FFI-RAPPORT

21/01132

Samfunnsutvikling frem mot 2030

— utfordringer for politiet, PST og påtalemyndigheten

Stig Rune Sellevåg
Arild Bergh
Janita Andreassen Bruvoll
Steinar Høibråten
Hedda Lærum Jacobsen
Martin Strand
Bjørn Barland[1]

[1]Politihøgskolen (PHS)

Samfunnsutvikling frem mot 2030
– utfordringer for politiet, PST og påtalemyndigheten

Stig Rune Sellevåg
Arild Bergh
Janita Andreassen Bruvoll
Steinar Høibråten
Hedda Lærum Jacobsen
Martin Strand
Bjørn Barland[1]

Forsvarets forskningsinstitutt (FFI)
[1] Politihøgskolen (PHS)

20. mai 2021

Emneord
Trusler
Nasjonal sikkerhet
Samfunnssikkerhet
Politi
Trendanalyser

FFI-rapport
21/01132

Prosjektnummer
5605

Elektronisk ISBN
978-82-464-3350-9

Engelsk tittel
Trends Shaping the Norwegian Society towards 2030 – Challenges for the Police, the Police Security Service and the Prosecuting Authority

Godkjennere
Janet Martha Blatny, *forskningsdirektør*

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Sammendrag

Denne rapportens formål har vært å beskrive hva samfunnsutviklingen kan bety for det fremtidige utfordringsbildet som politiet, Politiets sikkerhetstjeneste (PST) og påtalemyndigheten kan møte frem mot 2030. Det fremtidige utfordringsbildet har blitt analysert basert på dokumentstudier av forventede utviklingstrekk innen politiske, sosiale, økonomiske, miljø- og klimamessige og teknologiske forhold, samt ekspertvurderinger av hva utviklingstrekkene kan bety for politi- og påtaletjenestene med et særskilt fokus på beredskap og nasjonal sikkerhet.

Det fremtidige utfordringsbildet for politi- og påtaletjenestene fremstår som sammensatt, grenseoverskridende og sektorovergripende. Studien har identifisert fire viktige endringsdrivere som påvirker det fremtidige utfordringsbildet. Den første er relatert til fremtidig konfliktutvikling; ikke minst stormaktsrivaliseringen mellom USA, Kina og Russland og hva disse landene velger å gjøre fremover, noe som henger sammen med innenrikspolitiske utvikling og utfallet av fremtidige maktskifter. Den andre er relatert til endringer i sosiale og økonomiske forhold, hvor langtidskonsekvenser av covid-19-pandemien er en kilde til usikkerhet både nasjonalt og internasjonalt. Den tredje er relatert til teknologisk utvikling, særlig fremvoksende og disruptive teknologier, fordi teknologi er en viktig faktor for nesten alle kriminalitetsutfordringer og trusler mot nasjonal sikkerhet som politi- og påtaletjenestene står overfor. Samtidig kan teknologiutviklingen gi samfunnet store muligheter og økonomisk vekst. Den siste endringsdriveren er relatert til samfunnsendringer som følge av klimatiltak og tilpasninger til klimaendringer.

De fire endringsdriverne – fremtidig konfliktutvikling, teknologiutvikling, klimatiltak og endringer i sosiale og økonomiske forhold – er samtidig forbundet med betydelig usikkerhet. Spesielt gjelder dette fremvoksende og disruptive teknologiers potensial for trendbrudd. Dette vil påvirke hvordan politi- og påtaletjenestene må møte de fremtidige utfordringene. Skal befolkningens tillit til de tre tjenestene opprettholdes, er det avgjørende at politi- og påtaletjenestene klarer å møte de fremtidige utfordringene. Hvis ikke, kan det gi grobunn for mer kriminalitet, terrorisme eller fremmedstatlig påvirkningsaktivitet.

Med press på offentlige finanser vil politi- og påtaletjenestene måtte prioritere sin innsats mellom ulike utfordringskategorier. I spørsmål som omhandler beredskap og nasjonal sikkerhet, bør følgende temaer vies særskilt oppmerksomhet: (*i*) Skillet mellom statssikkerhet og samfunnssikkerhet blir mer utydelig, (*ii*) teknologiutviklingens muligheter og utfordringer, (*iii*) kompleksitet som en samfunnsutfordring, samt (*iv*) konspirasjonsteorier som et demokratisk problem.

Politiets hovedstrategi er og må være forebygging. Skal politi- og påtaletjenestene lykkes med sitt forebyggende arbeid, vil det kreve enighet om hva som ønskes oppnådd, aksept for at prioriteringer gjøres og tydeliggjøring av den enkelte etat sitt ansvar. I tillegg krever det evne til samarbeid på tvers av sektorer, effektive politiverktøy og et hjemmelsgrunnlag som er tilpasset utfordringene som tjenestene står overfor. Slik kan politi- og påtaletjenestene også i fremtiden være døråpner og portvakt, og instansen som bekrefter og sikrer borgernes rettssikkerhet.

Summary

The Norwegian Defence Research Establishment (FFI) has been commissioned by the Norwegian Ministry of Defence to analyse threats to national security towards 2030, to support long-term planning for the Police, the Police Security Service and the Prosecuting Authority. The threats have been analysed on the basis of a literature review of expected developments within security policy, demography, economy, climate and technology, along with expert assessments of the implications for the police and prosecuting services with a special focus on preparedness and national security.

The future challenges for the police and prosecuting services are complex, transboundary and cross-sectoral. This work has identified four important drivers of change that have an impact on future threats. The first relates to future conflicts, in particular the great power rivalry between USA, China and Russia. The second relates to socio-economic changes both nationally and internationally, especially long-term consequences from the Covid-19 pandemic. The third relates to technological developments, in particular emerging and disruptive technologies. Technology is an important driver of change for almost all types of crimes and threats to national security. The last driver of change relates to societal changes because of mitigation and adaptation to climate change.

These four drivers of change are affected by substantial uncertainty. This is especially the case for technological developments because of emerging and disruptive technologies' potential for creating so-called technological discontinuities, *i.e.* unanticipated or surprising shifts in trends. The uncertainty related to the drivers of change will not only impact the future threats, but also how the police services should meet the challenges.

It is paramount that the police and prosecuting services are able to meet the future challenges in order to sustain trust in society. If this is not the case, our society could become more vulnerable to crimes, terrorism or foreign influence and interference.

With the foreseen strain on public finances, the police and prosecuting services will have to prioritise their efforts and resources. In questions related to national security and preparedness, the following topics require consideration: (*i*) the blurring of lines between state security and societal security due to hybrid threats, (*ii*) the opportunities and challenges posed by emerging and disruptive technologies, (*iii*) complexity as a challenge to our society, and (*iv*) conspiracy theories as a democratic problem.

For the future, the police services' main strategy should still be prevention. This will, however, require agreement on the objectives to be achieved, acceptance for prioritisations, and clarification of roles and responsibilities. In addition, multidisciplinary collaboration across sectors, effective tools for law enforcement and policing, and a fit-for-purpose legal basis without compromising human rights or the state's governing principles under the rule of law are needed.

Innhold

Forord

En stor takk rettes til en rekke fagpersoner i Justis- og beredskapsdepartementet (JD), Politiets sikkerhetstjeneste (PST), Politidirektoratet (POD), Kripos, Riksadvokaten, Politihøgskolen (PHS), Nasjonal sikkerhetsmyndighet (NSM) og Direktoratet for samfunnssikkerhet og beredskap (DSB). Uten deres verdifulle bidrag ville denne rapporten ikke vært mulig. FFI-forskerne Truls Tønnessen og Rune Lausund takkes for diskusjoner og faglige bidrag.

Kjeller, 20. mai 2021

På vegne av forfatterne,
Stig Rune Sellevåg

1 Innledning

Politiets samfunnsoppdrag er å forebygge og bekjempe kriminalitet og skape trygghet for befolkningen. Oppgavene er de samme i hele krisespekteret – i fred, krise og væpnet konflikt, hvor politiets beredskap består av den samlede tilgjengelige kapasiteten og kompetansen innen operativ innsats, etterforskning, etterretning, sivil rettspleie og påtale (Politidirektoratet, 2020, s. 16).

I politiets omverdensanalyse fra 2015 ble det pekt på en rekke faktorer som påvirker kriminalitetsutviklingen. I forordet til omverdensanalysen skrev daværende politidirektør følgende (Politidirektoratet, 2015):

> *Utfordringsbildet for norsk politi har kanskje aldri vært mer sammensatt og krevende. Samfunnet blir stadig mer komplekst. Det er kraftig økning i migrasjon til Norge. Det globale trusselbildet blir stadig mer sammensatt og uoversiktlig. Globaliseringen knytter verden tettere sammen, og for Norge og norske interesser kan utvikling og hendelser langt unna raskt kunne få alvorlige konsekvenser. Ekstremismen har blitt mer grenseoverskridende og tettere knyttet til internasjonale forhold og konflikter. Internett benyttes for å spre ekstreme synspunkter. En utvikling med mer grenseoverskridende kriminalitet stiller krav til politiets evne til å tilpasse seg et stadig endret trusselbilde, og øker også viktigheten av internasjonalt politisamarbeid.*

Dagens utfordringsbilde preges av en negativ utvikling i den sikkerhetspolitiske situasjonen for Norge. Stormaktsrivalisering mellom USA, Russland og Kina vil ikke bare ha sikkerhetspolitiske konsekvenser, men også konsekvenser for økonomiske og teknologiske forhold. Den globale maktforskyvningen gjør også at den liberale verdensordenen, det vil si en regelbasert verdensorden basert på sentrale verdier som markedsbasert økonomi og frihandel, individets rettigheter, pressefirhet, rettsikkerhet og demokrati, er under press. Utviklingen preges også av at virkemiddelbruken i konflikter har endret seg, hvor sammensatte trusler visker ut skillet mellom krig og fred.

Samtidig vedvarer terrortrusselen. Selv om terrorgruppen kjent som Den islamske staten (IS) mistet sitt territorium i Irak og Syria, fortsetter jihadisme som ideologi å inspirere terror- og opprørsbevegelser over store deler av verden. Det har også vært en forverret utvikling i høyreekstreme miljøer, både når det gjelder hatkriminalitet og trusselen om terrorangrep. Ikke minst preges utfordringsbildet av kriminalitetsutviklingen i det digitale rom, hvor politiets evne til å avdekke og oppklare slik kriminalitet har klare svakheter ifølge Riksrevisjonen (2021b). Riksrevisjonen (2021a) har nylig også kommet med kritikk av Politiets sikkerhetstjeneste (PST) sin prioritering av det forebyggende arbeidet med eksportkontroll, og viser til økt risiko for at lisenspliktige strategiske varer eksporteres uten lisens.

Viktige samfunnsmessige faktorer som påvirker kriminalitetsutviklingen er teknologisk utvikling, trusselutviklingen, demografiske endringer, klima- og miljøutvikling, økte krav om effektiv ressursbruk og den kriminalpolitiske utviklingen (Meld. St. 29 (2019-2020), s. 15-16). I tillegg vil covid-19-pandemien, den alvorligste krisen Norge har opplevd siden andre verdenskrig, prege samfunnsutviklingen i lang tid fremover på måter vi ennå ikke ser rekkevidden av.

I et langtidsperspektiv er klimaendringer en av de største utfordringene som verdenssamfunnet står overfor. Antatte konsekvenser for Norge er et varmere og våtere klima, og endring i ressurstilgangen fra andre land. Konsekvenser av klimaendringer for konfliktutvikling globalt og for samfunn og økonomi i Norge er usikre, men det antas at følgeeffekter vil kunne påvirke norsk økonomi og samfunn. Dette vil følgelig også påvirke politi- og påtaletjenestens utfordringsbilde fremover.

1.1 Formål

Forsvarets forskningsinstitutt (FFI) har fått i oppdrag fra Justis- og beredskapsdepartementet (JD) å beskrive hva samfunnsutviklingen kan bety for det fremtidige trusselbildet som politiet, PST og påtalemyndigheten vil møte i tiden frem til 2030, med et særlig fokus på området «beredskap og nasjonal sikkerhet». Oppdraget er avgrenset mot oppgaver som politi- og påtaletjenestene vil ha ved væpnet konflikt, samt oppgaver som følge av ikke-intenderte hendelser som naturhendelser og ulykker.

FFIs leveranse består av tre rapporter: (*i*) En morfologisk analyse av trusler mot Norges sikkerhet med formål å identifisere utfordringskategorier for de tre tjenestene frem mot 2030 (Sellevåg, 2021), (*ii*) en gradert rapport som beskriver mulige scenarioer knyttet til utfordringskategoriene (Sellevåg & Buvarp, 2021), og (*iii*) denne rapporten som er en dokumentanalyse av publiserte utviklingstrekk som er av betydning for utfordringsbildet politi- og påtaletjenestene står overfor, samt en vurdering av hvilken betydning utviklingstrekkene kan ha for de tre tjenestene på kort (0-5 år) og på mellomlang sikt (5-10 år). Samlet vil dette bidra til et forskningsbasert kunnskapsgrunnlag til støtte for utarbeidelse av nasjonal plan for politi- og påtaletjenestene i tråd med regjeringens formål om å legge til rette for strategisk og langsiktig styring (Prop. 1 S (2019-2020), s. 104).

1.2 Rapportens organisering

Denne rapporten er organisert som følger: I kapittel 2 og 3 gis en kortfattet beskrivelse av politiets utvikling, oppgaver og beredskapssystem som grunnlag for å vurdere samfunnsutviklingens betydning for politi- og påtaletjenestene. Deretter gis det i kapittel 4 en oppdatert vurdering av sentrale utviklingstrekk (omverdensanalyse) som er av betydning for de tre tjenestene med bakgrunn i endringer som følger av covid-19-pandemien. I kapittel 5 sees det nærmere på utviklingen innen tematiske utfordringsområder innen kriminalitet, terrorisme og trusler mot nasjonal sikkerhet. Valg av utfordringsområder er basert på funn fra Sellevåg (2021). I kapittel 6 diskuteres implikasjoner av forventet utvikling, samt temaer som bør vies særskilt oppmerksomhet. Til

slutt presenteres det fremtidige utfordringsbildet i kapittel 7. Sentrale begreper og metodisk tilnærming utdypes i henholdsvis vedlegg A og B.

2 Politiets utvikling i et historisk perspektiv

Hva er politi? Dette spørsmålet ble stilt av Christian Magnus Falsen under arbeidet med en politilov i 1828 (Ellefsen, 2018a). Arbeidet med å etablere en statsforfatning i Norge etter 1814 måtte også gi et annet grunnlag for å definere politiet på. Frem til 1830 var politiet først og fremst kongens politi. Det var den eneveldige danske kongen som etablerte politiembeter i de store byene som et redskap for sin egen maktutøvelse. I lovutkastet til politilov som ble videreført etter Falsens død i 1830 ble det tatt til orde for et regjeringsstyrt politi som hadde en overordnet oppgave å beskytte rikets sikkerhet og velferd. Etter at Formannskapslovene ble vedtatt i 1836 fikk Norge som en ung nasjon et desentralisert politi og lensmenn i kommunene, mens det statsfinansierte politiet etablerte seg i byene (Ellefsen, 2018b). Dette var en ordning som mer eller mindre holdt seg frem til mellomkrigstiden.

> Det disiplinære samfunnet oppstod på bakgrunn av visse historiske prosesser av økonomisk, juridisk-politisk og vitenskapelig art (Foucault, 2018).

Langt på vei er utviklingen av politiet i Norge som resten av Europa en utvikling av den moderne rettsstaten. I en moderne rettstat er politiet både en forutsetning og en konsekvens. De store nasjonalstatenes fremvekst blir mulig fordi det også vokser fram virkekraftige makt- eller voldsmonopoler (Kolnar, 2006). Politiet som den objektive maktutøver er derfor ikke bare et produkt av moderniteten, men i like stor grad en forutsetning hvor statens suverenitet og monopol på makt er det som definerer en moderne stat (Turner, 2008).

> Politiet er en samfunnsmessig institusjon som er konstitutiv for eksistensen av et moderne samfunn (Birkeland, 2007).

Grovt sett kan vi skille mellom to politimodeller. M*aktbruk-modellen* er der politiet med militær presisjon slår ned brutalt og effektivt på alt som defineres som et ordensproblem. Det er ofte diffuse grenser mellom politiet og det militære. I den tilbakeholdende modellen slik den ble utviklet i England tidlig på 1800-tallet, skulle politiet være nær publikum, ubevæpnet og *borgere i uniform.* Det var denne modellen som Norge organiserte sitt politi etter og som langt på vei lå til grunn for opprettelsen av politiskolen i 1920. Utdanningen besto i de første årene av korte konstabelkurs, men frem mot 2. verdenskrig ble utdanningen utvidet med flere måneder. Dette var starten på en profesjonsutdanning som i dag, 100 år etter, er etablert som en 3-årig høgskoleutdanning.

Mellomkrigstiden i Norge var, som resten av verden, preget av konjunktursvikt, arbeidsløshet og stadige konflikter mellom en voksende arbeiderklasse og det konservative borgerskapet. Po-

litiet ble en del av denne konflikten og ofte sett på som borgerskapets forlengede arm mot arbeiderklassens krav om rettferdig fordeling og ordnet arbeidsliv. Disse konfliktene er i en historisk kontekst eksemplifisert gjennom det som har fått navnet «Menstad-slaget» i 1931. I 1936 kom en ny politilov som bestemte at alt politi skulle styres og lønnes av staten. Justis- og politidepartementet ble politiets øverste ledelse. Denne modellen ble reetablert etter 1945. Perioden etter 1945 var politiet i stor grad et speilbilde av samfunnets konformitet. Landet skulle gjenreises økonomisk og velferdsstaten skulle utvikles (Olstad, 2017).

Først på 1970-tallet ble samfunnets konformitet utfordret. Motstanden mot krigen i Vietnam og raseskille i USA bredte seg til studentopprør og uro i Europa. 1970-tallet ble i Norge preget av økonomiske kriser og politiske uenigheter rundt medlemskap i EU, og de første ikkevoldsdemonstrasjonene mot eksempelvis naturinngrep. I stor grad foregikk demonstrasjonene fredelige. I dette tiåret kom også utdanningssamfunnets store gjennombrudd. Høyere utdanning ble et tilbud til alle, og ikke bare en aktivitet for de få (Olstad, 2017). Profesjonsutdanninger skulle føre til en «akademisering» innenfor en rekke yrker. Dette var en utvikling som også skulle gjelde politiutdanningen som etter mye diskusjon gikk tidlig på 1990-tallet fra å være en etatsskole til en 3-årig høgskole.

1980-tallet ble et markant omdreiningspunkt for politiet på flere områder. I 1981 kom den første av to delutredninger som omhandlet politiets rolle i samfunnet (NOU 1981: 35). Denne og den påfølgende utredningen (del II) som kom 6 år senere, representerte noe helt nytt i å utfordre politiet gjennom offentlige utredninger (NOU 1987: 27). Tidligere hadde politiet blitt beskrevet med utgangspunkt i funksjon og forventninger. Disse delutredningene utfordret politiet på en helt ny måte. Om politiets rolle står det (NOU 1981: 35):

> *Politiets rolle reiser spørsmål som: Hvor står politiet i forhold til statsmakten? I forhold til befolkningen som helhet og til grupper innen befolkningen? Hvilken rolle har politiet spilt i landets historie? For opprettholdelse av den indre fred? I utviklingen av landets styresett? I den politiske prosess? Under sosiale omveltninger?*

NOU 1981: 35 tar også et oppgjør med tidligere utredninger og skriver om disse:

> *Vårt hovedinntrykk er at politiets rolle og oppgaver har vært et sekundært tema for samtlige utredningsutvalg. De ble alle nedsatt for å utrede andre spørsmål, som regel organisasjons- og personell-problemer som lå i tiden og som krevet snarlige løsninger. Der hvor politiets oppgaver har fått egne kapitler eller avsnitt, finner vi bare en oppregning av gjøremål, med henvisning til hvilke lover og forskrifter som danner bakgrunnen for dem. For Politirolleutvalgets arbeid har de tidligere utredninger knapt hatt noen praktisk betydning.*

Disse utredningene tar utgangspunkt i hva politiet skal være, og ikke bare en beskrivelse av hva politiet er. Utredningene bygger på følgende hovedtese (NOU 1981: 35):

En hovedtese i denne utredning er at politiet bare kan løse sine oppgaver gjennom et konstruktivt samspill med publikum. Å spille på publikums bistand og medvirkning må være politiets hovedstrategi, som alle andre strategier og metoder utledes fra. Samspillet forutsetter en positiv holdning hos begge parter, men også vilje og evne til å samarbeide i praksis.

Utredningene fra 1981 og 1987 rammet inn politiets utfordringer i ti grunnprinsipper (boks 3.1). Dette er prinsipper for politiets virke som siden har vært styrende og ble bekreftet i den siste stortingsmeldingen (Meld. St. 29 (2019-2020)).

Boks 3.1: Politiets ti grunnprinsipper (NOU 1981: 35, s. 13-15)

1. Politiet skal avspeile samfunnets idealer
2. Politiet skal ha et sivilt preg
3. Vi skal ha et enhetspoliti
4. Politiet skal være desentralisert
5. Politimannen skal være en generalist
6. Politiet skal virke i samspill med publikum
7. Politiet skal være integrert i lokalsamfunnet
8. Politiet skal ha bred rekruttering
9. Politiet skal prioritere mellom sine oppgaver og legge hovedvekten på forebyggende virksomhet
10. Politiet skal være underlagt effektiv kontroll fra samfunnets side

Om utredningen på 1980-tallet utfordret politiet på sin samfunnsrolle, er terrorangrepet på Norge 22. juli 2011 et omdreiningspunkt i politiets operative evne. Kritikken mot politiet (NOU 2012: 14) og myndigheter etter denne hendelsen har vært kraftfulle og avgjørende for prioriteringer og reformer i politiet (Prop. 61 LS (2014-2015)). Politiets arbeid de siste ni årene har langt på vei blitt styrt av denne katastrofen.

Over 180 år etter Falsen stilte spørsmålet *hva er politi?*, blir spørsmålet nå stilt på nytt (Finstad, 2018). Selv om politiet utfordres og presses fra mange interesser er det to forhold som fortsatt preger politiets virke: De er både døråpner og portvakt. Politiet er døråpner til et samfunn hvor alle som føler seg berettiget kan anmelde og få sine saker prøvd for en domstol. Samtidig har politiet også en tidløs rolle som portvakt. Det er politiet som har fått statens monopol på å utøve makt overfor egne borgere. Dette gjør at den vanlige borger har beskyttelse av politiet og det er politiet som ordner opp for oss, felleskapet. Dette er langt på vei politiets imperativ, og dersom ikke politiet gjennom sitt virke opprettholder tilliten til borgerne forsvinner grunnlaget for det samme virket.

Politiet er instansen som gjennom *forebyggende, håndhevende og hjelpende virksomhet* bekrefter og sikrer borgernes rettssikkerhet (Finstad, 2018).

3 Politiets oppgaver og beredskapssystem

3.1 Politiloven

Prinsippet om et statlig politi og politiets maktmonopol er nedfelt i politiloven § 1, som fastsetter at det er staten som skal sørge for den polititjenesten samfunnet har behov for. Politiets primæroppgaver er beskrevet i politiloven § 2 og innebærer blant annet å beskytte personer, eiendom og fellesgoder, verne om all lovlig virksomhet, opprettholde offentlig orden og sikkerhet og enten alene eller sammen med andre myndigheter verne mot alt som truer den alminnelige tryggheten i samfunnet. I tillegg skal politiet yte borgerne hjelp og tjenester i faresituasjoner (politiloven § 2).

For å kunne ivareta oppgavene er politiet gitt omfattende fullmakter i politiloven §§ 7 og 27, med utfyllende bestemmelser gitt i politiinstruksen. Rammene for politiets adgang til å bruke makt er regulert i politiloven § 6. Politiloven § 27 tredje ledd pålegger politiet å iverksette nødvendige tiltak for å avverge fare og begrense skade i forbindelse med ulykkes- og katastrofesituasjoner. Bestemmelsen innebærer at politiet har et akutt, sektorovergripende ansvar for å håndtere ulykker og katastrofer i fredstid på alle samfunnsområder. I akuttfasen har politimesteren myndighet til å fatte beslutninger på andre myndigheters ansvarsområde inntil dette ansvaret overtas av den ansvarlige myndigheten i henhold til ansvarsprinsippet. Politiet er blant annet ansvarlig for evakuering, generell bistand til befolkningen, vakthold og sikring, samt etterforskning. Politiet har et særskilt ansvar for å lede søk etter antatt omkomne og ta hånd om døde, og til å varsle pårørende (Politidirektoratet, 2020, s. 16-17).

> Politiet skal gjennom forebyggende, håndhevende og hjelpende virksomhet være et ledd i samfunnets samlede innsats for å fremme og befeste borgernes rettssikkerhet, trygghet og alminnelige velferd for øvrig.

3.2 Politiets beredskapssystem

Politiets beredskapssystem (PBS) er en del av nasjonalt beredskapssystem (NBS) og består av tre deler:

- PBS I – Retningslinjer for politiets beredskap: Beskriver forutsetninger, prinsipper og mekanismer for politiets rolle, ansvar og oppgaver innen forebygging og håndtering samt relevante samvirkeaktører og –mekanismer.
- PBS II – Politidirektoratets styringsdokumenter: Inneholder styringsdokumenter innenfor de ulike beredskapsområdene, som er med på å danne grunnlaget for politidistriktenes egne planer.

- PBS III – Politidistriktenes planverk: Med utgangspunkt i PBS I og II tilpasses politidistriktenes egne planverk lokale forhold.

Til sammen utgjør disse tre delene en helhetlig sammenstilling av beslutninger og føringer for politiets beredskapssystem. PBS er et oversiktlig og fleksibelt beredskapsplanverk som er utarbeidet for at politiets oppgaver skal kunne håndteres på en effektiv måte.

Politiberedskap er et begrep som spenner bredt og forstås som tiltak for å forebygge, begrense eller håndtere daglige uønskede hendelser, så vel som ekstraordinære hendelser og kriser. Det innebærer at politiet er forberedt på at slike hendelser og kriser kan inntreffe, og at det finnes planer og tiltak for å avverge dem eller begrense konsekvensene. Politiet har derfor en døgnkontinuerlig beredskap for å håndtere ordinære politioppgaver. Politiberedskapen omfatter i tillegg beredskap i form av planverk, tiltak, kompetanse og organisering som gjør politiet i stand til å forebygge, begrense, avverge, stanse, etterforske og håndtere ekstraordinære hendelser og kriser (Politidirektoratet, 2020, s. 22).

3.3 Dagens organisering

Politi- og lensmannsetaten består av i dag av tolv politidistrikter og politiets særorganer,[1] som skal løse samfunnsoppdraget innenfor sine respektive områder. De skal på selvstendig grunnlag håndtere alle politioppgaver som kan oppstå i forbindelse med tilsiktede uønskede handlinger og utilsiktede uønskede hendelser i en normalsituasjon, og ved ekstraordinære hendelser og kriser. Politidirektoratet leder og samordner dette arbeidet.

PST er direkte underlagt Justis- og beredskapsdepartementet. PST er Norges nasjonale innenlands etterretnings- og sikkerhetstjeneste, hvis hovedoppgave er å forebygge og etterforske alvorlig kriminalitet som angår nasjonens sikkerhet. PST gjør dette gjennom følgende tre funksjoner:

- Etterretningstjeneste som identifiserer og avklarer trusler og bekymringer
- Sikkerhetstjeneste som iverksetter trussel- og sårbarhetsreduserende tiltak
- Etterforskningsorgan og påtalemyndighet som etterforsker og iretteører straffesaker

PSTs hovedoppgaver er å avdekke spionasje, forebygge terror, hindre spredning av masseødeleggelsesvåpen og forhindre trusler mot myndighetspersoner. Dette gjør tjenesten blant annet gjennom innsamling av informasjon om personer og grupper som kan utgjøre en trussel, utarbeidelse av ulike analyser og trusselvurderinger, etterforskning og andre operative tiltak og rådgivning. PST skal bistå når det iverksettes sikkerhetstiltak i statsadministrasjonen og i tilknytning til sårbar infrastruktur, forsknings- og undervisningsinstitusjoner, offentlig og privat næringsvirksomhet og annen virksomhet som ivaretar viktige samfunnsinteresser (Politidirektoratet, 2020, s. 53-54).

[1] Grensekommissæren for den norsk-russiske grense, Kripos, Politihøgskolen, Politiets utlendingsenhet, Utrykningspolitiet og Økokrim.

Påtalemyndigheten i politiet (integrert påtale) utgjør det laveste påtalenivået og ledes av politimesteren (Politidirektoratet, 2020, s. 18). Den er imidlertid faglig underlagt statsadvokatene. Påtalemyndigheten i politiet leder politiets etterforskning. Integrert påtale i politiet legger til rette for at påtalemyndigheten kan lede etterforskningen i nært samarbeid med politiets etterforskere. Denne ordningen gjør det mulig for påtalemyndigheten å lede politiets etterforskning mer effektivt og kontrollere at den utføres i tråd med straffeprosessloven, påtaleinstruksen og direktiver fra den høyere påtalemyndighet.

4 Omverdensanalyse

I dette kapitlet gis en oppdatert vurdering av sentrale utviklingstrekk som er av betydning for politiet, PST og påtalemyndigheten med bakgrunn i endringer som følger av covid-19-pandemien. Oppsummeringen av de langsiktige utviklingstrekkene frem mot 2030 er basert på gjengivelser av vurderinger gitt i Beadle *et al.* (2019) og Sellevåg *et al.* (2020) der hvor ikke annet er oppgitt.

4.1 Politiske forhold

Sammendrag av sentrale utviklingstrekk innen politiske forhold:

- Fortsatt stormaktsrivalisering som følge av maktforskyvning fra Vesten til Kina og andre fremvoksende stormakter i Asia og Latin-Amerika.
- Forskyvning av makt til store multinasjonale selskaper og andre ikke-statlige organisasjoner.

Den langsiktige globale sikkerhetspolitiske utviklingen preges av tre hovedtrender (Beadle *et al.*, 2019): (*i*) Maktforskyvning fra Vesten til Kina og andre fremvoksende stormakter i Asia og Latin-Amerika; (*ii*) maktforskyvning fra statlige til ikke-statlige aktører; og (*iii*) endringer i bruk av virkemidler, hvor stater i større grad bruker en kombinasjon av ulike virkemidler for å utøve press. I det følgende av kapittel 4.1 diskuteres stormaktsrivaliseringen mellom USA, Russland og Kina, og hvilken betydning dette kan ha for Europa basert på vurderinger i Beadle *et al.* (2019), med hovedfokus på forhold som kan være viktige for politi- og påtaletjenestene. Maktforskyvning fra statlige til ikke-statlige aktører vil berøres i kapitlene 4.1.2 og 4.5, mens endringer i virkemiddelbruk vil diskuteres i kapittel 5.1.1.

4.1.1 Stormaktsrivalisering

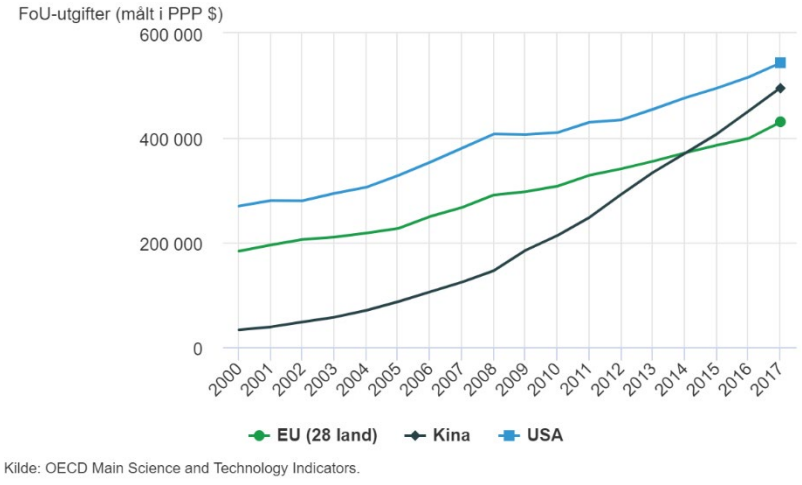
Maktforskyvningen fra Vesten til fremvoksende stormakter i Asia og Latin-Amerika skyldes i første rekke at særlig Kina og India, men også andre store land som Brasil, har hatt betydelig høyere økonomisk vekst enn vestlige industriland. I tillegg til å påvirke den militære maktbalansen, har den økonomiske forskyvningen også ført til økt rivalisering om innflytelse og ressurser, også når det gjelder hvordan internasjonal avtaler og ordninger skal tolkes og innrettes.

Stormaktsrivalisering og den globale maktforskyvningen gjør at den liberale verdensordenen, det vil si en regelbasert verdensorden basert på sentrale verdier som markedsbasert økonomi og frihandel, individets rettigheter, en fri presse, rettsikkerhet og demokrati, utfordres. Dette har medført at internasjonale normer, avtaler, rettsprinsipper og institusjoner svekkes.

USAs posisjon i verden utfordres særlig av Russland og Kina, hvor sistnevnte vurderes å utgjøre en større og mer langvarig utfordring for USA. Samtidig har den liberale verdensordenen også blitt utfordret av USA. Under Trump-administrasjonen trakk USA seg fra en rekke internasjonale avtaler og sådde tvil om samholdet i Nato. For Norge som småstat er tvil rundt alliert støtte særlig bekymringsfullt; spesielt hvis utviklingen går i retning av en regionalisert verden hvor stormakter opptrer mer selvhevdende innenfor sine innflytelsessfærer. Med Biden-administrasjonen forventes økt amerikansk oppslutning om internasjonale avtaler og organisasjoner.

Selv om faren for konflikter i Arktis vurderes å være lavere enn i mange andre deler av verden, fremstår situasjonen som mer usikker enn det den gjorde for noen år tilbake. Med økende aktivitet i nordområdene som følge av issmelting i Arktis, er det fare for mer stormaktsrivalisering også i denne regionen. Dersom Russland velger å føre en mer aggressiv utenrikspolitikk i nord, kan dette blant annet få betydning for norske interesser på Svalbard og norsk tolkning av Svalbardtraktaten. Samtidig har Norge og Russland felles interesser knyttet til havmiljøsamarbeid i nordområdene.

Ser man på forholdet mellom USA og Kina spesielt, er forholdet ikke bare preget av handelskrig. Det er også et kappløp om innovasjon og teknologi. Tradisjonelt har USA hatt et ubestridt teknologisk forsprang. For ti år siden stod USA for rundt 35 % av verdens utgifter til forskning og utvikling (FoU). Imidlertid har Kina satset kraftig de siste årene med en gjennomsnittlig årlig vekst i FoU-utgifter på 12 % fra 2007 til 2017. I 2017 var USAs og Kinas FoU-utgifter nesten like store med henholdsvis 28 % og 26 % av verdens totale utgifter, hvor EU med Storbritannia var forbigått av Kina. Dersom Kinas vekst fortsetter som vist i Figur 4.1, vil Kina kunne gå forbi USA om få år som verdens største FoU-nasjon (Bjørkholt, 2019). Ser man på FoU-innsats som andel av bruttonasjonalprodukt (BNP) eller på FoU-innsats per innbygger, er USAs posisjon i mindre grad truet. Like fullt har Kina hatt en betydelig økning i FoU som andel av BNP de siste ti årene.



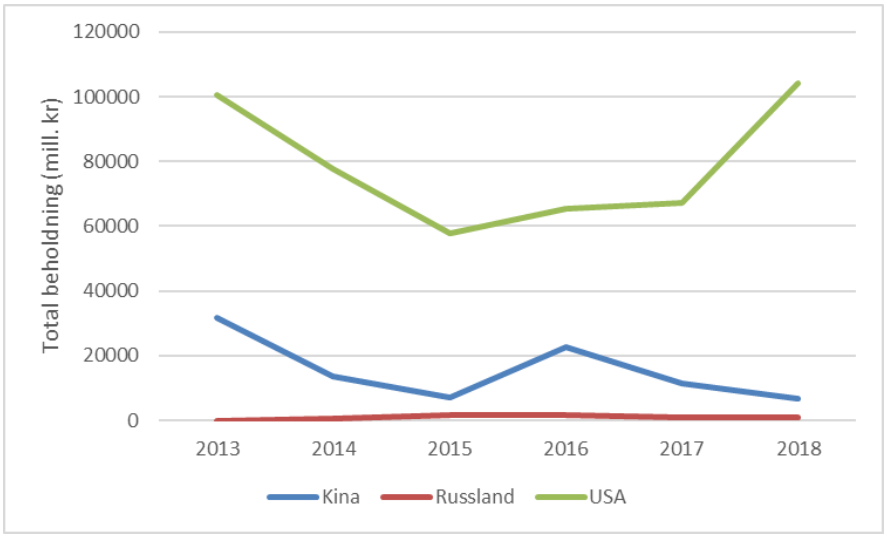
Figur 4.1 Utgifter til forskning og utvikling (FoU) for USA, Kina og EU målt som kjøpekraftspariteter (PPP; prisnivåindikator).

Kinas satsning innen FoU er et ledd i planen om å bli selvforsynt i høyteknologiske bransjer innen 2025; den såkalte «Made in China 2025»-strategien (Bjørkholt, 2019). Av militærteknologisk betydning er det særlig forbedringer i menneskers fysiske og kognitive evner, robotikk og autonome systemer som utnytter kunstig intelligens, additiv tilvirkning, kvantedatamaskiner, romteknologi, stordata og nye energikilder og -lagringsmedier som er viktige satsningsområder (Forsvarets forskningsinstitutt, 2016). Disse teknologiområdene vil også være viktige for utviklingen av det sivile såkalte «smartsamfunnet» (jf. kapittel 4.5). Følgelig er det sterk konkurranse mellom USA og Kina om å bli verdensledende på disse teknologiområdene. Når USA og Kina setter som mål å bli teknologisk selvforsynte, vil dette påvirke globale verdikjeder fordi komponenter til høyteknologiprodukter som oftest vil leveres fra flere lands teknologiselskaper.

To forhold har vært av særlig bekymring knyttet til Kinas teknologisatsning: (*i*) mangelfull respekt for immaterielle rettigheter (IPR)[2] og (*ii*) direkteinvesteringer i teknologi- og forskningsaktive selskaper. Når det gjelder det første forholdet, satser Kina nå sterkt på beskyttelse av patenter og opphavsrettigheter fordi kinesiske selskaper selv i økende grad er avhengig av IPR-beskyttelse. Samtidig krever Kina at amerikanske selskaper lokaliserer FoU-avdelinger i landet for å få tilgang til det kinesiske markedet, noe som representerer en lovlig, men tvungen form for teknologioverføring.

Når det gjelder kinesiske direkteinvesteringer i utlandet, var det en betydelig økning fra 2004 til 2016 innen sektorer knyttet til naturressurser og infrastruktur. Imidlertid har kinesiske direkteinvesteringer i vestlige land falt med 50 % fra toppåret 2016. Dette skyldes sterkere kontroll over kinesisk kapitalflyt fra myndighetene i Beijing, samt mer oppmerksomhet og strengere søknadsbehandling fra EUs side (Hanemann *et al.*, 2019). Denne trenden finner vi også i Norge (Figur 4.2). Ser man imidlertid på utenlandske direkteinvesteringer i Norge etter ultimat eierland, det vil si landet hvor enheten som ultimat kontrollerer den største direkteinvestoren til en norsk enhet er registrert, har det vært en økning i kinesiske direkteinvesteringer i Norge fra 2017 til 2018.[3] Dog har det ifølge Statistisk sentralbyrå (SSB) til nå ikke vært noen tydelig trend mot at kinesiske selskaper kjøper opp FoU-aktive norske selskaper; kun 4% av multinasjonale FoU-aktive selskaper i Norge har vært eid fra Kina og denne andelen har vært stabil i perioden 2011–2017 (Bjørkholt, 2019; se også Sverdrup-Thygeson & Mathy, 2020). Samtidig er det grunn til å forvente at den totale beholdningen av kinesiske direkteinvesteringer i Norge vil vedvare og bli mer målrettet. Andelen av kinesisk kapital i Europa kan også raskt øke dersom noen av Kinas statseide selskaper gjør store investeringer som en del av det såkalte «Belte- og vei-initiativet» (BRI) (Kristoffersen, 2019).

[2] Immaterielle rettigheter er en samlebetegnelse på rettigheter knyttet til patenter, design og varemerke.
[3] Kilde: Statistisk sentralbyrå, tabell 12754.



Figur 4.2 Utenlandske direkteinvesteringer (mill. kr.) i Norge etter land og år. Kilde: Statistisk sentralbyrå (tabell 11326).

Enn så lenge har covid-19-pandemien ført til en ytterligere forverring av forholdet mellom USA og Kina, og USA har rettet en rekke alvorlige anklager mot Kina. Blant annet mener amerikanske myndigheter at Kina bevisst skjulte smitteomfanget for å kunne hamstre medisinsk utstyr i starten av pandemien (Barlup, 2020). USA valgte også å formelt trekke seg fra Verdens helseorganisasjon (WHO) med virkning fra 6. juli 2021 med begrunnelse om manglende reformer i forbindelse med håndteringen av pandemien. Trump-administrasjonen anklaget også WHO for å «fremme Kinas falske informasjon» (Ekroll, 2020). Trump-administrasjonen valgte også å stå utenfor det internasjonale covid-19-vaksinesamarbeidet (COVAX) i regi av WHO og vaksinealliansene CEPI og GAVI (Hansen & NTB, 2020). Etter først å ha valgt å stå utenfor, snudde Kina og har siden valgt å slutte seg til COVAX. Under Biden-administrasjonen har USA igjen tilknyttet seg WHO og COVAX.

Stormaktsrivaliseringen kommer også til uttrykk når det gjelder utvikling av covid-19-vaksine. Blant annet har britiske «National Cyber Security Centre» utstedt en advarsel om målrettede datanettverksangrep fra gruppen APT29 (også kjent som «Cozy Bear») mot organisasjoner som er involvert i vaksineutvikling, hvor intensjonen høyst sannsynlig har vært å stjele informasjon og IPR knyttet til utvikling og testing av covid-19-vaksinekandidater (United Kingdom National Cyber Security Centre, 2020).

Når det gjelder situasjonen i Europa, har EU (etter en treg start) iverksatt en rekke tiltak for å begrense konsekvensene av covid-19-pandemien. Blant annet har EU opprettet en langsiktig plan hvor nærmere 780 milliarder euro settes av til å finansiere gjenreising av økonomien, hvilket er første gang EU oppretter felles gjeld (NTB, 2020a). På kort sikt er det derfor ikke noe som tilsier at EU-samarbeidet svekkes vesentlig som en konsekvens av pandemien (Riddervold

& Trondal, 2020). Imidlertid sliter EU-landene med samhold rundt covid-19-vaksinering. I tillegg må utfordringene med Polen og Ungarns autoritære utvikling løses. EU-landene preges også av ulike oppfatninger rundt hva som utgjør den største sikkerhetsutfordringen (Meijer & Brooks, 2021).

For Norge sin del blir det et spørsmål om hvor stort Norges økonomiske bidrag vil være for å bidra til europeisk solidaritet og gjenreising av økonomien. Dette kan på nytt reise en politisk diskusjon rundt Norges tilknytning til EU (Sverdrup, 2020). Det er imidlertid for tidlig å si hvilke langvarige konsekvenser covid-19-pandemien kan ha for sikkerhetspolitiske forhold som berører Europa og Norge.

4.1.2 Forskyvning av makt fra statlige til ikke-statlige aktører

Selv om de politiske trendene peker på økende stormaktsrivalisering, forventes det likevel at ikke-statlige aktører vil få stadig mer makt på bekostning av statlige aktører (Beadle *et al.*, 2019, s. 161). Allerede i dag spiller ikke-statlige aktører en fremtredende rolle i mange av dagens konflikter; den arabiske våren, fremveksten av IS og protestbevegelsen «de gule vestene» i Frankrike er ulike eksempler på hvordan motstand fra ikke-statlige aktører kan komme til uttrykk. Samtidig er det utviklingstrekk som peker på at urbanisering kan medføre at megabyer får større politisk og økonomisk innflytelse på bekostning av nasjonalstaten i fremtiden. I tillegg kan noen multinasjonale selskaper få betydelig innflytelse gjennom tjenestene de leverer til samfunnet, og det er grunn til å frykte at noen selskaper kan forsøke å utnytte denne makten (DCDC, 2018, s. 12). I det følgende vil det siste forholdet diskuteres i nærmere detalj med hovedfokus på maktforskyvning til store multinasjonale selskaper innen digitale teknologier.

Utviklingen av IKT-samfunnet og tilgang til internett og elektronisk kommunikasjon er i dag nærmest grunnleggende for all næringsvirksomhet. Siden den såkalte «IT-boblen» sprakk på slutten av 1990-tallet, har selskaper innen digitale teknologier fått en enorm markedsposisjon. De fem store teknologigigantene –Alphabet (Google), Amazon, Facebook, Apple og Microsoft, ofte omtalt som GAFAM – er nå de mest verdifulle selskapene på verdens børser. Karakteristisk for disse selskapene er deres dominerende markedsmakt («vinneren tar alt»).

Gjennom sine tjenester kan selskapene samle inn enorme mengder persondata som kan utnyttes for å forbedre tjenestene, tilby tilpasset reklame etc. for slik å generere profitt. Dataene kan også videreselges til andre virksomheter av såkalte dataforhandlere. I en undersøkelse utført av Forbrukerrådet i 2020, ble det funnet at 10 utvalgte apper sender brukerdata til 135 forskjellige tredjeparts virksomheter som er involvert i reklame og/eller profilering av adferd (Forbrukerrådet, 2020). Av de ti appene, mottok Google data fra åtte av appene, mens Facebook mottok data fra ni av appene. En stor del av mengden av persondata som ble samlet inn, ble vurdert å være ulovlig etter EUs personvernforordning (GDPR).

Denne forretningsmodellen, hvor brukeren får tilbudt tjenester, resultater eller produkter ut fra predikert adferd og preferanser gjennom utnyttelse og analyse av innsamlede persondata, er karakterisert som *overvåkningskapitalisme* av Harvard-professor Shoshana Zuboff (2019). Over-

våkningskapitalismen utfordrer ikke bare personvernet, men i ytterste konsekvens også ytringsfriheten og demokratiet. Eksempelvis har Facebook vært involvert i flere kontroverser. I 2016 ble Facebook anklaget for urettmessig sensur etter å ha slettet Tom Egelands deling av Nick Uts berømte bilde av jenta som hadde blitt utsatt for napalm under Vietnamkrigen. Statsminister Erna Solbergs og Aftenpostens deling av samme bilde ble også sensurert, noe som medførte at Aftenposten sendte et åpent brev til Mark Zuckerberg (Hansen, 2016). I 2018 var Facebook igjen i kontroverser i den såkalte Facebook-Cambridge Analytica-saken hvor Cambridge Analytica hadde brukt data fra millioner av Facebook-profiler for å påvirke valg (Wikipedia, u.å.-b).

Fremveksten av sosiale medier i form av en global, høyteknologisk og automatisert digital infrastruktur, har muliggjort såkalte skjulte cyber-sosiale påvirkningsoperasjoner. Slike påvirkningsoperasjoner undergraver tilliten i samfunnet gjennom å forsterke eksisterende konfliktlinjer slik at samfunnsdebatten polariseres (Bergh, 2020, s. 34). Karakteristisk for slike påvirkningsoperasjoner er at de medfører liten risiko for aktøren som står bak samtidig som sosiale medie-selskapene har få incentiver for å begrense slike operasjoner fordi det generer aktivitet (og dermed profitt) på det sosiale mediet som utnyttes. På grunn av den underliggende forretningsmodellen, kulturen i sosiale medie-selskaper og algoritmer som promoterer visse typer adferd, er det all grunn til å tro at Norge og andre vestlige land må leve med muligheten for cyber-sosiale påvirkningsforsøk i overskuelig fremtid (Bergh, 2020, s. 33-34) (sosiale medier og algoritmenes betydning vil omtales nærmere i kapittel 4.5.4).

Posisjonen til de amerikanske teknologigigantene, i første rekke Google, Amazon, Facebook og Apple (GAFA), utfordres også av kinesiske selskaper, spesielt selskapene kjent som BATX (Baidu, Alibaba, Tencent og Xiaomi). I tillegg kan Huawei og ByteDance (selskapet bak TikTok) nevnes. Selv om den amerikanske kongressen har gjennomført høringer med toppsjefene til GAFA om monopolanklager, er det grunn til å stille spørsmål ved om amerikanske myndigheter har reell vilje til å bryte opp selskapene i frykt for at USA skal tape i konkurransen mot Kina. Sammen med den digitale transformasjonen av samfunnet som er forventet (Sellevåg *et al.*, 2020, s. 51-55), er det grunn til å tro at maktforskyvningen til multinasjonale selskaper innen digitale teknologier vil vedvare.

4.2 Sosiale forhold

Sammendrag av sentrale utviklingstrekk innen sosiale forhold:

- Befolkningsvekst og urbanisering i utviklingsland.
- Voksende byer og aldrende befolkning på bygdene i Norge.
- Fortsatt nettoinnvandring til Norge, men ikke like stor som den var i perioden 2000-2020.

