anser de som verdt å vente lenge på å nå, andre utnyttes der det tilfeldigvis oppstår en mulighet.

Det er behov for tett samarbeid mellom myndigheter og virksomheter for å øke kompetansen om forebyggende sikkerhet. Ulike myndigheter legger til rette med råd, veiledninger og kurs. Det er også behov for at sikkerhetsfaglig kompetanse kommer tydeligere frem i høyere utdanning. I denne forbindelse lanserte regjeringen i 2019 en strategi for digital sikkerhetskompetanse. [38]

NSM har flere tiltak for å bistå virksomheter som ønsker å forbedre sitt sikkerhetsarbeid. Vi tilbyr tjenester som inntrengingstesting av sikkerhetstiltak, scanning av sårbarheter mot internett ved hjelp av Allvis NOR og kontinuerlig monitorering og varsling av kjente digitale sårbarheter gjennom vårt varslingssystem for digital infrastruktur (VDI). I tillegg er NSM aktiv gjennom sosiale medier, podcast og foredrag. **NSM anbefaler alle virksomheter å søke informasjon på www.nsm.no. Der finnes det veiledere, håndbøker og mye annen informasjon, blant annet konkrete anbefalinger om hva som utgjør god passordsikkerhet.** Der finner man også informasjon om noen av kursene NSMs kurssenter tilbyr.

NSM har utarbeidet grunnprinsipper

### Sikkerhetsstyring

Det overordnede ansvaret for sikkerheten ligger hos ledelsen, gjennom at de setter mål og føringer for sikkerhetsarbeidet. God helhetlig forståelse av sikkerhetsstyring og integrasjon i virksomhetsstyringen er sentralt for å oppnå et forsvarlig sikkerhetsnivå. Dette har blitt enda viktigere i møte med stadig mer komplekse verdikjeder og et næringsliv preget av internasjonalisering. I og med at virksomhetene knyttes sammen gjennom stadig nye avhengigheter, kan sårbarheter i én virksomhet få konsekvenser for andre virksomheter. Mangelfull sikkerhetsstyring og ledelse fører til at de viktigste risikoene ikke blir identifisert, håndtert og redusert. Sikkerhetsstyring

- omfatter alle aktiviteter som er nødvendige for å opprettholde og beskytte virksomhetens verdier
- skal etablere og ivareta helhetlig og forsvarlig sikkerhetsnivå for virksomhetens verdier
- må være en integrert del av virksomhetens styring

som beskriver de sentrale grepene virksomhetene bør ta for å bedre forebyggende sikkerhet. Flere av disse er tilgjengelige på NSMs nettside:

- Grunnprinsipper for IKT-sikkerhet
- Grunnprinsipper for personellsikkerhet
- Grunnprinsipper for fysisk sikring (blir tilgjengelig på NSMs hjemmesider ila. 2020)
- Grunnprinsipper for sikkerhetsstyring er også under utarbeidelse

NSM erfarer at mange virksomheter har mye kompetanse innen sikkerhet, men at denne ikke alltid er satt tilstrekkelig i et system. Dette gjelder spesielt virksomheter som ikke har forebyggende sikkerhet som en del av sin kjernevirksomhet.

Ny sikkerhetslov stiller imidlertid større krav til kompetanse. Denne bør derfor vedlikeholdes og videreutvikles av den enkelte virksomhet og settes inn i et helhetlig system. Dette krever at virksomheten innfører en kombinasjon av tekniske, organisatoriske og menneskelige tiltak for å oppnå forsvarlig sikkerhetsnivå.

God forebyggende sikkerhet fordrer at vi vet hvilke verdier som må beskyttes, enten av hensyn til egen virksomhet, andre virksomheter eller av nasjonale hensyn. Det kan være utfordrende for den enkelte virksomhet å kjenne til hvilke verdier som kan være interessante for en trusselaktør. Trusselinformasjonen som Etterretningstjenesten og PST hvert år deler i sine ugraderte rapporter, kan da være til stor hjelp.[39] Sikkerhetsarbeidet krever også at virksomhetene avdekker egne sårbarheter, og at de basert på en helhetlig risikovurdering iverksetter tiltak for å lukke disse sårbarhetene.