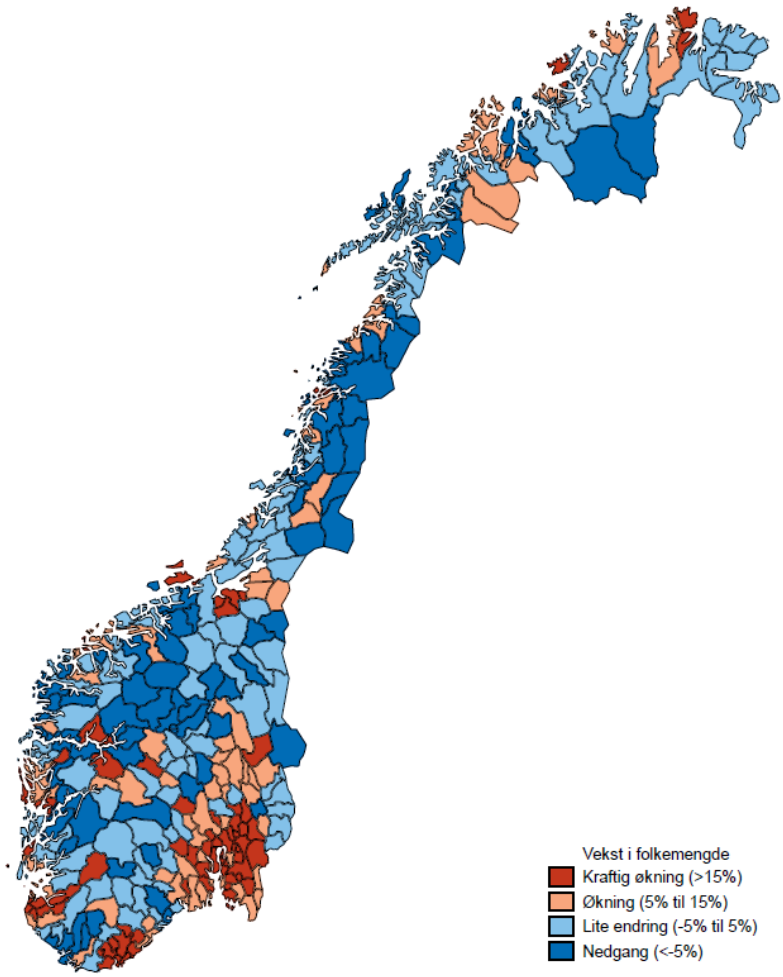
4.2.1 Demografiske trender

I Beadle *et al.* (2019, s. 21) er det tre globale demografiske trender som fremstår som relativt sikre: Verdens befolkning blir stadig (*i*) større, (*ii*) eldre og (*iii*) mer urbanisert. Imidlertid er de regionale forskjellene store. Størsteparten av befolkningsveksten og urbaniseringen vil skje i Afrika og i deler av Asia, og det forventes at halvparten av all befolkningsvekst frem mot 2050 vil finne sted i India, Nigeria, Pakistan, DR Kongo, Etiopia, Tanzania, Indonesia, Egypt og USA (United Nations Department of Economic and Social Affairs, 2019). Urbaniseringen vil i hovedsak skje i de mindre utviklede delene av verden hvor befolkningsveksten er stor og hvor andelen som allerede bor i urbane områder er relativt liten (Beadle *et al.*, 2019, s. 33). Når det gjelder aldring, har den globale medianalderen økt fra 24 år i 1950 til 30 år i 2015, og det forventes at den vil øke til 35 år i 2040; personer over 65 år er nå den raskest voksende aldersgruppen i verden sett under ett (Beadle *et al.*, 2019, s. 33).

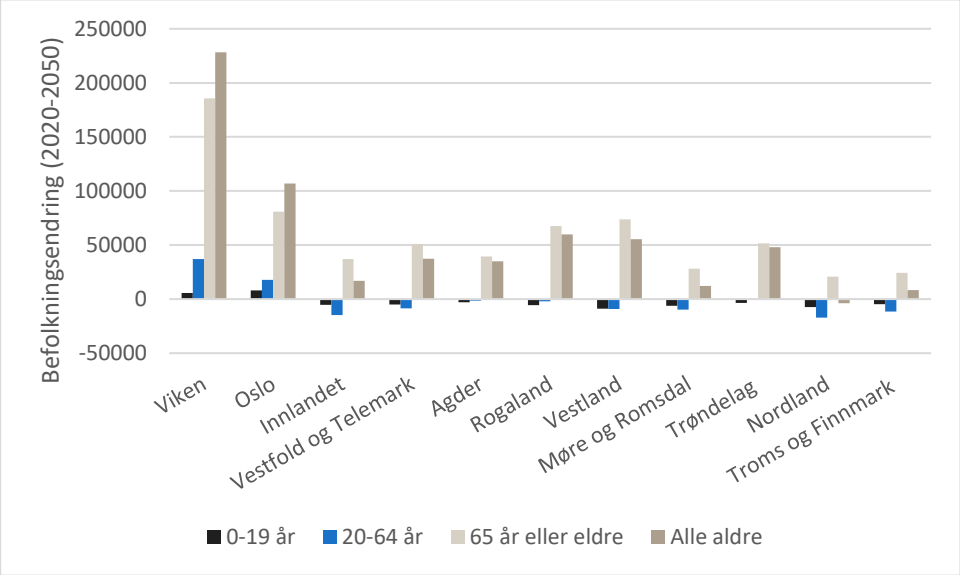
De tre demografiske hovedtrendene er også gjeldende for fastlands-Norge når SSBs hovedalternativ for befolkningsutviklingen legges til grunn. Det forventes at befolkningen samlet sett vil vokse med 11 % fra 2020 til 2050, men med store geografiske forskjeller (Figur 4.3). Forventet folketall i 2050 er ca. 6,0 millioner med et spenn fra ca. 5,37 til ca. 6,65 millioner. Rundt 60 % av alle kommuner er forventet å vokse, mens 140 kommuner er forventet å få en nedgang i folketallet. Befolkningsveksten er særlig tydelig på Østlandet og i og rundt de store byene, mens mange av nedgangskommunene ligger i distriktene. Eksempelvis er Viken forventet å vokse med over 18 %, mens Nordlands befolkning forventes å krympe med 1,6 % (Leknes & Løkken, 2020, s. 4). Resultatet er en sentralisering av befolkningen til det sentrale Østlandet. Videre vil økt forventet levealder og stor fraflytting av unge personer bidra til en sterk aldring i distriktene, både frem til 2030 og frem til 2050 (Figur 4.4). I noen av de minst sentrale kommunene vil eldre over 65 år utgjøre rundt én tredjedel av befolkningen i kommunen. Distriktskommunenes[4] demografiutfordringer kan derfor karakteriseres ved *befolkningsnedgang*, *aldring* og *spredt bosetting* (NOU 2020: 15, s. 11). Av de nevnte demografiske trendene for Norge, er det aldringstrenden som fremstår som minst usikker.

[4] Distriktskommuner kjennetegnes ved at det bor få folk på store arealer (lav såkalt sentralitet).

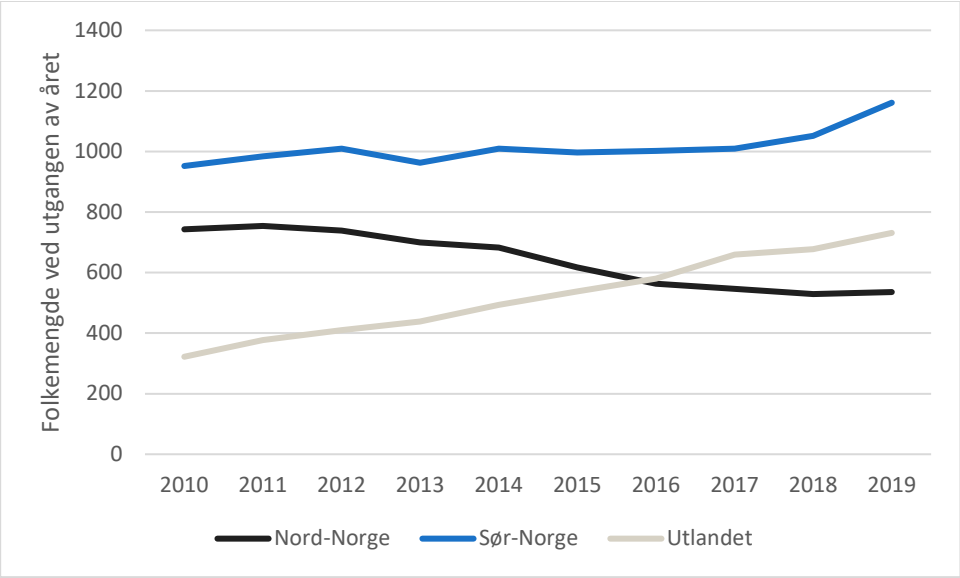
Ser vi på befolkningen på Svalbard, det vil si bosatte i Longyearbyen og Ny-Ålesund, er andelen fra Nord-Norge nesten halvert siden 2010, mens det blir stadig flere utenlandske statsborgere (Figur 4.5). Andelen fra Sør-Norge har holdt seg mer eller mindre stabilt i perioden 2010-2019. Inkluderes Barentsburg, har nesten halvparten av Svalbards innbyggere utenlandsk statsborgerskap og man må tilbake til slutten av 1990-tallet for å finne en høyere andel fra utlandet, men da hadde Barentsburg to til tre ganger så mange innbyggere som nå ifølge SSB (Høydahl, 2020). Det er imidlertid vanskelig å si noe om fremtidig befolkningsutvikling på Svalbard siden innbyggertallet i utgangspunktet er lavt.



Figur 4.3 Befolkningsvekst i kommunene fra 2020 til 2050. Kilde: Statistisk sentralbyrå (hovedalternativet) (Leknes & Løkken, 2020).



Figur 4.4 Endring i folkemengde etter region og alder fra 2020 til 2050. Kilde: Statistisk sentralbyrå (tabell 12882, hovedalternativet).

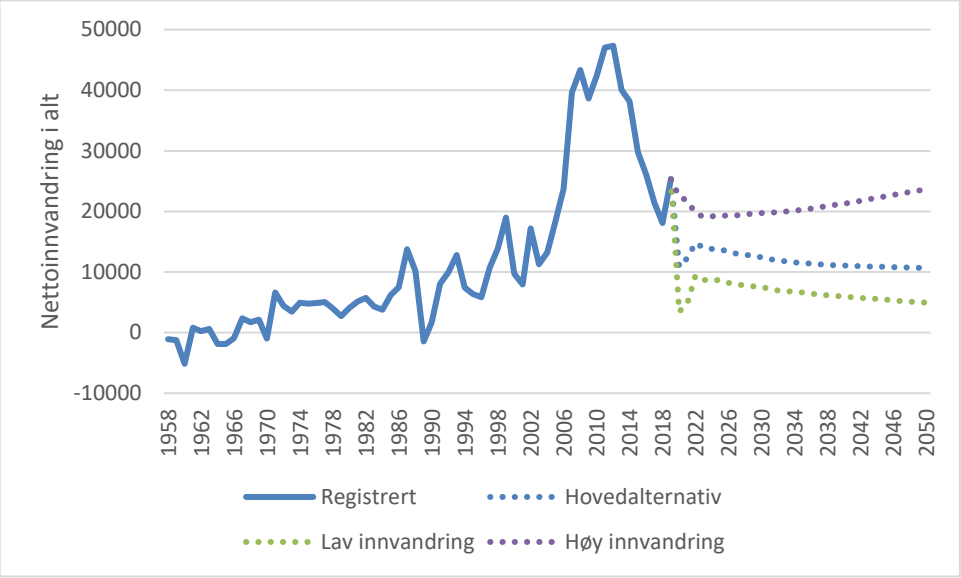


Figur 4.5 Befolkningsendring i Longyearbyen og Ny-Ålesund etter bosted eller del av land. Kilde: Statistisk sentralbyrå (tabell 08739).

4.2.2 Migrasjon og innvandring

Siden 2000-tallet og frem til nå har det vært en økning i internasjonal migrasjon. Forklaringer som trekkes frem er åpnere grenser, transnasjonale nettverk, kommunikasjonsteknologi, behov for arbeidskraft og økonomiske forskjeller (Beadle *et al.*, 2019, s. 36). For Norge sin del var det et toppår i nettoinnvandring[5] i 2012 med over 47 000 nettotilflyttinger, men deretter har nettoinnvandringen falt markant frem mot 2020 som følge av redusert innvandring og økt utvandring (Figur 4.6) (Gleditsch *et al.*, 2020, s. 77).

Generelt er det vanskelig å anslå fremtidig migrasjon fordi migrasjonsstrømmene påvirkes av forhold som er svært vanskelige å forutse med dagens kunnskap. Migrasjonsstrømmer og innvandring til Norge påvirkes ikke bare av naturkatastrofer og væpnede konflikter, men også av regelendringer og asyl- og innvandringspolitikken som føres i Norge og Europa. Eventuelle utvidelser av EU til nye medlemsland kan også medføre økt innvandring til Norge slik man så etter EU-utvidelsene i 2004 og 2007. Aldringen av befolkningen i Norge vil sannsynligvis medføre økt behov for helse- og omsorgsarbeidere, noe som kan medføre økt arbeidsinnvandring hvis de i hovedsak rekrutteres fra utlandet (Gleditsch *et al.*, 2020, s. 95). Det er også per april 2021 uklart hva Brexit vil bety for fremtidig innvandring til Norge.



Figur 4.6 Registrert og fremskrevet (tre alternativer) nettoinnvandring til Norge. Kilde: Statistisk sentralbyrå (tabell 05869 og tabell 12884).

[5] Nettoinnvandring er antall innvandringer minus antall utvandringer.

Vurderinger av fremtidige migrasjonsstrømmer er altså forbundet med svært stor usikkerhet. Denne usikkerheten har SSB vurdert gjennom sine alternativer for høy og lav innvandring. Som vist i Figur 4.6, er det lite som tyder på at nettoinnvandringen i kommende tiår vil være like stor som det den var de to foregående tiårene.

SSB har også vurdert covid-19-pandemiens betydning for inn- og utvandring. I tider med stor usikkerhet, vil folk ofte forbli i ro der de er med mindre omstendighetene blir svært vanskelige (Gleditsch *et al.*, 2020, s. 80). Pandemien har gjort at internasjonale reiser har blitt svært vanskelig og dette har påvirket alle former for migrasjon. Det er derfor grunn til å forvente en markant nedgang i antall innvandringer til Norge i 2021. Samtidig er Norge mindre berørt av pandemien enn mange andre land. Dette kan medføre en reduksjon i antall utvandringer fordi det er trygt å forbli i ro i usikre tider. Det er også svært usikkert hvor lenge covid-19-pandemien vil vare og hva de langsiktige konsekvensene vil bli. SSB har antatt at situasjonen begynner å normalisere seg fra 2022 og fremover, men det må tas høyde for trendbrudd; både at nettoinnvandringen i perioder kan bli lavere enn forventet *og* at den kan bli vesentlig høyere avhengig av hvordan situasjonen utvikler seg. Den langsiktige trenden peker imidlertid mot at nettoinnvandringen vil ligge i størrelsesorden rundt 10 000 personer per år, men med store usikkerheter.

4.3 Økonomiske forhold

Sammendrag av sentrale utviklingstrekk innen økonomiske forhold:

- Økt etterspørsel etter naturressurser som følge av global økonomisk vekst.
- Norges økonomiske vekst vil gradvis avta.
- Økende andel av verdens befolkning vil leve i ekstrem fattigdom etter covid-19-pandemien.
- Økende andel av personer med vedvarende lavinntekt i Norge.
- Økende grad av sosioøkonomisk segregering og opphoping av levekårsutfordringer i norske storbyer.

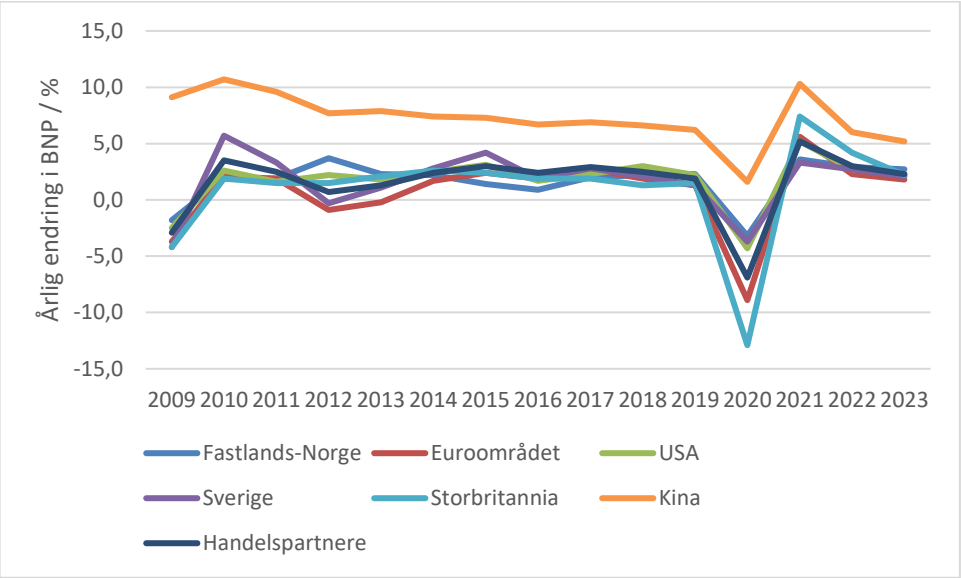
4.3.1 Økonomisk utvikling nasjonalt og internasjonalt

Før covid-19-pandemien var det forventet fortsatt økonomisk vekst i verdensøkonomien frem mot 2030, men veksten var forventet å være gradvis avtagende og med betydelig skjevhet mot Kina, India og andre fremvoksende økonomier (Beadle *et al.*, 2019, s. 62; Sellevåg *et al.*, 2020, s. 18).

Covid-19-pandemien har ført til en global økonomisk nedtur som savner sidestykke i tiden etter andre verdenskrig. Samtidig ser det per april 2021 ut til at gjenopphentingen i norsk økonomi går raskere enn hva man kunne frykte på forsommeren i 2020. Dog er usikkerheten rundt den

videre utviklingen stor, og en ny smittebølge som følge av mutantvirus vil kunne føre til at gjenopphentingen går saktere eller stopper opp. Imidlertid har myndighetene nå mye mer erfaring med pandemien og hvilke tiltak som virker.

Nedgangen i bruttonasjonalprodukt (BNP) for Norges handelspartnere var svært kraftig i andre kvartal i 2020. Det samlede fallet var nær 12 % for euroområdet og spesielt Storbritannia opplevde et kraftig fall på hele 20,4 % (Statistisk sentralbyrå, 2020b, s. 3). SSBs prognose for 2020-2023 er at fallet i BNP vil vedvare i 2020, men at fastlands-Norge og Norges handelspartnere vil oppleve BNP-vekst i 2021 (Figur 4.7). Når det gjelder Kina, er det SSBs vurdering at gjenopphentingen i større grad ser ut til å være drevet av oppgang i industriproduksjonen, snarere enn endringer i konsum, hvilket kan bety at det produseres for lager (Statistisk sentralbyrå, 2020b, s. 3).



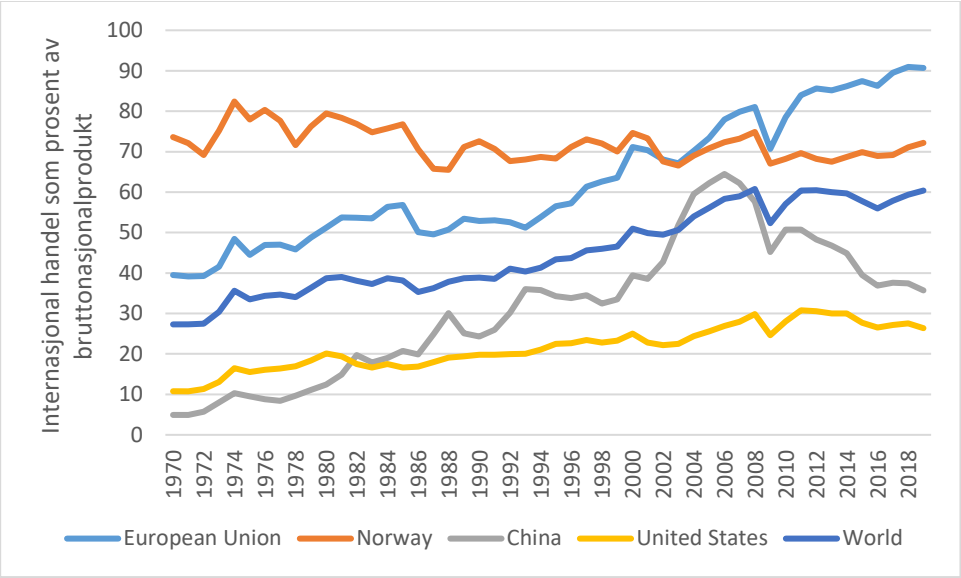
Figur 4.7 Vekst i bruttonasjonalprodukt (BNP) med prognoser for 2020-2023 for utvalgte land, områder og handelspartnere (euroområdet, Sverige, USA, Storbritannia, Danmark, Kina, Sør-Korea, Polen, Russland og Japan). Kilde: Statistisk sentralbyrå.[6]

Det er SSBs vurdering at gjenopphentingen vil ta lengre tid i Europa enn i USA på grunn av en mindre ekspansiv finanspolitikk (Statistisk sentralbyrå, 2020b, s. 8). I tillegg ser amerikanske selskaper ut til å være mer tilpasningsdyktige enn europeiske selskaper. Samtidig pågår stormaktsrivaliseringen mellom USA og Kina (jf. kapittel 4.1.1). Hvis konflikten vedvarer og forsterkes ytterligere, kan dette bidra til å svekke de globale økonomiske vekstutsiktene. Usikkerheten er imidlertid størst når det gjelder utviklingen i Storbritannia. Reduksjon i privat konsum

[6] BNP-tall for fastlands-Norge er hentet fra statistikktabell 12880, mens resterende tall er hentet fra Statistisk sentralbyrå (2020), Tabell 1.1.

stod for 70 % av BNP-fallet i andre kvartal i 2020. Samtidig viser undersøkelser at investeringsviljen er lav, både på grunn av pandemien og på grunn av usikkerhet rundt en eventuell handelsavtale mellom Storbritannia og EU etter Brexit (Statistisk sentralbyrå, 2020b, s. 8).

Selv om de økonomiske konsekvensene av covid-19 har vært store, vil trolig den økonomiske globaliseringen fortsette (Du *et al.*, 2020). Informasjonsteknologi, billig og rask transport, lave tollsatser og felles standarder har vært viktige drivere for økningen i verdenshandel som andel av BNP de siste tiårene (Figur 4.8) (Nordås, 2020). Dette har medført svært komplekse, men effektive globale verdikjeder gjennom spesialisering og internasjonal arbeidsdeling. Likevel er det grunn til å forvente endringer i globale verdikjeder som følge av covid-19-pandemien, spesielt når det gjelder varer og tjenester som er av betydning for nasjonal sikkerhet og beredskap. På lengre sikt vil den økonomiske globaliseringen være avhengig av at internasjonale regler for elektronisk handel (netthandel) kommer på plass (Nordås, 2020).



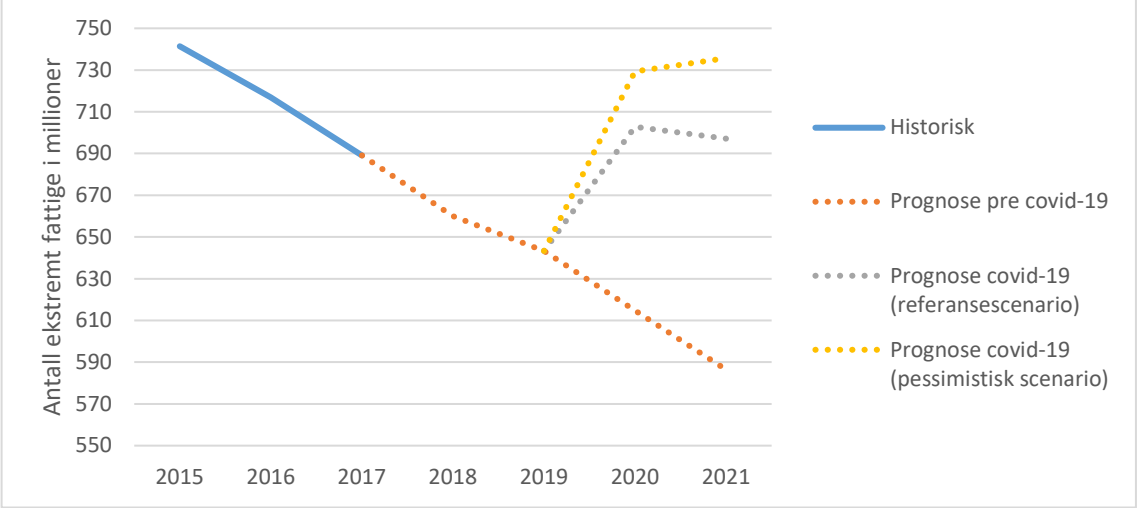
Figur 4.8 Internasjonal handel som andel av bruttonasjonalprodukt. Kilde: Verdensbanken.

For Norge sin del ser de verste økonomiske effektene av covid-19 ut til å være bak oss. Blant annet er antall registrerte helt arbeidsledige personer mer enn halvert fra mars til september 2020. Samtidig mener SSB at ettervirkningene av smitteverntiltakene og den økonomiske nedgangen internasjonalt vil føre til at norsk økonomi vil være i en lavkonjunktur i flere år fremover (Statistisk sentralbyrå, 2020b, s. 10). Det er også mange permitterte som fortsatt ikke er tilbake i jobb. Likevel er det grunn til å forvente at arbeidsledigheten vil synke etter hvert som den økonomiske aktiviteten tar seg opp. SSB anslår derfor at arbeidsledigheten vil bli rundt 4,9 % i 2020 for deretter å gradvis avta til rundt 4 % i 2023 (Statistisk sentralbyrå, 2020b, s. 12).

4.3.2 Fattigdomsutvikling

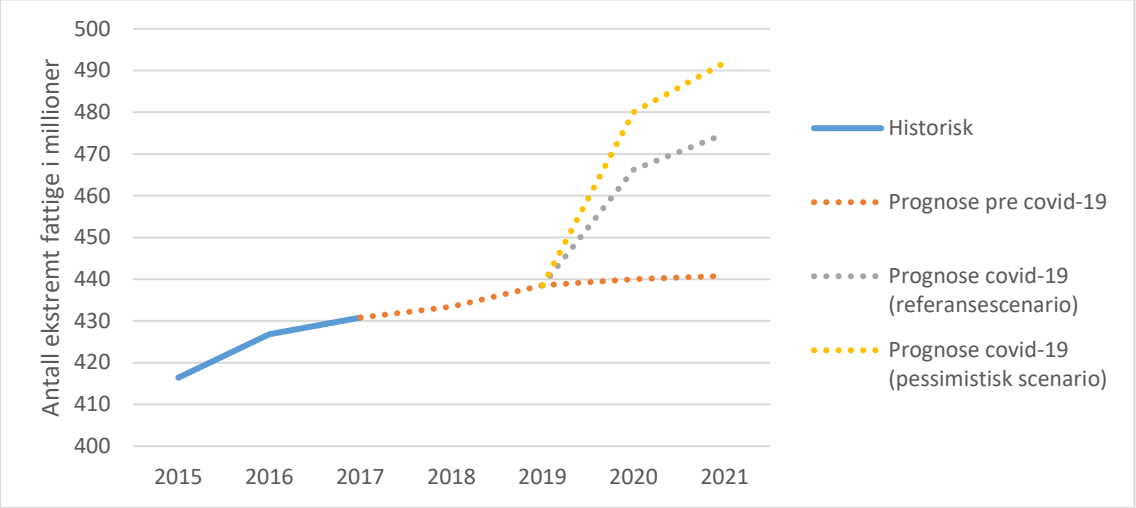
En grunn til bekymring som følge av covid-19-pandemien, er prognosen for økningen i antall mennesker som lever i ekstrem fattigdom[7] på verdensbasis. I 2017 levde 9,2 %, tilsvarende 689 millioner, av verdens befolkning i ekstrem fattigdom (Lakner *et al.*, 2020). Verdensbanken mener nå at pandemien kan føre til at mellom 88 og 115 millioner flere mennesker lever i ekstrem fattigdom sammenliknet med prognostisert andel for 2020 (Figur 4.9) (Lakner *et al.*, 2020). Bare i Afrika sør for Sahara er det ventet at antallet som lever i ekstrem fattigdom skal øke med 26–40 millioner mennesker i 2020 (Figur 4.10). I tillegg vil Nord-Afrika, Midtøsten og Sør-Asia oppleve kraftig økning i fattigdom.

Dette er første gang global fattigdom øker på flere tiår; verdens arbeid med å redusere global fattigdom settes derfor flere år tilbake (United Nations, 2020). I tillegg var mattrygghet utfordret allerede før pandemien. Samtidig vil klimaendringer forsterke problemene knyttet til fattigdom (Sellevåg *et al.*, 2020, s. 20-24). Dersom verdenssamfunnet og landene selv ikke klarer å redusere forventet økning i global fattigdom, vil dette kunne medføre en rekke negative, selvforsterkende effekter som illustrert i Figur 4.11.

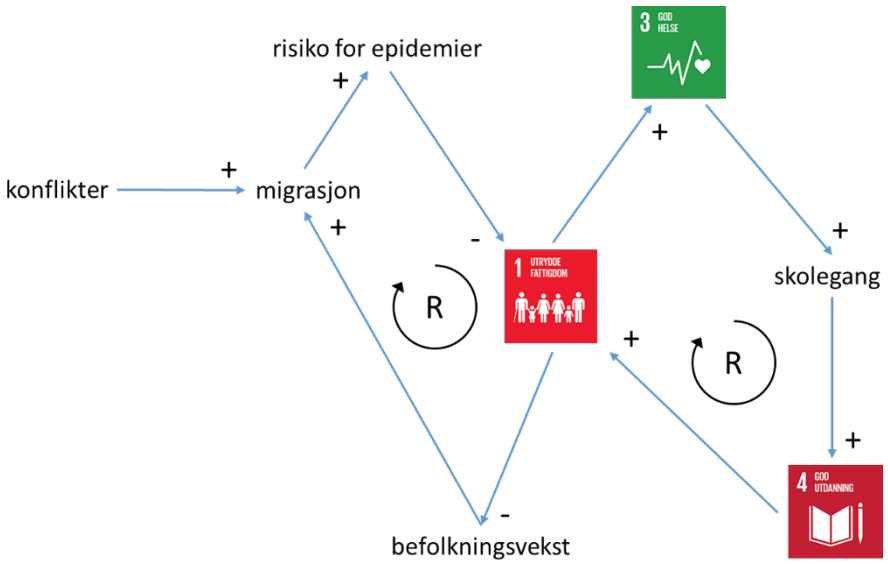


Figur 4.9 Prognose for antall mennesker som lever i ekstrem fattigdom globalt (mindre enn 1.9 USD per dag) (Lakner et al., 2020).

[7] Ekstrem fattigdom er definert som at man har mindre enn 1,9 USD å leve for per dag.



Figur 4.10 Prognose for antall mennesker som lever i ekstrem fattigdom i Afrika sør for Sahara (mindre enn 1.9 USD per dag) (Lakner et al., 2020).



Figur 4.11 Mulige forsterkende effekter (R) relatert til FNs bærekraftsmål om å utrydde fattigdom (etter Cernev & Fenner, 2020).

Ser vi på fattigdomsutviklingen i Norge, fant SSB i sin rapport fra 2019 om økonomi og levekår for lavinntektsgrupper noe større inntektsforskjeller i 2017 enn i 2014. Samtidig hadde andelen av personer med lavinntekt økt. Når studenter holdes utenfor, var det i 2017 i alt 11,2 % av hele befolkningen som tilhørte en husholdning med lavinntekt. Til sammenligning utgjorde andelen av personer med lavinntekt 10,8 % i 2014 og 9,6 % i 2011 (Omholt, 2019, s. 4).

I følge SSB er lavinntekt ofte forbundet med det å stå utenfor eller ha en svak tilknytning til arbeidslivet. Over 65 % av aleneboende med minste alderspensjonsnivå eller minsteytelse for uføretrygd, samt mottakere av sosialhjelp, kvalifiseringsstønad, introduksjonsstønad og supplerende stønad har lavinntekt. Imidlertid er det blant personer med nedsatt arbeidsevne, enslige og par med barn under 18 år og uføretrygdede hvor andelene med lavinntekt har økt mest mellom 2014 og 2017. På den positive siden har andelene med lavinntekt blitt mindre blant innvandrere fra EU/EØS, norskfødte med innvandrerforeldre, langtids arbeidsledige, aleneboende over 67 år og alderspensjonister generelt (Omholt, 2019, s. 4).

Mer bekymringsfullt er det at andelen av personer med vedvarende lavinntekt har økt for hvert år etter å ha vært relativt stabil rundt 8 % i mange år frem til perioden 2010–2012. Selv om Norge har en liten andel av befolkningen under lavinntektsgrensen i internasjonal sammenheng, er andelen barn i lavinntektshusholdninger relativt stor i Norge sammenlignet med nordiske land som Danmark og Finland, og andelen har vokst de siste årene ifølge SSB.

I tillegg fant by- og levekårsutvalget som ble nedsatt i 2018, at den sosioøkonomiske segregeringen i Norge har økt noe de siste tiårene (NOU 2020: 16, s. 13). Spesielt gjelder dette Oslo og Oslo-regionen, hvor det har blitt vanligere å bo enten i et lavinntektsområde eller et høyinntektsområde. Dette gir en opphoping av levekårsutfordringer. Ifølge utvalget ser økt segregering etter inntekt å henge sammen med at innvandrere bor mer segregert enn den øvrige befolkningen. I tillegg ser det ut til at høyinntektshusstander er minst villige til å blande seg med andre grupper. Segregeringen i Oslo ser ut til å være moderat sammenlignet med andre europeiske byer, men resultatene er ikke entydige (NOU 2020: 16, s. 45). Økonomisk ulikhet og segregering i byer har også sammenheng med boligmarkedet og boligpolitikken som føres. Økonomiske forskjeller og hvor attraktive boligområdene er, kan derfor være selvforsterkende prosesser med hensyn på segregering. Utvalget peker derfor på at flytting og offentlige og private aktørers vilje til å investere i boområder kan bidra til å forsterke, opprettholde eller svekke eksisterende segregering og ulikhetsmønstre (NOU 2020: 16, s. 126). Dersom utviklingen går i retning av forsterket segregering og ulikhet, kan dette bidra til å svekke tilliten til den norske samfunnsmodellens legitimitet.

Avslutningsvis skal det sies at det er relativt få som er i risiko for fattigdom eller sosial eksklusjon. I EU-/OECD-sammenheng er Norge blant landene som har minst andel av befolkningen som mangler materielle goder (Omholt, 2019, s. 4).

4.4 Miljø- og klimaforhold

Sammendrag av sentrale utviklingstrekk innen miljø- og klimaforhold:

- Klimaendringer forsterker knapphet på mat og vann.
- Økt politisk vektlegging av klima- og miljøspørsmål.
- Det grønne skiftet medfører gjennomgripende endringer i energi- og transportsystemet.

4.4.1 Klimaendringer

Det er bred enighet om at økt konsentrasjon av drivhusgasser i atmosfæren fører til global oppvarming og klimaendringer, og at dette er tilknyttet menneskelig aktivitet. Global gjennomsnittstemperatur har økt med omtrent 1 °C siden førindustriell tid. De tre siste tiår har vært suksessivt varmere enn alle andre tiår siden 1850, og de siste fire årene er de varmeste som er målt hittil. Observerte klimaendringer inkluderer blant annet økt is- og snøsmelting, økt havnivå, havforsuring, endret nedbørsmønster og stadig mer ekstremvær. Selv om verdenssamfunnet begrenser temperaturstigningen gjennom utslippsreduksjoner, vil overflatetemperaturen forbli høy. Klimaendringer vil derfor få konsekvenser i flere tiår framover (Sellevåg *et al.*, 2020).

Konsekvensene av klimaendringene vil variere i ulike regioner, og er antatt å ramme utviklingsland hardest. Konsekvensene henger ofte sammen, og inkluderer blant annet migrasjon som følge av havnivåstigning, tørke og vannressursmangel, redusert produktivitet i jordbruket, økt sannsynlighet for vektor- og vannbårne sykdommer, hetebølger, økt skogbrannfare og konsekvenser for økosystemer og økosystemtjenester (Pörtner *et al.*, 2019).

Når det gjelder spesifikke konsekvenser for Norge har blant annet CICERO Senter for klimaforskning sett på dette, på oppdrag fra Miljødirektoratet. Noen av hovedfunnene er (Aamaas *et al.*, 2018):

- De mest sannsynlige effektene av klimaendringene er kraftigere nedbør, flere og større regnflommer, stigende havnivå og flere jord-, flom- og sørpeskred.
- Klimaendringer i Norge vil påvirke mange sektorer, hvor trolig jordbruk, skogbruk, fiskeri og oppdrett vil rammes hardest.
- De samfunnsøkonomiske konsekvensene av en temperaturendring i Norge opp mot 2,5 °C for 2031–2060 kan bli forholdvis moderate, men resultatene er usikre.

- Fordi Norge har en åpen økonomi med betydelig eksport og import, er Norge i en internasjonal sammenheng blant landene som er mest utsatt for å bli påvirket av klimaendringer i andre land. Det er imidlertid begrenset kunnskap om hvilke utslag dette kan medføre.

Per 2020 er verdenssamfunnet langt unna å nå målsetningene i Parisavtalen. For at selv togradersmålet skal nås, må de globale utslippene av drivhusgasser falle med 7,6 % hver år fra 2020. Selv med de omfattende reduksjonene i menneskelig aktivitet som følge av covid-19-pandemien, anslås det at utslipp av drivhusgasser bare vil reduseres med rundt 6 % for 2020 på verdensbasis (United Nations, 2020, bærekraftsmål 13).

Når det gjelder sammenhengen mellom klimaendringer og konflikt og vold er det flere syn på hvordan dette kan arte seg. På den ene siden hevder enkelte at redusert tilgang på naturressurser, som følge av klimaendring, uunngåelig vil føre til mer vold, konflikt og fordelingsproblematikk (Barnett & Adger, 2007). På den andre siden finnes det et langt mer positivt syn, hvor det hevdes at klimakrisen er et av få politikkområder som kan lede til mer internasjonalt samarbeid grunnet en felles interesse for å minimere konsekvensene (Beadle *et al.*, 2019).

I den nyeste stortingsmeldingen om politiet pekes det på at hendelser knyttet til ekstremvær, som flom, skred og skogbrann, øker. Effekten av dette er vurdert å være todelt. For det første vil det kunne bli flere og mer omfattende akutte hendelser. For det andre i form av globale utviklingstrekk som økte migrasjonsstrømmer og endrede bosettingsmønstre. Den økte bevisstheten omkring miljø antas å lede til ytterligere regulering og mer tilhørende straffeforfølgning av miljøskadelig virksomhet enn i dag (Meld. St. 29 (2019-2020)).

Den nyeste britiske fremtidsstudien peker på flere sikkerhetsforhold som kan påvirkes av klimaendringer. Blant annet vil endringene kunne kreve at kjøretøy, skip og fly må operere i mer ekstreme forhold. Klimaendringer vil kunne føre til økt migrasjon og mer kamp om naturressurser. Kriminelle, og til og med terrorister, kan tenkes å utnytte seg av utfordringene og påkjenningene klimaendringene medfører (DCDC, 2018).

4.4.2 Forurensning, ressursbruk og tap av naturmangfold

Tap av naturmangfold er økende. Ifølge OECD vil globalt naturmangfold reduseres ytterligere med 10 % frem mot 2050 hvis nye tiltak ikke iverksettes, spesielt i Asia, Europa og sørlige deler av Afrika (OECD, 2012). Dette skyldes særlig bruk av biologiske ressurser (blant annet ved avskoging i tropiske områder), mer intensivt jord- og skogbruk, spredning av fremmede arter, forurensing og bygging av fysisk infrastruktur som følge av global befolkningsvekst og økende forbruk per innbygger kombinert med mangelfull ressursreguleringer. Når det gjelder fiskeriressurser, anslår OECD i samme rapport at mer enn 30 % av verdens fiskebestander er overutnyttet eller utarmet, rundt 50 % er fullt utnyttet og mindre enn 20 % har potensial for økt utnyttelse.

Selv om det har vært noe fremgang, rapporterer FN at kun en tredjedel av landene er på riktig spor med hensyn på å nå bærekraftsmålet om livet på land (United Nations, 2020, bærekraftsmål

15). For livet i havet fortsetter forsuringen av verdenshavene (United Nations, 2020, bærekraftsmål 14).

Samtidig øker verdens behov for naturressurser. Verdens behov for metaller, fossilt brennstoff, biomasse og ikke-metalliske mineraler økte fra 73,2 milliarder tonn i 2010 til 85,9 milliarder tonn i 2017, noe som tilsvarer en økning på 17,4 % (United Nations, 2020, bærekraftsmål 12).

FN rapporterer også at mengden av såkalt EE-avfall[8] fortsetter å øke. Fra 2010 til 2019 økte EE-avfallet fra 5,3 kg til 7,3 kg per capita på global årlig basis. Imidlertid økte gjenvinningen av EE-avfall bare fra 0,8 kg til 1,3 kg (United Nations, 2020). I sin trusselvurdering for 2020 peker Økokrim på at det anslås at rundt 400 000 tonn av EE-avfall eksporteres ulovlig ut fra Europa hvert år (Økokrim, 2020, s. 14). For Norge melder Økokrim at en økende andel av EE-avfallet går utenfor etablerte retursystemer og det estimeres at 4 000 til 10 000 tonn EE-avfall kommer på avveie fra norske mottak per år. Fordi elektrisk utstyr og elektroniske komponenter inneholder tungmetaller og andre miljøgifter, kan behandling av EE-avfall i fattige og sårbare land føre til økt forurensning. Som følge av utviklingen av digitale teknologier og økt etterspørsel av elektroniske produkter (jf. kapittel 4.5), mener Økokrim det grunn til å forvente at illegal handel med EE-avfall vil fortsette (Økokrim, 2020, s. 14).

Skal tapet av naturmangfold reduseres, er det ifølge regjeringens perspektivmelding fra 2017, behov for langt strengere regulering av miljøskadelig aktivitet enn i dag i de fleste land (Meld. St. 29 (2016-2017)).

4.4.3 Det grønne skiftet

Det såkalte «grønne skiftet» handler om hvordan Norge skal bli et lavutslippsland innen 2050, hvor vekst og utvikling skjer innenfor naturens tålegrenser. Dette krever en overgang til betydelig mer miljø- og klimavennlige produkter og tjenester og en omstilling for samtlige samfunnsområder og aktører, skal målene i Parisavtalen nås. Sentrale virkemidler i det grønne skiftet er (Klima- og miljødepartementet, 2020):

- Strategiske satsninger gjennom Norges forskningsråd
- Innovasjon og utvikling av nye energi- og klimaløsninger gjennom Enova
- Investeringer i selskaper med fremtidsrettede løsninger for reduksjon av klimagassutslipp gjennom det statlige investeringsselskapet Nysnø Klimainvesteringer AS
- Tilskuddsordninger til utvikling, bygging og testing av ny miljøteknologi gjennom Innovasjon Norge
- Synliggjøre norsk miljø- og klimateknologi i det globale markedet og trekke internasjonale investorer til Norge ved hjelp av den digitale plattformen The Explorer.

Som tidligere omtalt i Sellevåg *et al.* (2020) med tilhørende referanser, krever det grønne skiftet gjennomgripende endringer i energisystemet skal klimamålene nås. Disse endringene vil foregå langs tre dimensjoner: (*i*) Endringer i den fysiske infrastrukturen for å håndtere større innslag av

[8] EE-avfall er utrangerte elektriske og elektroniske produkter.

fornybar kraftproduksjon, CO_2-innfanging, ladeinfrastruktur og fyllestasjoner for alternative drivstoff som hydrogen; (*ii*) Utnyttelse av elektronisk kommunikasjon og digitale teknologier for å oppnå mer effektiv drift og vedlikehold av energiinfrastrukturen; (*iii*) Etablere kunnskap om hvordan samfunnsmessige, miljømessige og markedsmessige forhold påvirker utviklingen av energisystemet.

Det er også forventet betydelige endringer i transportsystemet som en del av det grønne skiftet. I tillegg til elektrifisering og bruk av andre nullutslippsløsninger, kan såkalte samhandlende intelligente transportsystemer og nye forretningsmodeller som delingsmobilitet, bidra til en mer bærekraftig transportsektor (*Teknologi for bærekraftig bevegelsesfrihet og mobilitet*, 2019).

Skal det grønne skiftet realiseres mener forskere ved FME CenSES som er et nasjonalt forskningssenter for studier av bærekraftig energiomstilling, at det er behov for nytenkning om samfunnets organisering. Blant annet peker forskerne på behov for ny kunnskap om hvordan eksisterende teknologier og infrastrukturer kan fases ut for å unngå å bli «lukket inne» med gamle løsninger. I tillegg er det behov for å få eksisterende løsninger til å «snakke sammen» på tvers av sektorer, samfunnsfelt og teknologier. Dette krever ny kunnskap om hvordan politikk, regulering og markedsdesign kan legge til rette for vellykket sektorsamspill (Andersen *et al.*, 2019). I denne forbindelse kan det nevnes at EU-kommisjonen ser på muligheter for å styrke samspillet mellom energiinfrastrukturen i EUs medlemsland gjennom det såkalte «Trans-European Networks for Energy» (European Commission, 2020).

4.5 Teknologisk utvikling

Sammendrag av sentrale utviklingstrekk innen teknologisk utvikling:

- Større spredning av avansert teknologi til nye aktører, både statlige og ikke-statlige.
- Fortsatt digital transformasjon og videreutvikling av det såkalte «smartsamfunnet».
- Omfanget av person- og befolkningsdata vil bli større som et resultat av den digitale transformasjonen. Dette vil føre til at utnyttelse av slike data får større økonomisk verdi. Samtidig vil det bli sterkere fokus på personvern.

4.5.1 Generelt om teknologiutviklingen

Teknologisk utvikling er en av de store endringsdriverne i samfunnet. Oppbyggingen av den norske oljeindustrien og innføring av IKT-baserte betalingstjenester er noen eksempler på hvordan teknologiutviklingen kan føre til samfunnsendringer når rammebetingelsene er tilstede eller når det skjer endringer i oppgavene som ønskes løst (Skule & Grytli, 1997). Kommunikasjonsteknologi, informasjonsteknologi, skybaserte tjenester, kunstig intelligens (AI), tingenes inter-

nett (IoT), robotisering og autonome systemer, romteknologi og rombaserte tjenester, kvanteteknologier, samt syntetisk biologi og bioteknologi er alle eksempler på teknologier som vil gi muligheter og utfordringer for samfunnssikkerheten frem mot 2030 (Sellevåg *et al.*, 2020, s. 31-55). Det samme vil teknologier som additiv tilvirkning, blokkjeder og sensorer. I tillegg til våpenutvikling innen eksempelvis missiler, masseeffektvåpen, direktive energivåpen og presisjonsstyrt ammunisjon, vil mange av de ovennevnte teknologiområdene også være drivende for den militærteknologiske utviklingen (Andås, 2020; Forsvarets forskningsinstitutt, 2016).

Teknologiutviklingen kjennetegnes også ved at de ulike teknologiområdene nevnt ovenfor, samspiller med hverandre for å gi oss nye og bedre tjenester og produkter. Dette fenomenet omtales gjerne som *konvergens*, og er spesielt synlig innenfor utviklingen av informasjons- og kommunikasjonsteknologi (IKT). Eksempelvis kan man si at dagens smarttelefon er en sammensmelting av blant annet den tradisjonelle mobiltelefonen, fotokameraet, GPS-mottakeren og datamaskinen. Et annet kjennetegn er at mange av teknologiområdene har potensial for *disruptiv innovasjon*, det vil si, utvikling av nyskapende teknologier som forstyrrer et eksisterende marked (Christensen *et al.*, 2015). Apples lansering av iPhone i 2007 er et eksempel på en disruptiv innovasjon som forstyrret og overtok datidens eksisterende mobiltelefonmarked.

Norge er et av landene som ligger lengst fremme i Europa når det gjelder å ta i bruk digitale teknologier, også når det gjelder barn og unge (European Commission, 2019). Covid-19-pandemien har ført til at digitale teknologier har blitt tatt i bruk i enda større grad; ikke bare i næringslivet og i offentlig sektor med økende bruk av digitale hjemmekontorløsninger, men også i helsevesenet med økt utvikling og bruk av digitale smittesporingsteknologier og helsekonsultasjoner via internett. Samtidig ser man at covid-19-pandemien og økt bruk av digitale tjenester utnyttes av kriminelle (Interpol, 2020; Nasjonal sikkerhetsmyndighet, 2020b; Politiet, 2021). Kriminalitet i det digitale rom vil beskrives nærmere i kapittel 5.5.2.

I det følgende beskrives noen fremtidige utfordringer for utvalgte teknologiske områder som har potensial for konvergens og disrupsjon. Utvalget er basert på vurderinger av teknologisk utvikling i FFI-rapporten «Samfunnssikkerhet mot 2030 – utviklingstrekk» (Sellevåg *et al.*, 2020), Europols vurdering av teknologier som kan være av betydning for alvorlig og organisert kriminalitet (Europol, 2017a, 2017c), samt teknologier som er av militærteknologisk betydning (Andås, 2020). De utvalgte teknologiområdene er: (*i*) kryptografi, (*ii*) kunstig intelligens («Artificial Intelligence»; AI), (*iii*) tingenes internett («Internet of Things»; IoT), (*iv*) autonome systemer og droneteknologi, (*v*) additiv tilvirkning, samt (*vi*) syntetisk biologi og bioteknologi. Omtalen av teknologiområdene er basert på en vurdering av hvilke utfordringer de kan medføre for politiet, PST og påtalemyndigheten i tiden frem mot 2030 dersom adekvate sikkerhetsløsninger eller andre forebyggende eller avhjelpende tiltak ikke iverksettes.

4.5.2 Kryptografi og digital sikkerhet

4.5.2.1 Konfidensialitet og anonymitet

Bruk av kryptografi er en forutsetning for sikker informasjonsutveksling. I «Digital sårbarhet – sikkert samfunn» kom Lysne-utvalget med en sterk anbefaling om at innbyggernes bruk av

kryptografi ikke burde reguleres (NOU 2015: 13, s. 307). Denne tilrådingen ble tatt til følge i Meld. St. 38 (2016-2017) (s. 81), der Regjeringen slår fast at «tilgang til robuste krypteringsmetoder er en forutsetning for å kunne kommunisere med trygghet […]».

Utviklingen de siste årene er i tråd med denne forventningen. Introduksjonen av den såkalte Signal-protokollen var en betydelig utvikling, og protokollen har svært sterke sikkerhetsegenskaper. Først og fremst er den i bruk i Signal selv, men den er også implementert i blant annet WhatsApp og Facebook Messenger. Hvem som helst kan derfor beskytte samtalene sine med ende-til-ende-kryptering med veldig lav teknisk terskel. Det er ingen grunn til å tro at denne trenden skal snu. Enkeltpersoner har altså en historisk god mulighet til å beskytte sitt eget privatliv. I tillegg har det blitt mye vanligere å bruke TLS-protokollen for å sikre trafikk til nettsider og andre tjenester. TLS krypterer trafikken slik at den blir utilgjengelig for uvedkommende, og gjør det mulig for brukeren å verifisere at hun bruker den nettsiden hun faktisk ønsker å bruke. Tidligere var den primært brukt til særlig verdifulle tjenester, som nettbank, Altinn og andre sensitive tjenester som krever innlogging.

Mange bruker også virtuelle private nettverk (VPN). Med VPN oppretter man en sikker kanal fra egen datamaskin og til endepunktet for nettverket. Brukerens egen internettleverandør kan da bare se at det foregår kryptert trafikk mellom brukeren og VPN-leverandøren, men kan ikke se hvilke tjenester brukeren kobler seg til. En vanlig anvendelse er å bruke en VPN med endepunkt i et annet land, slik at man kan bruke nettjenester som er geografisk begrenset, for eksempel filmutvalget i Netflix. VPN-tjenester blir ofte framstilt som et sikkerhetstiltak. Det forutsetter imidlertid leverandøren er pålitelig og ikke påvirker eller kartlegger brukerens trafikk.

En mer avansert måte å forsøke å skaffe seg anonymitet på internett er gjennom såkalt løk-ruting, for eksempel *The Onion Router* (TOR). I slike nettverk kobler brukeren seg til et endepunkt med en kryptert forbindelse. Forespørselen fra brukeren blir da videresendt gjennom flere punkter i nettverket. Hver node kan blande forespørselen sammen med andre forespørsler og fjerne lag på lag med kryptering inntil den virkelige forespørselen til en annen nettjeneste kommer ut på den andre siden av nettverket. Det er vist at det er tilstrekkelig at motstanderen kontrollerer et relativt lite antall maskiner i et slikt nettverk før mye av sikkerheten forsvinner (Galteland & Gjøsteen, 2018).

Privatpersoner og bedrifter har også mye bedre tilgang til sterk diskkryptering nå enn tidligere. Det kan gjøre det vanskeligere å hente ut bevis fra beslaglagt materiale hvis utstyrets eier ikke ønsker å samarbeide. Det er å forvente at sterk diskkryptering vil bli standard i løpet av de neste årene.

4.5.2.2 Blokkjeder og kryptovaluta

En annen trend de siste årene er utviklingen av digital valuta, som Bitcoin, Monero og Ethereum. Disse er basert på et konsept som kalles *blokkjede*. Man kan abstrahere konseptet som en skrivebeskyttet logg med noe ekstra funksjonalitet. Hver blokk inneholder ny informasjon i tillegg til å ta med en sjekksum av forrige blokk. Dermed er det ikke lenger mulig å endre tidligere blokker uten at det også utløser et behov for å oppdatere alle senere blokker i tillegg.

Dersom man har en sentralisert myndighet kan denne vedta hva som er neste blokk. Imidlertid er blokkjeder ment å være distribuerte, som betyr at man er avhengig av en mekanisme for å oppnå enighet blant brukerne om hva som er gjeldende blokker.

Mekanismen for å gjøre dette i Bitcoin er *proof of work*, som essensielt sett er et selv-verifiserende lotteri med veldig lav vinnersjanse. Den som først trekker det store tallet som vinner lotteriet, vinner en premie (det er dette som er omtalt som *mining*), og blokken blir distribuert blant alle andre. Fordi det er så vanskelig å vinne lotteriet er det stor sjanse for at en ny blokk har bygd på denne innen noen andre har greid å finne en alternativ blokk. Dermed er den for alltid støpt inn i kjeden. Det er en enorm energisløsing knyttet til proof of work, og det jobbes derfor med alternative innfallsvinkler, som *proof of stake*. Ingen har hittil hatt samme suksess som Bitcoin. Legg merke til at disse teknikkene primært sørger for integritet, og ikke konfidensialitet. I blant annet Monero er det i tillegg gjort ekstra grep for å sørge for konfidensialitet (både mottaker og avsenders identitet er skjult).[9]

På grunn av problemene med energiforbruk – og mer fundamentalt det underliggende konsensusproblemet – er praktisk bruk av digitale valutaer ikke allment utbredt ennå. I mange av de foreslåtte anvendelsene av blokkjeder forventes det at det vil være mer hensiktsmessig å bruke enklere konstruksjoner for å beskytte integriteten til en offentlig logg.

4.5.2.3 Kvantedatamaskiner og nye teknikker innen kryptografi

Som nevnt i Sellevåg *et al.* (2020), er en kvantedatamaskin fundamentalt annerledes enn en vanlig datamaskin med hensyn til hvordan logiske operasjoner utføres. På grunn av måten de logiske operasjonene utføres på, vil det være usikkerhet i informasjonen som produseres. Kvantedatamaskiner må derfor foreløpig betraktes som avanserte problemløsere som kan anvendes på områder hvor dagens datamaskiner ikke kan benyttes. Det er særlig to anvendelsesområder som trekkes frem (Government Office for Science, 2016): faktorisering av store tall og søk gjennom store mengder ustrukturerte data, hvor sistnevnte kan gi helt nye muligheter for dataanalyse og maskinlæring (jf. kapittel 4.5.3).

Når det gjelder det første anvendelsesområdet, står mye av dagens kryptografi i fare for å bli verdiløs dersom noen greier å konstruere en tilstrekkelig stor kvantedatamaskin. På grunnlag av teoretisk arbeid fra 1990-tallet vet vi at etablerte teknikker for såkalt asymmetrisk kryptografi vil være sårbare. Det foregår for øyeblikket arbeid med å standardisere nye teknikker som skal kunne motstå en kvantedatamaskin, og de er forventet klare i løpet av perioden 2022–2024.

Det er langt frem til kvantedatamaskiner vil erstatte vanlige datamaskiner, hvis det noen gang vil skje. En kapabel kvantedatamaskin er derfor antageligvis primært et verktøy for fremmede stater for å forsøke å få tak i svært sensitiv informasjon, mens ikke-statlige aktører nok vil fortsette med å benytte seg av sosial manipulasjon og svakheter i implementasjoner for å skaffe seg adgang til opplysninger.

[9] I forbindelse med forsvinningssaken på Lørenskog hvor Anne-Elisabeth Falkevik Hagen forsvant 31. oktober 2018, ble det fremmet krav om løsepenger gjennom Monero.

I forbindelse med trusselen fra kvantedatamaskiner trekkes det også ofte fram muligheten for å gjøre sikker nøkkelutveksling med kvantemekaniske prinsipper (såkalt *quantum key exchange*). Selv om teknikken forankrer beviselig sikkerhet i fysiske lover er det likevel flere praktiske utfordringer, og det er nødvendig med en egen, parallell infrastruktur for å gjennomføre slik nøkkelutveksling. Det forventes ikke at den vil være til særlig praktisk nytte i tiden frem mot 2030.

Det finnes også nye teknikker innen kryptografi som kan styrke sikkerheten til privatpersoner, bedrifter og andre. Gjennom sikre flerpartsberegninger (*secure multiparty computation*; MPC) er det mulig å distribuere data og beregninger på flere parter slik at man kan gi absolutte garantier for at det er umulig for den enkelte å lese sensitiv informasjon. Forutsatt at ikke for mange samarbeider om å opptre uærlig vil de øvrige partene kunne verifisere at beregninger har blitt utført korrekt. For eksempel kan bedrifter trygt beregne felles statistikk uten å røpe sine egne sensitive data, og på en slik måte at man ikke trenger å stole på en ekstern tredjepart. MPC har gjennomgått en betydelig modning de siste årene.

4.5.2.4 Sikker digital autentisering

Det har blitt vanligere å bruke flerfaktorautentisering for å logge inn på nettjenester. Ved å bruke mer enn ett passord sikrer man at en konto ikke kommer på avveie dersom passordet blir kjent, og at en angriper i tillegg er avhengig av å ha kontroll over for eksempel brukerens telefon, eller i mer avanserte tilfeller: smartkort eller dedikerte enheter. Det er vanlig å bruke SMS som en andre faktor. Selv om det kan være bedre enn passord alene er SMS ikke en sikker kanal som garanterer beskyttelse mot overvåkning. Blant annet kan SMS som metode for tofaktorautentisering omgås gjennom såkalte «SIM-swap-angrep», hvor en trusselaktør får overbevist kundeservice til mobiltilbyderen til offeret om at de har mistet mobilen og må flytte abonnementet over på et nytt SIM-kort som trusselaktøren kontrollerer (Europol, 2020c).

BankID er en elektronisk legitimasjon for sikker identifisering og signering på nett, som brukes til å logge inn i alle norske banker. BankID har blitt en vanlig autentiseringsløsning også til mange andre nettsteder enn hos bankene selv. Selv om sikkerheten til BankID og andre løsninger for sikker digital autentisering stadig blir bedre, må man forvente at kriminelle aktører både vil utnytte eksisterende svakheter og finne nye måter å misbruke eller omgå slike tjenester som et ledd i bedragerier eller ID-tyverier.

Avslutningsvis kan man si at kryptografi har gått fra noe som i all hovedsak ble brukt for å beskytte seg mot enkeltpersoner, til situasjonen i dag hvor privatpersoner i langt større grad bruker kryptografi til å beskytte seg selv. Det er ingen grunn til å tro at denne trenden vil endre seg. Det er heller ingen grunn til å tro at et forsøk på å begrense trenden vil gjøre det enklere å avsløre forsøk på gjennomføring av kriminelle handlinger eller terrorisme, men det vil derimot kunne føre til dårligere beskyttelse for alle andre.

4.5.3 Kunstig intelligens

Kunstig intelligens (engelsk: «artificial intelligence», AI) handler om å få maskiner til å utføre oppgaver som normalt krever menneskelig intelligens. Eksempler på slike oppgaver kan være

tolkning av tale, språkoversettelse eller gjenkjenning av objekter i bilder. Maskinlæring og såkalt dyp læring er eksempler på metoder innen kunstig intelligens som kan benyttes for å løse slike oppgaver.

Interessen for kunstig intelligens har variert i perioder, men siden 2012 har det vært en kraftig økning i utnyttelsen av AI. Sentralt i denne utviklingen har vært tilgang på store datamengder og tilstrekkelig regnekraft. Det foregår derfor et kappløp mellom USA, Kina og EU om å bli verdensledende på teknologier innen kunstig intelligens, og det ventes at kunstig intelligens vil ha en rekke nyttige anvendelser innen sektorer som transport, helse- og omsorg, utdanning og øvrig næringsliv, men også i hjemmet og til underholdning (Stone *et al.*, 2016).

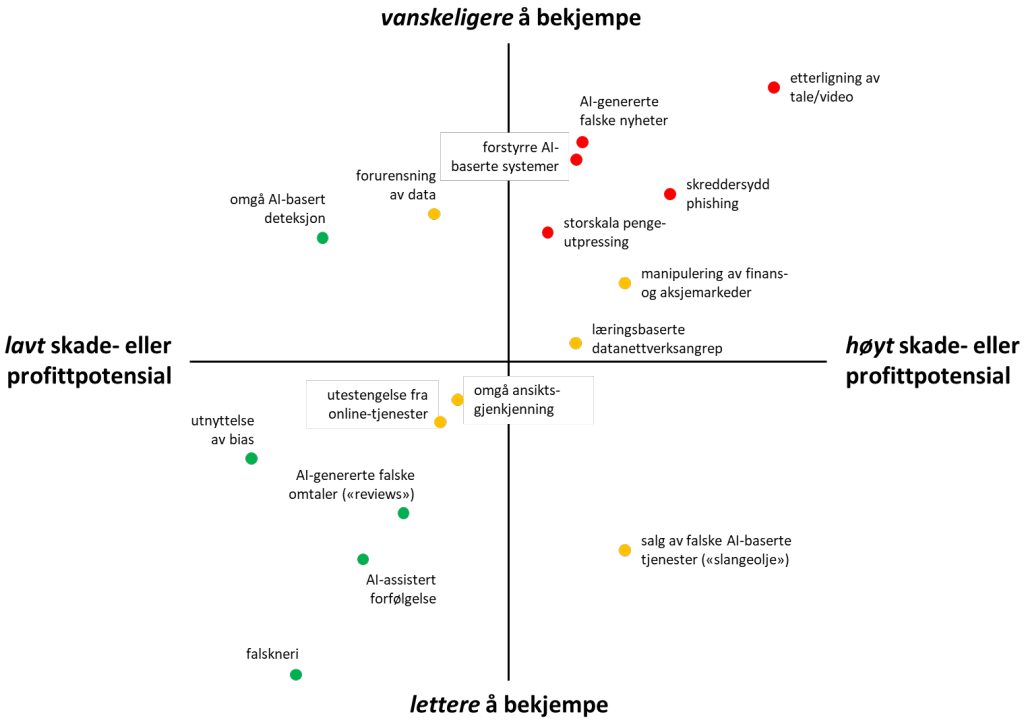
Samtidig kan kunstig intelligens utnyttes av trusselaktører med ondsinnede hensikter. Dette kan skje på ulike måter som ikke er gjensidig utelukkende (Caldwell *et al.*, 2020). For det første kan kunstig intelligens brukes som et virkemiddel for å begå (tradisjonelle) lovbrudd i det digitale rom. For det andre kan AI-baserte systemer være målet for den tilsiktede handlingen. Til slutt kan kunstig intelligens inngå i konteksten for den kriminelle handlingen, hvor for eksempel noen bedras til å kjøpe en AI-basert tjeneste som ikke eksisterer eller er mulig.

Forskere ved Dawes Centre for Future Crime ved University College London (UCL) publiserte i 2020 en studie hvor de hadde undersøkt mulige former for kriminalitet basert på eller fasilitert gjennom bruk av AI (Caldwell *et al.*, 2020). Resultatene fra studien er oppsummert i Figur 4.12 (autonome systemer og droneteknologi omtales i kapittel 4.5.6). Av de identifiserte kriminalitetsformene, er fem fremhevet som særlig bekymringsfulle på grunn av deres skadepotensial og vanskeligheter forbundet med bekjempelse av kriminalitetsformene (Tabell 4.1).

Etterligning av personers tale eller opptreden på video (såkalte «deepfakes») ble vurdert å ha høyt skadepotensial og lett å gjennomføre (Caldwell *et al.*, 2020). Selv om det pågår utvikling av teknologiske mottiltak mot deepfakes, ble deepfakes likevel vurdert som vanskelig å bekjempe. Potensialet for misbruk av denne teknologien er derfor stort; noen eksempler er sosial manipulasjon, bedrageri, utpressing eller ID-misbruk. Forskere har også vist at det er mulig å lure «state-of-the-art» ansiktsgjenkjenningsalgoritmer (Korshunov & Marcel, 2019), noe som kan gi tilgang til systemer som er beskyttet av slike algoritmer (SySS, 2018).[10]

Kunstig intelligens er et verktøy som også kan benyttes til å lage falske nyheter. For eksempel kan teknologien benyttes til å lage mange versjoner av samme falske nyhet slik at det ser ut som den kommer fra flere ulike kilder, noe som vil gi økt synlighet og kredibilitet til den falske nyheten. Det vil også gjøre det enklere å skreddersy innholdet til ulike personer. I studien til UCL ble gevinsten for kriminelle vurdert som lav (Tabell 4.1), men dette vil ikke gjelde for fremmede staters påvirkningsaktiviteter i sosiale medier (Bergh, 2019).

[10] Se også https://github.com/mitre/advmlthreatmatrix/blob/master/pages/case-studies-page.md#mitre---physical-adversarial-attack-on-face-identification.



Figur 4.12 Kvalitativ vurdering av vanskelighet med å bekjempe versus skade-/profittpotensialet til ulike former for kriminalitet basert på eller fasilitert av bruk av kunstig intelligens (AI). Kriminalitetsformer med høyest og lavest farepotensial er markert med henholdsvis rødt og grønt. Kilde: Caldwell et al. (2020).

Tabell 4.1 Kvalitativ vurdering av skadepotensial, gevinst for kriminelle, gjennomførbarhet og vanskeligheter med å bekjempe for fem AI-relaterte kriminalitetsformer av høy bekymring. Kilde: Caldwell et al. (2020).

AI-relaterte kriminalitetsformer av høy bekymring	Skade-potensial?	Gevinst for kriminelle?	Gjennom-førbarhet?	Vanskelig å bekjempe?
Etterligning av tale/video	Høy	Middels	Høy	Høy
Skreddersydd phishing	Middels	Høy	Høy	Høy
Forstyrre AI-baserte systemer	Høy	Høy	Lav	Høy
Storskala pengeutpressing	Middels	Høy	Lav	Høy
AI-genererte falske nyheter	Høy	Lav	Høy	Høy

Fordi kunstig intelligens gjør det mulig å generere troverdig tekst, tale, bilde og video, vil teknologien gjøre det lettere å gjennomføre såkalte phishingangrep via skreddersydd innhold.

Det er også mulig å gjennomføre utpressing i stor skala fordi kunstig intelligens gjør det lettere å finne spesifikke sårbarheter i store mengder innsamlede og potensielt sensitive persondata. Utfordringen for ikke-statlige aktører er at det kan være krevende å samle så store datamengder som vil være nødvendig for å kunne gjennomføre pengeutpressing i stor skala (Tabell 4.1). Fremmede stater vil imidlertid i mindre grad være begrenset av dette, og kunstig intelligens kan bidra til å gjøre det lettere å identifisere sårbare personer som kan utnyttes i etterretnings- og påvirkningsøyemed.

Det er også mulig å forstyrre, lure eller omgå AI-baserte systemer. Angrep mot maskinlæringssystemer til blant annet Google (Ray, 2018), Amazon (Diaz, 2018), Microsoft (Hunt, 2016) og Tesla (Ackerman, 2019) er nylige eksempler på dette. Det foregår derfor et betydelig arbeid, blant annet i regi av MITRE,[11] for bedre å forstå trusler mot AI-baserte systemer. I rammeverket som er etablert av MITRE i samarbeid med blant annet Microsoft og IBM, er følgende kategorier foreslått for angrep mot maskinlæringssystemer (kategoriene er dataagnostiske):[12]

- *Modellomgåelse («model evasion»):* En angriper modifiserer en spørring mot systemet for å få ønsket resultat. Slike angrep foregår ved iterativt å spørre en modell og observere resultatet (angrep mot beslutningsprosessen).

- *Funksjonalitetsutvinning («functional extraction»):* En angriper klarer å utvinne en funksjonelt ekvivalent modell gjennom iterativt å spørre modellen. Dette tillater en angriper å undersøke den frakoblede kopien av modellen før videre angrep på modellen som er online (angrep mot beslutningsprosessen).

- *Modellforurensing («model poisoning»):* En angriper forurenser treningsdataene til maskinlæringssystemet for å oppnå et ønsket utfall i beslutningsprosessen (angrep mot treningsprosessen). Når en angriper kan påvirke treningsdataene, er det mulig å lage «bakdører» for videre angrep. For eksempel kan modellen «reprogrammeres» til å gjennomføre en uønsket oppgave. Tilgang til treningsdataene kan også resultere i kompromittering av sensitive data.

- *Modellinversjon («model inversion»):* En angriper klarer å utvinne egenskaper/faktorer som ble brukt for å trene modellen, noe som kan resultere i kompromittering av sensitive data (angrep mot beslutningsprosessen).

- *Tradisjonelle angrep:* En angriper bruker kjente taktikker, teknikker og prosedyrer for å oppnå sine målsetninger (angrep mot både trenings- og beslutningsprosessen).

[11] Se for eksempel https://github.com/mitre/advmlthreatmatrix.
[12] https://github.com/mitre/advmlthreatmatrix/blob/master/pages/adversarial-ml-101.md#adversarial-machine-learning-101.

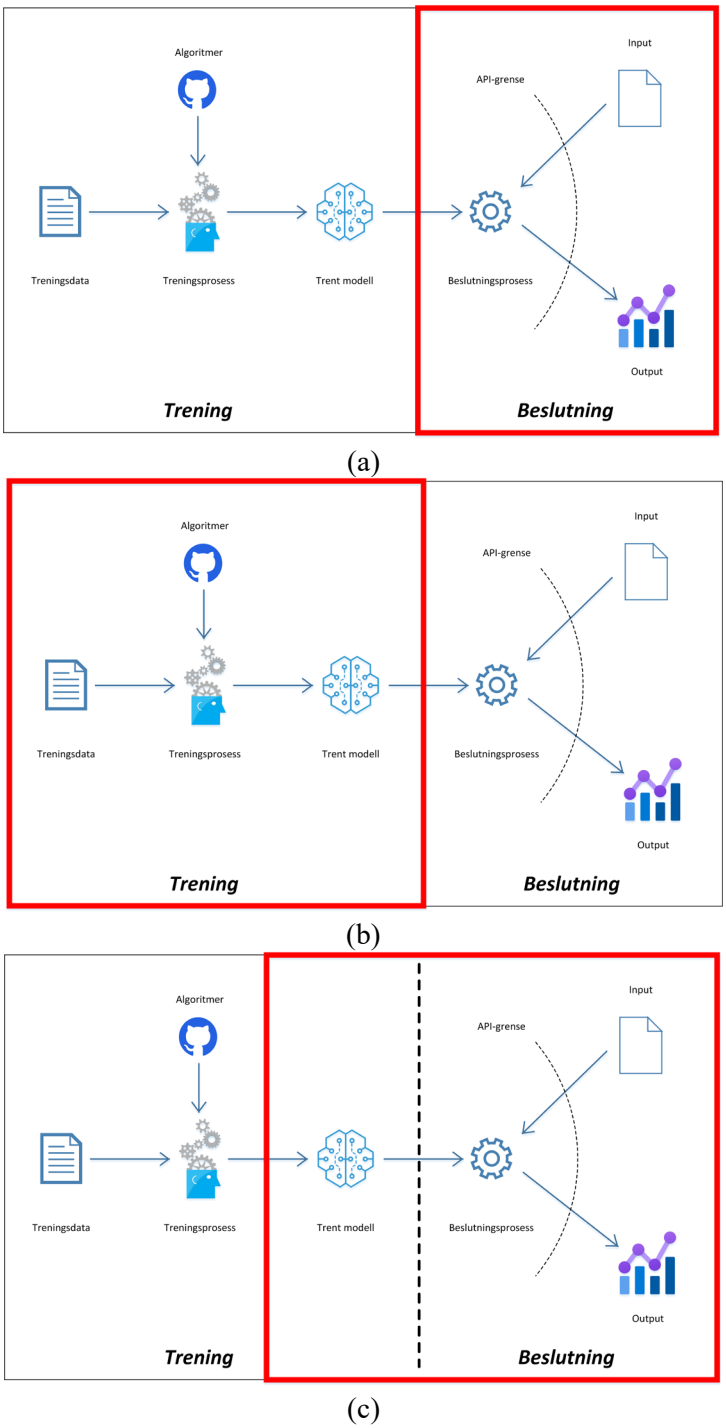
Angrepsscenarioer mot trenings- og/eller beslutningsprosessen er illustrert i Figur 4.13. Et eksempel på modellforurensning, det vil si et angrep på treningsprosessen, er det koordinerte angrepet mot Microsofts chatbot «Tay» på Twitter som resultert i at Tay begynte å uttrykke rasistiske og nedsettende meninger (Hunt, 2016). Som et eksempel på angrep mot beslutningsprosessen, viste forskere ved UC Berkeley i 2020 hvordan det er mulig å stjele IPR fra en språkoversettingstjeneste (Wallace *et al.*, 2020).

Angrepskategoriene nevnt ovenfor er ingen uttømmende liste og det etableres hele tiden ny kunnskap om både hvordan AI-baserte systemer kan angripes og hvordan AI kan misbrukes (Brundage *et al.*, 2018; Kaloudi & Li, 2020; King *et al.*, 2020). Generelt er det grunn til å forvente at kunstig intelligens vil bidra til (*i*) økt omfang av eksisterende digitale trusler fordi AI kan gjøre det lettere å automatisere oppgaver som ellers ville vært utført av mennesker, (*ii*) introduksjon av nye digitale trusler og (*iii*) endringer i karakteren til selve trusselen (eksempelvis mer målrettet og vanskeligere å attribuere) (Brundage *et al.*, 2018).

I hvilken grad er så offentlige etater, næringslivet og andre aktører forberedt på denne utviklingen? I en intervjuundersøkelse gjennomført av Microsoft i 2020 (Kumar *et al.*, 2020), ble det funnet at 25 av 28 små og store organisasjoner (offentlige, private og veldedige) ikke visste hvordan de skal sikre sine maskinlæringssystemer. Som én respondent svarte (Kumar *et al.*, 2020):

> *Traditional software attacks are a known unknown. Attacks on our ML [machine learning] models are unknown unknown.*

Studien til Microsoft peker på en rekke kunnskapshull som krever oppmerksomhet, både i implementeringsfasen og når et maskinlæringssystem utsettes for et datanettverksangrep. Et særlig relevant kunnskapshull for politi- og påtaletjenestene er hvordan meningsfull sporsikring skal gjøres når et maskinlæringssystem utsettes for angrep. Det henvises til Microsofts studie for en nærmere beskrivelse av disse utfordringene (Kumar *et al.*, 2020).



Figur 4.13 Mulige angrepsscenarioer (markert med rød ramme) mot maskinlæringssystemer: (a) Angrep mot beslutningsprosessen; (b) Angrep mot treningsprosessen; (c) Angrep mot en klient eller mot en IoT-ting i kanten av nettverket. Kilde: MITRE (https://github.com/mitre/advmlthreatmatrix/blob/master/pages/adversarial-ml-101.md#adversarial-machine-learning-101).

4.5.4 Sosiale medier og algoritmenes betydning

Sosiale medier har siden slutten på 2000-tallet hatt en eksplosiv vekst og i dag benytter de fleste nordmenn under 54 år sosiale medier daglig (Statistisk sentralbyrå, 2020a). Globalt har sosiale medier over 3,5 milliarder brukere (Rolandsen, 2021) og er en stadig voksende kilde til nyheter, spesielt blant yngre grupper. Sosiale medier er resultatet av konvergenser mellom en rekke program- og maskinvareteknologier, eksempelvis chatteprogrammer og nettlesere, sensorer og digitale kameraer. Disse og en rekke andre teknologier er omforent gjennom apper, internasjonale skytjenester og AI (spesielt maskinlæring). Brukerne kan benytte disse mediene på en rekke plattformer, fra jobb-PCer til smarttelefoner og smartklokker. Resultatet er en kontinuerlig toveis strøm av informasjon – alt fra brukernes geografiske posisjon eller direkte video av demonstrasjoner, til personlig meldinger fra venner eller Twitter-nyheter fra politiet.

Dette gir sosiale medier egenartede egenskaper som er tilgjengelig gratis for alle brukere: anonymitet, ubegrenset lagring av alt innhold som legges ut, umiddelbar distribusjon av innlegg uten geografiske begrensinger og et felles utseende på alle innlegg uansett opphav. Alt dette er tilgjengelig gjennom smarttelefoner og nettbrett 24 timer i døgnet uansett hvor man befinner seg hvor internett er tilgjengelig. Sosiale medier har ikke noe redaksjonelt ansvar; det er derfor kun et brøkdel av innlegg som vurderes av mennesker før de formidles. Det er disse egenskapene som gjør sosiale medier til et unikt, og unikt nyttig, verktøy for aktører som ønsker å anonymt påvirke eller skade andre utenfor sin egen geografiske tilhørighet, enten målet er stater, regioner, sosiale grupper eller individer. Slike aktører benytter hva man kan kalle «algoritmisk krigføring» (Layton, 2018) for å manipulere sosiale medie-plattformer til å distribuere sitt innhold.

Sosiale medier distribuerer innhold gjennom *algoritmer* som søker blant brukere for å finne et relevant publikum for innholdet. Innenfor IT er algoritmer en «oppskrift» som løser en oppgave, for eksempel hvordan man skal sortere navn alfabetisk. På sosiale medier benyttes algoritmer først for å analysere de enorme mengdene data som skapes i form av innlegg som tekst eller video og metadata som geografisk posisjon. Slike analyser gir en detaljert forståelse av hva informasjonen representerer. Tekst kan analyseres så man ser at katter og hunder er noe mennesker har et forhold til og at de tilhører gruppen «dyr». Brukernes handlinger på plattformen analyseres også. Hva velger de å lese, like, svare på, hvor lang tid bruker de på forskjellige aktiviteter og hvilke relasjoner har de til andre brukere? Disse oppgavene løses i hovedsak med maskinlæring (jf. kapittel 4.5.3). Det er denne kombinasjonen av oppskrifter og maskinlæring som klassifiserer informasjon og interesser man referer til når man snakker om algoritmer i sosiale medier.

Denne kunnskapen benyttes deretter av andre algoritmer som er utviklet for å få mest mulig oppmerksomhet fra brukerne, blant annet for reklame. Dette gjøres ved å koble innhold med brukeres interesser – katteelskere tilbys mer kattebilder og reklame for kattemat. Det er disse algoritmene angripere prøver å manipulere for å spre sin informasjon bredest mulig, til personer kan tenkes å være mottakelige for innholdet. Manipuleringen kan benytte kvantitative virkemidler som øker antall likerklikk eller delinger for et innlegg ved bruk av såkalte *click farms* i lavkostland eller bots (automatisert programvare). Da vil algoritmene anse temaet i innlegget som populært og tilby det til flere brukere eller vise det i lister over populære emner. Det kan også skje kvalitativt ved å benytte visse emneknagger eller nøkkelord som allerede er populære på de

individuelle sosiale medie-plattformene, noe som kan spre innholdet til brukere som allerede er interessert i emnet. Man kan også kombinere dette med andre tilnærminger. Trolling kan benyttes for å angripe kritiske røster i sosiale medier for å stoppe visse synspunkter fra å komme til i en debatt.

Dersom desinformasjon (bevisst feilinformasjon) og misinformasjon (feilinformasjon man tror er sann) spres i stor nok skala kan vanlige brukere få en fordreid virkelighetsoppfatning. Slik kan de bli en ressurs for aktøren som står bak algoritme-manipuleringen. For politi- og påtaletjenestene vil det være mange situasjoner hvor des- og misinformasjon skaper problemer som en del av et sammensatt trusselbilde. Overordnet kan man si at spredning av desinformasjon kan ha et langtidsperspektiv med relativt brede mål, eller det kan være mer spesifikt og kortsiktig i forbindelse med en aktuell situasjon.

Langsiktige mål dreier seg ofte om å påvirke visse grupper for å støtte opp under spesifikke narrativ til fordel for den som står bak desinformasjonen. Et nylig eksempel på dette er desinformasjon som hevder at covid-19-pandemien ikke startet i Kina. Det kan også fokusere på å øke polariseringen i samfunnet som angripes. Slikt kan bidra til å få demokratier til å virke mindre attraktive for egne innbyggere i mindre demokratiske land. Det kan også gjøre det vanskeligere å enes om visse beslutninger i samfunnet som angripes som ville være ufordelaktige for angriperen.

Kortsiktige, spesifikke formål kan være rekruttering til ekstremister eller terrorgrupper som IS, økonomisk gevinst gjennom økt trafikk til nettsteder med falske nyheter som lever av reklame eller spredning av konspirasjonsteorier. Desinformasjon kan også spres i forbindelse med lokale hendelser. Er det for eksempel et anspent forhold mellom politi og visse sosiale grupper kan falske nyheter og annen desinformasjon spres for å gjøre forholdet verre eller få den ene parten til å fremstå mer negativt.

Sosiale mediers ubegrensede aggregering og lagring av informasjon som lastes opp og algoritmene som velger innhold gjør at langsiktig og kortsiktig desinformasjon utfyller hverandre uten at de som sprer desinformasjonen behøver å tenke på det. I en krisesituasjon kan for eksempel et narrativ som i lengre tid har fremstilt Norges Nato-medlemskap som en aggressiv handling støttes av mer spesifikke innlegg i sosiale medier relatert til pågående hendelser. Algoritmene vil finne brukere som tidligere har interagert med anti-Nato-informasjon og vise nye innlegg med samme tema. Søker brukerne for mer informasjon vil så tidligere innlegg bli funnet, med innhold som støtter opp om nyere innlegg. På denne måten skapes det man kan kalle et algoritmisk narrativ, en overbevisende historie basert på ulike (og ofte vilkårlige) innlegg fra en rekke kilder med forskjellig ståsted som sammenstilles av algoritmer skapt for å promotere engasjement. I krisesituasjoner med mangel på relevante opplysninger (såkalt *information void*), kan desinformasjon prioriteres når man søker etter informasjon. Det har for eksempel vært flere større skyteepisoder i USA hvor sosiale medier har anbefalt konspirasjonsteori-videoer under og rett etter hendelsen.

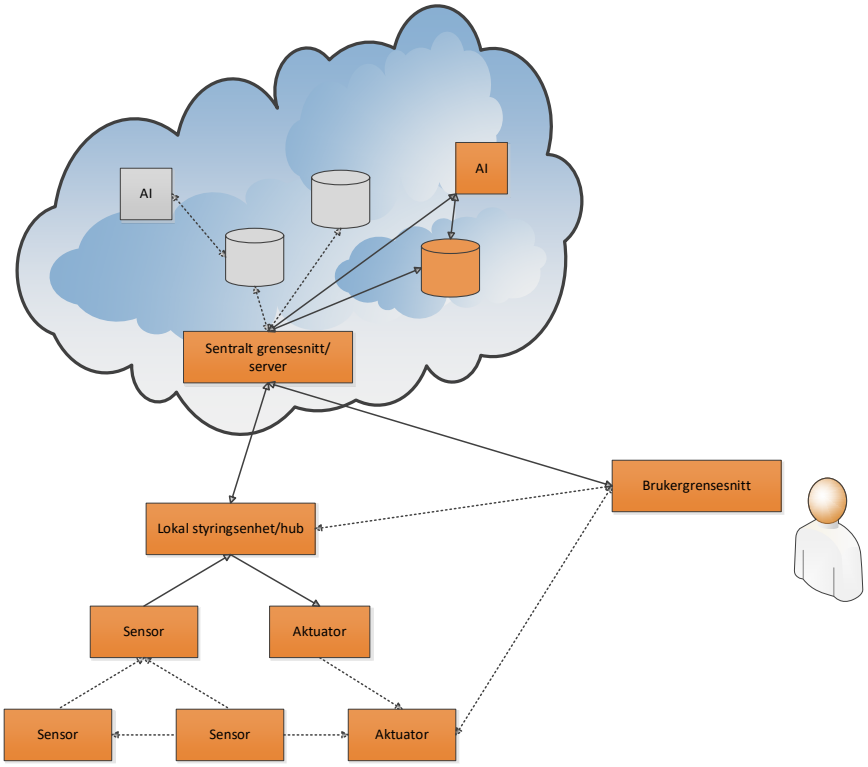
4.5.5 Tingenes internett

Tingenes internett, («Internet of Things» – IoT), kan karakteriseres som «en global infrastruktur for informasjonssamfunnet som muliggjør avanserte tjenester via sammenkoblede ting basert på eksisterende og nye informasjons- og kommunikasjonsteknologier (IKT)» (Sellevåg *et al.*, 2020, s. 39). Enkelt sagt refererer IoT til fysiske ting som er koblet til internett, hvor tingene kan være alt fra lyspærer til industriroboter.

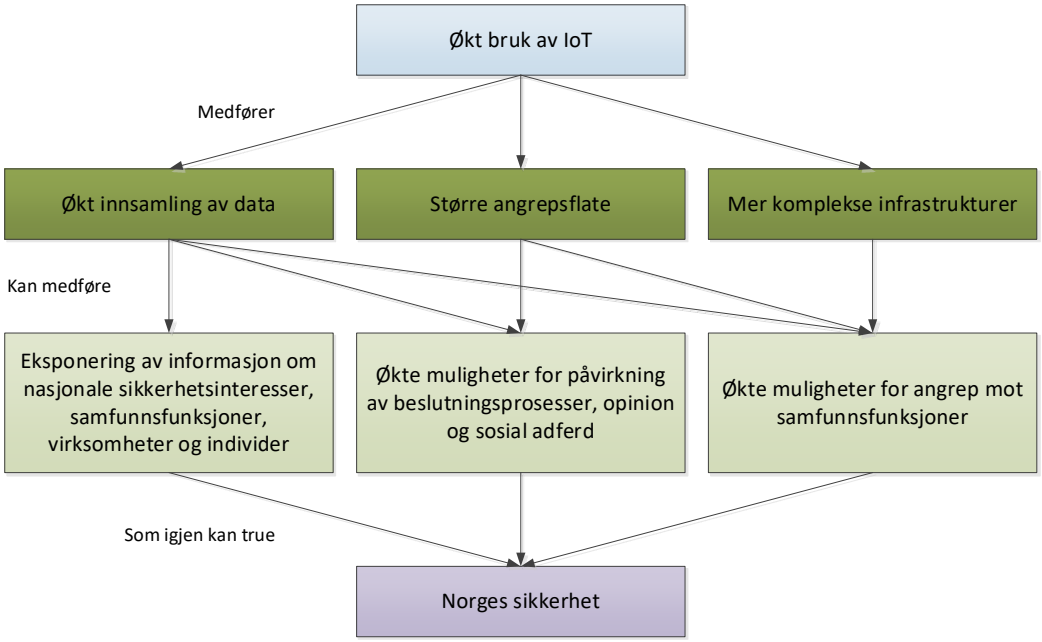
IoT-baserte tjenester benyttes allerede og det forventes stor vekst i IoT i tiden frem mot 2030. Sammen med utbyggingen av 5G (neste generasjons mobilnett) og bruk av kunstig intelligens, vil IoT i økende grad bli brukt til å underholde oss, gjøre hverdagen enklere (smarthjem), gjøre byer mer ressurseffektive (smartbyer), gjøre industribedrifter mer kostnadseffektive («Industri 4.0»), øke forsvarsevnen, samt til å gi oss bedre offentlige tjenester som for eksempel helsetjenester (e-helse) (Sellevåg *et al.*, 2020, s. 31, 39-42). I fremtidens «smartsamfunn» kan hva som helst kommunisere når som helst og hvor som helst via internett. Dette kan gi helt nye kriminalitets- og sikkerhetsutfordringer for politi- og påtaletjenestene.

FFI har nylig vurdert hvordan utviklingen av nye IoT-baserte tjenester kan påvirke nasjonal sikkerhet (Farsund *et al.*, 2020). I det følgende gis en kortfattet oppsummering av funnene fra dette arbeidet med fokus på hvordan utviklingen innen IoT negativt kan påvirke politi- og påtaletjenestene.

Et IoT-system består gjerne av sensorer (kameraer, temperaturmålere etc.), aktuatorer (døråpnere, brytere etc.), lokal styringsenhet, brukergrensesnitt og skytjenester knyttet til systemets funksjonalitet (se Figur 4.14). Sårbarhetene til IoT-systemet, det vil si faktorer som truer konfidensialiteten, integriteten og tilgjengeligheten til systemet og informasjonen som systemet behandler, er ikke bare avgrenset til komponentene i IoT-systemet, men de er også knyttet til avhengighetene som IoT-systemet har til andre systemer og infrastrukturer (Farsund *et al.*, 2020, s. 19-23). FFI har derfor pekt på følgende tre grunnleggende utfordringer knyttet til økt bruk av IoT: (*i*) *økt innsamling av data*, (*ii*) *større angrepsflate* og (*iii*) *mer komplekse infrastrukturer* (Figur 4.15) (Farsund *et al.*, 2020, s. 44). I det følgende vil disse utfordringene diskuteres nærmere.



Figur 4.14 Eksempel på komponenter i et IoT-system (Farsund et al., 2020, s. 11).



Figur 4.15 Mulige sikkerhetsutfordringer økt bruk av tingenes internett (IoT) kan medføre (etter Farsund et al., 2020).

Med økt bruk av IoT i samfunnet, vil mengden av data som samles inn om brukerne av IoT-systemet og om miljøet som IoT-systemet befinner seg i, øke betraktelig. Eksempelvis utstyres svært mange ting med kamera og/eller GPS. Datainnsamlingen kan i mange tilfeller være skjult for brukeren og en del av verdikjeden for en IoT-basert virksomhet kan være å selge dataene videre til såkalte dataforhandlere. Slike dataforhandlere kan aggregere data fra ulike kilder for deretter å berike, rense og/eller analysere dataene slik at de kan lisensieres videre til andre virksomheter (jf. kapittel 4.1.2; se også Farsund *et al.* (2020, s. 27-28)).

Økt innsamling av data kan medføre økt fare for eksponering av sensitiv informasjon om nasjonale sikkerhetsinteresser, samfunnsfunksjoner, virksomheter og individer. Denne informasjonen kan deretter utnyttes av ulike typer trusselaktører til å begå lovbrudd, gjennomføre påvirkningsoperasjoner eller angrep mot samfunnsfunksjoner, som igjen kan true Norges sikkerhet (Farsund *et al.*, 2020, s. 44-45).

En annen sikkerhetsutfordring knyttet til økt bruk av IoT, er at gjenstandene våre får større avhengigheter til andre systemer. Som vist i Figur 4.14, består et IoT-system av en rekke komponenter som kan ha avhengigheter til andre systemer. Dette gjør det mulig å angripe et IoT-system via andre systemer som IoT-systemet er avhengig av, og som nødvendigvis ikke er kjent for brukeren eller eieren av IoT-systemet. Selv om IoT-systemet i seg selv fremstår som sikkert, kan det likevel ha sårbarheter som kan utnyttes fordi det kan være avhengig av andre systemer som har lavere sikkerhetsnivå. Gjennom å koble fysiske gjenstander til internett og gjøre dem «smartere», vil derfor IoT-systemene ha en stor angrepsflate som kan utnyttes (Farsund *et al.*, 2020, s. 45).

Den tredje utfordringen er knyttet til økende kompleksitet. Ettersom IoT-systemer kan bruke flere andre komplekse infrastrukturer som 5G, internett og skytjenester, vil IoT-systemer inngå i dynamiske og svært komplekse digitale verdikjeder (Farsund *et al.*, 2020, s. 45). I praksis vil det være svært krevende, nærmest umulig, å ha oversikt over alle avhengighetene i verdikjedene, inkludert hvilke aktører som inngår som tjenestetilbydere eller underleverandører. Den økende kompleksiteten vil derfor gjøre det svært utfordrende å gjennomføre risiko- og sårbarhetsvurderinger av IoT-systemer. I tillegg vil datanettverksangrep mot IoT-systemer kunne få større konsekvenser i det fysiske rom etter hvert som flere aktuatorer kobles til systemene, og dermed til internett (Farsund *et al.*, 2020, s. 46).

Dersom tilstrekkelige sårbarhetsreduserende tiltak ikke iverksettes, er det grunn til å forvente økt risiko for cyberterrorisme hvor en ikke-statlig aktør søker å begå terrorhandlinger som får effekt i det fysiske rom, gjennom datanettverksangrep mot IoT-systemer. Vi må også forvente at kriminelle vil utnytte sårbarheter i IoT-systemer for å oppnå økonomisk vinning, eksempelvis gjennom krav om å utbetale løsepenger for å få tilgang til tjenesten igjen. Videre er det grunn til å frykte at IoT kan misbrukes til å begå seksuelle overgrep over internett. Til slutt er det også grunn til å forvente at IoT vil medføre økt risiko for at fremmede stater kan innhente store mengder informasjon som kan utnyttes til etterretning, påvirkning og/eller gjennomføring av angrep mot identifiserte mål.

4.5.6 Autonome systemer og droneteknologi

Utvikling innen robotikk og autonome systemer vil fortsette å gi samfunnet nye og endrede tjenester i tiden frem mot 2030 (Sellevåg *et al.*, 2020, s. 42-44). Trusler som følge av økt bruk av autonome systemer kan deles inn i to (ikke gjensidig utelukkende) kategorier: (*i*) bruk av autonome systemer til tilsiktede uønskede handlinger; (*ii*) tilsiktede uønskede angrep mot autonome systemer som benyttes i samfunnet.

Når det gjelder førstnevnte kategori, er droner av spesiell bekymring på grunn av deres mulighet til å omgå eksisterende fysiske beskyttelsestiltak (Sellevåg *et al.*, 2017). Bruk av droner representerer derfor en rekke utfordringer for samfunnssikkerheten og nasjonale sikkerhetsinteresser. Generelt kan disse utfordringene knyttes til: (*i*) bruk av droner for informasjonsinnhenting, (*ii*) bruk av droner til påvirkning (for eksempel ved å filme et pågående terrorangrep), (*iii*) bruk av droner som angrepsvåpen, og (*iv*) bruk av droner for transport av ulovlige varer. Nasjonalt har sikkerhetsmyndigheter registrert flere tilfeller av uautorisert droneaktivitet i nærheten av militære øvelser eller områder med fotoforbud (Nasjonal sikkerhetsmyndighet, 2020c). Økt datainnsamling fra dronebårne sensorer kan direkte eller indirekte utnyttes av fremmede staters etterretningstjenester. Internasjonalt har man blant annet sett at terrororganisasjonen IS har benyttet droner til informasjonsinnhenting, som propagandaverktøy gjennom å filme terrorangrep, og som plattform for levering av luftbårne improviserte eksplosivladninger (jf. kapittel 5.2.4; se også: Rassler (2016); Tønnessen (2017)). Man har også sett eksempler på bruk av droner for smugling av narkotika og andre ulovlige varer (Turkmen & Kuloglu, 2018).

Droneteknologien har utviklet seg svært raskt. Det forventes at dette vil fortsette etter hvert som flere produsenter og leverandører kommer på markedet. Generelt sett går teknologiutviklingen i retning av miniatyrisering; ytelsen til «gårsdagens» droner er nå tilgjengelig i en mye mindre innpakking. Et annet utviklingstrekk er at droner vil få høyere grad av autonomi, altså at de i større grad vil bli gitt mulighet til å ta egne beslutninger og fravike planen som er bestemt av operatøren. Dette kan for eksempel være knyttet til å omgå hindre basert på sceneanalyse. Videre finnes det allerede droner som kan følge objekter i bevegelse («object tracking»), og det er grunn til å forvente at denne teknologien vil utvides til også å inkludere ansiktsgjenkjenning i nær fremtid. En annen utvikling som forventes er evne til å navigere i omgivelser hvor GPS ikke er til stede. Sammen med teknologier for å unngå hindre, vil dette gi mulighet til navigasjon både utendørs og innendørs. Til slutt forventes det betydelige fremskritt innen såkalt «svermteknologi» hvor komplekse operasjoner gjennomføres ved at flere droner samarbeider (se for eksempel Engebråten *et al.* (2018)).

Når det gjelder tilsiktede uønskede angrep mot autonome systemer som benyttes i samfunnet, vil dette medføre mange av de samme sikkerhetsutfordringene som for IoT (jf. kapittel 4.5.3). FFI har nylig vurdert kryptografiske løsninger og digital sikkerhet i autonome systemer og for noen utvalgte eksisterende dronetyper. I studien ble en rekke sårbarheter og mangelfulle sikkerhetsløsninger i sivile droner for fritids- og kommersielt bruk avdekket (Wiik, 2020). Arbeidet med å implementere hensiktsmessige sikkerhetskrav og -løsninger for autonome systemer må derfor fortsette.