God forebyggende sikkerhet forutsetter derfor at virksomhetene tar i bruk regelverk, råd og veiledning om hvordan informasjon, informasjonssystemer, objekter og infrastruktur kan sikres, samt hvordan personellsikkerheten kan ivaretas.

### Sikkerhetsbevisste ledere

NSM har over flere år observert en klar sammenheng mellom sikkerhetsengasjerte ledere og sikkerhetstilstanden i virksomheten. Der ledelsen er fraværende i sikkerhetsspørsmål, blir avstanden til sikkerhetsarbeidet fort stor, og det blir vanskeligere å få besluttet, gjennomført og evaluert relevante tiltak. NSM erfarer at de mest alvorlige avvikene ved tilsyn gjerne forekommer i virksomheter hvor sikkerhet er noe litt «annerledes», noe som behandles i et eget fagområde og av en adskilt gruppe mennesker.

# Fotnoter

[1] I «Operasjon Muskedunder» i september 1942 ble Glomfjord kraftverk sabotert slik at kraftverket ble satt ut av spill i tre måneder, og den tyske okkupasjonsmakten gav opp utbyggingen av aluminiumsverket i Glomfjord. https://www.nrk.no/nordland/_-utforte-vellykket-sabotasjeaksjon_men-led-grusom-skjebne-1.12154577

[2] FFI-rapport 2001/02381 *En sårbar kraftforsyning – Sluttrapport etter BAS3* skriver at i fredstid er kraftforsyningen lite utsatt, i krise øker faren for aksjoner mot kraftforsyningen, og i krig er kraftforsyningen et klart utsatt mål.

[3] En distribuert sky innebærer en videreutvikling av den skybaserte infrastrukturen for å kunne tilby 5G-baserte tjenester nærmere kunden (såkalt *edge computing*).

[4] Nasjonal kommunikasjonsmyndighet (Nkom) (2019), *Risikovurdering av ekomsektoren, Den digitale grunnmuren*, hentet fra: https://www.nkom.no/aktuelt/nyheter/_attachment/42430?_ts=16b4a976ad8

[5] Norsk Romsenter https://www.romsenter.no/Fagomraader/Satellittnavigasjon/Satellittnavigasjon-og-bruk2

[6] https://sykepleien.no/2016/09/droner-i-sok-og-redningsarbeid-i-norge

[7] European Geostationary Navigation Overlay Service (EGNOS) er systemet som tilbyr den type tjenester i Europa og hele fastlands-Norge.

[8] Global Navigation Satellite System

[9] Financial Times, UKs Galileo rival delayed amid wrangling and rising costs. https://www.ft.com/content/e513f200-597e-11ea-a528-dd0f971febbc

[10] Trusselbeskrivelsen er i hovedsak basert på PSTs «Nasjonal trusselvurdering 2020», Etterretningstjenestens «Fokus 2020» samt NSMs egne data.

[11] Nettverksoperasjoner er en samlebetegnelse på digital sabotasje, digitale innbrudd, digital etterretning og forberedelse til slik aktivitet.

[12] Internet of Things (IoT), tingenes nternett, består av et nettverk av enheter utstyrt med elektronikk og programvare som fører til at enhetene kan kommunisere seg imellom og i nettverk.

[13] https://www.forbes.com/sites/zakdoffman/2020/02/05/fbi-drive-by-hacking-warning-just-got-real-heres-how-this-malicious-new-threat-works/#24228b635017

[14] Tekniske sikkerhetsundersøkelser er hjemlet i sikkerhetsloven §§ 5-5, 6-5 og 7-4.