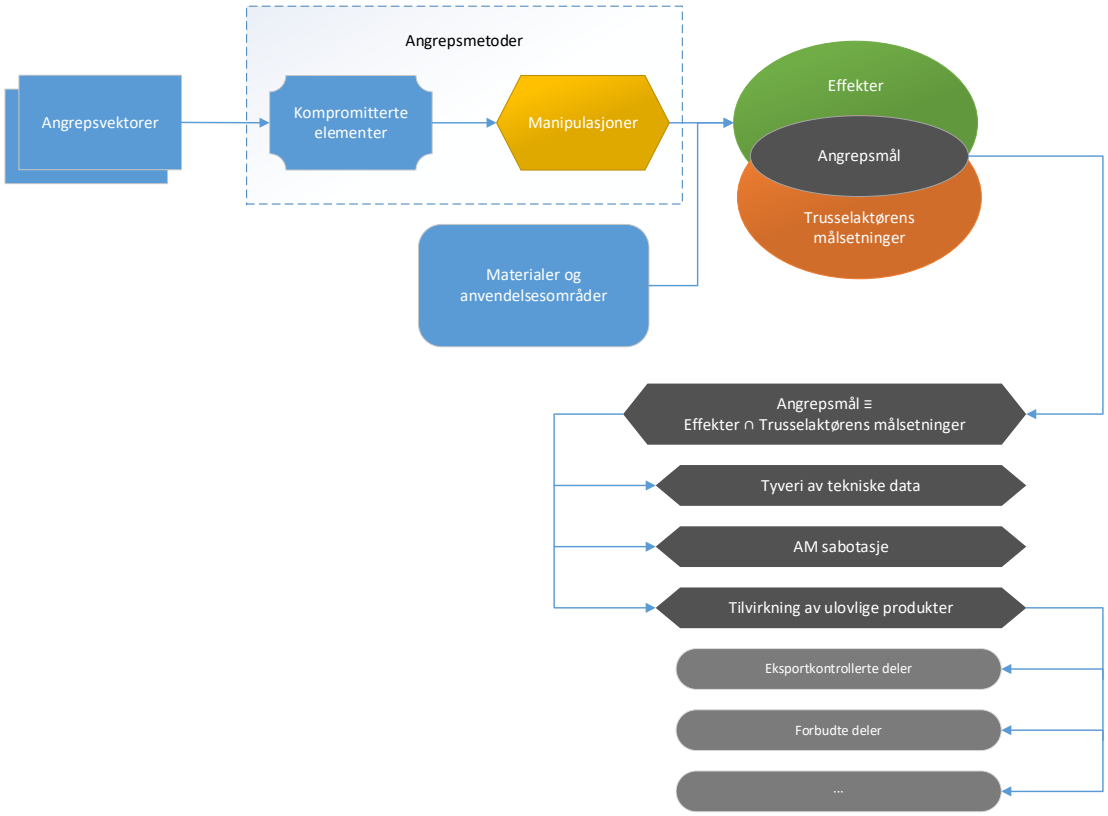
4.5.7 Additiv tilvirkning

Additiv tilvirkning er en fellesbetegnelse på produksjonsmetoder hvor det som skal produseres bygges opp, vanligvis lag for lag, fra en tredimensjonal datamodell. Det finnes flere ulike teknologier for additiv tilvirkning, hvor såkalt 3D-printing er den vanligste. Det er også mulig å tilvirke objekter som kan endre form (såkalt 4D-printing). Additiv tilvirkning er således et nytt produksjonsprinsipp som gir nye muligheter med hensyn til geometri og integrasjon av funksjoner, samtidig som man har stor fleksibilitet når det gjelder materialvalg (inkludert tilvirkning av biologisk materiale).

Med tilgang på en 3D-printer og materialer for additiv tilvirkning, er det nærmest ingen grenser for hva som kan produseres så lenge en tredimensjonal datamodell av objektet er tilgjengelig. Det er allerede mulig å tilvirke for eksempel våpen og våpendeler, beskyttelsesmaterialer og minibank-skimmere (Europol, 2017a, s. 7-8). Det har også vist seg mulig å lure fingeravtrykkslesere ved hjelp av 3D-printede fingeravtrykk (Kerner, 2020).

Det er derfor flere sikkerhetsutfordringer knyttet til additiv tilvirkning (jf. Figur 4.16). I tillegg til tilvirkning av ulovlige produkter, er det også mulig å stjele tekniske data eller immaterielle rettigheter. Blant annet har forskere vist at det er mulig å rekonstruere den tredimensjonale datamodellen gjennom å fange opp de akustiske signalene fra 3D-printeren (Al Faruque *et al.*, 2016). Det er også mulig å sabotere selve produksjonsprosessen. I den såkalte «dr0wned»-studien fra 2016 viste forskere at det var mulig å styrte en drone gjennom å sabotere en 3D-printet propell til dronen. Måten dette ble gjort på var å sende en phishing-epost med et ondsinnet vedlegg til datamaskinen som styrte 3D-printeren. Dette gjorde det mulig å introdusere svakheter i designet til dronepropellen som raskt medførte tretthetsbrudd uten at endringene var synlige for det blotte øyet (Belikovetsky *et al.*, 2016).

Når det gjelder tyveri av tekniske data eller sabotasje av produksjonsprosessen, vil dette være avhengige av hvilke manipulasjoner en trusselaktør kan gjøre. Dette er igjen avhengig av i hvilken grad en trusselaktør kan utøve kontroll over kompromitterte elementer og elementenes rolle i produksjonsprosessen. Disse manipulasjonene sammen med type produksjonsutstyr, materialvalg og anvendelsesområdet til produktet bestemmer hvilke effekter som er mulige å oppnå (Yampolskiy *et al.*, 2017). Jo mer informasjon en trusselaktør har om konkrete additiv tilvirkningssystemer, desto lettere vil det være for samme trusselaktør å oppnå sine målsetninger. I hvilken grad trusselaktøren vil lykkes, vil være avhengig av sikkerheten til systemet. Likevel er det grunn til å forvente at sikkerhetsutfordringer knyttet til additiv tilvirkning vil vedvare i tiden frem mot 2030.



Figur 4.16 Sikkerhetsutfordringer knyttet til additiv tilvirkning (AM). Kilde: Yampolskiy et al. (2017).

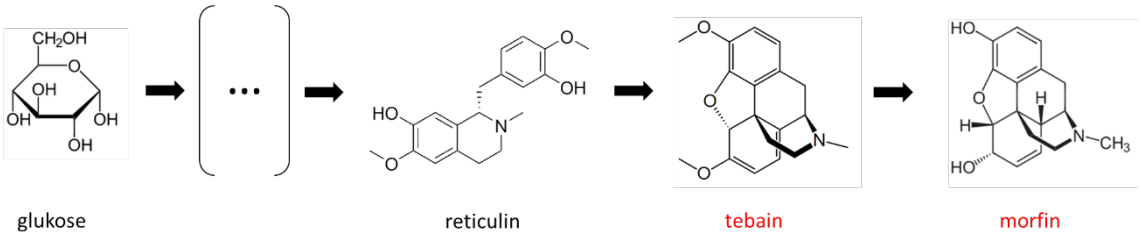
4.5.8 Syntetisk biologi og bioteknologi

4.5.8.1 Utfordringer relatert til syntetisk biologi

Syntetisk biologi forventes å gi samfunnet en rekke nye muligheter til nytte for samfunnet. Blant annet forventes det at teknologien kan bidra til produksjon av miljøvennlig energi, materialer, batterier, nye medisiner, samt nyttige anvendelser innen landbruk. Samtidig er en rekke utfordringer knyttet til syntetisk biologi identifisert, hvor uforsiktig eller ondsinnet bruk av teknologien kan gi ødeleggende konsekvenser (Sellevåg *et al.*, 2020, s. 50-51). Konkret er de største bekymringene knyttet til rekonstruksjon av kjente patogene virus, gjøre eksisterende bakterier farligere, omprogrammering av celler som utnyttes til produksjon av kjemikalier (såkalt *in situ*-syntese) og «gjør-det-selv-biologi». Sistnevnte representerer en demokratisering av teknologien som gjør det mulig for flere å utnytte syntetisk biologi. Således er det fare for at syntetisk biologi kan misbrukes til biologisk eller kjemisk terrorisme. Det vurderes derfor om teknologien som benyttes innen syntetisk biologi bør underlegges eksportkontroll for å hindre ondsinnet bruk (Sellevåg *et al.*, 2020, s. 51).

Når det gjelder faren for at syntetisk biologi skal gjøre det mulig å endre menneskets genom eller immunforsvar, er det flere tekniske barrierer og kunnskapsmangler som må løses før dette er mulig. National Academies of Sciences, Engineering, and Medicine og US Department of Defence (2018) har derfor vurdert dette til å være av middels relativ bekymring. Når det gjelder endring av menneskets genom gjennom såkalt «genkjøring», det vil si injeksjon av et gen som så «smitter» en hel befolkningspopulasjon gjennom arv, er dette av lav relativ bekymring. Det er en lite effektiv måte å påføre skade på befolkningen fordi det vil kreve flere generasjoner med menneskelig reproduksjon (skade på jordbruksavlinger vil imidlertid være mer effektivt på grunn av kortere reproduksjonstid) (National Academies of Sciences, Engineering, and Medicine, 2018, s. 3-7).

I tillegg til bekymringer rundt misbruk av syntetisk biologi til bio-/kjemisk terrorisme, er det også en fare for at teknologien kan misbrukes til produksjon av narkotika. I 2015 ble alle trinnene for å produsere opiater som tebain og morfin fra glukose (sukker) ved hjelp av genmodifisert gjær publisert i vitenskapelig litteratur (se Figur 4.17 for en forenklet fremstilling av produksjonsmetoden). Gjennom denne teknologien kan det være mulig å produsere enkelte smertestillende medisiner på en raskere og billigere måte enn i dag slik at de blir tilgjengelige for flere (Abate, 2015).



Figur 4.17 Forenklet fremstilling av hvordan de narkotiske stoffene morfin og tebain kan lages fra glukose (sukker) ved hjelp av genmodifisert gjær. Kilde: Galaine et al. (2015); Oye et al. (2015).

Imidlertid advarer forskere om at samme teknologi kan misbrukes til narkotikaproduksjon (Oye *et al.*, 2015). I prinsippet kan teknologien medføre at opiater kan fremstilles ved hjelp av samme utstyr som benyttes til hjemmebrygging av øl. Fordi slik genmodifisert gjær vil være enkel å skjule, få til å vokse og transportere, vil dette kunne medføre en desentralisert produksjon av opiater som vil være vanskelig å oppdage og som kan øke deres tilgjengeligheten til ulovlig bruk. Hvorvidt dette vil skje, vil blant annet være avhengig av tilgjengeligheten til genmodifisert gjær og de kriminelles økonomiske interesser i en slik fremstillingsmåte.

Enn så lenge er det trolig lav sannsynlighet for at vi vil se en betydelig narkotikaproduksjon ved hjelp av genmodifisert gjær. Det er likevel grunn til å være oppmerksom på problemstillingen

og iverksette nødvendige tiltak. Disse tiltakene bør først og fremst innrettes på bioteknologisiden slik at genmodifisert gjær blir mindre attraktiv for kriminelle, men forskere anbefaler også styrket biosikkerhet, screening-mekanismer og regulatoriske virkemidler (Oye *et al.*, 2015).

4.5.8.2 Dagens og fremtidige kriminalitetsformer relatert til bioteknologi

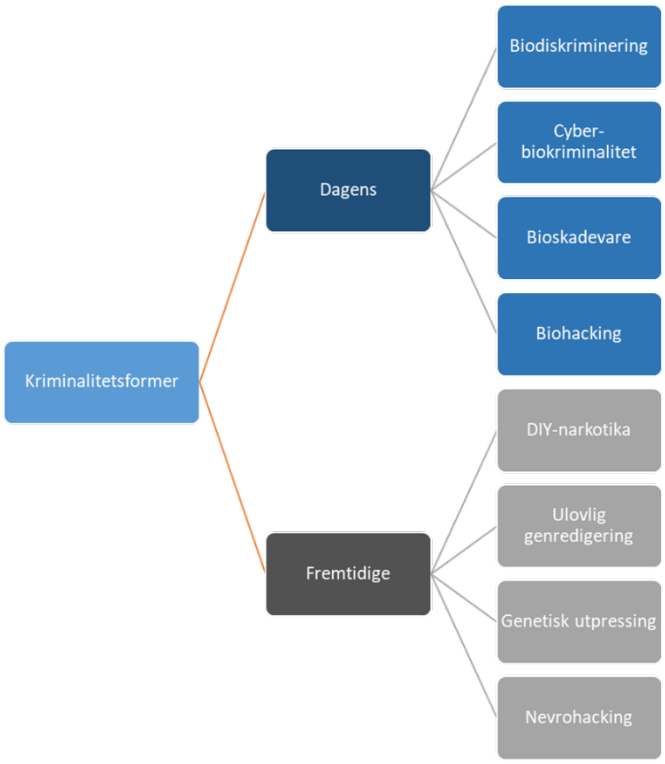
Elgabry *et al.* (2020) har sett på hvordan syntetisk biologi og bioteknologi kan misbrukes av kriminelle i et større perspektiv. Gjennom litteraturstudier har Elgaby *et al.* identifisert åtte mulige kriminalitetsformer, hvorav fire kan karakteriseres som fremtidige. Disse kriminalitetsformene er oppsummert i Figur 4.18.

Biodiskriminering er misbruk av helse-/biologiske data til diskriminering av personer eller folkegrupper basert på deres biologiske informasjon. *Cyberbiokriminalitet* beskriver kriminelle handlinger som utnytter det digitale rom (internett) og biologisk/biokjemisk materiale. For eksempel kan mangelfull sikkerhet knyttet til såkalte automatiserte skylaboratorier utnyttes til sabotasje av vaksine- eller legemiddelproduksjon. Et eksempel på *bioskadevare* er angrep mot datasystemer som benyttes i bioteknologi gjennom skadevare som er fysisk lagret i DNA. *Biohacking* er utnytting eller manipulering av genetisk materiale i eksisterende organismer, for eksempel for å øke menneskelig yteevne (Elgabry *et al.*, 2020).

Når det gjelder mulige fremtidige kriminalitetsformer, er hjemmeproduksjon av narkotika (såkalt *DIY*[13]*-narkotika*) allerede nevnt i kapittel 4.5.8.1. Det samme er *ulovlig genredigering* som eksempelvis kan utnyttes til rekonstruksjon av kjente patogene virus. *Genetisk utpressing* betyr trusler om avsløring av genetisk informasjon med mindre bestemte krav innfris. Siste foreslåtte kriminalitetstype er *nevrohacking*, det vil si endringer i vekselvirkninger mellom vertsorganismen og mikrobiotaen som lever i verten, som kan påvirke sentralnervesystemet til verten (Elgabry *et al.*, 2020).

I hvilken grad de foreslåtte kriminalitetsformene vil utnyttes av kriminelle, gjenstår å se. Mange av truslene som ble fremhevet av Elgabry *et al.* (2020) kan karakteriseres som «eksperimentelle» eller «teoretiske», snarere enn at de foregår i den faktiske verdenen. Det er imidlertid behov for mer kunnskap om hvilke kriminalitets- og sikkerhetsutfordringer som kan oppstå som følge av syntetisk biologi og i skjæringspunktet mellom bioteknologi og digitale teknologier. Det er også behov for mer kunnskap om hvordan syntetisk biologi og bioteknologi kan utfordre etiske og juridiske aspekter.

[13] DIY = «Do It Yourself» («gjør det selv»).



Figur 4.18 Dagens kriminalitetsformer relatert til bioteknologi og mulige fremtidige utfordringer. Kilde: Elgabry et al. (2020).

5 Utvikling innen tematiske utfordringsområder

I dette kapitlet sees det nærmere på utviklingen innen tematiske utfordringsområder for politiet, PST og påtalemyndigheten. Valg av utfordringsområder er basert på funn fra en FFI-studie på oppdrag fra JD, hvor det ble vurdert på hvilken måte eksterne eller interne aktører, nå eller i fremtiden, kan påvirke Norges sikkerhet negativt uten å ta i bruk konvensjonelle militære virkemidler (Sellevåg, 2021). De identifiserte utfordringskategoriene for tilsiktede handlinger som kan true Norges sikkerhet, er oppsummert i boks 5.1.

Boks 5.1: Utfordringskategorier for politiet, PST og påtalemyndigheten for tilsiktede handlinger som kan true Norges sikkerhet

Følgende utfordringskategorier for politiet, PST og påtalemyndigheten for tilsiktede handlinger som kan true Norges sikkerhet er identifisert (Sellevåg, 2021):

- *Voldelig statskupp*
- *Voldelig separatisme*
- *Statsstøttet opprør*
- *Skjulte angrep* på samfunnsfunksjoner og/eller mennesker, herunder også sabotasje
- *Angrep på viktige personer*, herunder også trusler om slike angrep
- *Statlig påvirkningsaktivitet*
- *Statlig etterretningsaktivitet*
- *Terror- og terrorrelaterte handlinger*
- *Voldelige, selvstyrende subkulturer*
- *Opptøyer*
- *Statsstøttet organisert kriminalitet*
- *Ikke-spredning*
- *Annen alvorlig kriminalitet*

De identifiserte utfordringskategoriene ble deretter gruppert i følgende scenarioklasser, hvor en scenarioklasse er en gruppe av scenarioer med fellestrekk og hvor scenarioene kan bestå av én eller flere av de identifiserte utfordringskategoriene (Sellevåg, 2021, boks 5.1):

- *Voldelig statskupp:* Statsstøttet ikke-statlig aktør ønsker å fremtvinge regimeendring gjennom å ta kontroll over hele Norges styringsevne og/eller suverenitet.

- *Voldelig separatisme:* Statsstøttet ikke-statlig aktør ønsker å fremtvinge regimeendring gjennom å ta kontroll over deler av Norges styringsevne og/eller suverenitet.

- *Statsstøttet opprør:* Statsstøttet ikke-statlig aktør demonstrerer evne og vilje til bruk av fysisk makt for å fremtvinge politisk endring eller endring i politikk.

- *Subversjon:* Statlig aktør ønsker å oppnå strategiske fordeler eller fremtvinge politisk endring/endring i politikk gjennom påvirkning av beslutningsprosesser, opinion og/eller sosial adferd, hvor også skjulte angrep på samfunnsfunksjoner, mennesker og/eller viktige personer kan inngå.

- *Terrorisme:* Ikke-statlig aktør ønsker å oppnå strategiske fordeler eller fremtvinge politisk endring/endring i politikk gjennom terrorangrep på samfunnsfunksjoner og/eller mennesker, samt gjennom relaterte handlinger for å muliggjøre terrorangrep.

- *Samfunnsforstyrrelser:* Ikke-statlig aktør ønsker å fremtvinge politisk endring/endring i politikk gjennom opptøyer, eller forsvare eget sosiale styresett gjennom å demonstrere evne og vilje til bruk av fysisk makt, påvirke sosial adferd og/eller andre kriminelle handlinger.

- *Ikke-spredning:* Hindre spredning av materiale, teknologi og kunnskap som kan brukes til utvikling av masseødeleggelsesvåpen, samt hindre spredning av strategiske varer, tjenester og teknologi m.m. i henhold til vedtak i FNs sikkerhetsråd eller annen lovgivning.

- *Annen alvorlig kriminalitet*

I det følgende vil relevante utviklingstrekk for disse scenarioklassene presenteres. Voldelig statskupp, voldelig separatisme, statsstøttet opprør og subversjon er omtalt som *trusler mot nasjonal sikkerhet*. Før utviklingstrekkene presenteres, knyttes det en kommentar til begrepet *subversjon*. Subversjon er nært knyttet til *sammensatte trusler*. I dette arbeidet er det valgt å bruke subversjon fremfor sammensatte trusler som beskrivelse for det tematiske utfordringsområdet fordi subversjon vurderes å være mer beskrivende for *hva* en trusselaktør ønsker å oppnå, mens sammensatte trusler er mer beskrivende for *hvordan* trusselaktøren går frem for å nå sine målsetninger.

5.1 Trusler mot nasjonal sikkerhet

5.1.1 Subversjon: Etterretning, påvirkning og skjulte angrep

> *[f]uture war will not be fought on the front lines, but throughout the entire territories of both opponents, because behind the front lines, political, social, and economic fronts will appear; they will fight not on a two-dimensional plane, as in olden days, not in a three-dimensional space as has been the case since the birth of military aviation, but in a four-dimensional space, where the psyche of the combatant nations will serve as the fourth dimension.*
>
> — *Evgenii Messner (1960)*

I kapittel 4.1 ble det nevnt at nevnt at den langsiktige globale sikkerhetspolitiske utviklingen preges av at stater i større grad bruker en kombinasjon av ulike virkemidler for å utøve press. Både i gjeldende langtidsplan for forsvarssektoren (Prop. 14 S (2020-2021)) og i siste samfunnssikkerhetsmelding (Meld. St. 5 (2020-2021)) er utfordringer knyttet til slike *sammensatte trusler* fremhevet. Selv om det ikke finnes noen ensartet definisjon av sammensatte trusler, brukes begrepet om «situasjoner hvor en aktør bruker ulike virkemidler for å påvirke oss» (Meld. St. 5 (2020-2021), s. 92, boks 9.1). Én mulig beskrivelse er «[…] bruk av ulike virkemidler i kombinasjon for å påvirke en motstander med størst mulig effekt. Dette kan innebære å skape usikkerhet, tvil og forvirring, vanskeliggjøre beslutningsprosesser og påvirke beslutninger i en retning som er gunstig for den aktuelle aktøren, herunder å oppnå strategiske fordeler som tradisjonelt oppnås gjennom seier i krig» (Prop. 14 S (2020-2021), s. 72). Sammensatte trusler som begrep er således nært beslektet med begrepet *hybride trusler* som kan karakteriseres som «[…] kombinasjonen av militære og ikke-militære [virke]midler» benyttet for å gjøre det «vanskelig for den som blir angrepet å definere situasjonen som en krigshandling, vite hvem som står bak, og dermed finne den riktige responsen» (Beadle *et al.*, 2019, s. 18).

Utfordringen som sammensatte trusler representerer er at skillet mellom krig og fred viskes ut uten at konflikten eskalerer til et konvensjonelt militært motsvar. Samtidig utnytter en trusselaktør risikoen for at konflikten *kan* eskalere til bruk av konvensjonell militærmakt. Hensikten med bruk av sammensatte trusler er dermed å oppnå strategiske målsetninger uten å overskride grensen til konvensjonell krigføring hvor både militære og ikke-militære virkemidler benyttes. For å forstå sammensatte trusler er det derfor nødvendig å forstå konteksten som det oppstår i, deriblant historiske utviklingstrender, samt karakteristiske trekk og drivere for fenomenet.

Det er særlig fire viktige drivere for fremvekst av sammensatte trusler (Diesen, 2018, s. 9):

- Økende økonomiske kostnader ved anvendelse av konvensjonell maktbruk
- Økende politiske kostnader ved anvendelse av konvensjonell maktbruk
- Risiko for eskalering til kjernefysisk nivå
- En stadig tiltakende teknologisk utvikling

Ut fra denne konteksten blir derfor utnyttelse av sammensatte trusler en sammensetning av strategisk mulighet og nødvendighet. Den strategiske muligheten oppstår som følge av økte gjensidige avhengigheter mellom ulike samfunnssektorer, mellom det sivile og det militære og mellom ulike stater, hvor sårbarheter i de gjensidige avhengighetene kan utnyttes og manipuleres. Den strategiske nødvendigheten følger derimot av en innstramming av statlig handlefrihet og en vegring mot å ta høy økonomisk, militær eller diplomatisk risiko (Palmer, 2015, s. 2). Noe forenklet kan man derfor si at videreføring eller økning av drivkreftene som gav vekst til sammensatte trusler, vil bidra til en tilsvarende videreføring eller økning av fenomenet.

Det såkalte MPECI-rammeverket (Cullen & Reichborn-Kjennerud, 2017) kan danne grunnlag for å forstå hvordan ulike virkemidler kan benyttes i kombinasjon. Virkemidlene som er inkludert i dette rammeverket er militære (M), politiske (P), økonomiske (E), sivile/juridiske (C) og informasjonsrelaterte (I), inkludert cyberoperasjoner. Det antas at virkemidlene blir mer virkningsfulle jo flere som kombineres (såkalt horisontal eskalering). I tillegg kan virkemidlene benyttes med økende styrke (såkalt vertikal eskalering). Generelt kan man si at kombinasjoner av virkemidler kan (Waage *et al.*, 2021):

i) skape sårbarheter,
ii) forsterke effekten av virkemiddelbruken, eller
iii) legitimere bruk av andre virkemidler.

Spesielt kan kombinasjonen av økonomiske virkemidler og virkemidler i informasjonsdomenet kan være effektive (Waage *et al.*, 2021). Eksempelvis kan utenlandske direkteinvesteringer i Norge skape en sårbarhet gjennom å legge til rette for statlig etterretningsaktivitet ved at investoren får en innsiderrolle og derav bedre informasjonstilgang (Waage *et al.*, 2021, s. 61). Denne sårbarheten kan senere utnyttes gjennom datanettverksoperasjoner (horisontal eskalering). Et annet eksempel er bruk av handelssanksjoner mot norsk eksport for å utøve press på norske myndigheter. Denne effekten kan forsterkes gjennom påvirkningsoperasjoner og bruk av sosiale medier hvor den utenlandske aktøren forsterker sitt narrativ og svekker det norske synspunktet (Waage *et al.*, 2021, s. 63). Når det gjelder det siste punktet, er dette gjerne koblet til beskyttelse av strategiske interesser. Dersom en aktør mener at en økonomisk investering eller ressurstilgang er truet, for eksempel på Svalbard eller i norsk økonomisk sone, kan dette legitimere bruk av andre virkemidler. Informasjonsrelaterte virkemidler som bidrar til å støtte oppunder narrativet vil i så måte være relevante. Det samme vil politisk press, fordelaktige juridiske tolkninger av internasjonale avtaler eller i ytterste konsekvens, bruk av militærmakt (Waage *et al.*, 2021, s. 64).

Norge som en nasjon med åpen økonomi og høy grad av digitalisering, kan derfor være sårbar for fremmede staters kombinerte bruk av informasjonsrelaterte og økonomiske maktmidler. Det blir derfor et spørsmål om hvor tett norsk økonomi og handel bør knyttes mot land som både har betydelige evner innen offensive cyberoperasjoner og som regelmessig bruker økonomiske virkemidler på måter som kan true våre nasjonale sikkerhetsinteresser (Waage *et al.*, 2021, s. 78). I dette spørsmålet må det hensyntas at både teknologiutviklingen (jf. kapittel 4.5) og det grønne skiftet (jf. kapittel 4.4.3) vil kunne medføre nye sårbarheter i samfunnet. Samtidig vil teknologi-

utviklingen gi fremmede stater nye evner innen geografisk etterretning (GEOINT), signaletterretning (SIGINT), bruk av åpne kilder (OSINT) og menneskebasert etterretning (HUMINT), kanskje særlig gjennom utnyttelse av kunstig intelligens og bedre sensorer (Katz, 2020). Det må derfor forventes at utenlandsk etterretnings- og påvirkningsaktivitet mot både offentlige og private sektorer vil forbli en betydelig trussel mot Norge og norske interesser i tiden frem mot 2030.

5.1.2 Opprør, separatisme og statskupp

Opprør kan karakteriseres som «enhver væpnet reisning mot forfatningen eller statlige myndigheter» (*opprør*, u.å.). Opprør mot statlige myndigheter kan for eksempel knyttes til krav om reformer som følge av systematisk undertrykking av hele eller deler av befolkningen i landet, eller det kan relateres til sosial nød. Et eksempel på opprør er den arabiske våren som startet 17. desember 2010 i Tunisia, og som senere spredte seg til Egypt, Libya og Syria. I tillegg ble Jemen og Bahrain berørt (Lodgaard, 2020).

Selv om det synes svært lite sannsynlig at opprør skal kunne skje i Norge, kan opprør i andre land indirekte true norske sikkerhetsinteresser. Et eksempel på dette så man under den fremdeles pågående borgerkrigen i Syria hvor norske fremmedkrigere dro til Syria for å tilslutte seg ulike opprørsgrupper, inkludert jihadistgruppene Jabhat al-Nusra[14] og IS (Leraand *et al.*, 2019). Bekymringen for norske sikkerhetstjenester var knyttet til fremmedkrigeres tilbakekomst til Norge og faren for at ytterligere radikalisering i krigssonen kombinert med krigserfaring kunne medføre at tilbakevendte fremmedkrigere ville gjennomføre terrorhandlinger i Norge. Denne faren er fremdeles tilstede (mer om dette i kapittel 5.2).

Når det gjelder *separatisme*, har ikke Norge noen separatistbevegelse slik man for eksempel har i Catalonia i Spania (Wikipedia, u.å.-a). Slikt sett vurderes det som svært lite sannsynlig at voldelig separatisme skal kunne skje i Norge i tiden frem mot 2030. Samtidig advarte professor Frank Aarebrot i 2008 om at den sterke misnøyen med sentralstyringen av Norge kan føre til at det blir etablert et nytt regionalt parti på Vestlandet, og sammenlignet med etablering av det skotske nasjonalistpartiet (Fauske, 2008). Dersom det skapes en oppfatning av at det er store forskjeller i fordeling av velferd og ressurser ut fra hvor verdiene skapes, gjerne gjennom utnyttelse av konspirasjonsteorier (se kapittel 6.2.4), kan dette bidra til å fremtvinge økt regionalt selvstyre. Nå, over tolv år etter advarselen til professor Frank Aarebrot, er det ikke noen tegn som tilsier at en region i Norge går i retning av å søke økt regionalt selvstyre.

Ser vi videre på statskupp,[15] må vi tilbake til andre verdenskrig for å finne eksempel på dette i Norge, hvor Vidkun Quisling 9. april 1940 erklærte at han ville danne en nasjonal regjering og avsette regjeringen Nygaardsvold. Imidlertid har det forekommet flere statskupp på verdensbasis i etterkrigstiden. Bare mellom januar 2008 og desember 2010 er det dokumentert syv kupp

[14] Fra 2016: Jabhat Fateh al-Sham.

[15] Med statskupp menes en ulovlig og synlig omveltning som settes i verk «ovenfra» i strid med forfatningen, for eksempel ved at statsoverhodet eller militæret avskaffer nasjonalforsamlingen; se: *statskupp*. (u.å.). Store norske leksikon. Hentet 8. april 2021 fra https://snl.no/statskupp.

(Powell & Thyne, 2011). Forekomsten av kuppforsøk er høyest i Afrika, etterfulgt av Sør-Amerika, Midtøsten og Asia. I Europa er det dokumentert tolv kuppforsøk i perioden 1950-2010, hvorav en tredjedel har vært suksessfulle; det siste kuppforsøket skjedde i Aserbajdsjan i 1995 (Powell & Thyne, 2011). Etter 2010 kan både kuppet i Egypt 3. juli 2013 og kuppforsøket 16. juli 2016 mot den tyrkiske regjeringen til president Erdoğan nevnes (Fosshagen *et al.*, 2020; Nilsen & Tjørhom, 2013).

Ifølge forskerne Jonathan M. Powell og Clayton L. Thyne ved Universitetet i Kentucky, kan følgende tre spørsmål bidra til å avgjøre om et opprør er et kuppforsøk (Powell & Thyne, 2011):

1. Tilhører gjerningspersonene statsapparatet, slik som militære offiserer eller medlemmer av regjeringsapparatet?

2. Er målet for opprøret statsoverhodet/regjeringssjefen?

3. Bruker gjerningspersonene ulovlige og ikke-konstitusjonelle metoder for å overta statsmakten?

I en slikt kontekst og ut fra det første spørsmålet, vurderes det som svært lite sannsynlig, nærmest utenkelig, at et statskupp skal kunne skje i Norge i tiden frem mot 2030. Med bakgrunn i stormingen av den amerikanske kongressen 6. januar 2021, kan det ikke utelukkes at opprør tilsvarende spørsmål 2 og 3 kan skje i Norge.

5.2 Terrorisme

Utviklingstrekk innen terrorisme har nylig blitt vurdert av FFI (Johansen & Gråtrud, 2018). I det følgende gis en oppdatert vurdering av funnene til Johansen og Gråtrud, supplert med annet kildemateriale og trusselvurderinger, med hovedfokus på utviklingen i Vest-Europa. Ulike kategorier innen terrorisme er gitt i boks 5.2.

Boks 5.2: Ulike former for voldelig ekstremisme (Europol, 2020b)

Jihadistisk terrorisme er en voldelig retning innen islamisme tuftet på væpnet kamp i form av hellig krig.

Høyreekstrem terrorisme er en voldelig retning med utspring i svært ytterliggående holdninger på den politiske høyresiden. Varianter innen høyreekstremisme er nynazisme, nyfascisme og ultranasjonalistiske grupperinger. Til forskjell fra høyreradikale som mener at demokratiet skal opprettholdes, mener høyreekstremister at demokratiet skal avvikles, universelle menneskerettigheter gjelder ikke og vold mot fiender av folkefellesskapet er legitimt (Bjørgo, 2018, s. 16-17).

Venstreekstrem terrorisme er en voldelig retning med utspring i politisk radikalisme som har utspring i ideologier som ligger til venstre for den parlamentariske sosialismen, ofte marxisme-leninisme.

Anarkistisk terrorisme er et samlebegrep for å beskrive terrorhandlinger begått av aktører med ulik anarkistisk ideologi og som fremmer en revolusjonær, antikapitalistisk og/eller antiautoritær agenda.

Etnonasjonalistisk og separatistisk terrorisme er et samlebegrep for aktører hvis voldshandlinger motiveres ut fra nasjonalisme, etnisitet og/eller religion. Grupperinger som den irske republikanske armé (IRA) og ETA – «Baskerland og frihet» hører innunder denne kategorien.

Ensaksterrorisme er et samlebegrep for aktører som benytter vold for å endre en spesifikk politikk eller praksis. Aktører innen denne kategorien har til nå gjerne vært voldelige dyrerettighetsekstremister, miljøekstremister eller antiabortekstremister.

5.2.1 Terrorisme i et historisk perspektiv

For å beskrive utviklingen innen moderne terrorisme henvises det ofte til Rapoport (2004) sin inndeling i fire såkalte bølger. Den første omtales som den anarkistiske bølgen, og varte fra 1880-tallet fram til starten på første verdenskrig; den andre bølgen var fra slutten av første verdenskrig fra til 1960-tallet og refereres til som den antikoloniale; den ideologisk-revolusjonerende bølgen på 1970-tallet, og til sist den fjerde bølgen – den religiøst motiverte som har vart fra 1979 til i dag.

Ser man på utviklingen i Vest-Europa siden 1970-tallet, er det fire overordnede utviklingstrekk som er tydelige ifølge Johansen og Gråtrud (2018, s. 24). For det første har det vært en klar nedgang i statsstøttet terrorisme, særlig som følge av bortfall av støtte til marxistiske og nasjonalistiske opprørs- og terrorgrupper i Vest-Europa etter den kalde krigens slutt. Et annet sentralt utviklingstrekk er hvordan religiøst motivert terrorisme og spesielt ekstrem islamisme har dominert trusselbildet de siste tjue årene. Et tredje utviklingstrekk er at terrortrusselen har blitt mer transnasjonal. Der hvor IRA i Nord-Irland eller den baskiske separatistgruppen ETA hovedsakelig fokuserte på geografisk avgrensede områder, er terrortrusselen fra jihadistiske grupper som IS og al-Qaida global. Til slutt har internasjonal terrorisme blitt mer dødelig, spesielt jihadistisk terrorisme; først gjennom al-Qaida-nettverket, deretter gjennom terrorgruppen som for tiden kaller seg Den islamske staten (IS; også kjent som ISIL).

For Norge sin del var 22. juli-angrepene i 2011 skjellsettende og en av de verste terrorhendelsene i moderne europeisk historie. Til sammen 77 personer ble drept i terrorangrepene i Oslo og på Utøya.

5.2.2 Endringer i strategi og taktikk i Vest-Europa

Utviklingen i terroristers valg av angrepsmål og -metoder preges i høy grad av kontinuitet (Johansen & Gråtrud, 2018). Hovedtrekkene de siste fire tiårene er at sikkerhetsstyrker, sivilbefolkningen og nærings- eller myndighetsmål har vært de vanligste angrepsmålene, mens bombeangrep, bruk av skytevåpen eller bruk av hugg-/stikkvåpen har vært de mest brukte angrepsmetodene. Storparten av terrorangrep skjer på land, mens det har vært en nedgang i antall terrorplott mot luftfarten de siste ti årene. Terrorangrep mot maritime mål er svært sjelden i Vest-Europa.

Det har likevel skjedd noen endringer. I en gjennomgang av jihadistiske terrorangrep i Vest-Europa fra 1994-2013, fant Nesser og Stenersen (2014) at utviklingen har gått fra å drepe flest mulig vilkårlige personer til mer målrettede angrep mot bestemte institusjoner eller samfunnsgrupper. I en nyere studie hvor det ble sett på hvilken effekt IS har hatt på terrortrusselen i Vest-Europa, fant Nesser *et al.* (2016) mer kontinuitet enn endring. Hovedmotivasjonen for jihadistisk terrorisme var også omtrent som før; avskrekke og hevne europeisk deltagelse i militære intervensjoner.

Bombeangrep med improviserte eksplosive innretninger (IED-er) har over en lang periode vært det foretrukne angrepsvåpenet (Europol, 2020b; Nesser & Stenersen, 2014; Nesser *et al.*, 2016).

I perioden 2008–2013 involverte 65 % av alle terrorplott bruk av IED-er. Til sammenligning rapporterte Europol (2020b, s. 19-20) at nærmere halvparten av alle rapporterte jihadist-inspirerte terrorangrep eller avvergede terrorplott, involverte bruk av eksplosiver. Når det gjelder type eksplosiver, har hjemmelagde eksplosiver blitt mer vanlige. Spesielt gjelder dette bruk av triaceton triperoksid (TATP), men også andre blandinger er vanlige. Ifølge Europol (2020b) synes det som at også høyreekstreme grupperinger viser økende interesse for eksplosiver.

Samtidig har det vært en dreining mot bruk av skytevåpen og hugg-/stikkvåpen (Nesser & Stenersen, 2014; Nesser *et al.*, 2016). Man har også sett at kjøretøy i økende grad har blitt brukt som våpen (Johansen & Gråtrud, 2018, s. 25; Nesser *et al.*, 2016). Særlig etter 2015 har bruk av kjøretøy og hugg-/stikkvåpen vært dominerende. Det kan være flere grunner til trenden med bruk av enklere våpen, men det er nærliggende å peke på at vesteuropeiske sikkerhetstjenester blitt bedre på å avverge angrep; terroristene har tilpasset seg dette ved å gjøre taktiske grep for å unngå å bli oppdaget (Johansen & Gråtrud, 2018, s. 26).

Det har svært få hendelser med bruk av kjemiske, biologiske eller radioaktive stoffer i nyere tid i Vest-Europa. I 2019 rapporterte ingen EU-land om CBRN-relaterte terrorhendelser (Europol, 2020b, s. 20). Imidlertid rapporterer Europol (2020b) at terroraktører fortsetter å diskutere CBRN i lukkede internettforum og sosiale medier, spesielt når det gjelder fremstilling og spredning av kjemiske eller biologiske trusselstoffer. Det er også en vedvarende bekymring fra myndighetenes side knyttet til stjålet radioaktivt materiale og radioaktivt materiale på avveie på verdensbasis (Europol, 2020b, s. 21).

En annen endring er dreiningen fra sentralstyrte og komplekse terrorangrep med flere utøvere, til terrorangrep hvor det kun er én utøver under angrepet.[16] Både Politiets sikkerhetstjeneste (2017) og en nyere litteraturstudie av såkalt *soloterrorisme* (Kenyon *et al.*, 2021), peker på mange av de samme drivkreftene for fenomenet. For det første kan soloterrorisme forstås som en taktikk i et større repertoar av angrepsformer, hvor soloterror kan være sentralstyrte, delegerte eller inspirerte angrep. For det andre kan soloterror være en strategi som kan omtales som «lederløs motstand», noe som gjerne er forbundet med høyreekstremisme. For det tredje er soloterror et resultat av terrorgrupperingers egne ressurser (eller rettere sagt mangel på sådanne), samt innsatsen fra etterretnings- og sikkerhetstjenester mot ekstreme miljøer. Videre er internett en sentral drivkraft, både når det gjelder radikalisering og opparbeidelse av kunnskap om gjennomføring av terrorhandlinger. Det er derfor få soloaktører som kan karakteriseres som «ensomme ulver». Imidlertid finnes det ikke noen unik sosiodemografisk profil for soloaktører, selv om utenforskap og psykiske lidelser synes å være sårbarhetsfaktorer (Kenyon *et al.*, 2021; Politiets sikkerhetstjeneste, 2017). Et annet trekk er at soloaktører bruker lang tid på å planlegge og forberede terrorangrep. Videre opplever en betydelig andel en form for situasjonelt stress

[16] Her skal det dog nevnes at soloterrorisme har vært relativt utbredt blant høyreekstremister siden 1980-tallet; se Ellis, C., Pantucci, R., de Roy van Zuijdewijn, J., Bakker, E., Gomis, B., Palombi, S. & Smith, M. (2016). *Lone-Actor Terrorism. Final Report* (Countering Lone-Actor Terrorism Series No. 11). Royal United Services Institute for Defence and Security Studies.

(frustrasjon, krenkelse) i perioden før de gjennomfører en terrorhandling. Påkjenninger og stressede livssituasjoner kan derfor medføre økt sårbarhet overfor terrorpropaganda og radikalisering over internett (Politiets sikkerhetstjeneste, 2017, s. 9).

5.2.3 Terrorisme i Vest-Europa i tiden fremover

Selv om empiriske funn tilsier en betydelig grad av konsistens og stabilitet i terroraktørers angrepsmål og -metoder (jf. kapittel 5.2.2), er det likevel knyttet stor usikkerhet til forventet utvikling innenfor terrorisme. Terrortrusselen er kompleks og må ses i sammenheng med påvirkende faktorer som samfunns- og sikkerhetspolitiske forhold. Både kapasiteter som utgjør trusselen og evnen myndighetene har til å forebygge, detektere og håndtere vil variere fra land til land. Dette gjør det også vanskelig å se på langsiktige utviklingstrekk innen feltet. For å vurdere forventet utvikling av terrorisme i Vest-Europa i tiden fremover, er det derfor nødvendig å vurdere sentrale drivkrefter for terrorisme, samt hvordan etterretningstjenester- og sikkerhetstjenester vurderer terroraktørers intensjoner og kapabiliteter.

5.2.3.1 Fremtidig konfliktutvikling

Fremtidig konfliktutvikling er en viktig drivkraft for terrorisme. Dette skyldes både fordi internasjonale konflikter kan føre til radikalisering i Norge og fordi konfliktene kan bli en arena for trening eller fremmedkrigervirksomhet. I de senere årene har det store skillet mellom jihadister og høyreekstremister vært at førstnevnte har hatt konfliktområder hvor de har kunnet være aktive (Afghanistan, Irak, Syria og nå Sahel), mens høyreekstremister har manglet en samlende konflikt. Internett har derfor relativt sett vært viktigere for høyreekstremister. Dog ser det nå ut til at Ukrainakonflikten fra 2014 kan være en samlende konflikt for høyreekstremister.

Konfliktutviklingen både globalt og regionalt i et langsiktig perspektiv vurderes som usikker. På én side observerer man i dag en nedgang i mellomstatlige konflikter. Samtidig har det blitt mange flere konflikter siden 2012 hvor én eller flere sider består av ikke-statlige aktører (Beadle *et al.*, 2019). Sistnevnte trend har også betydning for terrorisme. Det er grunn til å forvente at oppslutningen om terrornettverk fortsetter å være tilstede i regioner hvor konflikter vedvarer (Hegghammer, 2016). Spesielt gjelder dette Midtøsten, Nord-Afrika og Sør-Asia (Beadle *et al.*, 2019, s. 208-209). Uttrekkelse av vestlige militære styrker fra Afghanistan, Irak og Syria kan gjøre situasjonen i regionen og særlig i Afghanistan, mer ustabil. Videre kan tilbakekomst av fremmedkrigere øke antallet av såkalte entreprenører i Vest-Europa som fungerer som bindeledd i terrornettverk og som har stor betydning for planlegging av terrorangrep (Hegghammer, 2016). I tillegg kan økende stormaktsrivalisering gjøre internasjonalt samarbeid om terrorbekjempelse vanskeligere. Det amerikanske National Intelligence Council (2021, s. 107) vurderer det som mulig at Kina og andre fremvoksende stormakter kan gjøre det vanskeligere for USA å hindre at fremmedkrigere reiser til konfliktsoner eller å drive kontraterroroperasjoner i andre land.

5.2.3.2 Terroraktørers bruk av teknologi og internett

Større spredning av avansert teknologi til ikke-statlige aktører kan også få betydning for terrorismeområdet og endre det gjeldende trusselbildet. Eksempelvis kan autonome systemer og droneteknologi (kapittel 4.5.6) benyttes til gjennomføring av terrorangrep. Man ser også i økende grad at terroraktører benytter krypterte kommunikasjonsløsninger (kapittel 4.5.2) for radikalisering, rekruttering og deling av terrorangrep. Det samme gjelder bruk av kryptovaluta (kapittel 4.5.2.2).

Videre kan kunstig intelligens (kapittel 4.5.3) og sosiale medier (kapittel 4.5.4) benyttes til generering og spredning av (målrettet) terrorpropaganda. Nedslagsfeltet, rekkevidden og tidsaspektet for spredning av informasjon (og desinformasjon) på internett gir aktører mulighet til å kommunisere hva som helst til hvem som helst i løpet av sekunder. Dette kan gi en rekke utfordringer: For det første er det utfordrende å finne den informasjonen en trenger. For det andre vil en alltid finne informasjon – riktig eller gal – som er med på å støtte de fleste synspunkt. Dette krever at brukere av informasjon har kunnskap om kildekritikk og evner å både dobbeltsjekke kilder og lete etter motstridende argumenter for å finne valide svar. Og kanskje vanskeligst – akseptere at det ikke finnes én sannhet, men at forskningsresultater, løsninger, påstander og tiltak baserer seg på best tilgjengelige kunnskap og i de aller fleste tilfeller er beheftet med usikkerhet. En slik fragmentering av informasjons- og nyhetskilder kombinert med sosiale medier-algoritmer, kan forsterke fremvekst av konspirasjonsteorier. En slik utvikling hvor fakta stadig utfordres og hvor myndighetene i økende grad mister kontrollen over «narrativet», kan få store konsekvenser for samfunnssikkerheten fremover. Dette fremheves også i Politiets sikkerhetstjeneste (2021) sin nasjonale trusselvurdering, hvor det trekkes frem at 10-20 år gammel terrorpropaganda fortsatt diskuteres og distribueres på internett. Utfordringer knyttet til konspirasjonsteorier omtales nærmere i kapittel 6.2.4.

Demokratisering av kunnskap om syntetisk biologi og bioteknologi (kapittel 4.5.8) kan også gjøre det lettere for terroraktører å fremstille og spre biologiske trusselstoffer. Enn så lenge har imidlertid dette vist seg å være vanskelig for slike aktører (Europol, 2020b, s. 21). Det er også grunn til å frykte at terroraktører vil fortsette å utnytte 3D-printing til fremstilling av våpen.

Terrorangrepet 9. oktober 2019 i Halle i Tyskland eksemplifiserer hvordan en soloaktør kan utnytte teknologi for å begå terrorhandlinger. Den 27-år gamle mannen er den første kjente terroraktøren i Vest-Europa som har benyttet selvlagde våpen, inkludert et automatvåpen og flere IED-er. Videre ble terrorangrepet livestreamet på en online spillplattform. Ifølge hans manifest, ønsket han å demonstrere gjennomførbarheten til selvlagde våpen (Europol, 2020b; Koehler, 2019). Det er grunn til å tro at dette terrorangrepet vil inspirere flere til lignende forsøk.

Tønnessen (2017) har sett på nærmere IS og deres bruk av teknologi. Funnene viser at terrororganisasjonen ikke nødvendigvis benytter den mest avanserte og kostbare teknologien, men er svært dyktig på å benytte teknologi som er billig og lett tilgjengelig. Både IS og andre terrorgrupper benytter i hovedsak teknologi i defensive fremfor offensive operasjoner. Det vil si at de tilsynelatende bruker mer ressurser på å beskytte seg mot teknologien som motstanderen benytter enn å utnytte teknologien i egne angrep. Litteraturen om teknologibruk i terrororganisasjoner

kan deles inn i tre områder: droneteknologi, kommunikasjonsteknologi og CBRN. Størst suksess har IS hatt med relativt enkle krypterte kommunikasjonsverktøy for å fjernassistere og veilede angripere i Europa. Innen droneteknologi og CBRN har angrepene frem til 2017 i all hovedsak vært preget av improvisasjon og hjemmelagde løsninger (Tønnessen, 2017).

Når det gjelder terroraktørers fremtidige bruk av teknologi, mener Tønnessen (2017) at spørsmålet om «hvorfor, og under hvilke forhold, vil en terrorgruppe benytte sine begrensede ressurser på å tilegne seg nye teknologiske kapabiliteter?» bør besvares. Det må også tas i betraktning at teknologiutviklingen vil gi myndigheter nye muligheter til å avdekke og bekjempe terrorplanlegging. I tillegg kan langtrekkende presisjonsvåpen gjøre det lettere å angripe terrorleirer i land hvor det er vanskelig å gå inn med militære landstyrker (National Intelligence Council, 2021, s. 107). En slik utvikling kan peke i retning av dreining mot fordekte terroroperasjoner som strategi (Stenersen, 2017).

5.2.3.3 Forholdet mellom terrorisme og migrasjon

Helbling og Meierrieks (2020) har nylig sett på sammenhengen mellom terrorisme og migrasjon. Deres litteraturgjennomgang viser at det er lite forskning som uten forbehold tilsier at migrasjon fører til mer terrorisme, spesielt i vestlige land. Imidlertid pekes det på at innvandring fra konfliktland kan medføre spredning av terrorisme, men det medfører nødvendigvis ikke til *økt* terrorisme i mottakerlandet. Dette vil være avhengig av forholdene i mottakerlandene og hvor godt innvandrerne integreres.

Videre viser data fra 154 land for årene 1970-2007 at land som tar mot flyktninger, er mer utsatt for terrorhandlinger (Helbling & Meierrieks, 2020). Enkelte studier peker på dårlige forhold i flyktningeleirer som forklarende årsaker, mens andre studier konkluderer med at enhver økning i terrorisme som følge av innvandring, skyldes at flyktninger blir syndebukker; altså målet for terrorhandlinger. Ifølge Helbling og Meierrieks (2020) er denne dimensjonen underkommunisert både i den offentlige debatten og i empiriske studier.

Helbling og Meierrieks (2020) peker også på at transnasjonal terrorisme kan endre folks holdninger til migrasjon og innvandring. Dette kan igjen påvirke valgresultater og føre til endringer i innvandringspolitikk. Det kan også føre til fremvekst av ytterliggående grupperinger på ytre høyre (jf. kapittel 5.3.1). Forskningen indikerer også at strengere innvandrings- og integreringspolitikk har begrenset effektivitet med hensyn på å bekjempe terrorisme. Spesielt kan politikk som fører til segregering (jf. kapittel 4.3.2), bidra til fremmedgjøring og radikalisering (Dreher *et al.*, 2020). Dette kan tyde på det er en forsterkende koblingsmekanisme mellom transnasjonal jihadisme, anti-innvandrings- og segregeringspolitikk og høyreekstremisme (Helbling & Meierrieks, 2020). Dette er en potensiell sårbarhet som kan utnyttes av fremmede stater til subversjon, og er et forhold som bør studeres nærmere.

5.2.3.4 Myndighetenes bekjempelse av terrorisme

Hvordan myndighetene møter terrorisme er også av sentral betydning for den videre utviklingen. Gjennom de ulike bølgene av terrorisme som Rapoport har identifisert (jf. kapittel 5.2.1),

finner man noen karakteristiske trekk for terrorgruppers strategi som går igjen: asymmetrisk krigføring, utkjempelse av en utmattende krig, bruk av propaganda, karismatisk lederskap, fremprovosering av en overreaksjon fra myndighetenes side, samt etablering av legitimitet for sin sak (Parker, 2014). Likevel har myndighetene ofte møtt terrorisme med omfattende – gjerne militær – maktbruk, internering og til og med tortur. Terrorangrepene 11. september 2001 i USA og den påfølgende krigen mot terror er et eksempel på dette, hvor Amnesty International (2005) og andre har kritisert tiltakene og metodene for å bryte menneskerettigheter. I tillegg ser man ofte at befolkningen blir skadelidende i bekjempelsen av terrorhandlinger og tvinges til å «velge side» (Nyadera & Bincof, 2019; Parker, 2014).

For myndigheter i Vest-Europa er det et dilemma å finne riktige mottiltak etter perioder med mange terrorangrep. Etter hvert som mottiltakene begynner å virke og myndighetene blir bedre kjent med aktørene, går antall angrep ned. Da kan det bli vanskelig både av økonomiske og demokratiske grunner å fortsette med like repressive tiltak, og mottiltakene slippes opp igjen. Dette kan gi terroraktørene mulighet til å bli mer aktive. Det er en frykt for at denne dynamikken gjentar seg nå med IS.

Riktig kalibrering og utforming av mottiltak mot terrorisme er derfor en av de aller viktigste faktorene både for å bekjempe og for å forklare fenomenet. Så lenge terrorisme bekjempes som en militær kampanje og ikke som en langvarig prosess hvor menneskerettigheter og individets rettssikkerhet ivaretas, er det grunn til å frykte at fenomenet vil vedvare og finne nye former (Morris *et al.*, 2021; Nyadera & Bincof, 2019; Parker, 2014). Samtidig må det forventes at terroraktører vil fortsette å forsøke å akselerere kampen for sin sak gjennom å fremprovosere en overreaksjon fra myndighetenes side.

5.2.3.5 Utvikling i terroraktørbildet i Norge

I sin nasjonale trusselvurdering forventer Politiets sikkerhetstjeneste (2021) at ekstrem islamisme og høyreekstremisme fortsatt vil utgjøre de største terrortruslene mot Norge på kort sikt. Hvorvidt trusselen fra ekstreme islamister vil vedvare, tilspisse seg eller avta, vil avhenge av flere forhold; inkludert om islam- og innvandringsfiendtlige grupper vil fortsette med handlinger som oppfattes som krenkende blant muslimer og hvordan ekstreme islamister vil respondere. Hendelser som oppfattes som krenkende kan spres raskt via sosiale medier og nå et stort publikum på verdensbasis. Gjentagende slike hendelser kan øke risikoen for at det vokser frem en ny generasjon ekstreme islamister. PST har også sett eksempler på at bilder og videoer bevisst redigeres for å skape et inntrykk av at Norge er en nasjon som krenker islam. Det forventes derfor at digitale nettverk fortsatt vil være sentrale både når det gjelder radikalisering og angrepsplanlegging. PST forventer videre at norske ekstreme islamister fortsatt vil støtte globale terrornettverk, inkludert gjennom finansiering via banker eller såkalt hawala.

Når det gjelder høyreekstremisme, vurderer Politiets sikkerhetstjeneste (2021) at terrortrusselen primært kommer fra enkeltpersoner som har blitt radikalisert på digitale plattformer. I tillegg peker PST på at høyreekstremisme har blitt mer transnasjonal de senere årene. Følgelig kan internasjonale hendelser også påvirke det norske trusselbildet.

Muslimer, ikke-vestlige innvandrere, jøder, LHBT+,[17] tradisjonelle medier og myndigheter og politikere (oftest fra den politiske venstresiden) er sentralt i fiendebildet til høyreekstreme. På kort sikt forventer Politiets sikkerhetstjeneste (2021) at stadig flere vil radikaliseres til høyreekstremisme. PST ser også at rus, psykiatri, kriminalitet og tilpasningsproblemer er sårbarhetsfaktorer for personer som tilhører ytre høyre. Økonomisk usikkerhet, arbeidsledighet og sosial isolasjon som konsekvenser av covid-19-pandemien, kan derfor bidra til at flere trekkes mot ekstreme diskusjonsfora på internett hvor høyreekstrem ideologi blandes med såkalte memer, humor, klipp fra spill og filmer, samt konspirasjonsteorier. PST mener derfor at det er en fare for at høyreekstrem propaganda normaliseres og ufarliggjøres, noe som kan bidra til å senke terskelen for bruk av vold.

Særlig kan saker som oppleves som trusler mot den «hvite rase og kultur» bidra til å radikalisere enkelte til å forsøke å begå terrorhandlinger. Slike saker er gjerne knyttet til innvandringspolitikk eller økt globalisering. Politiets sikkerhetstjeneste (2021) er særlig bekymret for grupper som eksplisitt oppfordrer enkeltpersoner til fysisk kamp og som tar til orde for å fremskynde (akselerere) en total kollaps av samfunnet ved hjelp av terror. Såkalte akselerasjonister er av den oppfatning at en rasekrig mellom hvite og alle andre raser er nært forestående og at det derfor haster med å igangsette en konflikt som anses som uunngåelig. Gjerningspersoner i flere høyreekstreme terrorangrep har vært inspirert av dette tankesettet ifølge PST.

Når det gjelder trusselen fra venstreekstreme miljøer, har slike miljøer få aktive tilhengere i Norge og Politiets sikkerhetstjeneste (2021) forventer ikke at miljøene vil vokse i noen betydelig grad på kort sikt. Imidlertid kan internett bidra til informasjonsdeling og radikalisering på tvers av landegrenser også for disse miljøene. Bekjempelse av høyreekstremisme er fortsatt en samlende kampsak og det må derfor forventes at det kan skje voldelige sammenstøt mellom grupperinger på ytre venstre og ytre høyre i forbindelse med demonstrasjoner. Med økende fremvekst av høyreekstremisme, er det derfor fare for oppblomstring av venstreekstremisme som en motreaksjon. Det er derfor behov for mer kunnskap om venstreekstreme grupperinger.

Når det gjelder utviklingen innen annen ekstremisme, vurderer Politiets sikkerhetstjeneste (2021) at antistatlige strømninger (kapittel 5.3.3) kan ha et potensial for å radikalisere enkelte personer. PST peker også på at det har vært en vekst i radikale aktivistgrupper som fokuserer på klima-, miljø- og naturvernsaker. Selv om trusler og sjikane har forekommet i enkeltsaker, har de fleste aksjoner i Europa vært ikke-voldelige (Europol, 2020b).

5.2.3.6 Fremvekst av statsstøttet terrorisme?

Beadle *et al.* (2019, s. 163) peker på at hypotesen om at det vil bli vanligere for stater å bruke voldelige ikke-statlige aktører som et utenrikspolitisk virkemiddel, har styrket seg. Senere tids utvikling tilsier at en stadig større andel av verdens konflikter kan karakteriseres som såkalte «internasjonaliserte interne konflikter», hvor én eller begge parter i konflikten får militær støtte fra en ekstern stat. Beadle *et al.* (2019) viser blant annet til at siden 2015 har 37 % av verdens rundt 50 pågående interne konflikter vært internasjonaliserte, hvilket representerer det høyeste

[17] LHBT+ betegner lesbiske, homofile, bifile, transpersoner og andre seksuelle minoriteter og kjønnsminoriteter.

nivået av ekstern innblanding i interne konflikter siden andre verdenskrig. Til sammenligning var 20 % av rundt 35 konflikter internasjonaliserte i perioden 2005–2014.

Med økende stormaktsrivalisering (jf. kapittel 4.1.1) er det grunn til å spørre seg om man vil se en økning i statsstøttet terrorisme i tiden som kommer (Johansen & Gråtrud, 2018). En slik utvikling kan forsterkes gjennom staters økende bruk av sammensatte trusler (jf. kapittel 5.1.1). Dette kan føre til at terroraktørers kapasitet kan styrkes, både når det gjelder *modus operandi* og bruk av teknologi (Johansen & Gråtrud, 2018, s. 163). Eksempelvis kan angrepsformer som datanettverksangrep og bruk av CBRN, som tidligere har vært for avanserte for terroraktører, bli mulige. Terroraktører kan også få tilgang til tyngre våpen som missiler. Statlige aktørers etterretningstjenester kan også hjelpe til med planlegging og målutvelgelse, inkludert øke terroraktørers kapasitet til å angripe mål som er vanskelig tilgjengelig eller godt sikret.

5.3 Samfunnsforstyrrelser

Sellevåg (2021, s. 54) beskriver *samfunnsforstyrrelser* som handlinger hvor en «ikke-statlig aktør ønsker å fremtvinge politisk endring/endring i politikk gjennom opptøyer, eller forsvare eget sosiale styresett gjennom å demonstrere evne og vilje til bruk av fysisk makt, påvirke sosial adferd og/eller andre kriminelle handlinger».

Ikke-statlige aktører som har som målsetning å forsvare eget sosiale styresett, er karakteristisk for personer eller grupperinger som ikke vil anerkjenne eller underlegge seg storsamfunnets grunnverdier og institusjoner, men heller styres etter egne lover, normer og strukturer. Eksempelvis kan aktørene styres etter en æreskode eller det utøves intern sosial kontroll gjennom å påvirke sosial adferd for å forsvare det sosiale styresettet. Selv om slike grupperinger i seg selv ikke nødvendigvis kan karakteriseres som kriminelle nettverk, kan enkeltmedlemmer være involvert i kriminelle handlinger. Eksempler på slike *voldelige, selvstyrende subkulturer* kan være grupperinger innenfor det såkalte «ytre høyre», borgerverngrupper, antistatlige, anarkistiske eller antirasistiske grupperinger, eller kriminelle gjenger og nettverk. I det følgende gis en beskrivelse av hvordan slike grupperinger kan utfordre rettssikkerheten i Norge.

5.3.1 Ytre høyre

Siden 1970-tallet har Norge hatt nazistiske og rasistiske grupperinger som har vært villige til å bruke vold. Mange av disse grupperingene var organisert rundt en fragmentert ideologi og tilfeldig organisering. På 1980-tallet ledet Arne Myrdal en rasistisk organisasjon mot innvandring. I 2001 ble Benjamin Hermansen drept av to nynazister på Holmlia i Oslo. De politiske og spontane reaksjonene etter dette drapet var så kraftige at nynazister og høyreekstremister ble fraværende i offentligheten.

Først 22. juli 2011 ble Norge for alvor utsatt for en politisk motivert terrorhandling (Bjørgo & Gjelsvik, 2017). Etter 22. juli har det i Norge vokst fram grupper og politiske organisasjoner som ligger langt ute på høyresiden i det politiske landskapet. Dette har gitt et nytt «politisk land-

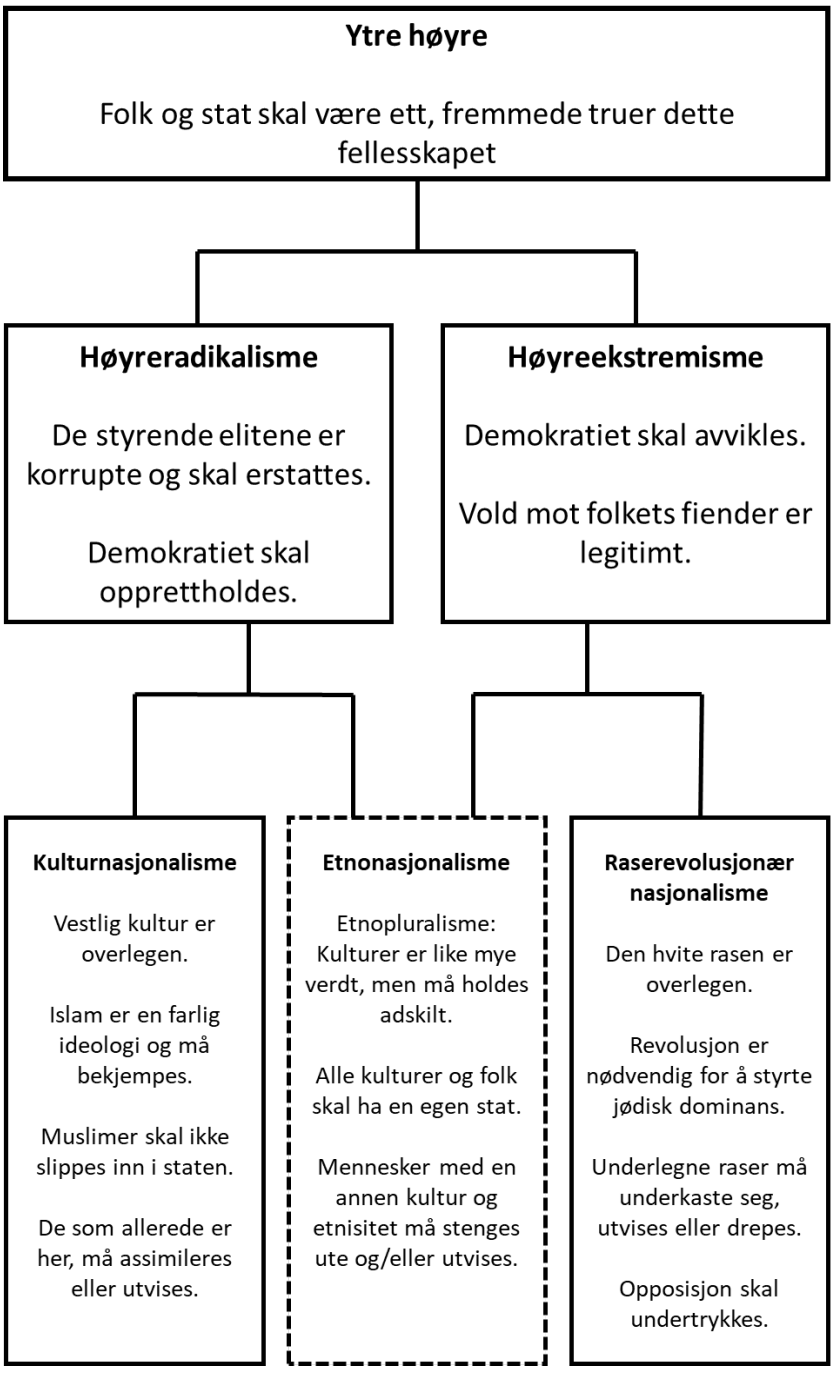
skap»; det såkalte «ytre høyre». De tradisjonelle samfunnsfiendtlige organisasjonene med antidemokratiske ideologier er fortsatt en realitet, men fremveksten av ekstreme, men legale høyreradikale grupper har vokst frem de siste årene. I Figur 5.1 er det gitt en fremstilling av hvordan disse miljøene skiller seg fra hverandre og hvilket ideologisk tankegods som utgjør grunnlaget for disse ulikhetene.

Under «ytre høyre» er det vanlig å skille mellom *høyreradikalisme* og *høyreekstremisme* (Figur 5.1). Til forskjell fra høyreradikale som mener at demokratiet skal opprettholdes, mener høyreekstremister at demokratiet skal avvikles, universelle menneskerettigheter gjelder ikke og vold mot fiender av folkefellesskapet er legitimt (Bjørgo, 2018, s. 16-17). Under høyreradikalisme finner man gjerne *kulturnasjonalister*, også omtalt som innvandringsmotstandere og islamkritikere. Eksempler på slike grupperinger er *Stopp Islamiseringen av Norge (SIAN)* og til en viss grad den nå oppløste borgervernsgruppen *Odins soldater*. *Raserevolusjonære nasjonalsosialister*, også omtalt som nynazister, er klassiske høyreekstremister som gjerne legitimerer bruk av vold. Eksempler på slike grupperinger er Norsk Front, Boot Boys, Vigrid og Den nordiske motstandsbevegelsen (DNM). Mellom kulturnasjonalister og raserevolusjonære nasjonalsosialister finnes *etnonasjonalister* som Alt-Right. Selv om etnonasjonalister vanligvis tar avstand fra vold, bryter slike grupperinger i så stor grad med samfunnets verdier at de grenser til ekstremisme (Bjørgo & Gjelsvik, 2018, s. 27-28).

Den nordiske motstandsbevegelsen representerer i dag den største og best organiserte grupperingen av raserevolusjonære nasjonalsosialister i Norge og Norden (Bjørgo & Gjelsvik, 2018, s. 68). DNM fremstår med en klassisk høyreekstrem raseideologi. De henter sine forbilder fra nazistiske ledere under 2. verdenskrig, fornekter Holocaust, praktiserer sterk intern kontroll og har en idé om at «noen» vil bryte ned kulturelle verdier i samfunnet og at de må gjøre seg «klare til kamp». Ifølge Bjørgo og Gjelsvik (2018, s. 143-144), må man forvente at DNM fortsatt vil være aktive i årene fremover og vokse noe. Denne vurderingen støttes av Politiets sikkerhetstjeneste (2021). Imidlertid pekes det på at vekstpotensialet for nasjonalsosialisme er mindre i Norge enn i for eksempel Sverige, blant annet av historiske årsaker. Det forventes også at DNM vil bli mer aktive i det offentlige rom og forsøke å gjennomføre minst en årlig demonstrasjon i en norsk by sammen med andre nordiske DNM-aktivister. Dersom den norske grenen av DNM blir større og sterkere, er det også grunn til å forvente at de blir mer aggressive og truende slik man har sett i Sverige.

Bjørgo og Gjelsvik (2018, s. 144) peker også på at miljøer inspirert av den såkalte identitær-bevegelsen og beslektede etnonasjonalistiske grupper, har blitt mer aktive. Det forventes at den pan-europeiske ungdomsbevegelsen *Generation Identitaire* vil få økende fotfeste i Norge. Slike bevegelser søker blant annet å fremme økt segregering langs etniske skillelinjer.

Kulturnasjonalistiske og antiislamske miljøer vil fortsatt være aktive. Spesielt gjelder dette på sosiale medier hvor enkelte går svært langt i å uttrykke hatefulle ytringer og trusler mot innvandrere, minoriteter, politikere og meningsmotstandere. Det forventes derfor at spredning av rasistiske, antidemokratiske og/eller voldsforherligende holdninger på nett vil fortsette å representere en stor utfordring for demokratiet og for politiet i årene fremover (Bjørgo & Gjelsvik, 2018, s. 144).



Figur 5.1 Kategorisering av grupperinger på det såkalte ytre høyre. Kilde: Bjørgo (2018).

5.3.2 Borgervern

Borgervern er et fenomen som i hovedsak omhandler «sivile som opptrer i en politirolle uten å ha politimyndighet», og som på ulike måter «tar loven i egne hender» (Bjørgo & Gjelsvik, 2018, s. 109-110). I følge Bjørgo og Gjelsvik (2018, s. 109-110), kan dette skje gjennom:

- Patruljering i gatene for å opprettholde lov og orden uten å ha politimyndighet eller annen autorisasjon
- Grensepatruljering rettet mot ulovlige immigranter
- Paramilitære militser som opptrer med uniformering og/eller bevæpning, enten med trening i det skjulte eller ute i offentligheten
- Vold og terror i form av privat avstraffelse uten lov og dom, gatejustis, og i ekstrem form, lynsjing og pogromer[18]

I tillegg har borgervernsgrupper også benyttet vold, trusler og trakassering for å underkue eller fordrive uønskede individer og grupper bort fra lokalsamfunnet.

Historisk er Ku Klux Klan i USA en av de mest omtalte borgerverngruppene. Ku Klux Klan ble etablert i 1870 og har med ulik intensitet vært en del av USAs mest kjente borgerverngrupper. Fremveksten av borgervern i en europeisk og til dels norsk kontekst har i nyere tid dels hentet et motiv og rekrutteringsgrunnlag i «migrasjonskrisen» som Europa har stått i de siste årene. Mye av aktiviteten og en ideologisk legitimitet spiller på dels fordekt rasisme, høyreekstrem politikk og fremmedfrykt.

I Norge har borgervernstanken resultert i blant annet to svært ulike former for borgervern, eksemplifisert gjennom *Odins soldater* og *Barnas Trygghet*. *Odins soldater* kan karakteriseres som et «tradisjonelt» borgervern. Odins soldater hevdet sin rett til å ta loven i egne hender når det gjaldt å forsvare kvinner fra mulige overgripere og andre truende krefter (Bjørgo & Gjelsvik, 2019). Organisasjonen eller grupperingen som kaller seg *Barnas Trygghet* er en annen form for borgervern, definert som *det digitale borgervernet*, og ble etablert som en Facebookgruppe som skulle drive en privatpraktiserende avsløring av pedofile og andre overgripere (Lomell, 2020).

Begge former for borgervern ønsker å fremstå som tilhengere av lov og orden og ønsker ikke å være i opposisjon til samfunnets verdier. De fremstår som idealistiske, de ønsker å bistå som gode borgere av samfunnet og å støtte politiets arbeid for å beskytte liv og helse.

Utfordringen med slike grupperinger er at de langt på vei er *overkonforme* (Heckert & Heckert, 2004; Herington & van de Fliert, 2018). De vil mere enn det samfunnet vil i en god sak. Nettopp i det faktum at de tilsynelatende fremstår som overkonforme i sin iver etter å forsvare grunnleggende verdier kommer problemene. Utfordringen for en rettsstat som den norske er at disse formene for borgervern spiller på eller rettferdiggjør sin aktivitet gjennom en dyp mistillit til det

[18] Pogrom er voldelige angrep på etniske minoriteter, først og fremst jøder og jødisk eiendom; se: *pogrom*. (u.å.). Store norske leksikon. Hentet 9. april 2021 fra https://snl.no/pogrom.

tradisjonelle rettsapparatet. Et viktig prinsipp i et moderne demokrati er at legitim rett til bruk av makt ligger til staten. Det er også en grunnleggende forutsetning i vårt demokrati å ha tillit til politiet (Meld. St. 29 (2019-2020), s. 8), og begge disse faktorene blir utfordret av slike former for borgervern.

En rettsstat er i sin grunnleggende form kjennetegnet av hvordan rettshåndhevelsen bygger på menneskerettigheter både for offer og gjerningspersoner. Utfordringen med borgervern er at det langt på vei er borgervernet selv som definerer situasjonen de selv er en løsning på. De etablerer en sannhet eller definerer et samfunnsproblem – gjerne fundert på en konspirasjonsteori – som de selv gir et tilbud til løsning på. Om problemet er et faktisk problem eller et innbilt problem og om borgervernet slik det organiseres er et svar på problemet, blir i mindre grad problematisert.

Borgervern utfordrer forestillingen om samfunnets og politiets evne til å løse sine oppgaver.

Hva fikk så unge menn til å slutte opp om Odins soldater? Flere teorier kan forklare dette, men innledningsvis kan Odins soldater forstås som en tradisjonell subkultur, eller mer presist et marginalt miljø. Det å være sammen i grupper, dele felles symboler og dyrke en imaginær ideologi er typisk i fremveksten av slike grupper. En annen forklaring er at 70 % av de registrerte medlemmene hadde kriminell fortid av ulik alvorlighetsgrad. Nå skulle de gjøre opp og representere noe positivt:

> *Rather than being known as the town's troublemakers and petty criminals they could now become heroes from whom people could seek protection (Bjørgo & Gjelsvik, 2019, s. 263).*

En tredje og helt åpenbar forklaring ligger til det politiske forsøkt skjult gjennom gode motiver. Odins soldater ble en ideologisk fordekt høyreradikal gruppering med en klar slagside mot de tradisjonelle høyreekstreme verdiene, kamuflert som en legitim og god samfunnsgjerning. På det meste hadde Odins soldaters Facebook-gruppe 4000 «medlemmer». I de politiske miljøene fikk dette liten støtte og politiet advarte mot denne formen for borgervern. Etter kort tid ble hele grupperingen oppløst. Interne stridigheter og en uklar eller helt fraværende organisasjonsstruktur gjorde Odins soldater til en politisk døgnflue. Politiet ble etter hvert klar over denne aktiviteten og nedla et forbud mot å patruljere i gatene i en selvkomponert uniform. Odins soldater fikk et kort «politisk liv», men fenomenet kan være verdt å se på fordi Odins soldater legitimerte hele sin eksistens og sine gjerninger som et uttrykk for mistillit til det bestående i kombinasjon med en klar fremmedfiendtlig ideologi. Dersom det oppstår mistillit i befolkningen til politiets evne til å bekjempe kriminalitet i det digitale rom, kan nye former for digitalt borgervern oppstå.

5.3.3 Antistatlige grupperinger

Den såkalte «Frimannbevegelsen» er et eksempel på en antistatlig gruppering som ikke ønsker å tilslutte seg samfunnets grunnverdier og institusjoner. Karakteristisk for slike miljøer er at de ikke anerkjenner sin tilhørighet til staten, men hevder sin rett til å leve på siden av samfunnet som «levende mennesker». I Norge er denne bevegelsen foreløpig relativt marginal, men den er et godt eksempel på hvor ressurskrevende slike bevegelser kan være når det gjelder å motarbeide offentlige myndigheter (Færseth, 2017).

Frimannbevegelsen har «spesialisert» seg på konspirasjonsteorier mot jurister og embetsmenn i rettsapparatet (Libell, 2018). Jurister og statsadvokater er ofte sentrale hovedpersoner i konspirasjonsuniverset, hvor advokater ansees å være en del av den sammensvergelsen som styrer og bestemmer i landet. Frimannsbevegelsen mener at grunnloven og lovverket forøvrig er falskt. Det er skrevet koder som bare noen (jurister og andre) forstår. Det skal finnes en opprinnelig juss som fritar alle fra å betale skatt, gjeld, barnebidrag og andre «falske», juridiske forpliktelser. Videre oppfatter de menneskerettighetene som viktige og som beskyttende for den aktiviteten de driver, samtidig som FN ansees som en falsk organisasjon og styrt av eliten. Gjennom å nekte å forholde seg til pålegg fra politiet og domstoler eller ved å ringe og skrive til offentlige kontorer og banker for å få slettet statsborgerskap og gjeld, kan de binde opp store offentlige ressurser og gjerne gjennom å mobilisere støtte fra likesinnede når de har problemer. Det er også eksempler på at de trakasserer eller utøver vold mot offentlige tjenestepersoner (Færseth, 2017).

5.3.4 Gjengkriminalitet og kriminelle nettverk

I NOU 2020: 4 (s. 125-129) er det gitt en overordnet beskrivelse av gjengkriminalitet i Norge. Her er en *kriminell gjeng* definert som (NOU 2020: 4, s. 128):

> *En selvdefinert eller eksternt definert gruppe med skremselskapital som utviser evne til å operere over tid med en orientering mot alvorlig kriminalitet, herunder narkotikaomsetning og aggressiv adferd i det offentlige rom. Andre fellestrekk er ofte; bruk av symbolske uttrykk for gruppeidentitet, geografisk tilhørighet, rekruttering av unge personer til kriminalitet, krav om lojalitet og organisering rundt noen få lederskikkelser.*

Kriminelle gjenger i Norge varierer fra «løst sammensatte nettverk til familiebaserte eller brorskapsliknende grupperinger med en tydelig hierarkisk struktur» (NOU 2020: 4, s. 125). Gjengrelaterte aktører kan således være kriminelle ungdomsgrupperinger, tradisjonelle gjenger som såkalte 1 % MC-gjenger,[19] gategjenger eller nye internasjonale gjenger, eller erfarne enkeltaktører/familier/bakmenn med deres kontaktnett (NOU 2020: 4, s. 128-129). Begrepet *kriminelle*

[19] 1 % MC-gjeng er beskrevet som en «motorsykkelklubb som selv definerer seg som lovløs og utenfor det norske samfunnet, med sine egne lover og regler»; se NOU 2020: 4. *Straffelovrådets utredning nr. 1 — Kriminalisering av deltakelse i og rekruttering til kriminelle grupper*. Justis- og beredskapsdepartementet.

gjenger er således nært knyttet til *kriminelle nettverk* som er beskrevet av politiet som (Politiet, 2021, s. 12):

> *[M]iljøer, gjenger, grupperinger eller sett av individer som er knyttet sammen gjennom kriminalitet.*

Samtlige politidistrikt rapporterer tilstedeværelse av en eller flere gjengaktører. Det sentrale Østlandet og særlig Oslo er hovedområdet for flere kriminelle gjenger, mens det er overvekt av 1 % MC-gjenger blant gjengaktører som har tilhold i flere politidistrikter. Gjengenes kriminelle virksomhet er i hovedsak relatert til alvorlig narkotikakriminalitet, volds- og trusselbasert kriminalitet, samt økonomisk kriminalitet (NOU 2020: 4, s. 125-126).

I sin trusselvurdering for 2021 anser politiet det som sannsynlig at internasjonale kriminelle nettverk vil forsøke å utvide sin aktivitet i Norge (Politiet, 2021, s. 12). Videre vurderes det som meget sannsynlig at unge personer vil rekrutteres til gjengkriminalitet, hvor en stor del av rekrutteringsaktiviteten foregår på sosiale medier (Politiet, 2021, s. 13). I den såkalte Saltorapporten viser statistikken at det har vært en tydelig stigende tendens for registrert kriminalitet i aldersgruppen 10–17 år fra 2015; barn og unge som blir registrert for gjentatt kriminalitet, utgjør nesten halvparten av anmeldelsene i 2019 (Oslo politidistrikt, 2019a, s. 5).

Særlig voldsbruk og såkalt skremselskapasitet trekkes frem som en nødvendig kapasitet og et varemerke for gjengaktørene. Vold er altså ikke bare akseptabelt, men også forventet av aktører som deltar i kriminelle gjenger. Eksempelvis forventes det å stille opp når andre i gjengen trenger det eller når det skal mobiliseres til hevnoppgjør. Politiet opplever også at det oppmuntres til motarbeidelse av politiets arbeid og at rettsprosesser påvirkes, eksempelvis ved at truende adferd mot politiet dokumenteres og spres via sosiale medier (NOU 2020: 4, s. 127).

Åpent narkotikasalg, ordensforstyrrelser og voldsbruk i det offentlige rom vil påvirke trygghetsfølelsen i det offentlige rom. Også i Norge observerer politiet at gjengaktører og særlig kriminelle ungdomsgjenger ofte er virksomme i boområder med sosioøkonomiske utfordringer (NOU 2020: 4, s. 127). Imidlertid er det bred enighet blant norsk politi og politikere om at såkalte «svenske tilstander» – altså områder hvor volden er av en slik karakter at det er forbundet med fare for politiet å gå inn i områdene (såkalte «no-go-soner») – ikke finnes i Norge (Egge & Solhjell, 2018, s. 39). Norge har hatt en annen økonomisk situasjon og bosettingspolitikk enn Sverige som har bidratt positivt i så måte (NOU 2020: 4, s. 127).

Samtidig kan boområder med sosioøkonomiske utfordringer bidra til såkalt territoriell stigmatisering og gutter som «leker ghetto» (Rosten, 2017). NOVA-forsker Monika Grønli Rosten (2017) beskriver hvordan unge menn bruker og forsterker fordommene de opplever andre har mot dem, som en håndteringsmekanisme:

> *Å «leke getto» handler om å «tøffe seg». […] Du vet, du er aldri så kul som når du akkurat har banka noen.*

Territoriell stigmatisering, dystopiske fremstillinger, sosioøkonomiske utfordringer og gjengkriminalitet kan således gjensidig påvirke og forsterke hverandre negativt (Egge & Solhjell, 2018, s. 53-54; NOU 2020: 4, s. 127; Rosten, 2017).

Egge og Solhjell (2018, s. 54-56) peker på følgende tre drivere for å forebygge fremvekst av voldelige subkulturer og utenforskap: (i) *Sosial mobilitet* gjennom utdanning, deltagelse i arbeidslivet og å komme seg inn på boligmarkedet. (ii) *Deltagelse og innflytelse*, det vil si demokratisk deltagelse og sivilsamfunnets inkluderende kapasitet. (iii) *Rettslig vern*, hvor publikums opplevelse av rettferdig og lik behandling er avgjørende for tilliten til politiet og rettsvesenet.

Samfunnets evne (eller mangel på sådan) til innsats på disse tre områdene vil derfor påvirke fremtidige utvikling innen gjengkriminalitet. Dette vil være avhengig av samfunnets politiske vilje og evne til å sikre innbyggerne lik tilgang på tjenester, rettigheter og beskyttelse, samt innbyggernes ønske, vilje og/eller mulighet for å tilslutte seg samfunnets grunnverdier og institusjoner (Egge & Solhjell, 2018, s. 45-50). Dersom samfunnet ikke lykkes på disse områdene, er det fare for at (unge) gjengaktører kan rekrutteres til organiserte kriminelle nettverk (jf. kapittel 5.5.2). Med økende økonomisk segregering og opphoping av levekårsutfordringer i norske storbyer (jf. kapittel 4.3.2), er det fare for at utviklingen går i negativ retning.

5.4 Ikke-spredning

Stormaktsrivaliseringen mellom USA, Kina og Russland påvirker også ikke-spredningsområdet,[20] særlig forhold som omhandler CBRNE.[21] For det første har flere rustningskontrollavtaler for kjernevåpen bortfalt eller blitt svekket. Bortfallet av INF-avtalen i 2020 gjør at det er igjen fritt frem for USA og Russland å utplassere landbaserte missiler med rekkevidde mellom 500 km og 5500 km, hvilket kan vesentlig endre sikkerhetssituasjonen for Europa (Høibråten & Kippe, 2020, s. 71-72, 83). I tillegg stod New START-avtalen mellom USA og Russland lenge i fare for å ikke bli fornyet etter utløpet i februar 2021, men denne ble reddet i siste liten etter presidentskiftet i USA i januar 2021. New START ble forlenget med fem år og kan ikke forlenges ytterligere.

Det er lite som tyder på at kjernevåpnenes rolle vil bli svekket i nærmeste fremtid, og det er mange moderniserings- og utviklingsprosesser i gang. En konsekvens av at våpnene er blitt mer presise, er at sprengkraften kan reduseres. Mange vil hevde at dette kan senke terskelen for å ta våpnene i bruk. Videre ser det ut til å bli stadig flere våpensystemer som kan utstyres med enten konvensjonell eller kjernefysisk ladning, noe som gjør det vanskeligere for motparten å vite om et angrep er kjernefysisk eller ikke. Resultatet kan bli at et konvensjonelt angrep møtes med et kjernefysisk motangrep og derav følgende eskalering. Nevnes bør også de fem til dels spektakulære kjernefysiske våpnene som ble lansert av Russlands president Vladimir Putin i 2018

[20] Ikke-spredning: Hindre spredning av materiale, teknologi og kunnskap som kan brukes til utvikling av masseødeleggelsesvåpen, samt hindre spredning av strategiske varer, tjenester og teknologi m.m. i henhold til vedtak i FNs sikkerhetsråd eller annen lovgivning.

[21] CBRNE er en fellesbetegnelse på hendelser som omfatter kjemiske stoffer (C), biologiske agens (B), radioaktie stoffer (R), nukleært materiale (N) og eksplosiver (E) med høyt farepotensiale.

(Etterretningstjenesten, 2020). Det forventes at Russland vil ha fullført den pågående moderniseringen av landets kjernefysiske styrker i tiden frem mot 2030 (NATO, 2020, s. 36). Samtidig moderniserer og utvider Kina sine konvensjonelle og kjernefysiske kapabiliteter (NATO, 2020, s. 36).

Det er også knyttet bekymring til at fremvoksende og disruptive teknologier skal forrykke den strategiske balansen mellom kjernevåpenstater (Bidwell & MacDonald, 2018; Futter, 2021). Dette gjelder ikke bare utvikling av nye våpentyper som hypersoniske missiler, utvikling av ballistisk missilforsvar eller nye sensorer for å oppdage eksempelvis strategiske atomubåter; det er også frykt for at det kan bli mulig å gjennomføre avanserte datanettverksangrep mot strategiske kommando- og kontrollsystemer (Kippe *et al.*, 2021).

Flere forhold kan også tyde på at terskelen for bruk av kjemiske våpen senkes. Av særlig bekymring er forgiftningstilfellene i Storbritannia i 2018 og forgiftningen av den russiske opposisjonspolitikeren Alexei Navalny i 2020 hvor fjerdegenerasjons kjemiske stridsmidler – såkalte novitsjok-forbindelser – ble brukt i begge tilfellene (FOI, 2020; OPCW, 2018). Hendelsen i Storbritannia i 2018 førte til utvisning av over 150 russiske diplomater, mens sistnevnte hendelse har ført til diskusjoner i Tyskland om hvorvidt samarbeidet med Russland om Nord Stream 2-gassrørledningen skal fullføres (Kramer, 2020). Det å hindre bruk og spredning av kunnskap om produksjon av fjerdegenerasjons kjemiske stridsmidler blir derfor viktig fremover; det samme blir eksportkontroll av utgangsstoffer for slike stridsmidler.

Det har derfor vært en negativ utvikling innen ikke-spredningsområdet i nyere tid. Denne negative utviklingen kan forsterkes ytterligere hvis syntetisk biologi og bioteknologi misbrukes til ondsinnede formål og utvikling av nye trusselstoffer (jf. kapittel 4.5.8). Samtidig driver den teknologiske utviklingen frem nye offensive og defensive våpentyper, «hvor rollene til, og skillelinjene mellom, ulike våpenklasser og plattformene som bærer dem blir mer diffuse» (Etterretningstjenesten, 2020, s. 80). Dette påvirker statenes vilje til å inngå rustningskontrollavtaler. Verden kan derfor stå overfor nye våpenkappløp hvor Kina vurderes å spille en større rolle enn i dag (Etterretningstjenesten, 2020, s. 80).

PST forventer derfor at flere stater vil forsøke å omgå eksportkontrollregelverket og vestlige sanksjoner. Norske bedrifter, forskningsinstitutter og høgskole- og universitetssektoren utvikler kunnskap og teknologi som har flerbrukspotensiale eller kan benyttes til utvikling av avanserte våpen, inkludert CBRNE. Dersom fremmede stater klarer å utvikle slike våpensystemer, kan dette påvirke Norges og alliertes sikkerhet negativt (Politiets sikkerhetstjeneste, 2021, s. 12). Det er også fare for at kunnskapspredning over internett kan gi ikke-statlige trusselaktører evne til å fremstille og benytte kjemiske eller biologiske trusselstoffer.

Siden utviklingen går i retning av større spredning av avansert teknologi til nye aktører (både statlige og ikke-statlige), blir ikke-spredningsinitiativer viktigere, men også vanskeligere å opprettholde i tiden fremover. God eksportkontroll og hindring av spredning av materialer og teknologi som kan benyttes til CBRNE, fordrer i tillegg god kontroll på slike materialer og teknologier innenfor våre egne grenser.

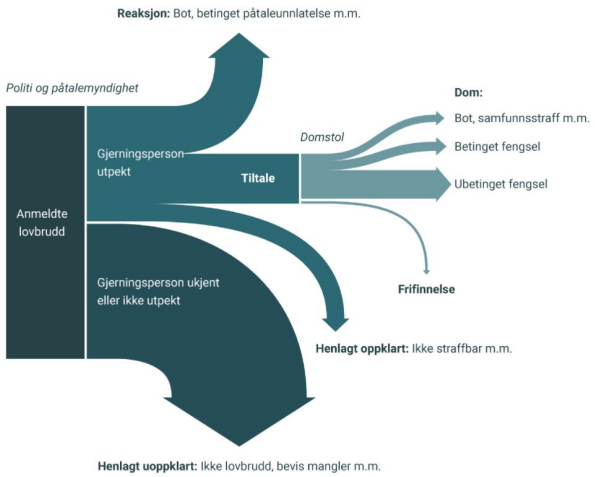
5.5 Annen alvorlig kriminalitet

I dette kapitlet diskuteres utviklingen innen annen alvorlig kriminalitet som direkte eller indirekte kan være av bekymring for samfunnssikkerheten. Valg av kriminalitetsområder har tatt utgangspunkt i politiets trusselvurdering (Politiet, 2021).

5.5.1 Generell kriminalitetsutvikling

I Norge har det generelt sett vært en betydelig nedgang i anmeldte lovbrudd per 1000 innbyggere de siste ti årene (til sammenligning har tallet vært stabilt i Sverige, se Figur 5.2). Imidlertid varierer kriminalitetsutviklingen de siste årene for ulike kriminalitetskategorier. Rapporter med fokus på trender innen kriminalitetsutviklingen i Norge og internasjonalt har pekt på at enkelte typer eller former for kriminalitet har økt, for eksempel seksual lovbrudd, mens andre typer (for eksempel bankran eller eiendomstyveri) nesten har forsvunnet fra kriminalitetsstatistikken (Europol, 2015; Meld. St. 29 (2019-2020)).

Det har vært stilt spørsmål ved om det har vært en reell nedgang i kriminalitetsstatistikken de siste årene, da hovedvekten av lovbrudd innen enkelte kriminalitetskategorier har blitt flyttet over i det digitale rom, og digitale lovbrudd i mindre grad har vært anmeldt sammenlignet med fysiske lovbrudd (Sætre *et al.*, 2018). Det skal også sies at kriminalitetsstatistikker i mindre grad er beskrivende for hvor mye ressurser politi- og påtaletjenestene benytter på ulike typer lovbrudd (jf. Figur 5.2). Ifølge informanter til denne studien, benytter politi- og påtaletjenestene i størrelsesorden 30% av ressursene på 3% av sakene som etterforskes. Karakteristisk for saker som binder opp store ressurser er at det er store og svært komplekse saker som ofte omfatter mange mistenkte eller fornærmede, lovbruddene begås ofte innenfor et lengre tidsrom eller flere jurisdiksjoner, og bevisbildet er gjerne meget omfattende. Dette er ofte nettovergrepssaker, økonomiske straffesaker, narkotikasaker eller straffesaker relatert til arbeidslivskriminalitet (Justis- og beredskapsdepartementet, 2020).

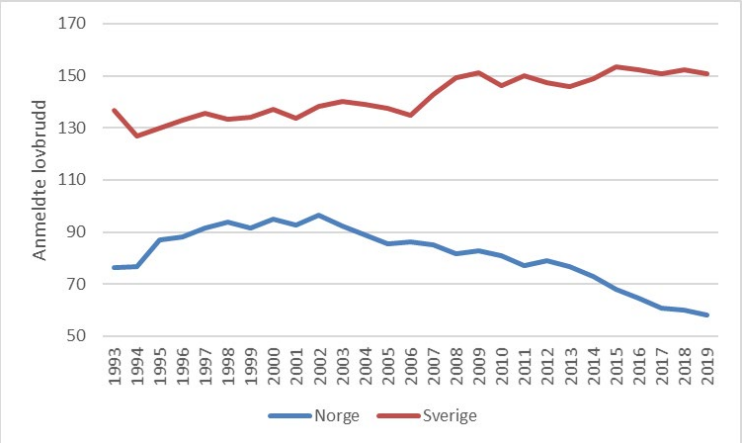


Figur 5.2 Illustrasjon av fordeling av anmeldte lovbrudd som fører til domfellelse. Kilde: Statistisk sentrabyrå (Kriminalitet - SSB).

En litteraturgjennomgang viser hvordan skillelinjene mellom de ulike kriminalitetskategoriene stadig blir mindre tydelig og definerte, og det fremgår hvordan tradisjonelt ulike kriminalitetskategorier smelter sammen (Europol, 2017b, 2020a). Innen en rekke kriminalitetsområder fremstår det mer og mer utfordrende å skille mellom målet og *modus operandi* for den kriminelle handlingen. Et eksempel på dette kan være digital svindel, hvor målet for den handlingen er økonomisk gevinst og sorterer inn under økonomisk kriminalitet. Samtidig gjennomføres handlingen digitalt, og sorterer således inn under kriminalitet i det digitale rom/cyberkriminalitet. Videre ser man også en tendens hvor flere kriminalitetstyper smelter sammen, og at hvert ledd blir mer profesjonalisert gjennom at «spesialister» utfører deloppgaver av en større kriminell handling (DNB, 2020; Europol, 2020a). En slik profesjonalisering kan også bidra til å viske ut skillet mellom de ulike kriminalitetskategoriene ytterligere. Et underliggende spørsmål er i hvilken grad dagens kriminalitetskategorier forblir meningsfulle i fremtiden eller om det vil være behov for å redefinere eller reformulere disse i fremtiden. Hvordan vi kategoriserer kriminaliteten vil ha betydning for hvordan man forebygger, etterforsker og straffeforfølger, men også hvordan ressurser prioriteres og politiet organiserer seg. Det bør derfor utredes nærmere hvordan kriminalitet bør kategoriseres for fremtiden og hva kriminalitetskategorier reflekterer (og ikke reflekterer).

En annen dimensjon som har blitt mer fremtredende de siste årene, spesielt innen kriminalitet i det digitale rom, er knyttet til aktører. Kriminalitet i det digitale rom fordrer ikke at den kriminelle aktøren har fysisk nærhet til målet sitt; aktører kan således operere globalt (Telenor, 2020). Det kan også være vanskelig å forstå intensjonen til enkelte aktører, da kriminelle grupper også kan ta på seg å gjennomfører oppdrag eller operasjoner på vegne av en stat (Telenor, 2020). Hvor går da grensen mellom et digitalt angrep i en forsvarskontekst og kriminalitet i det digitale rom?

Hvordan kriminalitetsstatistikken konkret vil utvikle seg det neste tiåret i Norge innenfor de ulike kriminalitetskategoriene er usikkert. I det følgende vil det derfor trekkes frem ulike utviklingstrekk som ansees som *mulig* retningsgivende de neste årene.



Figur 5.3 Anmeldte lovbrudd (alle lovbruddsgrupper) per 1000 innbyggere for Norge og Sverige. Kilder: Statistisk sentralbyrå (tabell 08484) og Brottsförebyggande rådet.

5.5.2 Viktige drivere for organisert og annen alvorlig kriminalitet

For å kunne peke på forventet fremtidig kriminalitetsutvikling, er det nødvendig å ha kunnskap om viktige drivkrefter for kriminalitet. Europol peker på fire viktige drivere for organisert og annen alvorlig kriminalitet (Europol, 2017b). For nesten alle former for organisert kriminalitet benyttes *teknologi*. Europol mener derfor at dette er en av de største utfordringene som politiet og rettsapparatet står overfor. Spesielt internett og utvikling innen digitale teknologier påvirker omtrent alle former for kriminalitet, og det forventes at denne utviklingen vil forsterkes med utbygging av tingenes internett. Teknologisk utvikling fremheves også av Politidirektoratet, hvor teknologier for konfidensialitet og anonymitet (jf. kapittel 4.5.2.1) benyttes ved planlegging, bestilling, utføring og betaling av kriminelle handlinger.

En annen viktig driver er *næringslivets selskapsstrukturer*. Organiserte kriminelle nettverk utnytter legale selskapsstrukturer for å skjule kriminell aktivitet og profitt. Samtidig muliggjør det hvitvasking og at kriminelle nettverk kan operere innenfor den legale økonomien (Europol, 2017b).

En tredje driver, som kan sies å være relatert til den forrige, er *utnyttelse av transportinfrastruktur*. Organiserte kriminelle nettverk utnytter transportsystemer for å skjule frakt av ulovlige varer i den lovlige varestrømmen. Transportvolumet sammen med effektive transportsystemer gjør det svært vanskelig, nærmest umulig, å sjekke lasten grundig. Europol (2017b) forventer også at kriminelle grupper vil utnytte svakheter som følger med nye transportteknologier som automatiserte transportsystemer, inkludert juridiske smutthull i regelverket som regulerer slike systemer.

Den siste driveren som Europol (2017b) fremhever, er den *geopolitiske konteksten*. Væpnede konflikter og fattigdom er de viktigste faktorene som fører til migrantstrømmer mot Europa. Kriminelle nettverk vil utnytte situasjonen i konfliktområder til smugling av migranter og våpen.

I tillegg til de overnevnte driverne, peker Kripos (2019b) på følgende drivkrefter for kriminalitetsutviklingen: For det første påvirkes kriminaliteten av *økonomisk utvikling og ulikhet*; ikke bare i samfunnet i Norge, men også mellom Norge og andre land. *Normer og holdninger i endring* er også en viktig drivkraft fordi hvordan ulike handlinger og ytringer oppfattes og hvilke reaksjoner de utløser, vil variere over tid. Kriminalitetsutviklingen i Norge påvirkes også av *internasjonalisering* fordi økte muligheter til å dele kunnskap, kontakter, varer, tjenester og kapital på tvers av landegrenser skaper ikke bare muligheter for samfunnet, men også sårbarheter helt ned til individnivå.