[15] https://www.nupi.no/nupi_school/HHD-Artikler/2019/Kan-demokratier-hackes

[16] Sikkerhetstruende virksomhet er i sikkerhetsloven definert som tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser. Det omfatter blant annet spionasje, sabotasje og terror, i tillegg til handlinger som for eksempel har som mål å undergrave eller påvirke norske myndigheters styringsevne.

[17] https://www.justice.gov/opa/pr/former-intelligence-officer-convicted-attempted-espionage-sentenced-10-years-federal-prison

[18] https://www.washingtontimes.com/news/2019/sep/24/ex-intelligence-officer-sentenced-in-espionage-cas/

[19] Cole, Eric and Sandra Ring (2005), Insider Threat: Protecting the Enterprise from Sabotage, Spying and Theft, Syngress Publishing Inc., Rockland, MA, USA.

[20] Nasjonal sikkerhetsmyndighet (2019), *Temarapport. Innsiderisiko.*

[21] Se brosjyren *«Sikkerhet ved ansettelsesforhold – før, under og ved avvikling»*, utgitt av PST, NSM, Politiet og Næringlivets Sikkerhetsråd.

[22] https://www.nsm.stat.no/globalassets/rapporter/temarapport-losepengevirus-200218.pdf

[23] https://www.nsm.stat.no/blogg/beskyttelse-mot-losepengevirus/

[24] Andersen, M. S., & Sverdrup, U. (2020). Holdninger til utenlandske investeringer fra Kina i de nordiske land. Internasjonal Politikk, 78(1), 106-116. https://doi.org/10.23865/intpol.v78.2086

[25] Etterretningstjenesten, *Fokus 2019*

[26] Politiets sikkerhetstjeneste, *Trusselvurdering 2019*

[27] Etterretningstjenesten, *Fokus 2020*

[28] Jf. sikkerhetsloven § 10-3.

[29] Jf. sikkerhetsloven § 2-5 *Vedtak ved risiko for skadevirkninger for nasjonale sikkerhetsinteresser*.

[30] Se også NSMs Helhetlig digitalt risikobilde, https://www.nsm.stat.no/globalassets/rapporter/2019--nsm-helhetlig-digitalt-risikobilde.pdf

[31] Næringslivets sikkerhetsråd (NSR), Kriminalitets- og sikkerhetsundersøkelsen i Norge 2019.

[32] Lov om informasjon om bestemt angitte områder, skjermingsverdige objekt og bunnforhold (LOV-2017-06-21-88)

[33] Forskrift om kontroll med informasjon innhentet med luftbårne sensorsystemer (FOR-2018-06-22-951)

[34] New York Times (2019), The Privacy Project. Twelve Million Phones, One Dataset, Zero Privacy https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html?action=click&module=Opinon&pgtype=Homepage

[35] New York Times (2019), *The Privacy Project. How to track President Trump*. https://www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html

[36] New York Times (2019), *The Privacy Project. Smartphones Are Spies. Here's Whom They Report To*. https://www.nytimes.com/interactive/2019/12/20/opinion/location-tracking-smartphone-marketing.html

[37] Sikkerhetsfaglige anbefalinger ved tjenesteutsetting, https://www.nsm.stat.no/globalassets/dokumenter/temahefter/tjenesteutsetting2018v1.1_web.pdf

[38] https://www.regjeringen.no/contentassets/8ed748d37e504a469874ce936551b4f8/nasjonal-strategi-for-digital-sikkerhetskompetanse.pdf

[39] Næringslivets Sikkerhetsråds *KRISINO 2019* viser at kun 17 prosent av de 2500 virksomhetene som var med i spørreundersøkelsen hadde lest PSTs trusselvurdering, og kun 10 prosent hadde lest NSMs risikorapport.

**NASJONAL SIKKERHETSMYNDIGHET**

Postboks 814, 1306 Sandvika

Tlf. 67 86 40 00
post@nsm.stat.no
www.nsm.stat.no