I det følgende sees det nærmere på kriminalitetsutviklingen innenfor områder som direkte eller indirekte kan påvirke samfunnssikkerheten.

5.5.3 Kriminalitetsutvikling i det digitale rom

Digitalisering handler i praksis om å bruke teknologi til å fornye, forenkle og forbedre i den hensikt å kunne tilby nye og bedre tjenester, som er enkle å bruke, effektive, og pålitelige

(Kommunal- og moderniseringsdepartementet, 2014). NHOs perspektivmelding frem mot 2050, peker på at digitalisering vil endre samfunns-, nærings- og arbeidslivet på flere avgjørende måter i årene som kommer (NHO, 2018).

Kriminalitet i det digitale rom er et område hvor *teknologiutviklingen* har vært sterkt drivende (jf. kapittel 5.5.2). Den digitale transformasjonen samfunnet går igjennom har gitt incentiver for potensielle lovbrytere til å vri sin kriminelle virksomhet over til digitale plattformer (Meld. St. 29 (2019-2020)). Ikke minst gjelder dette fremvekst av såkalt «Cybercrime-as-a-Service» (CaaS), hvor ulike nettverk tilbyr sine tjenester på det mørke nettet for å fasilitere annen kriminalitet gjennom utnyttelse av det digitale rom, eksempelvis gjennom å fasilitere phishing (Europol, 2020c). Dette gjør at det ikke er nødvendig å selv inneha avansert datakompetanse for å gjennomføre alvorlig datakriminalitet; tjenestene kan kjøpes av CaaS-tilbydere på det mørke nettet og betales for ved hjelp av kryptovaluta.

Digital kriminalitet har økt i både omfang og alvorlighetsgrad siden starten av 2000-tallet (Maimon & Louderback, 2019). I motsetning til mer tradisjonell kriminalitet, har kriminalitet i det digitale rom eller cyber-avhengig[22] kriminalitet hatt en jevn økning (FBI, 2016; Rantala, 2008). Kriminalitet i det digitale rom omfatter flere typer tradisjonelle former for kriminalitet, som for eksempel vinningskriminalitet, økonomisk kriminalitet, narkotikakriminalitet og seksuallovbrudd (jf. kapittel 5.5.5.2) etc. (Meld. St. 29 (2019-2020); Økokrim, 2020).

Trusselaktører innen digital kriminalitet kan deles inn i fem hovedkategorier basert på motivasjon og hvilke metoder og ressurser de har tilgjengelig. Disse kategoriene er: (*i*) stater, (*ii*) kontraktører, (*iii*) organisert kriminalitet, (*iv*) politisk motiverte «hactivister» og (*v*) enkeltkriminelle/svindlere (Telenor, 2020). Det er en økende trend at de kriminelle aktørene blir stadig mer organiserte ved at medlemmene i de kriminelle nettverkene spesialiserer seg på ulike prosesser innen kriminelle operasjoner (DNB, 2020; Telenor, 2020). Samtidig har hoveddelen av kriminelle aktører de senere årene rettet seg mer inn mot større bedrifter fremfor enkeltpersoner, hvor potensialet for et størst mulig økonomisk utbytte et tilstede (DNB, 2020). Digitale angrep mot større bedrifter kan medføre store økonomiske utgifter, noe Norsk Hydro-hendelsen i 2019 er et eksempel på. Denne hendelsen påførte selskapet et økonomisk tap 650 millioner kroner (DNB, 2020). Også samfunnskritiske funksjoner kan være særskilt utsatt for digitale angrep, og i en krisesituasjon med presset digital infrastruktur vil kriminelle aktører kunne utnytte seg av dette.

Samtidig ser man at utnyttelse av digitale teknologier og internett, endrer de tradisjonelle kriminalitetsformene (jf. kapittel 5.5.2). Et eksempel på dette er en fremvoksende trend hvor seksuell utnyttelse av barn på internett har blitt «kommersialisert» gjennom at personer laster opp overgrepsmateriale på nett for deretter å tjener penger på antall nedlastninger (Europol, 2020c, s. 8). Fremvekst av et økonomisk vinningsmotiv for denne typen kriminalitet er spesielt bekymringsfull og gjør at det er all grunn til å forvente fortsatt økning i denne kriminalitetsformen. I tillegg

[22] Det vil si, ulovlig aktivitet som bare kan utføres ved bruk av en datamaskin, et datanettverk eller andre former for informasjon- og kommunikasjonsnettverk.

gjør bruk av krypterings- og anonymitetsløsninger det stadig vanskeligere for politiet å oppdage og etterforske seksuelle overgrep på nett.

Et annet eksempel er relatert til vinningskriminalitet hvor kriminelle aktører søker økonomisk vinning gjennom bruk av løsepengevirus. I tillegg til økonomisk tap, kan det også medføre andre negative konsekvenser som tap av sensitiv informasjon. For det første har man sett eksempler på at informasjon offentliggjøres på det mørke nettet eller auksjoneres bort dersom offeret ikke betaler (Europol, 2020c, s. 25-28). Det kan heller ikke utelukkes at dataene videreselges selv om offeret betaler. En annen form for vinningskriminalitet i det digitale rom er tjenestenektangrep med påfølgende trusler om større tjenestenektangrep dersom det ikke blir utbetalt store pengebeløp.

Det ansees som svært sannsynlig at løsepengevirus og tjenestenektangrep vil øke i de kommende årene (Europol, 2020c, s. 32; Politiet, 2021, s. 22). Spesielt har bruken av løsepengevirus for å presse bedrifter for penger utpekt seg som en økende trend de siste årene, og Europol (2020c) peker på dette som den største digitale trusselen. Det fremholdes at bruk av løsepengevirus som metode vil overleve så lenge noen av ofrene velger å betale, og kriminelle vil fortsette å utvikle sine verktøy og metoder (jf. kapittel 4.5 om teknologisk utvikling) (DNB, 2020).

Meld. St. 29 (2019-2020) peker også på svindel som en form for kriminalitet som øker betydelig i omfang. DNB registrerte i likhet en massiv økning av bedrageri i 2019, og herunder en økning på 125% innen investeringsbedrageri. En tilsvarende eskalerende trend har vært tydelig i Sverige og Danmark over tid, og man ser at disse sakene pågår kontinuerlig. En fellesnevner for de metodene som knyttes til svindel er bruken av sosial manipulasjon som et viktig verktøyet for angriperen, da det hovedsakelig er mennesker som kan gi tilgang til informasjon som brukernavn og passord (DNB, 2020). Trusler i det digitale rom baserer seg på avansert teknologi, og metodene vil utvikle seg i takt med de teknologiske nyvinningene (jf. kapittel 4.5), men vil sannsynligvis beholde et vesentlig element av gamle metoder knyttet til sosial manipulasjon.

Covid-19-pandemien har bidratt til å økt digitalisering og nye arbeidsmønstre (Elster, 2020). Mange arbeidstagere jobber hjemmefra med andre sikkerhetsmekanismer og annet utstyr enn de har brukt tidligere, noe som blir pekt på av Nasjonal sikkerhetsmyndighet (2020a) som en sårbarhet kriminelle aktører vil utnytte fremover. NHO hevder at hjemmekontor og digitale møter er noe som vil bli vanlig i fremtiden og at halvparten av alle jobber i Norge i dag kan utføres fra hjemmekontor, noe som medfører at dette er tematikk som vil være svært relevant i årene fremover (NTB, 2020b).

Kriminalitet i det digitale rom ansees som en global trend som har kommet for å bli (Maimon & Louderback, 2019). Denne formen for kriminalitet er kompleks av natur, noe som gjør den vanskelig å etterforske og straffeforfølge. Denne utviklingen forsterkes gjennom kriminelles bruk av kryptovaluta og konfidensialitets- og anonymitetsløsninger for å opprettholde høy operasjonssikkerhet. Ifølge informanter til studien, er derfor det digitale rom et område hvor profesjonelle kriminelle kan operere med stor bevegelses- og handlefrihet. Eksempelvis har man sett at profesjonelle aktører bygger seg opp digitale merkenavn som «Lazarus Group», og hvor de kan vise til en lang historikk av at trusler gjennomføres dersom kravene ikke innfris. Samtidig

stiller kriminalitetsområdet krav til tverrfaglig kompetanse, noe som har bidratt til at det foreligger flere kunnskaps- og forskningshull innenfor dette området sammenlignet med andre kriminalitetsområder (Maimon & Louderback, 2019).

5.5.4 Kriminalitetsutvikling knyttet til trusler mot næringsliv, ressursgrunnlag og miljø

I sin trusselvurdering for 2021 peker politiet på en rekke alvorlige former for kriminalitet mot næringsliv, ressursgrunnlag og miljø. Slik kriminalitet kan være i form av såkalt faktura- og direktørbedrageri, investeringsbedrageri, konkurskriminalitet, unndragelse av skatt ved svart arbeid, utnyttelse av utenlandske arbeidstakere eller ulovlig fiske og underrapportering av fangst i fiskerinæringen (Politiet, 2021). Innenfor samtlige av disse områdene vurderer politiet det som sannsynlig til meget sannsynlig at den negative kriminalitetsutviklingen vil fortsette. I det følgende sees det nærmere på utviklingen innen økonomisk kriminalitet, arbeidslivskriminalitet og klima- og miljøkriminalitet.

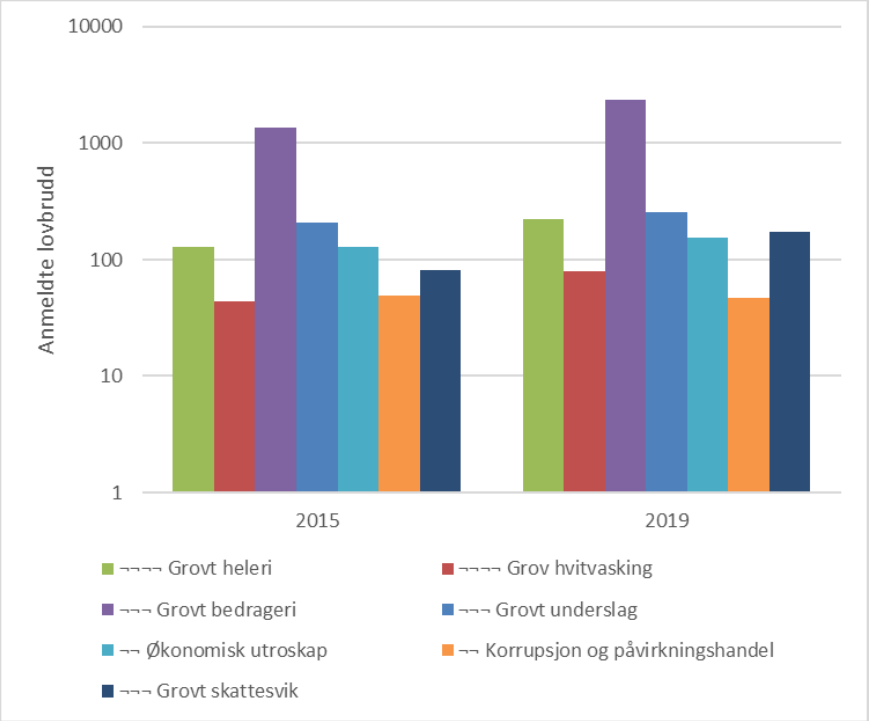
5.5.4.1 Økonomisk kriminalitet

Økokrim (2017) definer økonomisk kriminalitet som profittmotivert, lovstridige handlinger som ofte begås innenfor eller med utspring i en økonomisk virksomhet som i seg selv er eller gir seg ut for å være lovlig. I sin trusselvurdering fokuserer Økokrim på globalisering, bærekraft, digitalisering, pandemi og økonomisk usikkerhet som sentrale drivere for kriminalitetsutviklingen innenfor sitt ansvarsområde (Økokrim, 2020).[23]

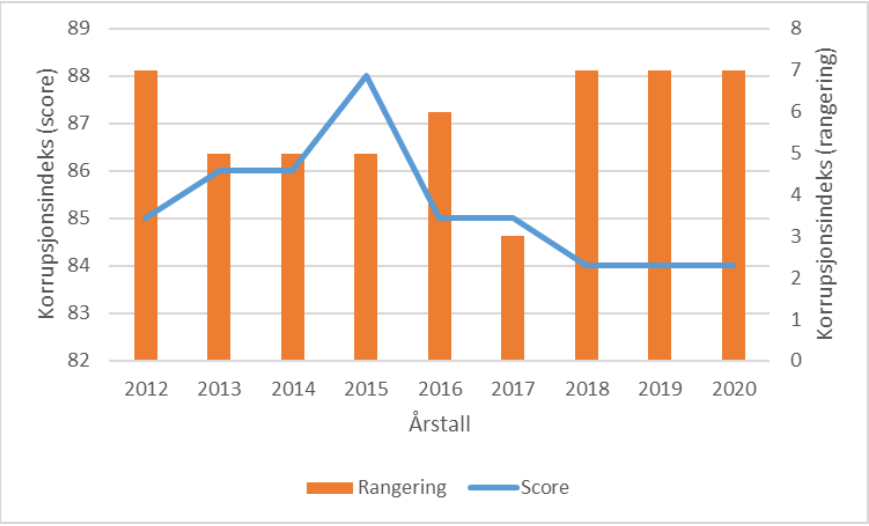
Meld. St. 29 (2019-2020) peker på at generelt er det nedgang i anmeldte økonomisk lovbrudd. Brudd på arbeidsmiljølovgivning har i stor grad vært stabilt, mens det har vært en kraftig reduksjon i anmeldelser av skatte- og avgiftsunndragelser de siste årene. Næringslivs- og økonomilovbrudd viser også i hovedsak en jevn nedgang over en lengre periode. Ifølge informanter til denne studien, er det imidlertid liten grunn til å tro at dette representerer en reell nedgang i denne typen lovbrudd, men snarere at færre saker anmeldes. For heleri har det vært en nedgang fra rundt 4500 anmeldelser i 2003 til under 2200 i 2018, noe som trolig henger sammen med den kraftige nedgangen i tradisjonell vinningskriminalitet. Imidlertid har det vært en økning i grovt heleri, grovt bedrageri, grov hvitvasking og grovt skattesvik fra 2015 til 2018 (Figur 5.3).

Det har også vært en negativ utvikling i befolkningens oppfatning av korrupsjon i offentlig sektor siden 2015 (Figur 5.4). Økokrim fremhever derfor i sin trusselvurdering for 2020 at norske kommuner er sårbare for korrupsjon, særlig på områder hvor privat sektor møter offentlig sektor og særlig knyttet til utbyggingsprosjekter i Norge (Økokrim, 2020, s. 37).

[23] Økokrims ansvarsområder er økonomisk kriminalitet, klima- og miljøkriminalitet og arbeidskriminalitet.



Figur 5.4 *Anmeldte lovbrudd per 1000 innbyggere for utvalgte typer lovbrudd knyttet til miljø- og økonomisk kriminalitet for 2015 og 2019 (logaritmisk skala). Kilde: Statistisk sentralbyrå (tabell 08484).*



Figur 5.5 *Norges rangering og score på Transparency International sin korrupsjonsindeks. Indeksen baserer seg på befolkningens oppfatning av korrupsjon i offentlig sektor. Kilde: https://www.transparency.org.*

Når det gjelder hvitvasking, er dette et område hvor *selskapsstrukturer* utnyttes (jf. kapittel 5.5.2). Ifølge Økokrims trusselvurdering for 2020, er eiendomsmarkedet egnet for hvitvasking av utbytte fra kriminalitet fordi det er et kapitalintensivt marked med store finansielle transaksjoner (Økokrim, 2020, s. 22). Siden utbyttet kan komme fra skatte- og avgiftsunndragelser, ikke-oppgitte inntekter fra uregistrerte arbeidere eller svart omsetning, er hvitvasking også nært knyttet til arbeidslivskriminalitet (jf. kapittel 5.5.4.2).

Økonomisk kriminalitet er en sammensatt og komplisert kriminalitetstype. Grensene mellom en god skatteplanlegging, skatteunndragelser og økonomisk kriminalitet gjør det utfordrende å gi en god og klar definisjon av hva som menes med økonomisk kriminalitet. Samtidig er kriminalitetsformen også utfordrende i sin utforming fordi den ofte utspiller seg i grenselandet mellom legalitet og legitimitet (Alalehto *et al.*, 2014; Myklebust & Larsson, 2004). Videre har ikke økonomisk kriminalitet i mange tilfeller veldefinerte ofre ved at konsekvensene bæres av alle konkurrentene i markedet, mens i andre tilfeller er anmeldelsestilbøyeligheten lav. Dette gjør at anmeldelser av økonomisk kriminalitet i stor grad er uttrykk for kontrollutøvelsen til ulike statlige myndigheter. Det er således uklart i hvilken grad nedgangen i registrert økonomisk kriminalitet avspeiler reelle endringer i kriminalitetsbildet. Eksempelvis har det overordnet vært en betydelig økning av rapportering vedrørende mistenkelige finansielle transaksjoner fra rapporteringspliktige virksomheter til Økokrim de siste årene (4 714 i 2015 mot 11 564 i 2019) (Økokrim, 2021). Dette kan likevel ikke utelukkende tolkes som et uttrykk for økt økonomisk kriminalitet, men kan også dels forklares med en høyere bevissthet hos de rapporteringspliktige virksomhetene om viktigheten av å følge med på å rapportere om mistenkelige transaksjoner.

5.5.4.2 Arbeidslivskriminalitet

Arbeidslivskriminalitet er beskrevet som «handlinger som bryter med norske lover om lønns- og arbeidsforhold, trygder, skatter og avgifter, gjerne utført organisert, som utnytter arbeidstakere eller virker konkurransedrivende og undergraver samfunnsstrukturen» (Departementene, 2019b, s. 5). I regjeringens strategi mot denne typen kriminalitet nevnes flere utfordringer og karakteristikker; først og fremst innslaget av multikriminalitet. Dette kan være skatte- og avgiftskriminalitet, grove regnskaps- og bokføringsovertredelser, korrupsjon, utroskap, konkurskriminalitet, hvitvasking, valutasmugling, menneskehandel, trygdesvindel, grove bedragerier, uriktige eller falske opplysninger og dokumentasjon til offentlige myndigheter, grove brudd på arbeidsmiljøloven og allmenngjøringsloven, utbytting av arbeidskraft i strid med lov og avtale, samt overtredelse av utlendingsloven (Departementene, 2019b, s. 5). Arbeidskriminalitet er således nært knyttet til økonomisk kriminalitet.

Som et mål på omfanget av arbeidslivskriminalitet, anslo Samfunnsøkonomisk analyse i 2015 at den skjulte verdiskapingen i Norge var på mellom 28 og 108 milliarder kroner (Eggen *et al.*, 2017). Videre tydet Samfunnsøkonomisk analyses funn at omfanget av arbeidslivskriminalitet var økende i perioden 2000-2009 for å deretter å flate ut frem til 2015.

Et karakteristisk trekk for trusselaktørene er at de opererer i flere bransjer og flytter gjerne virksomhet fra bransje til bransje. Dette er en utfordring i arbeidsintensive bransjer med lave krav til utdanning og med stort innslag av utenlandske arbeidere. Det har derfor vært spesielt fokus på

byggebransjen, men det avdekkes også lovbrudd i en rekke andre bransjer som eiendomsdrift, bilvask og -verksted, renhold, frisør/skjønnhetspleie, servering mv., samt godstransport på vei (Departementene, 2019b, s. 7). Ifølge informanter til studien, er også fiskerinæringen utsatt for arbeidslivskriminalitet.

I sin situasjonsbeskrivelse peker Nasjonalt tverretatlig analyse- og etterretningssenter (2020) (NTAES) på at utenlandske arbeidstakere er særlig sårbare for å bli underbetalt. Dette gjøres gjennom at de utenlandske virksomhetene benytter seg av falsk dokumentasjon tilpasset myndighetene for slik å kamuflere brudd på lønns- og arbeidsvilkår. I tillegg øker ID-misbruk i omfang (jf. kapittel 5.5.6). NTAES vurderer også at halvparten av nettverkene tilknyttet trusselaktører investerer kriminelt utbytte i eiendom. Flere av trusselaktørene inngår også i nettverk som er involvert i annen kriminalitet som omsetning av narkotika, og mange er anmeldt for trusler og vold. NTAES peker også på at stadig flere arbeidstakere kommer fra fattige land utenfor EØS, og vurderer at denne trenden forventes å øke. Slike arbeidstakere kan bli ført ulovlig inn i Norge for å arbeide og således stå i fare for å bli offer for menneskehandel i form av tvangsarbeid (Nasjonalt tverretatlig analyse- og etterretningssenter, 2020, s. 6).

Med økende turisme til Svalbard er det grunn til å forvente at utviklingen med ad-hoc og sesongbaserte aktører i markedet vil fortsette. I følge regjeringen er mange av disse ikke en del av det organiserte arbeidslivet og forholder seg heller ikke til næringens egne retningslinjer (Departementene, 2019a, s. 6). Imidlertid mangler Sysselmannen et robust lovverk for å regulere dette. Regjeringen vurderer derfor om flere lover og regler for fastlands-Norge bør gjøres gjeldende på Svalbard.

5.5.4.3 Klima- og miljøkriminalitet

Økokrim (2020) trekker i sin trusselvurdering frem flere miljørelaterte trusler som er aktuelle i perioden fremover. Som effekter av den globaliserte økonomien trekkes frem ulovligheter knyttet til opphugging av skip, handel med truede arter, eksport av EE-avfall fra Norge (jf. kapittel 4.4.2), feilmerking av sjømat, fiskevelferd i havbruksnæringen og annen grensekryssende fiskerikriminalitet. Økt trafikk av fartøy langs norskekysten vil sannsynligvis også øke faren for marin forsøpling og dumping av plast i havet de kommende årene (Økokrim, 2020). Ulovlig dumping av plast i havet er et økende problem, og det beskrives i en rapport fra Europol at kildesortert plast har blitt ett voksende marked for organisert kriminalitet etter at Kina stengte dørene for import av plastavfall i 2018 (Interpol, 2018). Økokrim peker også på at ulovlig motorferdsel, ulovlige byggetiltak og aktivitet i sårbare naturområder vil fortsette å være en utfordring. Spesielt kan økt aktivitet på Svalbard føre til press på isbjørnbestanden og annet sårbart fugle- og dyreliv. Det forventes også at det vil komme lovendringer med formål om å redusere klimaskadelige utslipp for å oppfylle Norges klimamål.

Fiskerikriminalitet fremheves av politiet som en kompleks kriminalitetsform bestående av ulike former for arbeidslivskriminalitet og økonomisk kriminalitet. Samtidig er fiskerikriminalitet også miljøkriminalitet fordi det bidrar til undergraving av en bærekraftig fiskeriforvaltning. I

politiets trusselvurdering vurderes det som meget sannsynlig at enkelte næringsutøvere vil videreføre et omfattende ulovlig fiske og under- og feilrapportering av fangst (Politiet, 2021, s. 28-29).

5.5.5 Kriminalitetsutvikling knyttet til trusler mot personlig integritet

5.5.5.1 Vold og mishandling

I politimeldingen fra 2020 fremheves det at andelen av den voksne befolkningen som oppgir å ha vært utsatt for vold eller trusler om vold har vært stabil siden starten av 1980-tallet (Meld. St. 29 (2019-2020)). Det samme gjelder drapsraten. Det er derfor grunn til å forvente at denne utviklingen vil vedvare, og politiet vurderer det som sannsynlig at flere personer med alvorlige psykiske lidelser enn tidligere vil begå grove voldshandlinger (Politiet, 2021, s. 17). Økt forekomst av psykiske problemer, samlivsproblemer eller økonomiske problemer etter covid-19-pandemien kan bidra til å forsterke faren for voldsutøvelse.

Samtidig har det vært en økt prioritering av bekjempelse av vold mot barn fra riksadvokatens side i senere tid. Som et ledd i dette arbeidet har Kripos utarbeidet en rapport for å styrke kunnskapsgrunnlaget om vold mot barn (Kripos, 2019a). I denne rapporten har Kripos gjennomgått straffesaker om alvorlig vold mot barn under fire år i perioden 2015–2018 (90 fornærmede). Over halvparten av de fornærmede barna var fem måneder eller yngre da skadene ble avdekket og det var i all hovedsak barnas egne foreldre som var anmeldt. Av de anmeldte var nesten en tredjedel utenfor arbeidslivet og over halvparten hadde en påvist diagnose og/eller en annen form for fysisk eller psykisk helseproblem. I tillegg hadde 43 % av de anmeldte tidligere vært involvert i en straffesak (Kripos, 2019a, s. 6).

Kripos peker på flere utfordringer når det gjelder vold mot små barn: For det første er det varierende kunnskap om og fokus på vold mot barn i politidistriktene og ved ulike helsestasjoner og barnevernstjenester. For det andre er dagens lovverk utydelig når det gjelder forholdet mellom taushetsplikt, opplysningsplikt, opplysningsrett og avvergeplikt. Videre har ikke barnevernet noen varslingsplikt overfor politiet når det er grunn til å tro at barn utsettes for vold eller mishandling. Til slutt peker Kripos på at mange av barna som utsettes for vold, er født inn i særlig sårbare familier (Kripos, 2019a, s. 7). Dersom samfunnsutviklingen fører til at flere faller utenfor arbeidslivet, er det grunn til å frykte at vold mot små barn kan øke i omfang uten gode forebyggende tiltak. Politiet (2021, s. 18) vurderer det som sannsynlig at det vil bli en økning av vold i hjemmet som følge av virkninger av covid-19-pandemien.

5.5.5.2 Seksuallovbrudd

Det har vært en betydelig økning i anmeldte seksuallovbrudd siden 2003, og seksuallovbrudd er området som har hatt prosentvis størst økning (Meld. St. 29 (2019-2020), s. 10). I politimeldingen fra 2020 fremheves det at det har vært en kraftig vekst i seksuallovbrudd relatert til barn og unge som ofre. Fra 2014 til 2018 økte antall personofre under 16 år fra omtrent 1 900 til over 3 150 (Meld. St. 29 (2019-2020), s. 14). Selv om politiet avdekker flere saker og at ofre for sek-

suallovbrudd i større grad anmelder forholdet, er det likevel grunn til å tro at det har vært en reell økning i antall overgrep, særlig over internett, og at mørketallene er høye (Meld. St. 29 (2019-2020), s. 14). Ifølge politiets trusselvurdering for 2021, rapporteres det om økning i henvendelser fra barn og unge som har opplevd seksuelle overgrep i hjemmet siden smitteverntiltak mot covid-19 ble innført i mars 2020 (Politiet, 2021, s. 19-20).

Kripos utga i 2019 en rapport hvor de har sett nærmere på seksuell utnyttelse av barn og unge over internett (Kripos, 2019c). I rapporten presenteres flere utfordringer som politiet og påtalemyndigheten møter i etterforskningen av slike seksuallovbrudd. Blant utfordringene som nevnes er problematikk knyttet til lagring og utveksling av IP-adresser, manglende regulering av VPN-leverandører, manglende regulering av kryptovaluta, manglende melde- og avvergingsplikt, lav strafferamme og behov for tettere internasjonalt politisamarbeid.

Kripos (2019c, s. 6) fremhever i sin rapport at internett har utviklet seg til å bli en utømmelig kilde til overgrepsmateriale. Dette gjelder både for det åpne, det dype og det mørke nettet. I tillegg øker mengden overgrepsmateriale for hver dag. Også for dette lovbruddsområdet bidrar konfidensialitets- og anonymiseringsløsninger (jf. kapittel 4.5.2.1) til lavere risiko for overgripere å bli oppdaget når de deler eller lagrer overgrepsmateriale. Politiet har derfor begrenset med kunnskap om gjerningspersonene.

Gjennomgang av straffesaker i inn- og utland viser at gjerningspersoner benytter falske profiler, stor tilpasningsevne og manipulatoriske evner til å komme i kontakt med barn og unge (Kripos, 2019c, s. 6-7). Det er grunn til å forvente at utviklingen innen kunstig intelligens (jf. kapittel 4.5.3) vil gi overgripere nye muligheter for manipulasjon og seksuell utnyttelse av barn og unge over internett. Allerede i dag har politiet etterforsket store sakskomplekser hvor det er avdekket at flere hundre barn har vært ofre for én og samme gjerningsperson. Selv om det først og fremst er barn som enten har blitt utsatt for fysiske overgrep eller som har blitt forledet/truet til å utføre seksuelle handlinger med seg selv som er utsatt for seksuelle overgrep over internett, fremhever Kripos at det også er mange ressurssterke barn blant ofrene og at «hvem som helst» kan bli utnyttet.

Når det gjelder fremtidsutsikter, fremhever Kripos at den globale digitaliseringen vil føre til flere potensielle overgripere og ofre etter hvert som en stadig større andel av verdens befolkning får internettilgang (Kripos, 2019c, s. 80). Særlig i fattige land kan seksuell utnyttelse av barn over internett bli en inntektskilde for voksne som har tilgang på barn. Som nevnt i kapittel 5.5.3, er økt kommersialisering av seksuell utnyttelse av barn over internett en fremvoksende trend. I sin rapport peker Kripos på at norsk og utenlandsk politi har avdekket et stort omfang av direkteoverførte bestillingsovergrep (Kripos, 2019c, s. 81). Med mindre mottiltak og sterkere fokus på forebygging får effekt mot seksuell utnyttelse av barn og unge over internett, er det dessverre grunn til å forvente at overgripere vil fortsette å utnytte utviklingen av digitale teknologier til å begå slike overgrep. Dette kan få alvorlige konsekvenser for ofrene og for samfunnet for øvrig.

5.5.5.3 Hatkriminalitet og hatefulle ytringer

Hatkriminalitet defineres som: «[…] straffbare handlinger som helt eller delvis er motivert av, eller som har bakgrunn i, hat eller negative holdninger til religion/livssyn, hudfarge, nasjonale eller etniske opprinnelse, homofile orientering og/eller nedsatt funksjonsevne» (Oslo politidistrikt, 2019b, s. 5). Generelt står ytringsfriheten sterkt i Norge. Noen ytringer sprer imidlertid hat og er derfor forbudt etter norsk lov. Antall anmeldte hatefulle ytringer har økt jevnt de siste årene etter at man begynte med en systematisk kartlegging, og utviklingen i Oslo viser at det over de fem siste årene har vært en dobling i antall anmeldte forhold (Oslo politidistrikt, 2019b). Utviklingen så langt viser at hovedvekten av anmeldte forhold innenfor hatkriminalitet kategorien er knyttet til etnisitet, og omfatter hatefulle ytringer og kroppskrenkelse (Oslo politidistrikt, 2019b). Det rapporteres også om at 25 % av forholdene er motivert av en kombinasjon av etnisitet og religion.

Ifølge politiets trusselvurdering for 2021 preges ytringer i det offentlige rom (både fysisk og digitalt) i økende grad av polarisering og ekstremisme. Politiet vurderer det derfor som sannsynlig at hatefulle ytringer vil fortsette å øke i omfang. Imidlertid vurderer politiet det som lite sannsynlig at de som fremsetter ytringene vil omsette truslene til vold. Likevel kan ytringene inspirere andre slik at potensialet for hatmotiverte voldshandlinger øker. Særlig er dette knyttet til markeringer som fremmer ytterliggående budskap hvor det vurderes som meget sannsynlig at det kan oppstå alvorlige ordensforstyrrelser i forbindelse med markeringene (Politiet, 2021, s. 14-15).

Likestillings- og diskrimineringsombudet peker på at det er mangel på norsk forskning på art, omfang og skadevirkning av hatytringer. Ombudet har derfor identifisert kunnskapshull knyttet til ulike gruppers erfaringer med hatytringer, hvem som står bak hatytringene, samt hvilke tiltak som kan forebygge og begrense omfanget av hatytringer (Likestillings- og diskrimineringsombudet, 2015). Det er derfor behov for mer kunnskap om den fremtidige utviklingen innenfor denne kriminalitetskategorien.

Hvis man ser på hatefulle ytringer mot norske politikere, gjennomførte Politihøgskolen i 2013 og i 2017 spørreundersøkelser blant norske stortingsrepresentanter og regjeringsmedlemmer om i hvilken grad de har blitt utsatt for trusler eller trusselhendelser (Bjelland & Bjørgo, 2014; Bjørgo & Silkoset, 2017). Funnene fra 2017 viste at 82 % har opplevd minst én form for uønsket adferd, mens 40 % har vært utsatt for alvorlige hendelser. Ifølge Bjørgo og Silkoset (2017) var mange av hendelsene av en slik karakter som stortingspolitikere og regjeringsmedlemmer må forvente å leve med. Sammenlignet med 2013 ser det ut til å være en økende trend at flere politikere utsettes for trakassering og trusler via sosiale medier. Dette er også en trend som man ser internasjonalt (Bjørgo & Silkoset, 2017) Videre viser funnene at graden av utsatthet for stortingsrepresentanter følger de politiske partiene og de politiske sakene, snarere enn hvilke partier som utgjør regjeringskoalisjonen. Funnene viser også at det er en tydelig sammenheng mellom alvorlighetsgraden på hendelsene og konsekvensene det får for politikernes adferd.

Tilsvarende funn finner man også for lokalpolitikere. I en spørreundersøkelse utført av Ipsos (2019) for Kommunenes sentralforbund, rapporterte 39 % av de spurte lokalpolitikerne at de

hadde blitt utsatt for hatefulle ytringer, 13 % hadde blitt utsatt for konkrete trusler og 8 % hadde opplevd både hatefulle ytringer og konkrete trusler. Felles for både nasjonalt og lokalt nivå er at det synes å være FrP-politikere som er mest utsatt (Bjørgo & Silkoset, 2017; Ipsos, 2019). Så sent som i juli 2020 advarte leder for Senter for ekstremismeforskning og professor ved Universitetet i Oslo og Politihøyskolen, Tore Bjørgo, om at trusler mot lokalpolitikere er egnet til å svekke demokratiet og at det er et økende problem (Næss, 2020).

Også personer som tilhører det som kan omtales som «den fjerde statsmakt» – journalister, karikaturtegnere, forfattere og forleggere, politiske aktivister og samfunnsdebattanter – utsettes i stor grad for hatefulle ytringer. Bjørgo og Silkoset (2017, s. 48) fremhever at dette er den mest trussel- og terrorutsatte kategorien mennesker i Skandinavia. I en intern undersøkelse blant egne journalister, fant NRK i 2019 at så mange som hver fjerde journalist får trusler (Myklebust, 2019). Slike trusler utgjør en fare for både presse- og ytringsfriheten. Det er grunn til forvente at også denne trenden vil vedvare, spesielt spredning av hatytringer og trusler på sosiale medier.

5.5.6 Kriminalitetsutvikling knyttet til ID-misbruk

Politiet vurderer ID-misbruk som en særlig alvorlig form for kriminalitet som kan true indre og ytre Schengengrense og tryggheten i Norge (Politiet, 2021, s. 33). Kriminalitetsformen er bekymringsfull fordi den legger til rette for annen alvorlig kriminalitet som menneskesmugling, menneskehandel og arbeidslivskriminalitet. Samtidig gjør ID-misbruk det vanskelig å utvise utenlandske personer som begår gjentatt og alvorlig kriminalitet, fordi de ikke kan returneres til hjemlandet når identiteten er ukjent.

Det er særlig to typer ID-misbruk som politiet er bekymret for (Politiet, 2021, s. 33-34):

- *Imposter*, det vil si en person som utgir seg for å være en annen ved å bruke et autentisk ID-dokument som tilhører en annen person.

- *Morfing*, det vil si en teknikk som sammenstiller to eller flere bilder og manipulerer dem slik at resultatet ligner på begge av de avbildede personene.

I 2019 registrerte Frontex over 7000 forsøk på ID-misbruk mot EUs yttergrense, en nedgang på 5% fra 2018 (Frontex, 2020, s. 28). Imidlertid økte antall avdekkede forsøk på ID-misbruk mot indre EU-/Schengengrense for tredje år på rad, hvor antallet i 2019 var 33% høyere enn i 2018 (Frontex, 2020, s. 29). Både politiet og Frontex rapporterer om økt etterspørsel etter ekte og falske ID-dokumenter innenfor EU/Schengenområdet (Frontex, 2020, s. 29; Politiet, 2021, s. 33-34). Politiet vurderer en fortsatt økning av impostere som meget sannsynlig. Selv om det ikke er avdekket tilfeller av morfing i Norge så langt, vurderer politiet det som mulig at også denne metoden vil bli benyttet ved ulovlig innreise til Norge (Politiet, 2021, s. 33). Det er grunn til å tro at kunstig intelligens (jf. kapittel 4.5.3) vil bidra til å gjøre morfing lettere å gjennomføre og trolig også vanskeligere å oppdage hvis effektive mottiltak ikke etableres.

5.5.7 Effekt av covid-19 på kriminalitetsutviklingen

Det er for tidlig å si noe om covid-19-pandemiens fulle påvirkning på kriminalitetsutviklingen (Meld. St. 29 (2019-2020)), men Europol skisserer i sin rapport noen hovedtrekk: Pandemiens påvirkning på kriminalitetsutviklingen kan hovedsakelig deles i to; den kortsiktige utviklingen relatert til selve pandemien og den mer langsiktige påvirkningen knyttet til konsekvenser over tid (Europol, 2020a).

Så langt i pandemien har kriminelle i Europa vært raske til å utnytte nye muligheter som har oppstått som følge av pandemien eller smitteverntiltak (Europol, 2020a). Europol viser til at det i Europa har vært tydelige tendenser til at kriminaliteten har blitt påvirket, da enkelte typer kriminalitet har gått drastisk opp, mens andre former for kriminalitet nesten har forsvunnet. Mye av den økende kriminaliteten som har vært relatert til selve pandemien, som for eksempel salg av forfalskede legemidler og helseprodukter, samt generell digitalt bedrageri og svindel. Eksempler på kriminalitet som har gått ned er migrantsmugling og salg av enkelte typer narkotika.

Europol (2020a) beskriver videre at etterhvert som man ser en gjenåpning av samfunnet og letting på restriksjoner i Europa, er det forventet at kriminalitetsbildet vil normalisere seg i tråd med situasjonen før pandemien. Det fremholdes likevel som sannsynlig at det vil ha oppstått nye muligheter ved krisens slutt som vil være områder for kriminell utnyttelse. En viktig premissgiver for utviklingen av alvorlig og organisert kriminalitet i perioden etter pandemien er den økonomiske utviklingen. Europol trekker frem eksempler som at vedvarende økonomisk nedgang i Europa vil kunne gi rom for investeringer av kriminell profitt i for eksempel eiendomsmarkedet. I tillegg vil man trolig se nye former for hvitvasking da relevansen av kontantintensive virksomheter (restauranter, kasinoer o.l.) som tradisjonelt har vært utgangspunkt for slik ulovlig aktivitet, muligens vil avta.

Tidligere kriser har vist seg å føre til endringer i det kriminelle markedet. I sin vurdering av langsiktige konsekvenser for kriminalitetsutviklingen viser Europol til finanskrisen i 2007–2008 for å kunne forutse en generell utvikling. I motsetning til tidligere kriser har pandemien økt bruken av kontantløse betalingsmåter betydelig for alle brukere. Dette vil også ha betydning for fremtidig kriminell virksomhet, da organiserte kriminelle grupper i stor grad er avhengig av den økonomiske utviklingen i et samfunn. Kriminelle grupper er tilpasningsdyktige og fleksible, og de identifiserer og utnytter nye muligheter.

Politimeldingen peker også på at enkelte utviklingstrekk knyttet til pandemien vil kunne ha betydning for kriminalitetsutviklingen på sikt (Meld. St. 29 (2019-2020)). Forskning på langsiktige konsekvenser viser at kriminaliteten vil øke om smitteverntiltakene vedvarer over tid, og da spesielt for gruppen av unge menn med lav utdanning (Mustard, 2010; Rege *et al.*, 2019). Også nyutdannede i økonomisk sårbar posisjon er i risikogruppen. I likhet med politimeldingen peker også Europol på at sårbare grupper har en tendens til å bli tilgjengelig for rekruttering inn i organiserte kriminelle miljøer under økonomiske nedgangstider (Meld. St. 29 (2019-2020)).

6 Samfunnsutviklingens betydning for politiet, PST og påtalemyndigheten

6.1 Implikasjoner som følge av forventet utvikling

I dette kapitlet er det formulert en rekke hypoteser for hvilke implikasjoner samfunnsutviklingen som er beskrevet i kapitlene 4 og 5, kan gi for politiet, PST og påtalemyndigheten frem mot 2030.[24] Med hypotese menes «en gjetning, antagelse eller forklaring som synes rimelig ut fra foreliggende kunnskap, og som man forsøker å avkrefte eller bekrefte» (*hypotese*, 2020).

Hensikten med hypotesene er å formulere hvilke konsekvenser langsiktige utviklingstrekk *kan* få for politi- og påtaletjenestene som et diskusjonsgrunnlag for å vurdere hva politiet, PST og påtalemyndigheten må være forberedt på å forebygge og eventuelt avdekke, avverge, håndtere, etterforske og straffeforfølge.

Det bør etableres et langsiktig og kontinuerlig strategisk analysearbeid som har som hensikt å bekrefte eller avkrefte de fremsatte hypotesene. Et slikt analysearbeid bør også ha som hensikt å gi oppdaterte vurderinger av utviklingstrekkenes betydning for politiet, PST og påtalemyndigheten.

I så stor grad som mulig er det forsøkt å formulere hypoteser for hvilken betydning et utviklingstrekk har for hvert av de identifiserte utfordringsområdene i kapittel 5. Der hvor dette ikke har vært mulig, har to eller flere utfordringsområder blitt slått sammen. Utviklingstrekkene er hentet fra omverdensanalysen i kapittel 4. I det følgende presenteres hypotesene.

[24] Flere av hypotesene har tatt utgangspunkt i Beadle, A. W. (2018). *Globale trender mot 2040 – hypoteser* (FFI-notat 18/02099). Forsvarets forskningsinstitutt.

6.1.1 Politiske forhold

Utvikling	Utfordringsområder	Implikasjoner for politiet, PST og påtalemyndigheten (hypoteser)
Fortsatt stormaktsrivalisering som følge av maktforskyvning fra tradisjonelle stormakter i Vesten til fremvoksende stormakter i Asia og Latin-Amerika	Trusler mot nasjonal sikkerhet:	Økt stormaktsrivalisering mellom USA og andre globale og regionale stormakter kan påvirke Norges sikkerhetsinteresser negativt gjennom svekket amerikansk interesse for europeisk sikkerhet og gjennom hardere konkurranse blant europeiske allierte om USAs oppmerksomhet. Med økende aktivitet i nordområdene, er det fare for mer stormaktsrivalisering også i denne regionen. Dette kan få betydning for norske strategiske interesser i nordområdene, herunder Svalbard og norsk tolkning av Svalbardtraktaten. Dersom den internasjonale rettsordenen, som Norge er avhengig av, svekkes ytterligere, vil det bli vanskeligere for norske myndigheter å få gjennomslag for norske interesser i internasjonale organisasjoner og organer. Utviklingen man har sett innen statlig etterretnings- og påvirkningsaktivitet mot Norge og norske interesser vil vedvare og ta nye former. Det samme gjelder skjulte angrep i form av datanettverksangrep mot offentlige og private sektorer i Norge. Økt tilstedeværelse av allierte styrker i Norge vil gi prinsipielle og praktiske konsekvenser for justissektoren med hensyn på jurisdiksjon, forståelse av hva som ligger i styrkebeskyttelsesbegrepet og forholdet til Den europeiske menneskerettsdomstolen.

	Terrorisme:	Økt stormaktrivalisering kan medføre flere væpnede konflikter i interesse-sfærer til stormaktene, for eksempel gjennom økt bruk av stedfortrederkrig. Væpnede konflikter er en risikofaktor for radikalisering og kan gi økning i terrorisme internasjonalt. Det kan også føre til økning i fremmedkrigere som drar fra Norge til konfliktområdene slik man har sett under den pågående borgerkrigen i Syria. Dette kan åpne for en kriminaliseringsdebatt om hvor stort ansvar Norge skal ta internasjonalt for forbrytelser begått i andre deler av verden.
	Samfunnsforstyrrelser:	Fremmede stater kan søke å påvirke voldelige, selvstyrende subkulturer som et ledd i å undergrave norske myndigheter. Økt migrasjon som følge av væpnede konflikter kan bidra til mobilisering av grupperinger på ytre høyre. Det kan oppstå opptøyer under politiske demonstrasjoner som følge av hen-delser i utlandet.
	Ikke-spredning:	Økt stormaktsrivalisering vil medføre en forverring innen ikke-spredning-sområdet som et resultat av modernisering av kjernevåpen og utvikling av nye våpentyper, inkludert kjemiske og biologiske våpen.
	Annen alvorlig kriminalitet:	Internasjonalt politisamarbeid knyttet til grensekryssende kriminalitet blir vanskeligere. Økt stormaktsrivalisering kan gi flere væpnede konflikter som igjen er en driver for organisert kriminalitet i form av våpen- og migrantsmugling.

Mulig(e) trendbrudd:	Russland bryter sammen. Nato går i oppløsning. EU går i oppløsning Nato styrker sin posisjon gjennom utvidelser østover (for eksempel at Finland blir medlem). USAs forhold til Kina utvikler seg i en mer positiv retning. Det bryter ut åpen krig mellom stormaktene.

Utvikling	**Utfordringsområder**	**Implikasjoner for politiet, PST og påtalemyndigheten (hypoteser)**
Forskyvning av makt til store multinasjonale selskaper og andre ikke-statlige organisasjoner	Trusler mot nasjonal sikkerhet:	Store multinasjonale selskaper vil få økt innflytelse over nasjonal kritisk infrastruktur, herunder rombaserte tjenester. Dette kan gi slike selskaper økt innflytelse på politiske beslutningsprosesser gjennom teknologiområdene som de kontrollerer. Det er fare for at norske myndigheter og Forsvaret kan miste handlefrihet over/tilgang til kritisk infrastruktur ved sikkerhetspolitiske kriser eller væpnet konflikt. Forskyvning av makt til store multinasjonale selskaper kan også føre til sterkere kobling mellom sikkerhet og økonomi. Uoversiktlige eierskapsstrukturer som krysser ulike jurisdiksjoner gjør det vanskelig å identifisere ultimate selskapseiere. Dette gjør det igjen vanskelig for norske sikkerhetsmyndigheter å få oversikt over hvordan en fremmed stat kan få tilgang til og innflytelse over selskapers aktiviteter.

	Terrorisme:	Forskyvning av makt til store multinasjonale selskaper vil ikke i seg selv medføre endret terrorisme.
	Samfunnsforstyrrelser:	Forskyvning av makt til store multinasjonale selskaper vil føre til økt globalisering. Dette kan igjen føre til opptøyer og fremvekst av voldelige subkulturer som ønsker å motsette seg globaliseringstrenden.
	Ikke-spredning:	Uoversiktlige eierskapsstrukturer og økt makt til multinasjonale selskaper kan gjøre eksportkontroll vanskeligere.
	Annen alvorlig kriminalitet:	Uoversiktlige eierskapsstrukturer til multinasjonale selskaper kan utnyttes av organiserte kriminelle til å skjule kriminell aktivitet og profitt blant lovlig økonomisk virksomhet. Økt makt til multinasjonale selskaper kan gjøre politietterforskning vanskeligere på grunn av eierskapsstrukturer som krysser flere jurisdiksjoner. Internasjonale avtaler og samarbeidsrelasjoner blir desto viktigere for politi- og påtaletjenestene.
Mulig(e) trendbrudd:	EU og/eller USA innfører strengere reguleringer, herunder oppsplitting, av store teknologiselskaper/multinasjonale selskaper.	

6.1.2 Sosiale forhold

Utvikling	Utfordringsområder	Implikasjoner for politiet, PST og påtalemyndigheten (hypoteser)
Befolkningsvekst og urbanisering i utviklingsland	Trusler mot nasjonal sikkerhet:	Befolkningsvekst og urbanisering i utviklingsland vil ikke i seg selv utgjøre en trussel mot Norges sikkerhet.
	Terrorisme: Samfunnsforstyrrelser:	Land som har en stor andel unge med begrensede muligheter for politisk deltagelse, utdanning og arbeid kan være sårbare for sosial uro, interne konflikter og fremvekst av terrorisme. Dette kan igjen føre til økt migrasjon mot Schengenområdets yttergrenser, samt radikalisering av diasporasamfunn i Norge. Befolkningsvekst i utviklingsland kan føre til fremvekst av grupperinger på ytre høyre som føler at vestlig kultur og etnisitet er under press.
	Ikke-spredning:	Befolkningsvekst og urbanisering i utviklingsland vil ikke i seg selv påvirke ikke-spredningsområdet.
	Annen alvorlig kriminalitet:	Befolkningsvekst vil føre til flere lovbrudd i landene det gjelder dersom kriminalitetsforebyggende tiltak ikke iverksettes. Det samme vil være tilfelle for byer som opplever økt tilflytting (urbanisering). Dette vil føre til økt grensekryssende kriminalitet, samt økt kriminalitet i det digitale rom etter hvert som flere får tilgang til internett.
Mulig(e) trendbrudd:	Ingen identifisert.	

Utvikling	Utfordringsområder	Implikasjoner for politiet, PST og påtalemyndigheten (hypoteser)
Voksende byer og aldrende befolkning på bygdene i Norge	Trusler mot nasjonal sikkerhet:	Demografiske endringer i Norge kan medføre økt politisk polarisering som en fremmed stat kan utnytte gjennom påvirkningsaktivitet.
	Terrorisme:	Dette utviklingstrekket vil ikke i seg selv medføre endringer i terrortrusselen, men det kan forventes at aktører som planlegger terrorhandlinger vil søke å ramme utvalgte mål i befolkningstette områder.
	Samfunnsforstyrrelser: Annen alvorlig kriminalitet:	Demografiske endringer i Norge kan medføre økt politisk polarisering og motsetninger mellom by og land og mellom fattig og rik i Norge. Dette kan igjen medføre økning i hatefulle ytringer. Urbaniseringen gir større byområder, høyere befolkningstetthet og endrede sosiale forhold, noe som kan gi opphoping av levekårsutfordringer. Dette kan påvirke kriminalitetsutviklingen negativt. Demografiske endringer kan medføre endringer i hvem som er ofre for kriminalitet i ulike deler av landet, hvor den eldste og den yngste delen av befolkningen er ofre for ulike typer lovbrudd. Fraflytting fra distriktene kan gjøre det vanskeligere å oppdage kriminelle handlinger i grissgrendte strøk.
	Ikke-spredning:	Dette utviklingstrekket vil ikke i seg selv påvirke ikke-spredningsområdet.
Mulig(e) trendbrudd:	Sentraliseringstrenden snur. Segregeringstrenden snur.	

Utvikling	Utfordringsområder	Implikasjoner for politiet, PST og påtalemyndigheten (hypoteser)
Fortsatt nettoinnvandring til Norge, men ikke like stor som den var i perioden 2000–2020	Trusler mot nasjonal sikkerhet:	Fremmede stater vil forsøke å påvirke diasporasamfunn i Norge. Flyktningespionasje vil vedvare, men omfanget vil avhenge av hvilke land innvandringen kommer fra. Fremmede staters etterretningstjenester kan benytte flyktningestrømmer til å skjule egne agenter.
	Terrorisme: Samfunnsforstyrrelser:	Høyreradikal/-ekstrem retorikk og nasjonalisme som en motreaksjon på globaliseringen vil vedvare og trolig endre karakter. Fortsatt nettoinnvandring til Norge fra ikke-vestlige og spesielt muslimske land kan føre til at trusselen fra høyreekstrem terrorisme vil vedvare.
	Ikke-spredning:	Fremmede staters etterretningstjenester kan forsøke å påvirke diasporasamfunn i Norge for å oppnå kunnskapsoverføring og tilgang til flerbruksteknologier.
	Annen alvorlig kriminalitet:	Mangelfull integrering kan medføre segregering og at minoritetsgruppe havner utenfor arbeidslivet, noe som er risikofaktorer for økt kriminalitet. Problemer med arbeidslivskriminalitet og ID-kriminalitet vil vedvare og kan ta nye former.
Mulig(e) trendbrudd:	Ny migrasjonskrise.	

6.1.3 Økonomiske forhold

Utvikling	Tilsiktede handlinger	Implikasjoner for politiet, PST og påtalemyndigheten (hypoteser)
Global økonomisk vekst vil gi økt etterspørsel etter naturressurser som energi, mat, vann og viktige mineraler	Trusler mot nasjonal sikkerhet:	Norge vil i økende grad utsettes for statlig etterretnings- og påvirkningsaktivitet knyttet til forvaltning av fiskeriressurser og forvaltning av naturressurser på Svalbard og i nordområdene for øvrig. Økt etterspørsel etter naturressurser kan føre til økt etterretningsaktivitet mot norsk næringsliv og mot norske interesser for øvrig. Tilgang på naturressurser, spesielt sjeldne jordartsmetaller til bruk i teknologisk utstyr, kan i økende grad brukes til å utøve press på andre land.
	Terrorisme:	Knapphet på ressurser kan øke faren for konflikt mellom samfunnsgrupper, sosial uro og kollaps av svake stater.
	Samfunnsforstyrrelser:	Motstand mot utarming av naturressurser kan føre til opptøyer.
	Ikke-spredning:	Dersom man ser en større etterspørsel etter enkelte typer sjeldne jordartsmetaller fra land Norge ikke har et sikkerhetspolitisk samarbeid med, vil Norge (og Nato) sannsynligvis forsøke å utvide eksportkontrollregelverket.
	Annen alvorlig kriminalitet:	Utviklingstrekket kan føre til økt handel med truede arter og økt ulovlig eksport av EE-avfall fra Norge. Utviklingstrekket kan føre til økt fiskerikriminalitet.

Mulig(e) trendbrudd:	Teknologiske gjennombrudd kan påvirke etterspørsel og produksjon. Rask utfasing av fossil energi vil redusere etterspørselen etter olje og gass.

Utvikling	**Utfordringsområder**	**Implikasjoner for politiet, PST og påtalemyndigheten (hypoteser)**
Norges økonomiske vekst vil gradvis avta	Trusler mot nasjonal sikkerhet: Terrorisme: Ikke-spredning:	Press på offentlige finanser kan føre til reduserte bevilgninger til politi- og påtaletjenestene som igjen kan påvirke tjenestenes evne til å forebygge, avdekke, avverge, håndtere, etterforske og straffeforfølge terrorisme, trusler mot nasjonal sikkerhet og/eller brudd på ikke-spredningsregimer og eksportkontroll.
	Samfunnsforstyrrelser:	Gradvis avtakende økonomisk vekst kan føre til økte sosiale ulikheter og utenforskap. Dette kan gi lavere tillit til politiet hos marginaliserte grupper i samfunnet, og føre til radikalisering. Lavere tillit til politiet kan også føre til fremvekst av borgervernsgrupper.
	Annen alvorlig kriminalitet:	Gradvis avtakende økonomisk vekst kan føre til press på velferdsstaten som igjen kan føre til økte sosiale ulikheter og utenforskap. Dette kan igjen føre til at spesielt unge menn med lav utdanning faller utenfor arbeidslivet, noe som en risikofaktor for kriminalitet. Press på offentlige finanser vil føre til at politiet må prioritere mellom ulike lovbruddsformer, for eksempel tradisjonell vinningskriminalitet i det fysiske rom mot kriminalitet i det digitale rom eller seksuallovbrudd over internett.

Mulig(e) trendbrudd:	Utfasing av fossil til fornybar energi kan gå mye raskere enn hva Norge er forberedt på. Økonomisk globalisering avtar. Global finanskrise og langvarig økonomisk resesjon.

Utvikling	**Utfordringsområder**	**Implikasjoner for politiet, PST og påtalemyndigheten (hypoteser)**
Økende andel av verdens befolkning vil leve i ekstrem fattigdom etter covid-19-pandemien	Trusler mot nasjonal sikkerhet:	Utviklingstrekket vil ikke i seg selv påvirke trusler mot nasjonal sikkerhet.
	Terrorisme: Samfunnsforstyrrelser:	Økende andel som lever i ekstrem fattigdom kan føre til befolkningsvekst. Dette kan igjen føre til kamp om ressurser, interne konflikter og migrasjon fra landene det gjelder. Økt migrasjon til Europa og Norge kan igjen føre til økt mobilisering av grupperinger på ytre høyre.
	Ikke-spredning:	Utviklingstrekket vil ikke i seg selv påvirke ikke-spredningsområdet.
	Annen alvorlig kriminalitet:	Økende fattigdom kan føre til økt kommersialisering av seksuell utnyttelse av barn over internett i fattige land.
Mulig(e) trendbrudd:	Verdenssamfunnet lykkes med å FNs bærekraftsmål om å bekjempe fattigdom.	

Utvikling	**Utfordringsområder**	**Implikasjoner for politiet, PST og påtalemyndigheten (hypoteser)**
Økende andel av personer med vedvarende lavinntekt i Norge, samt økende grad av sosioøkonomisk segregering og opphoping av levekårsutfordringer i norske storbyer	Trusler mot nasjonal sikkerhet: Terrorisme: Samfunnsforstyrrelser: Annen alvorlig kriminalitet:	Økende sosioøkonomiske forskjeller kan bidra til å undergrave tilliten til den norske samfunnsmodellen. Dette kan medføre økt politisk polarisering som en fremmed stat kan utnytte gjennom påvirkningsaktivitet. Utenforskap og fremmedgjøring kan påvirke kriminalitetsutviklingen negativt, spesielt i norske storbyer som følge av segregering. Det kan også føre til radikalisering og ekstremisme. Se for øvrig utviklingstrekket om demografiske endringer i Norge i kapittel 6.1.2.
	Ikke-spredning:	Dette utviklingstrekket vil ikke i seg selv påvirke ikke-spredningsområdet.
Mulig(e) trendbrudd:	Sentraliseringstrenden snur. Segregeringstrenden snur.	

6.1.4 Miljø- og klimaforhold

Utvikling	Utfordringsområder	Implikasjoner for politiet, PST og påtalemyndigheten (hypoteser)
Klimaendringer forsterker knapphet på mat og vann	Trusler mot nasjonal sikkerhet:	Utviklingstrekket vil ikke i seg selv påvirke trusler mot nasjonal sikkerhet, men Norges forsyningssikkerhet av matvarer og fôr til landbruket og til oppdrettsnæringen kan påvirkes.
	Terrorisme: Samfunnsforstyrrelser: Annen alvorlig kriminalitet:	Utviklingstrekket kan forsterke andre årsaker til konflikt og fungere som en «katalysator» selv om det er andre faktorer som er mest avgjørende for konfliktfaren som kan påvirke trusselen mot norske interesser. Utviklingstrekket kan føre til store folkevandringer bort fra de mest utsatte områdene og endre eksisterende migrasjonsstrømmer. Dette kan føre til migrasjonspress mot ytre Schengengrenser. Svikt i matvareleveranser som følge av klimaskapte naturkatastrofer kan føre til sosial uro, hamstring og opptøyer i Norge. Dersom Norge og det internasjonale samfunnet ikke lykkes med å redusere konsekvenser av klimaendringer, kan dette medføre uroligheter og fremvekst av ytterliggående aktører som har som målsetning å fremtvinge økt oppmerksomhet mot klimasaken, i ytterste konsekvens ved hjelp av vold og terrorhandlinger.
	Ikke-spredning:	Utviklingstrekket vil ikke i seg selv påvirke ikke-spredningsområdet.
Mulig(e) trendbrudd:	Arbeidet med klimatiltak og klimatilpasning går raskere.	

Utvikling	Utfordringsområder	Implikasjoner for politiet, PST og påtalemyndigheten (hypoteser)
Økt politisk vektlegging av klima- og miljøspørsmål	Trusler mot nasjonal sikkerhet:	Utviklingstrekket kan medføre økt statlig etterretnings- og påvirkningsaktivitet mot norske forhandlingsposisjoner i internasjonale miljø- og klimaspørsmål.
	Terrorisme:	Det forventes ikke at økt politisk vektlegging av klima- og miljøspørsmål vil bidra til økt terrorisme. Imidlertid kan det ikke utelukkes at enkeltaktører ønsker å fremskynde kampen for klimasaken ved hjelp av vold.
	Samfunnsforstyrrelser:	Utviklingstrekket kan føre til økt politisk polarisering og fremvekst av ytterliggående grupperinger som kan være enten for eller mot klimasaken, eller natur- og miljøspørsmål som rovdyrpolitikk og bruk av biler i byer. Dette kan medføre økt forekomst av hatefulle ytringer.
	Ikke-spredning:	Utviklingstrekket vil ikke i seg selv påvirke ikke-spredningsområdet.
	Annen alvorlig kriminalitet:	Utviklingstrekket kan føre til at det kommer lovendringer med formål om å redusere miljø- og klimaskadelige utslipp.
Mulig(e) trendbrudd:	Oppslutning om Parisavtalen og internasjonalt klimasamarbeid svekkes eller bortfaller helt. Forsterket internasjonal innsats for å oppnå FNs bærekraftsmål.	

Utvikling	**Utfordringsområder**	**Implikasjoner for politiet, PST og påtalemyndigheten (hypoteser)**
Det grønne skiftet medfører gjennomgripende endringer i energi- og transportsystemet.	Trusler mot nasjonal sikkerhet:	Fremmede stater vil forsøke å påvirke og skaffe seg innflytelse over fremtidens energi- og transportsystemer. Fremtidens energi- og transportsystemer vil ha andre sårbarheter enn dagens systemer og det vil være tettere koblinger mellom de kritiske infrastrukturene, inkludert mot elektronisk kommunikasjon. Det forventes at fremmede staters etterretningstjenester vil forsøke å kartlegge disse sårbarhetene og skaffe seg innflytelse over de nye infrastrukturene.
	Terrorisme:	Utviklingstrekket vil ikke i seg selv påvirke terrorismeområdet.
	Samfunnsforstyrrelser:	Utviklingstrekket kan føre til spredning av konspirasjonsteorier om negative konsekvenser av de nye grønne teknologiene. Dette kan igjen føre til fremvekst av ytterliggående/antistatlige subkulturer.
	Ikke-spredning:	Utvikling av «grønne teknologier» kan ha flerbrukspotensiale.
	Annen alvorlig kriminalitet:	Endringer i transportsystemet kan medføre at organiserte kriminelle finner nye måter å utnytte transportsystemet til å skjule frakt av ulovlige varer i den lovlige varestrømmen, hvor legal og illegal varetransport blir stadig mer sammenvevd.
Mulig(e) trendbrudd:	Raskere utfasing av olje- og gassindustrien enn hva Norge er forberedt på. Norge klarer ikke omstillingen til et «grønt samfunn/grønn økonomi».	

6.1.5 Teknologisk utvikling

Utvikling	Utfordringsområder	Implikasjoner for politiet, PST og påtalemyndigheten (hypoteser)
Større spredning av avansert teknologi til nye aktører, både statlige og ikke-statlige	Trusler mot nasjonal sikkerhet:	Vesten risikerer å miste sitt teknologiske hegemoni. Dette gjør det viktigere å beskytte kunnskapen bak fra statlig etterretningsaktivitet og industrispionasje. Teknologiutviklingen vil gi fremmede stater nye muligheter til å gjennomføre omfattende datanettverksangrep med stort skadepotensial mot norske sikkerhetsinteresser. Spektakulære datanettverksangrep kan ikke utelukkes.
	Terrorisme:	Terroraktører vil fortsette å utnytte krypterte kommunikasjonsverktøy, droneteknologi, CBRNE, samt 3D-printing for tilvirkning av våpen. Selv enkeltpersoner kan få svært stor ødeleggende kraft gjennom bruk av droneleverte eksplosivladninger eller dersom de klarer å utnytte teknologi til å fremstille biologiske smittestoffer eller kjemiske trusselstoffer.
	Samfunnsforstyrrelser:	Selv om aktører som *Facebook* og *Twitter* tar større ansvar for å hindre spredning av falske nyheter og konspirasjonsteorier, må det forventes at spredning av slike fenomener vil forflytte seg til andre sosiale medier som utøver mindre redaksjonell kontroll. Problematikk knyttet til digitale subkulturer vil derfor vedvare. Mangelfull evne til å bekjempe kriminalitet i det digitale rom kan medføre nye former for digitalt borgervern.

	Ikke-spredning:	Ikke-spredningsavtaler og -initiativer blir viktigere, men vanskeligere å opprettholde. Ikke-spredningsproblematikk knyttet til terrorisme vil også bli viktigere.
	Annen alvorlig kriminalitet:	Kriminalitetsutviklingen i det digitale rom vil vedvare og ta nye former, spesielt gjennom utnyttelse av kunstig intelligens og maskinlæring. Dette kan medføre storskala pengeutpressing ved bruk av løsepengevirus, skreddersydde phishing-forsøk og AI-generert falsk tekst, bilder og videoer. Fordi iretteføringen i slike saker er svært krevende, er det en fare for at rettssikkerhetsprinsipper ikke opprettholdes i tilstrekkelig grad.
Mulig(e) trendbrudd:	Ingen identifisert.	

Utvikling	**Utfordringsområder**	**Implikasjoner for politiet, PST og påtalemyndigheten (hypoteser)**
Fortsatt digital transformasjon og videreutvikling av det såkalte «smartsamfunnet»	Trusler mot nasjonal sikkerhet: Annen alvorlig kriminalitet:	Økt bruk av digitale teknologier som IoT og AI vil medføre økt innsamling av data, større angrepsflate og mer komplekse infrastrukturer. Dette kan igjen medføre eksponering av informasjon om nasjonale sikkerhetsinteresser, samfunnsfunksjoner, virksomheter og individer, økte muligheter for påvirkning av beslutningsprosesser, opinion og sosial adferd, samt økte muligheter for datanettverksangrep mot samfunnsfunksjoner. Digital transformasjon av kritiske infrastrukturer vil øke avhengigheten til rombaserte tjenester.

		Kritiske infrastrukturer kan bli mer resiliente gjennom å gjøre de «smartere». Samtidig kan dette føre til større og uforutsette konsekvenser hvis noe går galt på en måte som systemet ikke er i stand til å håndtere.
	Terrorisme:	Overgang til et «smartsamfunn» kan gjøre det mer attraktivt for terrorister å utvikle evne til å gjennomføre datanettverksangrep i terrorøyemed.
	Samfunnsforstyrrelser:	Utviklingstrekket kan føre til ytterligere spredning av 5G-konspirasjonsterorier, samt fremvekst av nye konspirasjonsteorier rundt de nye IoT-/AI-baserte tjenestene. Dette kan igjen føre til fremvekst av ytterliggående/anti-statlige grupperinger som ikke ønsker å være en del av «smartsamfunnet».
	Ikke-spredning:	Mange smartsamfunnsteknologier vil sannsynligvis ha flerbruksegenskaper.
Mulig(e) trendbrudd:	Global økonomisk resesjon kan bremse den digitale transformasjonen.	

Utvikling	Utfordringsområder	Implikasjoner for politiet, PST og påtalemyndigheten (hypoteser)
Omfanget av person- og befolkningsdata vil bli større som et resultat av den digitale transformasjonen. Dette vil føre til at utnyttelse av slike data får større økonomisk verdi. Samtidig vil det bli sterkere fokus på personvern.	Trusler mot nasjonal sikkerhet: Terrorisme: Samfunnsforstyrrelser: Ikke-spredning: Annen alvorlig kriminalitet:	Økt fokus på personvern vil gi statlige og ikke-statlige trusselaktører nye konfidensialitets- og anonymitetsløsninger som kan benyttes for å skjule identiteten til trusselaktøren, samt kommunikasjonen mellom trusselaktører. Økt bruk av sosiale medier i samfunnet vil øke betydningen av slike medier og mulighetene for å gjennomføre cyber-sosiale påvirkningsoperasjoner. Dersom store mengder person- og befolkningsdata kommer på avveie, vil statlige og ikke-statlige trusselaktører få nye muligheter for å identifisere sårbare personer, gjennomføre målrettede datanettverksangrep og/eller gjennomføre datanettverksangrep i stort omfang. Kompleksiteten i straffesakskjeden vil fortsette å øke. Dette vil gi utslag i blant annet økt konfliktnivå, mer bruk av sakkyndige, gjentatte omkamper og utfordringer med å «ramme inn» enkeltsaker.
Mulig(e) trendbrudd:	Mindre fokus på personvern og svekkelse av personvernlovgivning.	

6.2 Temaer som bør vies særskilt oppmerksomhet

I dette kapitlet diskuteres fire temaer som bør vies særskilt oppmerksomhet fremover fordi de representerer problemstillinger som går på tvers av utfordringskategoriene som politiet, PST og påtalemyndigheten står overfor frem mot 2030.

Det bør videreutvikles forskningsbasert kunnskap og et strategisk analysearbeid knyttet til temaene som trekkes frem, som grunnlag å gjøre oppdaterte vurderinger av utfordringene som politiet, PST og påtale-myndigheten står overfor frem mot 2030.

6.2.1 Skillet mellom statssikkerhet og samfunnssikkerhet blir mer utydelig

Nasjonal sikkerhet er som kjent definert som statssikkerhetsområdet og en avgrenset del av samfunnssikkerhetsområdet som er av vesentlig betydning for statens evne til å ivareta nasjonale sikkerhetsinteresser slik de er gitt i lov om nasjonal sikkerhet § 1-5 (se også vedlegg A). En konsekvens av samfunnsutviklingen er at det blir vanskeligere og vanskeligere å peke på hvor skillet mellom statssikkerhet og samfunnssikkerhet går når det gjelder tilsiktede handlinger som grenser opp mot væpnet angrep, spesielt når en statlig aktør står bak.

Gjennom FFIs oppdrag for JD i forbindelse med utarbeidelse av nasjonal plan for politiet, PST og påtalemyndigheten, er en rekke utfordringskategorier for politi- og påtaletjenestene identifisert (se boks 5.1 og Sellevåg (2021)). I tillegg kommer utfordringer som involverer konvensjonelle militære maktmidler, det vil si væpnede angrep i form av strategisk overfall og begrenset angrep, samt trusler om væpnede angrep i form av tvangsdiplomati (militær styrkemarkering). Tilsiktede handlinger under terskelen for et væpnet angrep eller for bruk av militære maktmidler, kan derfor direkte eller indirekte true nasjonale sikkerhetsinteresser gjennom at en trusselaktør utnytter sårbarheter i sivilsamfunnet «hvor som helst» og «når som helst» ved å bruke et bredt spektrum av ulike virkemidler (jf. kapittel 5.1.1).

I kapittel 6.2.4 blir det diskutert hvordan konspirasjonsteorier kan utgjøre et demokratisk problem. Spørsmålet som diskuteres her, er hvordan man kan forstå sikkerhetstruende virksomhet, det vil si tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser,[25] opp mot *trusler mot demokratiet*. En mulig tolkning av trusler mot demokratiet er å se på det som trusler mot grunnleggende verdier nedfelt i Norges grunnlov, det vil si statens suverenitet, demokratisk styresett, rettsstatsprinsippet og ivaretagelse av menneskerettigheter. Evnen til gjennomføring av frie, direkte og hemmelige valg til Stortinget, kommunestyrer, fylkesting og Sametinget er utpekt som en grunnleggende nasjonal funksjon (GNF) etter lov om nasjonal sikkerhet (Prop. 1 S (2020-2021), s. 122-123). Det samme er departementenes virksomhet, handlefrihet og beslutningsevne. Trusler mot disse GNF-ene vil derfor utgjøre en trussel mot nasjonale

[25] Jf. lov om nasjonal sikkerhet § 1-5.

sikkerhetsinteresser. Uten å gå inn i juridiske betraktninger, er det grunn til å mene at trusler mot myndighetspersoner tilknyttet departementene kan sies å utgjøre en trussel mot nasjonal sikkerhet dersom det påvirker departementenes virksomhet, handlefrihet og beslutningsevne. Trusler mot politikere og trusler mot ytringsfriheten kan åpenbart sies å være trusler mot demokratiet og demokratiske prosesser, men når blir det en bekymring for nasjonal sikkerhet? Tilsvarende betraktninger kan gjøres for annen alvorlig kriminalitet; i hvilken grad utgjør alvorlig kriminalitet sikkerhetstruende virksomhet og når kan man med sikkerhet si at kriminalitet *ikke* truer nasjonale sikkerhetsinteresser?

På samme måte som skillet mellom stats- og samfunnssikkerheten blir mer utydelig, gjør samfunnsutviklingen og spesielt kriminalitetsutviklingen i det digitale rom det vanskeligere å trekke skillet mellom kriminalitet og sikkerhetstruende virksomhet. Det er derfor behov for i større grad å se trusler mot statssikkerheten, mot samfunnssikkerheten og mot individets sikkerhet i sammenheng. Samtidig må hensynet til personvernet og rettsstatsprinsippene holdes opp mot hensynet til nasjonal sikkerhet. Dette vil utfordre politi- og påtaletjenestenes evne til å tilpasse seg et dynamisk og komplekst trusselbilde samtidig som befolkningens tillit til politiet opprettholdes. Som det påpekes av en informant til denne studien:

> *Jo mer uforutsett en hendelse er, jo vanskeligere er den å forebygge.*

Når skillet mellom stats- og samfunnssikkerhet blir mer utydelig, blir en funksjonsbasert tilnærming til hvilke verdier som skal beskyttes viktigere.

6.2.2 Teknologiutviklingens muligheter og utfordringer

I FFI-rapporten «Samfunnssikkerhet mot 2030 – utviklingstrekk» ble det pekt på en rekke teknologier som kan gi samfunnet bedre og mer effektive offentlige tjenester og økt verdiskaping i næringslivet (Sellevåg *et al.*, 2020). Spesielt gjelder dette digitale teknologier som skytjenester, IoT, AI, robotisering/autonome systemer og 5G. I tillegg skjer det en økt kommersialisering av verdensrommet og etablering av nye rombaserte tjenester som vil komme samfunnet til gode. Teknologiene kan også gi bedre samfunnssikkerhet gjennom eksempelvis bedre vær-, flom- og skredvarsling.

Samtidig vil teknologiutviklingen gi nye utfordringer for politi- og påtaletjenestene. For det første har kriminelle (spesielt organiserte) alltid vært raske med å ta i bruk ny teknologi, enten gjennom å endre *modus operandi* eller gjennom å endre deres «forretningsmodell» (Europol, 2017b). Kriminalitet drives derfor ikke bare av sosioøkonomiske forhold, men også av teknologisk utvikling. Teknologiområder som er sentrale for sivilsamfunnet og/eller forsvarssektoren, vil derfor høyst trolig også utnyttes av kriminelle. Det er også grunn til å forvente at høykompetente kriminelle vil utnytte konvergens av teknologier og teknologienes evne til disrupsjon (jf. kapittel 4.5.1) i deres anvendelse av eksisterende og kommende teknologier.

For det andre er teknologiutvikling også en sentral endringsdriver når det gjelder trusler mot nasjonal sikkerhet. Som det påpekes i «The Longer Telegram: Toward A New American China Strategy» (Anonymous, 2021):

[…] technology has become the major determinant of future national power

Det foregår derfor et kappløp mellom spesielt USA og Kina om å bli verdensledende og selvforsynt innen høyteknologi (jf. kapittel 4.1.1).

For det tredje drives den digitale transformasjonen frem gjennom utnyttelse og analyse av data, herunder også person- og befolkningsdata. Storparten av volumet av data er i dag ikke knyttet til noen landegrenser, og knyttes i økende grad til leveranse av varer og tjenester. Gjennom å knytte sammen persondata på tvers av næringssektorer, det offentlige og våre private liv, oppstår store muligheter. Samtidig ser man at ulike trusselaktører, inkludert fremmede stater, utvikler avanserte metoder for å utnytte person- og befolkningsdata (Government Office for Science, 2020, s. 3). Vi ser også at ulike land og regioner har ulik tilnærming til personvern. EU har vært en pådriver internasjonalt for bedre personvern gjennom GDPR. Imidlertid samtykker de fleste uten å lese personvernerklæringene for å få tilgang til nettjenestene, noe som fører til at vi ikke har kontroll over hvilke data vi gir fra oss (Hansen, 2019). I Kina er persondata nært knyttet til statlig sosial kontroll (Buckley & Mozur, 2019), mens USA har vært mer tilbakeholden med reguleringer. I tillegg har covid-19-pandemien bidratt til å endre hvordan persondata brukes. Hvis befolkningen og den enkelte ikke kan stole på at persondata blir behandlet på rett måte, kan dette begrense villigheten til å dele data. Dette kan igjen utfordre ytringsfriheten og befolkningens tillit til myndighetene (Datatilsynet, 2018, s. 3). Samtidig kan høy grad av tillit i samfunnet bli en sårbarhet når befolkningen i slike samfunn møter aktiviteter fra totalitære regimer i det digitale rom.

6.2.3 Kompleksitet som en samfunnsutfordring

En annen konsekvens av teknologiutviklingen er økende kompleksitet i gjensidige avhengigheter mellom ulike infrastrukturbaserte tjenester (Oughton *et al.*, 2018). Denne kompleksiteten kommer i hovedsak som et resultat av digital transformasjon og elektrifisering av samfunnet (Sellevåg *et al.*, 2020, s. 80). Kompleksiteten kan komme til uttrykk på ulike måter:

- i form av økende samspillkompleksitet som følge av interne og eksterne avhengigheter hvor koblingene kan være tette eller løse,
- i form av økende organisatorisk kompleksitet hvor det blir mer uoversiktlig hvor mange aktører som er involvert, hvem som har ansvaret og hvor dataene havner,
- i form av økende verdikompleksitet når infrastrukturen blir brukt av mange og det er vanskelig å ha full oversikt over hvilke verdier infrastrukturen bidrar til, og/eller
- i form av dynamisk kompleksitet knyttet til hvordan infrastrukturen endrer seg over tid.

Når verdikompleksiteten øker, blir sammensmeltingen mellom kriminalitet og sikkerhetstruende virksomhet mer utfordrende fordi samfunnets verdier kan rammes på mange måter med ulike

virkemidler. Som Bruce Schneier, en kjent forfatter og foredragsholder innen kryptografi og informasjonssikkerhet, påpeker (Schneier, 1999):

> *The worst enemy of security is complexity*

I hvilken grad kompleksiteten kommer til uttrykk, vil være avhengig av hvor dyp og gjennomgripende den digitale transformasjoner blir. Særlig gjelder dette i hvilken grad IoT og AI vil benyttes i kritiske styringssystemer og i hvilken grad samfunnssikkerhetsaspekter er adressert i implementeringen (Sellevåg *et al.*, 2020, s. 52). Fremtidens IoT-baserte infrastrukturer bør derfor ikke utelukkende betraktes som tekniske systemer, men snarere som cyber-fysiske-sosiale systemer (Wang, 2010). Dette betyr at sikkerhetsaspekter knyttet til den digitale transformasjonen også må ta hensyn til sosiale, politiske og økonomiske faktorer og ikke avgrenses til datasikkerhet og personvern i enkeltsystemer (Sellevåg *et al.*, 2020, s. 53).

Samtidig er ikke kompleksitet som en samfunnsutfordring kun avgrenset til den teknologiske utviklingen. Store demografiske endringer som følge av tilstrømning av mange innvandrere, er en form for kompleksitet som tradisjonelt har fremprovosert autoritære tilbøyeligheter hos befolkningen. Som Anne Applebaum (2021) skriver i sin bok «Demokratiets svanesang» om Karen Stenners forskning på autoritære tilbøyeligheter:

> *Folk blir ofte tiltrukket av autoritære ideer fordi de misliker kompleksitet. De misliker splid. De foretrekker enhet. En brå økning i mangfold – meningsmangfold, erfaringsmangfold – kan derfor gjøre dem sinte. De leter etter løsninger i et nytt politisk språk som får dem til å føle seg tryggere og sikrere.*

Slike personer kan være sårbare for konspirasjonsteorier.

6.2.4 Konspirasjonsteorier som et demokratisk problem

> *Ethvert samfunn kan snu ryggen til demokratiet hvis omstendighetene ligger til rette for det.*
>
> ─ *Anne Applebaum (2021)*

Utviklingen i vår tid kan fortelle om konspirasjonsteorier som trussel mot en demokratisk rettsstat hvor blant annet ytringsfriheten holdes opp som en viktig verdi. Den 6. januar 2021 stormet mange hundre mennesker den amerikanske kongressen. Det var en sprikende politisk gruppering, men mange sentrale personer var medlemmer av konspirasjonssamfunnet *QAnon*. QAnon var i utgangspunktet et lite internettforum som nå har vokst seg store og baserer hele sin legitimitet på å spre «de mest fantastiske historiene» om presidentvalget i USA høsten 2020. Med president Donald Trump selv i spissen har det hele tiden blitt fremsatt påstander og konspiratoriske teorier om juks og bedrag under presidentvalget. Kombinasjonen av konspirasjonsteorier og direkte løgner oppildnet av sentrale maktpersoner viste seg å være en farlig kombinasjon. Stormingen av kongressen var et sjokk for de fleste i USA. Noe slikt trodde ingen kunne skje.

Problemet er at dette har skjedd før. Nazistenes overtagelse av makten i Tyskland tidlig på 1930-tallet hadde mange av de samme kjennetegnene som de vi så denne januardagen i Washington i 2021 (Hagtvet, 2020; Karterud, 2021).

Konspirasjonsteorier har en lenger historie enn fra januar 2021 og stormingen av den amerikanske kongressen. En av de mest alvorlige konspirasjonsteoriene i moderne tid er *Sions vises protokoller* (Simonsen, 2020). Dette er en tekst hvor vi kan lese et sammensurium av tanker om den jødiske globale sammensvergelsen som søker verdensherredømme, og var en ideologisk legitimering av jødeforfølgelsen og Holocaust under andre verdenskrig. Selv om teksten ble avslørt som et falsum i 1921, har den levd sitt liv og ble så sent som i 1988 brukt politisk (Dyrendal & Emberland, 2019, s. 10).

Terrorangrepet mot Norge i 2011 var også ideologisk basert på en konspirasjonstanke hentet fra høyreekstreme miljøer kultivert i ulike internettforum. Budskapet var: «Europa befinner seg i en kulturkrig mot den muslimske fare. Muslimene utgjør ikke bare en religiøs trussel, de skal utrydde vår kultur og den hvite rasen». Anders Behring Breivik hadde forfattet et manifest hvor disse tankene var samlet og hvor hatet mot den «kulturmarxistiske» og den «multikulturelle eliten» var nedfelt. Dette er høyst reelle tanker, ideer og konspirasjonsteorier i det høyreorienterte «internettsamfunnet» (Dyrendal & Emberland, 2019, s. 7-11).

Hva er så en konspirasjonsteori? Begrepet er sammensatt, men kan defineres som: «relativt utarbeidede tanker om sammensvergelser som kjennetegnes av en del typiske feil både når det gjelder logisk resonnement og hva som er faktisk forhold» (Dyrendal & Emberland, 2019, s. 17). Ofte er det fortellinger om hvorfor noe har gått galt, hvem som har skylden og at det er en bevist handling av noen. Konspirasjonsteorier utrykker konflikter og konkrete sammensvergelser og retorikken i måten historiene blir formidlet på skjerper konflikten som konspirasjonen selv har konstruert.

I utgangspunktet virker konspirasjonsteorier uangripelige. De har ingen indre logikk og de bygger ikke objektive fakta. Et eksempel er konspirasjonsteorier som etter terroren på Utøya begynte florere på internett. Det ble lansert teorier om at terroren egentlig var isenesatt av Arbeiderpartiet og statsapparatet for å få mer sympati og makt. Gjerningsmannen var hjernevasket for å gjennomføre denne planen. Dette er en «sannhet» fordi styresmaktene holder dette hemmelig fordi de vil ikke bli avslørt. En måte å oppsummere eller forstå hvordan slike teorier blir til kan således ligger i tredelingen: (*i*) ingenting er tilfeldig, (*ii*) ingenting er hva det utgir seg for å være, og (*iii*) alt henger sammen.

Hvorfor skal vi bekymre oss for fremveksten av konspirasjonsteorier? Svaret på dette spørsmålet er at konspirasjonsteorier og grupper som samler seg rundt konspirasjonsteorier, kan utgjøre en trussel mot demokratiet. Episoden mot kongressbygningen i USA er et eksempel på det. Terrorangrepet mot Norge i 2011 er et annet eksempel når noen tror og utfører handlinger inspirert og dels legitimert i konspirasjonsteoriens ekstreme form. Et tredje eksempel er fremvekst av antistatlige grupperinger som *Frimannbevegelsen* (jf. kapittel 5.3.3), som organiserer seg rundt en konspirasjonsteori og motsetter seg samfunnets grunnverdier og institusjoner. På samme måte

som fremveksten av borgervern, er konspirasjonsteoriene en trussel mot demokratiets viktigste ressurs; nemlig tillit (Libell, 2018):

> *Forestillingen om at staten Norge er gjennomkorrupt, undergraver tiltroen til demokratiet. Forestillingen om at norske domstoler og Norges lover er falske, kan på sikt uthule selve fundamentet for lov og rett nedenfra, i alle fall i en del miljøer.*

Konspirasjonsteorier kan også brukes av makthaver og eliten i et land. I USA har president Donald Trump bevisst valgt å spre konspirasjoner for skape splittelse, usikkerhet og forvirring. Dette er en utvikling som aktualiserer farepotensialet i konspirasjonsuniverset (Leivestad, 2020; Libell, 2018):

> *Vi bør være bekymret hvis norske politikere begynner å bruke allment utbredte konspirasjonsideer bare for å sanke stemmer. Det virker polariserende og kan undergrave troen på legitime valg og alminnelig lov og rett.*

Den underliggende drivkraften i konspirasjonsuniverset er mistillit som igjen kan forklare maktesløshet og fremmedgjøring. Konspirasjonsteorier kan således også brukes som et maktmiddel fra de som styrer ved at de skaper eller spiller på de samme følelsene, det vil si maktesløshet og fremmedgjøring.

Allerede i dag ser man at konspirasjonsteorier spres raskt og over hele verden via internett. Spredning av konspirasjonsteorier akselereres ved at de deles, ikke bare av personer, men også godt hjulpet av såkalte trollkontoer på sosiale medier og sosiale medie-algoritmer (jf. kapittel 4.5.4). Det er grunn til å forvente at trusselaktører vil utnytte kunstig intelligens (jf. kapittel 4.5.3) både for å lage nye konspirasjonsteorier og for å spre konspirasjonsteorier via sosiale medier ved hjelp av det algoritmiske narrativet som slike medier skaper.

En god begynnelse for å forebygge konspirasjonsteorier er å skape politiske, økonomiske og sosiale forhold som skaper grunnlag for gjensidig tillit (Dyrendal & Emberland, 2019, s. 146). Dette krever både åpenhet, medbestemmelse og innflytelse i politiske prosesser, òg kritisk deltagelse og aktiv tilbakevisning av konspirasjoner på sosiale medier. I tillegg vil utdanning med vekt på kildekritikk og demokratiske læreprosesser, samt oppøve den kritiske nysgjerrighet være gode tiltak. På noen samfunnskritiske områder kan det imidlertid være nødvendig å bruke forskrifter og lover (Dyrendal & Emberland, 2019, s. 128-146). Sistnevnte kan medføre nye oppgaver for politi- og påtaletjenestene.

7 Utfordringsbildet frem mot 2030

Utfordringsbildet som politiet, PST og påtalemyndigheten står overfor frem mot 2030 er nødvendigvis heftet med betydelig usikkerhet. Ikke minst skyldes dette at verdenssamfunnet fremdeles står i en covid-19-pandemikrise selv ett år etter at Verdens helseorganisasjon erklærte at utbruddet var en pandemi. Selv om vaksinering er godt i gang i flere land og det forventes økonomisk vekst i 2021 (jf. kapittel 4.3.1), er det fremdeles usikkerhet rundt effekter av nye muterte varianter.

Det er også betydelig usikkerhet rundt langtidseffektene av pandemien, herunder hvordan sosial distansering påvirker barn og unges psykiske helse (Bekkhus *et al.*, 2020). På verdensbasis anslår UNESCO (2021) at i gjennomsnitt har to tredjedeler av et skoleår gått tapt som følge av skolestenginger; åpenbart med store regionale forskjeller. Hvilke effekter dette kan få, gjenstår å se. Undersøkelser har imidlertid vist at psykologiske reaksjoner hos befolkningen påvirkes av befolkningens tiltro til myndighetenes iverksatte tiltak og tro på at myndighetene har kontroll på covid-19-utbruddet (Mækelæ *et al.*, 2020). Misnøye med myndighetenes håndtering skaper således frykt i befolkningen, noe som igjen kan undergrave befolkningens tillit til de samme myndighetene. Dette kan igjen utnyttes av ulike trusselaktører. For Norge sin del viser spørreundersøkelser at folks tillit til myndighetene økte markant i 2020 under covid-19-pandemien (Berge, 2021).

Selv om det fremtidige utfordringsbildet er forbundet med betydelig usikkerhet på grunn av covid-19, er det likevel noen langsiktige utviklingstrekk som fremstår som relativt tydelige. I en tidligere FFI-studie som så på hvordan samfunnssikkerheten kan utvikle seg frem mot 2030, ble klimatiltak, teknologisk utvikling og fremtidige konflikter tatt frem som noen av de viktigste endringsdriverne for samfunnets fremtidige utvikling (Sellevåg *et al.*, 2020, s. 59). Disse endringsdriverne vil også påvirke utfordringsbildet som politi- og påtaletjenestene står overfor. I tillegg vil effekten av mulige endringer i sosiale og økonomiske forhold. En sammenstilling av det fremtidige utfordringsbildet på kort (0–5 år) og på mellomlang (5–10 år) sikt vil derfor gis med utgangspunkt i de fire nevnte endringsdriverne.

7.1 Terrorisme og trusler mot nasjonal sikkerhet

Innenfor den politiske dimensjonen går utviklingen i retning av maktforskyvning til fremvoksende stormakter og økt stormaktsrivalisering. Maktforskyvningen til fremvoksende stormakter er ventet å fortsette i flere tiår (Beadle *et al.*, 2019). Samtidig er det flere faktorer som vil være betydningsfulle for konfliktutviklingen fremover (Beadle *et al.*, 2019, s. 220-221):

- Utviklingen i regionale konflikter, særlig i Midtøsten og i Sahel
- Mulig bremsing av økonomisk utvikling i utviklingsland kan øke konfliktnivået
- Klimaendringer kan øke spenninger globalt og forsterke knapphet på viktige ressurser som mat og vann

- Erodering av den liberale verdensorden kan svekke internasjonalt samarbeid, herunder politisamarbeid, og sikkerhetspolitiske garantier
- Kinas økende rolle internasjonalt kan utfordre USAs globale posisjon

Økt stormaktsrivalisering mellom USA og andre globale og regionale stormakter kan påvirke norske og alliertes sikkerhetsinteresser negativt. For Norge sin del er det først og fremst forholdet til Russland som vil være av betydning når det gjelder trusler mot nasjonal sikkerhet. Russlands brudd på folkeretten gjennom annektering av Krim i 2014 og hvor Russland viste både vilje og betydelig forbedret evne til militærmakt, har ført til en – enn så lenge – varig endring i rammebetingelsene for norsk og europeisk sikkerhetspolitikk (Stortinget, 2014). I årene etter 2014 har man sett at Russland har opptrådd mer aggressivt overfor Norge gjennom bruk av både militære[26] og ikke-militære[27] virkemidler. Så lenge Russlands forhold til Vesten forblir dårlig og så lenge Nato og Norges nære allierte viser økt militær tilstedeværelse i nordområdene, må det på kort sikt (0-5 år) forventes at Norge vil fortsette å bli gjenstand for russisk misnøye (Beadle *et al.*, 2019, s. 108-109). Etterretningstjenesten (2021, s. 46) vurderer derfor i sin åpne trusselvurdering at Norge i større grad blir oppfattet som et Nato-land enn som en nabo av Russland. Samtidig er det verdt å påpeke at Norge og Russland fortsatt samarbeider på områder som kystvakt og fiskeriforvaltning. På lengre sikt (5-10 år) er den videre utviklingen i Norges forhold til Russland mer usikker, og den vil avhenge av Russlands fremtidige økonomiske utvikling og russisk politikk etter Putin. Siden 2015 har Russland vært inne i en periode med økonomisk stagnasjon, mye på grunn av vestlige sanksjoner og lavere oljepriser. Russlands økonomiske situasjon har blitt ytterligere svekket som følge av covid-19, og Russland er nå i den dypeste resesjonen siden finanskrisen i 2008 (Etterretningstjenesten, 2021, s. 49). På lengre sikt kan derfor yngre russeres misnøye utfordre regimets legitimitet og stabilitet dersom økonomisk vekst uteblir.

Med økende aktivitet i nordområdene er det fare for mer stormaktsrivalisering også i denne regionen. Dette kan få betydning for norske interesser på Svalbard og norsk tolkning av Svalbardtraktaten, spesielt dersom Russland velger å føre en mer aggressiv utenrikspolitikk i nordområdene. Man ser også at Kina styrker evnen til å operere i Arktis og har som ambisjoner om å etablere en «polar silkevei» (Etterretningstjenesten, 2021, s. 77). Imidlertid har ikke Kina kystlinje mot nordområdene. Det må derfor forventes at Kina vil søke å utnytte Norges sårbarhet knyttet til Svalbard-spørsmålet for styrke sin posisjon i Arktis både på kort og mellomlang sikt gjennom oppkjøp av eiendom, etablering av næringsaktivitet og FoU-virksomhet på Svalbard.

[26] Eksempelvis har Russland øvd på militære angrep mot Nord-Norge og forstyrret GPS-signaler i Finnmark.
[27] Eksempelvis ble datanettverksangrepet mot Stortinget høsten 2020 attribuert til Russland av norske myndigheter.

Det forventes at utenlandsk etterretnings- og påvirkningsaktivitet mot både offentlige og private sektorer vil forbli en betydelig trussel mot Norge og norske interesser i tiden frem mot 2030. Undergraving av demokratiet og sammensatte trusler som svekker tilliten mellom befolkningen og myndighetene vil være de farligste truslene mot nasjonal sikkerhet under terskelen for væpnet angrep.

I tillegg til de pågående regionale konfliktene i Midtøsten og i Sahel, kan økt stormaktsrivalisering medføre flere væpnede konflikter i interessesfærene til stormaktene. Væpnede konflikter er en risikofaktor for radikalisering og kan gi økning i internasjonal terrorisme. Samtidig kan knapphet på ressurser øke faren for sosial uro og konflikt mellom samfunnsgrupper i svake stater.

Videre vurderer både Politiets sikkerhetstjeneste (2021, s. 18) og Etterretningstjenesten (2021, s. 26) at trusselen fra ekstreme islamister er skjerpet. Til tross for tapet av det såkalte kalifatet, forventes det at IS vil være den mest samlede inspirasjonskilden for ekstreme islamister i Europa, inkludert Norge. Selv om det har vært en utvikling i jihadisters *modus operandi*, har motivasjonen bak islamistiske terrorangrep vært relativ stabil: Jihadister søker å ta «hevn» på krenkelse av islam og på vestlige land som intervenerer i konflikter og stater (jf. kapittel 5.2).

På kort sikt (0–5 år) forventes det at jihadister vil radikalisere, oppfordre til terror og drive faktisk angrepsplanlegging på tvers av landegrenser. Forsøk på terrorangrep i Norge fra ekstreme islamister må derfor forventes. Så lenge de sosiale og strukturelle faktorene som har bidratt til ekstrem islamisme ikke ser ut til å bli borte og den ustabile situasjonen i Midtøsten og i Sahel vedvarer, må det forventes at trusselen fra ekstreme islamister vil vedvare i tiden frem mot 2030.

Høyreekstremisme har i senere tid i økende grad blitt transnasjonal. I særlig grad skyldes dette digitale subkulturer på nett hvor det spres konspirasjonsteorier og alternative virkelighetsoppfatninger om at «den hvite rasen» er truet. Ifølge PST er det to faktorer som kan føre til økt radikalisering: (*i*) store internasjonale høyreekstreme terrorangrep kunne ha en inspirerende effekt; (*ii*) økt oppslutning og angrep knyttet til ekstrem islamisme kan legitimere høyreekstreme hevnaksjoner. Angrepet mot den amerikanske kongressbygningen 6. januar 2021 har hatt en særlig inspirerende effekt. Ifølge Etterretningstjenesten anser flere høyreekstreme i Europa hendelsene i USA som en forsmak på den kommende vestlige rasekrigen (Etterretningstjenesten, 2021, s. 33). Et annet trekk som har endret seg når det gjelder høyreekstremisme, er hvordan vold utøves. Der hvor voldsutøvelsen fra høyreekstreme tidligere (med visse unntak) kunne karakteriseres som relativt hyppig men med få dødsfall, ser man nå gjennom 22. juli-angrepene i Norge og Christchurch-angrepet på New Zealand 15. mars 2019 at høyreekstreme soloterrorister klarer å utføre terrorangrep som tar livet av mange mennesker (Bjørgo & Ravndal, 2019, s. 9).

Som nevnt i kapittel 5.2.3.5, er PST særlig bekymret for høyreekstremister som eksplisitt oppfordrer enkeltpersoner til fysisk kamp og som tar til orde for å fremskynde en total kollaps av samfunnet ved hjelp av terror. Slike akselerasjonister er av den oppfatning at en rasekrig mellom hvite og alle andre raser er nært forestående og at det derfor haster med å igangsette en konflikt som anses som uunngåelig. Det kan derfor stilles spørsmål om en global høyreekstrem terrorbølge er på trappene (Auger, 2020).

På kort sikt (0–5 år) forventes det at høyreekstremisme vil utgjøre en like stor terrortrussel i Norge som ekstrem islamisme. Utviklingen på lengre sikt (5–10 år) er mer usikker og vil avhenge av den videre samfunnsutviklingen i Europa og i USA. Det kan ikke utelukkes at en eventuell masseinnvandring til Europa kan være en utløsende faktor for det som høyreekstreme anser som den kommende vestlige rasekrigen, spesielt hvis ettervirkningene av covid-19 er vedvarende høy arbeidsledighet blant menn med lav eller ingen utdanning.

7.2 Teknologiutviklingens betydning

Teknologiutviklingen er en svært viktig endringsdriver for bortimot alle utfordringskategoriene (boks 5.1) som politi- og påtaletjenestene står overfor. Som nevnt i kapittel 6.2.2, har kriminelle alltid vært raske med å ta i bruk ny teknologi. Stormaktsrivaliseringen har også ført til et kappløp mellom spesielt USA og Kina om å bli verdensledende på og selvforsynt med høyteknologi.

Større spredning av avansert teknologi til statlige og ikke-statlige aktører gjør at Vesten risikerer å miste sitt teknologiske hegemoni. I tillegg bidrar teknologiutviklingen til at fremmede stater får nye og bedre verktøy til å begå etterretnings- og påvirkningsaktivitet, samt muligheter til å gjennomføre omfattende datanettverksangrep med stort skadepotensiale. Med fortsatt spredning av teknologi og demokratisering av kunnskap kan selv enkeltpersoner få stor ødeleggende kraft. Ikke-spredningsavtaler og -initiativer blir derfor viktigere, men vanskeligere å opprettholde; både med hensyn på eksportkontroll og kunnskapsoverføring.

Kriminalitetsutviklingen i det digitale rom forventes å vedvare og ta nye former, spesielt gjennom utnyttelse av tingenes internett og kunstig intelligens. Trenden man har sett med løsepengevirus forventes derfor å øke i omfang dersom ikke effektive mot- og sikringstiltak iverksettes. I tillegg vil nye konfidensialitets- og anonymitetsløsninger vil utnyttes for å skjule identiteten til trusselaktøren, samt kommunikasjonen mellom trusselaktører.

Den digitale transformasjonen av samfunnet drives frem gjennom utnyttelse og analyse av data. Utnyttelse av data, og kanskje særlig person- og befolkningsdata, vil derfor ha høy økonomisk verdi. Økt bruk av digitale teknologier som IoT og AI forventes å medføre økt innsamling av data. I tillegg øker angrepsflaten. Dette kan igjen medføre eksponering av informasjon om nasjonale sikkerhetsinteresser, samfunnsfunksjoner, virksomheter og individer. Dersom store mengder person- og befolkningsdata kommer på avveie, kan det bli lettere for statlige og ikke-

statlige trusselaktører å identifisere sårbare personer, gjennomføre påvirkningsoperasjoner eller gjennomføre datanettverksangrep. Samfunnets manglende evne til å beskytte person- og befolkningsdata kan utfordre ytringsfriheten og befolkningens tillit til myndighetene. Høy grad av tillit i samfunnet kan også bli en sårbarhet når befolkningen i slike samfunn møter aktiviteter fra totalitære regimer i det digitale rom.

Det forventes at utviklingen innen sosiale medier vil videreføres og at nye sosiale medietjenester vil tilkomme. Problemstillinger knyttet til sosiale mediers ubegrensede aggregering og lagring av informasjon og algoritmer som velger innhold for brukeren vil derfor vedvare og ta nye former. Selv om aktører som *Facebook* og *Twitter* tar større ansvar for å hindre spredning av falske nyheter og konspirasjonsteorier, må det forventes at spredning av slike fenomener vil forflytte seg til andre sosiale medier som utøver mindre redaksjonell kontroll. Problematikk knyttet til digitale subkulturer vil derfor vedvare. Økt bruk av sosiale medier i samfunnet vil øke betydningen av slike medier og således også mulighetene for å gjennomføre cyber-sosiale påvirkningsoperasjoner.

På kort sikt (0–5 år) forventes det kriminalitetsutviklingen som følge av teknologiutviklingen vil følge utviklingstrekkene man ser i dag. Samtidig er denne vurderingen forbundet med høy usikkerhet på grunn av fremvoksende og disruptive teknologiers potensial for trendbrudd. Utviklingstrekkene som fremstår med minst usikkerhet er at trusselaktører vil fortsette å utnytte konfidensialitets- og anonymitetsløsninger for å skjule sin identitet og kommunikasjon, utnytte kunstig intelligens for å gjennomføre tilsiktede handlinger, samt at det vil blir flere og mer avanserte kriminelle handlinger i det digitale rom som vil tilbys som en tjeneste («Cybercrime as a Service»). Fremvekst av nye former for digitalt borgervern kan ikke utelukkes dersom befolkningen ikke har tilstrekkelig tillit til at politiet klarer å bekjempe kriminalitet i det digitale rom.

På lengre sikt (5-10 år) vil usikkerheten være knyttet til i hvilken grad prinsipper som «resiliens» og «sikkerhet gjennom design» følges opp i den digitale transformasjonen og videreutviklingen av smartsamfunnet, og i hvilken grad politiske, sosiale og økonomiske aspekter ved teknologiutviklingen tas hensyn til. Potensialet for endringer (både positive og negative) er størst når IoT-baserte tjenester blir utbredt i samfunnet. Dette vil henge sammen med utbyggingen av 5G. Det må forventes at teknologiutviklingen vil gi helt nye tjenester av stor betydning for samfunnet og som vi i dag ikke ser rekkevidden av. I hele tidsperioden frem til 2030 forventes det derfor at teknologiutviklingen fortsatt vil være en av de aller viktigste endringsdriverne for utfordringskategoriene som politi- og påtaletjenestene står overfor.

Innenfor ikke-spredningsområdet driver den teknologiske utviklingen frem nye offensive og defensive våpentyper, «hvor rollene til, og skillelinjene mellom, ulike våpenklasser og plattformene som bærer dem blir mer diffuse» ifølge Etterretningstjenesten (2020). Dette påvirker statenes vilje til å inngå rustningskontrollavtaler. Verden kan derfor stå overfor nye våpenkappløp hvor Kina vurderes å spille en større rolle enn i dag.

Med demokratisering av kunnskap og større spredning av avansert teknologi til både statlige og ikke-statlige aktører, blir ikke-spredningsinitiativer viktigere, men også vanskeligere å opprettholde i tiden frem mot 2030.

7.3 Konsekvenser av klimaendringer

Klimaendringer vil gi konsekvenser for samfunnet i flere tiår fremover. For Norge sin del vil dette først og fremst gi utslag i varmere og våtere klima med mer ekstremvær. Samtidig er det en gryende erkjennelse av at klimaendringer kan ha destabiliserende effekter på global sikkerhet. Selv om klimakonsekvensene vil variere mellom ulike regioner, antas det at utviklingsland vil rammes hardest. Konsekvenser som tørke og vannmangel, redusert jordbruksproduksjon og økt fare for utbrudd av smittsomme sykdommer, kan igjen føre til økt migrasjon. For Norge sin del kan klimaendringer påvirke forsyningssikkerheten av matvarer og fôr til landbruket og til oppdrettsnæringen. Dette kan igjen føre til sosial uro.

Tap av naturmangfold er økende. Samtidig øker verdens behov for naturressurser. Med økt bruk av digitale teknologier og økt etterspørsel av elektroniske produkter, øker også mengden av såkalt EE-avfall i samfunnet. Skal tapet av naturmangfold og illegal handel med truede dyrearter og EE-avfall reduseres, er det behov for langt strengere regulering av miljøskadelig aktivitet og bedre bekjempelse av slik kriminalitet enn i dag (jf. kapittel 4.4.2).

Skal klimamålene i Parisavtalen oppfylles, er det behov for en overgang til betydelig mer miljø- og klimavennlige produkter og tjenester. Dette «grønne skiftet» vil kreve omstilling for samtlige samfunnsområder og -aktører, inkludert store endringer i energi- og transportsystemene gjennom større innfasing av fornybar energi, elektrifisering og bruk av andre nullutslippsløsninger.

Fremtidens energi- og transportsystemer vil ha andre sårbarheter enn dagens systemer og det vil være tettere koblinger mellom de kritiske infrastrukturene, inkludert mot elektronisk kommunikasjon. Det må forventes at fremmede staters etterretningstjenester vil forsøke å kartlegge disse sårbarhetene og forsøke å skaffe seg innflytelse over de nye infrastrukturene. Utvikling av «grønne teknologier» kan også ha flerbrukspotensial. Endringer i transportsystemet kan også medføre at organiserte kriminelle finner nye måter å utnytte transportsystemet til å skjule frakt av ulovlige varer i den lovlige varestrømmen.

På kort sikt (0–5 år) forventes det at dagens trender innen natur- og miljølovbrudd vil videreføres. På lengre sikt (5–10 år) er flere utviklingsløp mulige: Dersom Norge og det internasjonale samfunnet ikke lykkes med å redusere konsekvenser av klimaendringer, kan dette medføre fremvekst av ekstremister som har som målsetning å fremtvinge økt oppmerksomhet mot klimasaken ved hjelp av vold og terrorhandlinger. På den annen side kan økt politisk vektlegging av klima- og miljøspørsmål føre til økt politisk polarisering som igjen kan gi fremvekst av ytterliggående grupperinger som kan være enten for eller mot klimasaken, noe som kan medføre økt forekomst av hatefulle ytringer. Det grønne skiftet og økt politisk vektlegging av klima- og miljøspørsmål kan også føre til at disse områdene i større grad blir gjenstand for fremmede staters etterretnings- og påvirkningsaktivitet.

7.4 Endringer i sosiale og økonomiske forhold

Tre demografiske trender som fremstår som relativt sikre frem mot 2030: Norges befolkning blir stadig flere, eldre og mer urbanisert (jf. kapittel 4.2.1). Befolkningsveksten er særlig tydelig på det sentrale Østlandet, mens mange av nedgangskommunene ligger i distriktene. Videre forventes det at økt levealder og stor fraflytting av unge personer vil bidra til en sterk aldring i distriktene. Når det gjelder fremtidig migrasjon og innvandring til Norge, er dette forbundet med svært stor usikkerhet. Imidlertid viser SSBs analyser at det er lite som tyder på at nettoinnvandringen frem mot 2030 vil være like stor som den var i de to foregående tiårene (jf. kapittel 4.2.2). Imidlertid må det tas høyde for trendbrudd og episoder med stor masseinnvandring til Europa.

Når det gjelder økonomiske forhold, har covid-19-pandemien ført til den største økonomiske krisen siden andre verdenskrig. Samtidig har norsk økonomi per mars 2021 hentet inn store deler av det kraftige fallet i 2020. Usikkerheten rundt den videre utviklingen er imidlertid stor, og en ny smittebølge eller reduserte vaksineleveranser vil kunne føre til at gjenopphentingen går saktere eller stopper opp. Den økonomiske nedturen har også rammet skjevt; mange av de som har mistet jobben eller som har blitt permittert kommer fra lavtlønnsyrker. SSB forventer imidlertid at arbeidsledigheten vil gå ned etter hvert som den økonomiske situasjonen tar seg opp (jf. kapittel 4.3.1).

På lengre sikt forventes det at den økonomiske globaliseringen og veksten i verdensøkonomien vil fortsette, men med betydelige skjevheter. Det forventes også endringer i globale verdikjeder som følge av covid-19-pandemien når det gjelder varer og tjenester som er av betydning for nasjonal sikkerhet og beredskap. For Norge sin del forventes det at den økonomiske veksten gradvis vil avta. Dette kan føre til press på velferdsstaten som igjen kan føre til økte sosiale ulikheter. Dette kan forsterke trenden man har sett siden 2012 med økende andel av personer med vedvarende lavinntekt i Norge og opphoping av levekårsutfordringer i store norske byer (jf. kapittel

4.3.2). SSB advarer også om at inntektsulikhetene i Norge er betydelig større enn hva den offentlige statistikken viser fordi den bare tar med inntekt som er rapportert i de personlige skattemeldingene (Aaberge *et al.*, 2020). Dette betyr igjen økende økonomisk makt til den rikeste ene prosenten i Norge og større forskjeller mellom fattig og rik.

På verdensbasis er den forventede økningen i andelen av verdens befolkning som lever i ekstrem fattigdom av særlig bekymring. Verdensbanken har estimert at covid-19-pandemien kan føre mellom 88 og 115 millioner flere mennesker ut i ekstrem fattigdom (jf. kapittel 4.3.2). Den største andelen forventes i Afrika sør for Sahara, men også Nord-Afrika, Midtøsten og Sør-Asia forventes å få kraftig økning i fattigdom. Dersom verdenssamfunnet ikke lykkes med å bekjempe ekstrem fattigdom, kan dette utviklingstrekket føre til befolkningsvekst, kamp om ressurser, interne konflikter og migrasjon fra landene det gjelder.

På kort sikt (0–5 år) forventes det ikke vesentlige endringer i kriminalitetsbildet som følge av endringer sosiale og/eller økonomiske forhold i Norge. Internasjonalt er det imidlertid en fare for at økende fattigdom kan føre til migrasjon og økt kommersialisering av seksuell utnyttelse av barn over internett.

På lengre sikt (5–10 år) er utviklingen mer usikker og vil avhenge av langtidsvirkningene etter covid-19. Imidlertid kan demografiske endringer, avtakende økonomisk vekst og økende økonomisk segregering føre til økte sosiale ulikheter og utenforskap, noe som er risikofaktorer for kriminalitet og radikalisering. Det kan også føre til økt politisk polarisering og motsetninger mellom by og land og/eller mellom fattig og rik. Dette kan igjen svekke befolkningens tillit til myndighetene, inkludert til politiet, PST og påtalemyndigheten.

8 Sluttkommentarer

Denne rapportens formål har vært å beskrive hva samfunnsutviklingen kan bety for det fremtidige utfordringsbildet som politiet, PST og påtalemyndigheten kan møte frem mot 2030. Gjennom et slik arbeid er det alltid fare for at trusler overdrives eller tillegges for lite vekt. En annen fare oppstår ved å ta utgangspunkt i dagens trender; det er alltid en fare for at store hendelser fullstendig kan endre antagelsene om fremtiden. Sovjetunionens kollaps, terrorangrepene 11. september 2001 og covid-19-pandemien er alle eksempel på dette.

Det er særlig tre kilder som bidrar til usikkerheten i det fremtidige utfordringsbildet for politi- og påtaletjenestene. Den første kilden er knyttet til hva stormaktene USA, Kina og Russland *faktisk velger å gjøre* fremover, som igjen henger sammen med landenes innenrikspolitiske utvikling og utfallet av fremtidige maktskifter (Beadle *et al.*, 2019, s. 239). Den andre kilden til usikkerhet er knyttet til langtidskonsekvenser av covid-19-pandemien og hvordan dette kan påvirke sosiale og økonomiske forhold både nasjonalt og internasjonalt. Den siste kilden til usikkerhet er knyttet til teknologiutviklingen og spesielt til fremvoksende og disruptive teknologier. Slike teknologier kan gi samfunnet store muligheter og økonomisk vekst, men potensialet for misbruk er også svært stort. I tillegg vil samfunnet stå overfor store endringer som følge av klimatiltak og tilpasninger til klimaendringer.

Disse fire faktorene – fremtidig konfliktutvikling, teknologiutvikling, klimatiltak og endringer i sosiale og økonomiske forhold – er samtidig noen av de viktigste endringsdriverne i utfordringsbildet som politi- og påtaletjenestene står overfor. Når disse endringsdriverne er forbundet med betydelig usikkerhet, vil dette påvirke hvordan de samme tjenestene må møte de fremtidige utfordringene.

Samtidig er det flere faktorer som politi- og påtaletjenestene ikke kan velge bort. Én av disse faktorene er økende grad av rettighetssamfunn og forventninger til hva tjenestene skal være i stand til å levere. Som en informant til denne studien påpeker:

> *Et svar er ikke godt nok.*

Skal befolkningens tillit til politi- og påtaletjenestene opprettholdes, er det avgjørende at tjenestene klarer å møte de fremtidige utfordringene. Tidligere erfaringer har vist at internasjonalt politisamarbeid er viktig i så måte. Informanter til studien peker også på at større grad av spesialisering i politiutdanningen vil være nødvendig.

Dersom politi- og påtaletjenestene går i retning av større grad av spesialisering og satsning mot den alvorlige og ressurskrevende kriminaliteten, er det fare for at tjenestene kan fjerne seg fra befolkningen. Som en informant påpeker:

> *Hvordan skal service-rollen fylles av et politi som i økende grad har et beredskapsfokus?*

Hvis politiet ikke oppleves å være integrert i lokalsamfunnet slik det syvende grunnprinsippet tilsier (boks 3.1), kan dette medføre misnøye med politiet. Dette kan igjen føre til at det treffes politiske beslutninger for å svare opp befolkningens forventninger som ikke nødvendigvis samsvarer med politi- og påtaletjenestens egne analyser og vurderinger. Samtidig, hvis politiet har manglende evne til å håndtere alvorlig kriminalitet, kan dette igjen føre til redusert tillit mellom politiet og befolkningen. Dette kan igjen gi grobunn for mer kriminalitet, nye former for borgervern eller fremmedstatlig påvirkningsaktivitet. Når det gjelder kriminalitet i det digitale rom rettet mot næringslivet, kan utviklingen også gå i retning av økt kommersialisering av hendelseshåndtering og -etterforskning dersom politi- og påtaletjenestene ikke klarer å holde tritt med utviklingen.

For at fremmede stater skal kunne oppnå sine målsetninger gjennom bruk av sammensatte trusler, er de avhengige av å kunne utnytte samfunnets sårbarheter. Som forskeren András Rácz (2015, s. 92) påpeker:

> *Hybrid warfare is built on capitalizing on the weaknesses of a country, on flaws in its political system, administration, economy and society. If an adversary cannot detect sufficient weaknesses, then no full-scale attack can be launched, meaning that hybrid warfare never reaches the second, attack phase. Hence, the best defence against hybrid warfare is good governance.*

Videre skriver Rácz (2015, s. 92):

> *[G]ood governance needs to be interpreted in the broad sense. In addition to a democratic political structure and wellfunctioning public administration, it includes respect for human rights, transparency, media freedom, the rule of law and proper rights guaranteed to ethnic, national, religious and other minorities, all in order to improve the domestic democratic legitimacy and support of the government, and hence the very stability of the state.*

Med press på offentlige finanser vil også politi- og påtaletjenestene måtte prioritere sin innsats mellom de ulike utfordringskategoriene (boks 5.1). I dette spørsmålet bør utviklingstrekket som tilsier at skillet mellom alvorlig kriminalitet og sikkerhetstruende virksomhet blir mer utydelig, vies oppmerksomhet. Særlig gjelder dette kriminalitetsutviklingen i det digitale rom og fremmede staters etterretnings- og påvirkningsaktivitet. Samtidig må politi- og påtaletjenestene ha tilstrekkelig beredskap til å avverge og håndtere terrorangrep og andre alvorlige handlinger og hendelser. Utfordringen fremover vil ligge i avveiningen mellom prioritering av løpende oppgaver og beredskap og hvordan disse to skal vektes mot hverandre.

Et svar vil være å ha et felles situasjonsbilde og forståelse av hva situasjonsbildet betyr for den enkelte politietat. Et annet svar vil være evne til rask tilpasning og omstilling, inkludert evne til

å utnytte teknologienes muligheter. Et tredje svar vil være helhetlig og tverrsektorielt forebyggende arbeid.

Politiets hovedstrategi er og må være forebygging. Skal politi- og påtaletjenestene lykkes med sitt forebyggende arbeid, peker en informant til studien på at dette vil kreve enighet om hva som ønskes oppnådd, aksept for at prioriteringer gjøres og tydeliggjøring av den enkelte etat sitt ansvar. Ikke minst krever det evne til samarbeid på tvers av sektorer, effektive politiverktøy og et hjemmelsgrunnlag som er tilpasset utfordringene som politi- og påtaletjenestene står overfor slik at politiet, PST og påtalemyndigheten også i fremtiden kan være døråpner og portvakt, og instansen som bekrefter og sikrer borgernes rettssikkerhet.

> *Innumerable confusions and a profound feeling of despair invariably emerge in periods of great technological and cultural transitions. Our 'Age of Anxiety' is, in great part, the result of trying to do today's job with yesterday's tools – with yesterday's concepts.*
>
> *– Marshall McLuhan (1967)*

Referanser

Abate, T. (2015, 15. august). Stanford researchers genetically engineer yeast to produce opioids. *Stanford Engineering*. https://engineering.stanford.edu/magazine/article/stanford-researchers-genetically-engineer-yeast-produce-opioids

Ackerman, E. (2019, 1. april). Three Small Stickers in Intersection Can Cause Tesla Autopilot to Swerve Into Wrong Lane. *IEEE Spectrum*. https://spectrum.ieee.org/cars-that-think/transportation/self-driving/three-small-stickers-on-road-can-steer-tesla-autopilot-into-oncoming-lane

Al Faruque, M. A., Chhetri, S. R., Canedo, A. & Wan, J. (2016). *Acoustic Side-Channel Attacks on Additive Manufacturing Systems*. ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS), Vienna. https://doi.org/10.1109/ICCPS.2016.7479068

Alalehto, T., Korsell, L. & Larsson, P. (2014). *Ekonomisk brottslighet: en nordisk reader*. Studentlitteratur AB.

Amnesty International. (2005, 25. februar). - *Menneskerettigheter ofres i "krigen mot terror"*. Hentet 1. mai 2021 fra https://amnesty.no/menneskerettigheter-ofres-i-krigen-mot-terror

Andersen, A. D., Bjørgum, Ø., Espegren, K., Holden, E., Skjølsvold, T. M. & Steen, M. (2019, 7. januar). *Grønt skifte handler like mye om samfunnet som om teknologi*. https://forskning.no/klima-kronikk-politikk/gront-skifte-handler-like-mye-om-samfunnet-som-om-teknologi/1276592

Andås, H. (2020). *Emerging technology trends for defence and security* (FFI-rapport 20/01050). Forsvarets forskningsinstitutt.

Anonymous. (2021). *The Longer Telegram: Toward a New American China Strategy*. Atlantic Council.

Applebaum, A. (2021). *Demokratiets svanesang. Politikk som svikter og vennskap som tar slutt*. Cappelen Damm.

Auger, V. A. (2020). Right-Wing Terror: A Fifth Global Wave? *Perspectives on Terrorism*, *14*(3), 87-97.

Barlup, V. (2020, 4. mai). Amerikansk etterretning: – Kina skjulte omfanget av koronaviruset. *TV2 Nyheter*. https://www.tv2.no/nyheter/11421755/

Barnett, J. & Adger, W. N. (2007). Climate change, human security and violent conflict. *Political geography*, *26*(6), 639-655.

Beadle, A. W., Diesen, S., Nyhamar, T. & Bostad, E. K. (2019). *Globale trender mot 2040 – et oppdatert fremtidsbilde* (FFI-rapport 19/00045). Forsvarets forskningsinstitutt.

Bekkhus, M., Von Soest, T. & Fredriksen, E. (2020). Psykisk helse hos ungdom under covid-19 – Ensomhet, venner og sosiale medier. *Tidsskrift for Norsk Psykologiforening*. https://psykologtidsskriftet.no/vitenskapelig-artikkel/2020/06/psykisk-helse-hos-ungdom-under-covid-19

Belikovetsky, S., Yampolskiy, M., Toh, J. & Elovici, Y. (2016). dr0wned – Cyber-Physical Attack with Additive Manufacturing. https://arxiv.org/abs/1609.00133

Berge, J. (2021, 5. januar). Topp tiltro til myndighetene under koronapandemien. *Aftenposten*. https://www.aftenposten.no/norge/politikk/i/PR5eJR/topp-tiltro-til-myndighetene-under-koronapandemien

Bergh, A. (2019). *Social network centric warfare – understanding influence operations in social media* (FFI-rapport 19/01194). Forsvarets forskningsinstitutt.

Bergh, A. (2020). *Påvirkningsoperasjoner i sosiale medier - oversikt og utfordringer* (FFI-rapport 20/01694). Forsvarets forskningsinstitutt.

Bidwell, C. A. & MacDonald, B. W. (2018). *Emerging Disruptive Technologies and Their Potential Threat to Strategic Stability and National Security*. Federation of American Scientists.

Birkeland, Å. (2007). Politigeneralisten, Den moderne staten og politiets legitimitet. I H. Gundhus, P. Larsson & T.-G. Myhrer (Red.), *Polisiær virksomhet: hva er det - hvem gjør det?* (Bd. 7). Politihøgskolen, Forskningskonferansen 2007.

Bjelland, H. F. & Bjørgo, T. (2014). *Trusler og trusselhendelser mot politikere. En spørreundersøkelse blant norske stortingsrepresentanter og regjeringsmedlemmer* (PHS Forskning 2014: 4). Politihøgskolen.

Bjørgo, T. (2018). Introduksjon til rapporten. I T. Bjørgo (Red.), *Høyreekstremisme i Norge. Utviklingstrekk, konspirasjonsteorier og forebyggingsstrategier* (PHS Forskning 2018: 4). Politihøgskolen.

Bjørgo, T. & Gjelsvik, I. M. (2017). *Right-wing Extremists and anti-Islam Activists in Norway: Constraints against Violence* (C-REX Working Paper Series No. 3/2017). Center for Research on Extremism (C-REX), University of Oslo.

Bjørgo, T. & Gjelsvik, I. M. (2018). Utvikling og utbredelse av høyreekstremisme i Norge. I T. Bjørgo (Red.), *Høyreekstremisme i Norge. Utviklingstrekk, konspirasjonsteorier og forebyggingsstrategier* (PHS Forskning 2018: 4). Politihøgskolen.

Bjørgo, T. & Gjelsvik, I. M. (2019). Sheep in wolf's clothing?: The taming of the Soldiers of Odin in Norway. I T. Bjørgo & M. Mareš (Red.), *Vigilantism against Migrants and Minorities*. Routledge.

Bjørgo, T. & Ravndal, J. A. (2019). Extreme-Right Violence and Terrorism: Concepts, Patterns, and Responses. *ICCT Policy Brief*, September 2019. https://icct.nl/wp-content/uploads/2019/09/Extreme-Right-Violence-and-TerrorismConcepts-Patterns-and-Responses.pdf

Bjørgo, T. & Silkoset, E. (2017). *Trusler og trusselhendelser mot politikere. En spørreundersøkelse blant stortingsrepresentanter og regjeringsmedlemmer* (PHS Forskning 2017: 5). Politihøgskolen.

Bjørkholt, S. (2019). *FoU og innovasjon i Norge og Kina* (SSB Analyse 2019/32). Statistisk sentralbyrå.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., Ó hÉigeartaigh, S., Beard, S., Belfield, H., Farquhar, S., Lyle, C., Crootof, R., Evans, O., Page, M., Bryson, J., Yampolskiy, R. & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention and mitigation. https://arxiv.org/abs/1802.07228

Buckley, C. & Mozur, P. (2019, 22. mai). How China Uses High-Tech Surveillance to Subdue Minorities. *The New York Times*. https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html

Caldwell, M., Andrews, J. T. A., Tanay, T. & Griffin, L. D. (2020). AI-enabled future crime. *Crime Science*, *9*, 14. https://doi.org/10.1186/s40163-020-00123-8

Cernev, T. & Fenner, R. (2020). The importance of achieving foundational Sustainable Development Goals in reducing global risk. *Futures*, *115*, 102492.

Christensen, C. M., Raynor, M. E. & McDonald, R. (2015). What is disruptive innovation? *Harvard Business Review*, (December), 44-53. https://hbr.org/2015/12/what-is-disruptive-innovation

Cullen, P. J. & Reichborn-Kjennerud, E. (2017). *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare. A Multinational Capability Development Campaign project*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

Datatilsynet. (2018). *Artificial intelligence and privacy*. https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf

DCDC. (2018). *Global Strategic Trends: The Future Starts Today (Sixth Edition)*. Development, Concepts and Doctrine Centre (DCDC), UK Ministry of Defence. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/771309/Global_Strategic_Trends_-_The_Future_Starts_Today.pdf

Departementene. (2019a, 3. oktober). *Strategi for innovasjon og næringsutvikling på Svalbard*. Hentet 16. januar 2021 fra https://www.regjeringen.no/no/dokumenter/innovasjon-og-naringsutvikling-pa-svalbard/id2671061/

Departementene. (2019b, 5. februar). *Strategi mot arbeidslivskriminalitet*. Hentet 16. januar 2021 fra https://www.regjeringen.no/contentassets/7f4788717a724ef79921004f211350b5/no/pdfs/strategi-mot-arbedslivskriminalitet-2019.pdf

Diaz, J. (2018, 28. september). Alexa can be hacked – by chirping birds. *Fastcompany*. https://www.fastcompany.com/90240975/alexa-can-be-hacked-by-chirping-birds

Diesen, S. (2018). *Lavintensivt hybridangrep på Norge i en fremtidig konflikt* (FFI-rapport 18/00080). Forsvarets forskningsinstitutt.

DNB. (2020). *Trusselvurdering 2020*. Hentet 9. april 2021 fra https://www.digi.no/filer/DNB_Trusselvurdering_2020_NOR_FINAL_PUB.pdf

Dreher, A., Gassebner, M. & Schaudt, P. (2020). The effect of migration on terror: Made at home or imported from abroad? *Canadian Journal of Economics/Revue canadienne d'économique*, *53*(4), 1703-1744. https://doi.org/https://doi.org/10.1111/caje.12469

Du, J., Delis, A. & Douch, M. (2020, 25. mai). Lessons from China: This is how COVID-19 could affect globalization. *World Economic Forum*. https://www.weforum.org/agenda/2020/05/coronavirus-globalisation-shakeup-is-inevitable

Dyrendal, A. & Emberland, T. (2019). *Hva er konspirasjonsteorier*. Universitetsforlaget.

Egge, M. & Solhjell, R. (2018). *Parallellsamfunn - en del av den norske virkeligheten?* (PHS Forskning 2018: 2). Politihøgskolen.

Eggen, F. W., Gottschalk, P., Nymoen, R., Ognedal, T. & Rybalka, M. (2017). *Analyse av former, omfang og utvikling av arbeidslivskriminalitet* (Rapport nr. 69-2017). Samfunnsøkonomisk analyse AS.

Ekroll, H. C. (2020, 29. mai). Trump: USA kutter alle bånd til Verdens helseorganisasjon. *Aftenposten*. https://www.aftenposten.no/verden/i/zGn28w/trump-usa-kutter-alle-baand-til-verdens-helseorganisasjon

Elgabry, M., Nesbeth, D. & Johnson, S. D. (2020). A systematic review of the criminogenic potential of synthetic biology and routes to future crime prevention. *Bioengineering and Biotechnology*, *8*, 571672.

Ellefsen, H. B. (2018a). *Politiens politikk og politikkens politi. Norske politireformer i perioden 1682-1866* [Ph.D.-avhandling, Universitetet i Bergen].

Ellefsen, H. B. (2018b). Tidenes politireform? I V. L. Sørli & P. Larsson (Red.), *Politireformer. Idealer, realiteter, retorikk og praksis*. Cappelen Damm Akademisk.

Ellis, C., Pantucci, R., de Roy van Zuijdewijn, J., Bakker, E., Gomis, B., Palombi, S. & Smith, M. (2016). *Lone-Actor Terrorism. Final Report* (Countering Lone-Actor Terrorism Series No. 11). Royal United Services Institute for Defence and Security Studies.

Elster, K. (2020, 17. mars). Myndighetene advarer mot dataangrep når folk har hjemmekontor på grunn av koronaviruset. *NRK*. https://www.nrk.no/norge/myndighetene-advarer-mot-dataangrep-nar-folk-har-hjemmekontor-pa-grunn-av-koronaviruset-1.14947414

Engebråten, S., Glette, K. & Yakimenko, O. (2018, 12.-15. juni). *Networking-enabling enhancement for a swarm of COTS drones*. IEEE International Conference on Control and Automation, https://doi.org/10.1109/ICCA.2018.8444274

Etterretningstjenesten. (2020). *Fokus 2020. Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer*. Hentet 8. april 2021 fra https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus/rapporter/Fokus%202020.pdf/_/attachment/inline/639faaf2-7009-4056-9e0d-6dc5a6c5519b:1b228e374a207c8f79b1d8a166d902d7c0edd5e1/Fokus%202020.pdf

Etterretningstjenesten. (2021). *Fokus 2021. Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer*. Hentet 3. april 2021 fra https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus/rapporter/Fokus2021-web.pdf/_/attachment/inline/b9d52b53-0abe-4d1c-9c51-bf95796560bf:8dd66029b7efb38aab37d13e8b387d2e6ed0bd05/Fokus2021-web.pdf

European Commission. (2019). *The Digital Economy and Society Index (DESI) for 2019*. Hentet 15. oktober 2019 fra https://ec.europa.eu/digital-single-market/en/desi

European Commission. (2020, 7. desember). *Trans-European Networks for Energy*. Hentet 11. desember 2020 fra https://ec.europa.eu/energy/topics/infrastructure/trans-european-networks-energy_en

Europol. (2015). *Exploring tomorrow's organised crime*. https://www.europol.europa.eu/sites/default/files/documents/Europol_OrgCrimeReport_web-final.pdf

Europol. (2017a). *Crime in the Age of Technology (EDOC# 924156 v7)*. Hentet 3. november 2020 fra https://www.cepol.europa.eu/sites/default/files/924156-v7-Crime_in_the_age_of_technology_.pdf

Europol. (2017b). *European Union (EU) Serious and Organised Crime Threat Assessment 2017 (SOCTA 2017)*. https://www.europol.europa.eu/sites/default/files/documents/report_socta2017_1.pdf

Europol. (2017c). *Serious and Organised Crime Threat Assessment (SOCTA). Crime in the Age of Techno-logy*. Hentet 2. november 2020 fra https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017

Europol. (2020a). *Beyond the pandemic - how COVID-19 will shape the serious and organised crime landscape in the EU*. https://www.europol.europa.eu/publications-documents/beyond-pandemic-how-covid-19-will-shape-serious-and-organised-crime-landscape-in-eu

Europol. (2020b). *European Union Terrorism Situation and Trend report 2020*. https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020

Europol. (2020c). *Internet Organised Crime Threat Assessment (IOCTA) 2020*. Hentet 8. april 2020 fra https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

Farsund, B. H., Søndrol, T., Nystuen, K. O., Hornfelt, L., Sellevåg, S. R. & Pham, V. (2020). *Utviklingen av nye IoT-baserte infrastrukturer i samfunnet – utfordringer for nasjonal sikkerhet* (FFI-rapport 20/01745; Unntatt offentlighet). Forsvarets forskningsinstitutt.

Fauske, R. R. (2008, 7. mars). – Vestlandet er farleg. *NRK*. https://www.nrk.no/vestland/--vestlandet-er-farleg-1.5032592

FBI. (2016). *2016 Internet Crime Report*. https://www.ic3.gov/Media/PDF/AnnualReport/2016_IC3Report.pdf

Finstad, L. (2018). *Hva er politi?* Universitetsforlaget.

FOI. (2020, 15. september). *FOI confirms German results on Novichok*. Hentet 16. september 2020 fra https://www.foi.se/en/foi/news-and-pressroom/news/2020-09-15-foi-confirms-german-results-on-novichok.html

Forbrukerrådet. (2020, 14. januar). *Out of Control*. Hentet 23. september 2020 fra https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf

Forsvarets forskningsinstitutt. (2016). Teknologien Forsvaret trenger. *Viten*, s. nr. 2.

Fosshagen, K., Goplen, Å. & Wiborg, S. (2020, 2. desember). *Tyrkias samtidshistorie*. Store norske leksikon. Hentet 18. januar 2021 fra https://snl.no/Tyrkias_samtidshistorie

Foucault, M. (2018). *Overvåkning og straff: et moderne fengsels historie* (6. utg.). Gyldendal Akademiske.

Frontex. (2020). *Risk Analysis for 2020*. https://euagenda.eu/upload/publications/untitled-301445-ea.pdf

Futter, A. (2021). Explaining the nuclear challenges posed by emerging and disruptive technology: A primer for European policymakers and professionals. *Non-Proliferation and Disarmament Papers*. https://www.nonproliferation.eu/wp-content/uploads/2021/03/EUNPDC_no-73_FINAL-1.pdf

Færseth, J. (2017, 11. desember). *Nordmenn inspirert av amerikansk høyreekstremisme: Tror det er mulig å «melde seg ut av samfunnet»*. Hentet 27. januar 2021 fra https://fritanke.no/tror-det-er-mulig-a-melde-seg-ut-av-samfunnet/19.10674

Galaine, S., Thodey, K., Trenchard, I. J., Interrante, M. F. & Smolke, C. D. (2015). Complete biosynthesis of opioids in yeast. *Science*, *349*, 1095-1100.

Galteland, H. & Gjøsteen, K. (2018). Adversaries monitoring Tor traffic crossing their jurisdictional border and reconstruc-ting Tor circuits. *CoRR*, abs/1808.09237. https://dblp.org/rec/journals/corr/abs-1808-09237.html

Gleditsch, R. F., Thomas, M. J. & Syse, A. (2020). *Nasjonale befolkningsframskrivinger 2002. Modeller, forutsetninger og resultater* (Rapporter 2020/24). Statistisk sentralbyrå.

Government Office for Science. (2016). *The Quantum Age: technological opportunities*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/564946/gs-16-18-quantum-technologies-report.pdf

Government Office for Science. (2017). *The Futures Toolkit: Tools for Futures Thinking and Foresight Across UK Government. Edition 1.0*. UK Government Office for Science. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674209/futures-toolkit-edition-1.pdf

Government Office for Science. (2020). *Evidence and scenarios for global data systems. The future of citizens data systems*. UK Government Office for Science. https://www.gov.uk/government/publications/the-future-of-citizen-data-systems

Hagtvet, B. (2020, 14. desember). Selv ikke Hitler gjorde dette. *Dagbladet*. https://www.dagbladet.no/meninger/selv-ikke-hitler-gjorde-dette/73164919

Hanemann, T., Huotari, M. & Kratz, A. (2019). *Chinese FDI in Europe: 2018 trends and impact of new screening policies*. Rhodium Group and Mercator Institute for China Studies. https://merics.org/en/report/chinese-fdi-europe-2018-trends-and-impact-new-screening-policies

Hansen, E. E. (2016, 8. september). Dear Mark. I am writing this to inform you that I shall not comply with your require-ment to remove this picture. *Aftenposten*. https://www.aftenposten.no/meninger/kommentar/i/G892Q/dear-mark-i-am-writing-this-to-inform-you-that-i-shall-not-comply-wit

Hansen, K. A. & NTB. (2020, 2. september). Trump og USA dropper internasjonalt vaksinesamarbeid. *VG*. https://www.vg.no/nyheter/utenriks/i/BR5Xow/trump-og-usa-dropper-internasjonalt-vaksinesamarbeid

Hansen, T. K. (2019). *Personalisering og personvern – kompatible brikker i et puslespill kalt GDPR?* [Masteroppgave, Universitetet i Oslo].

Heckert, A. & Heckert, D. M. (2004). Using an integrated typology of deviance to expand Merton's anomie theory. *Criminal Justice Studies*, *17*(1), 75-90.

Hegghammer, T. (2016). The Future of Jihadism in Europe: A Pessimistic View. *Perspectives on Terrorism*, *10*(6), 156-170.

Helbling, M. & Meierrieks, D. (2020). Terrorism and Migration: An Overview. *British Journal of Political Science*, 1-20. https://doi.org/10.1017/S0007123420000587

Herington, M. J. & van de Fliert, E. (2018). Positive deviance in theory and practice: A conceptual review. *Deviant Behavior*, *39*(5), 664-678.

Hunt, E. (2016, 24. mars). Tay, Microsoft's AI chatbot, gets a crash course in racism from Twitter. *The Guardian*. https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter

hypotese. (2020, 16. juli). Store norske leksikon. Hentet 10. april 2021 fra https://snl.no/hypotese

Høibråten, S. & Kippe, H. (2020). *Russiske kjernefysiske styrker* (FFI-rapport 20/00131). Forsvarets forskningsinstitutt.

Høydahl, E. (2020, 24. september). *Svalbard: Nordlendinger ut, utlendinger inn*. Statistisk sentralbyrå,. Hentet 6. oktober 2020 fra https://www.ssb.no/befolkning/artikler-og-publikasjoner/svalbard-nordlendinger-ut-utlendinger-inn

Interpol. (2018). *Strategic Analysis Report: Emerging criminal trends in the global plastic waste market since January 2018*.

Interpol. (2020). *Global landscape on Covid-19 cyberthreat*. Hentet 2. november 2020 fra https://www.interpol.int/en/content/download/15217/file/Global%20landscape%20on%20COVID-19%20cyberthreat.pdf

Ipsos. (2019). *Hat og trusler mot folkevalgte*. https://www.ks.no/globalassets/fagomrader/forskning-og-utvikling/nyhetssaker/Hat-og-trusler-mot-folkevalgte.pdf

Johansen, I. & Gråtrud, H. (2018). *Fra taktisk elite til strategisk tilrettelegger - hvordan Forsvarets spesialstyrker kan møte fremtidens utfordringer* (FFI-rapport 18/01435). Forsvarets forskningsinstitutt.

Justis- og beredskapsdepartementet. (2020). *Høring - endringer i straffeprosessloven og straffeloven (etterforsknings- og påtaleplikt i store straffesaker, nytt straffebud om serieovergrep mv.)*. https://www.regjeringen.no/contentassets/ff323796d35a4665bcc78c0554de0ec6/horingsnotat-forslag-til-endringer-i-straffeprosessloven-og-straffeloven-etterforskings-og-pataleplikt-i-store-straffesaker-nytt-straffebud-om-serieovergrep-mv..pdf

Kaloudi, N. & Li, J. (2020). The AI-based cyber threat landscape: A survey. *ACM Computing Surveys*, Article No. 20. https://doi.org/10.1145/3372823

Karterud, S. (2021, 15. januar). Massepsykologien i det vi har sett, er en tro kopi av Hitlers massemønstringer i mellomkrigstiden. *Aftenposten*. https://www.aftenposten.no/meninger/kronikk/i/oAk5b0/massepsykologien-i-det-vi-har-sett-er-en-tro-kopi-av-hitlers-massemoen

Katz, B. (2020). *The Intelligence Edge. Opportunities and Challenges from Emerging Technologies for U.S. Intelligence*. Center for Strategic & International Studies. https://www.csis.org/analysis/intelligence-edge-opportunities-and-challenges-emerging-technologies-us-intelligence

Kenyon, J., Baker-Beall, C. & Binder, J. (2021). Lone-Actor Terrorism – A Systematic Literature Review. *Studies in Conflict & Terrorism*, 1-24. https://doi.org/10.1080/1057610X.2021.1892635

Kerner, S. M. (2020, 10. august). #DEFCON: Bypassing biometric scanners with 3D printed fingerprints. *Infosecurity Magazine*. https://www.infosecurity-magazine.com/news/defcon-bypassing-biometric-scanners/

King, T. C., Aggarwal, N., Taddeo, M. & Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and Engineering Ethics*, *26*, 89-120.

Kippe, H., Sellevåg, S. R. & Lausund, P. L. (2021). Understanding the Threat of Nuclear, Biological and Chemical Warfare. I H. Sæverot (Red.), *Meeting the Challenges of Existential Threats through Educational Innovation. A Proposal for an Expanded Curriculum*. Routledge.

Klima- og miljødepartementet. (2020, 11. november). *Det grønne skiftet i Norge*. Hentet 11. desember 2020 fra https://www.regjeringen.no/no/tema/klima-og-miljo/klima/innsiktsartikler-klima/gront-skifte/id2076832/?expand=factbox2686986

Koehler, D. (2019, 10. oktober). *What does the Halle attack say about Far-Right terrorism in Germany?* C-REX - Center for Research on Extremism. Hentet 24. april 2021 fra https://www.sv.uio.no/c-rex/english/news-and-events/right-now/2019/the-halle-attack.html

Kolnar, K. (2006). Volden. I I. J. Lorentzen & C. Ekenstam (Red.), *Män i Norden. Manlighet och modernitet 1840 - 1940*. Gidlunds forlag.

Kommunal- og moderniseringsdepartementet. (2014, 6. desember). *Digitalisering i offentlig sektor*. Hentet 9. april 2021 fra https://www.regjeringen.no/no/tema/statlig-forvaltning/ikt-politikk/digitaliseringen-i-offentlig-sektor/id2340245/

Korshunov, P. & Marcel, S. (2019). Vulnerability of face recognition to deep morphing. https://arxiv.org/abs/1910.01933

Kramer, A. E. (2020, 14. september). Pipeline politics: Why Nord Stream 2 is back in the spotlight. *The New York Times*. https://www.nytimes.com/2020/09/14/world/europe/nord-stream-2-russia-germany.html

Kripos. (2019a). *Alvorlig vold mot små barn*.

Kripos. (2019b). *Arbeid med drivkrefter*.

Kripos. (2019c). *Seksuell utnyttelse av barn og unge over internett*.

Kristoffersen, H. (2019, 15. april). *Kina: Utfordringer og muligheter for norsk næringsliv*. Næringslivets hovedorganisasjon. Hentet 18. september 2020 fra https://www.nho.no/contentassets/90adbb0dd12043cc995f4239c2fdc9d3/nho_notat_kina-utfordringer-og-muligheter-for-norsk-naringsliv_henning_17.04.2019_pdf.pdf

Kumar, R. S. S., Nyström, M., Lambert, J., Marshall, A., Goertzel, M., Comissoneru, A., Swann, M. & Xia, S. (2020). Adversarial Machine Learning – Industry Perspectives. https://arxiv.org/pdf/2002.05646.pdf

Lakner, C., Yonzan, N., Mahler, D. G., Aguilar, A. C., Wu, H. & Fleury, M. (2020, 7. oktober). *Updated estimates of the impact of COVID-19 on global poverty: The effect of new*

data. World Bank Blogs. Hentet 9. oktober 2020 fra https://blogs.worldbank.org/opendata/updated-estimates-impact-covid-19-global-poverty-effect-new-data

Layton, P. (2018, 25. april). Duelling Algorithms: Using Artificial Intelligence in Warfighting. *Over the Horizon*. https://othjournal.com/2018/04/25/duelling-algorithms-using-artificial-intelligence-in-warfighting/

Leivestad, E. H. (2020). *Frykt og avsky i demokratiet*. Vagant.

Leknes, S. & Løkken, S. A. (2020). *Befolkningsframskrivinger for kommunene, 2020-2050* (Rapporter 2020/27). Statistisk sentralbyrå.

Leraand, D., Stenersen, A. & Larsen, K. M. (2019, 20. september). *fremmedkriger*. Store norske leksikon. Hentet 17. januar 2021 fra https://snl.no/fremmedkriger

Libell, H. P. (2018, 29. mai). *Jussens konspirasjonsteorier*. Hentet 9. april 2021 fra https://juridika.no/innsikt/jussens-konspirasjonsteorier

Likestillings- og diskrimineringsombudet. (2015). *Hatytringer og hatkriminalitet*. https://www.ldo.no/diskriminert_oldstart/nyheiter-og-fag/brosjyrar-og-publikasjonar/rapporter/hatytringer-og-hatkriminalitet/

Lodgaard, S. (2020, 18. desember). Den arabiske våren: Ti år etter. *NUPI Hvor hender det?* https://www.nupi.no/nupi/Publikasjoner/Innsikt-og-kommentar/Hvor-hender-det/HHD-2020/Den-arabiske-vaaren-Ti-aar-etter

Lomell, H. M. (2020). Selvoppnevnte rettshåndhevere: Om fremveksten av «pedojegere» på nett. *Tidsskrift for Rettsvitenskap*, *154*(5), 660-690.

Maimon, D. & Louderback, E. R. (2019). Cyber-Dependent Crimes: An Interdisciplinary Review. *Annual Review of Criminology*, *2*, 191-216.

Meijer, H. & Brooks, S. G. (2021). Illusions of Autonomy: Why Europe Cannot Provide for Its Security If the United States Pulls Back. *International Security*, *45*(4), 7-43. https://doi.org/10.1162/isec_a_00405

Meld. St. 5 (2020-2021). *Samfunnssikkerhet i en usikker verden*. Justis- og beredskapsdepartementet,.

Meld. St. 29 (2016-2017). *Perspektivmeldingen 2017*. Finansdepartementet.

Meld. St. 29 (2019-2020). *Politimeldingen – et politi for fremtiden*. Justis- og beredskapsdepartementet.

Meld. St. 38 (2016-2017). *IKT-sikkerhet. Et felles ansvar*. Justis- og beredskapsdepartementet.

Morris, N. A., LaFree, G. & Karlidag, E. (2021). Counter-terrorism policies in the Middle East: Why democracy has failed to reduce terrorism in the Middle East and why protecting human rights might be more successful. *Criminology & Public Policy*, *20*(1), 153-175. https://doi.org/https://doi.org/10.1111/1745-9133.12532

Mustard, D. B. (2010). Labor Markets and Crime: New Evidence on an Old Puzzle. I B. L. Benson & P. R. Zimmerman (Red.), *Handbook on the Economics of Crime*. Edward Elgar Publishing.

Myklebust, M. (2019, 19. oktober). Norske journalister trues med øks, pistol og avkuttet sauehode. *NRK*. https://www.nrk.no/dokumentar/xl/norske-journalister-trues-med-oks_-pistol-og-avkuttet-sauehode-1.14729649

Myklebust, T. & Larsson, P. (2004). *Organisert og økonomisk kriminalitet: myter og realiteter*. Politihøgskolen.

Mækelæ, M. J., Reggev, N., Dutra, N., Tamayo, R. M., Silva-Sobrinho, R. A., Klevjer, K. & Pfuhl, G. (2020). Perceived efficacy of COVID-19 restrictions, reactions and their impact on mental health during the early phase of the outbreak in six countries. *Royal Societiy Open Science*. https://doi.org/10.1098/rsos.200644

Nasjonal sikkerhetsmyndighet. (2020a, 16. mars). *Mer hjemmekontor – store muligheter, men også risikoer*. Hentet 10. april 2021 fra https://nsm.no/aktuelt/mer-hjemmekontor-store-muligheter-men-ogsa-risikoer

Nasjonal sikkerhetsmyndighet. (2020b, 8. april). *Oppdatert varsel om digital risiko i forbindelse med COVID-19*. Hentet 2. november 2020 fra https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/varsler-fra-ncsc/oppdatert-varsel-om-digital-risiko-i-forbindelse-med-covid-19

Nasjonal sikkerhetsmyndighet. (2020c). *Risiko 2020*. Hentet 2. november 2020 fra https://nsm.no/getfile.php/133684-1592833706/Demo/Dokumenter/Rapporter/nsm-risiko-2020.pdf

Nasjonalt tverretatlig analyse- og etterretningssenter. (2020). *Situasjonsbeskrivelse 2020 – arbeidslivskriminalitet*. Hentet 16. januar 2021 fra https://www.okokrim.no/getfile.php/4632632.2528.kitjs7bwisslml/NTAES+Rapport+Situasjonsbeskrivelse+2020-web.pdf

National Academies of Sciences, Engineering, and Medicine. (2018). *Biodefense in the age of synthetic biology*. The National Academies Press. https://doi.org/10.17226/24890

National Intelligence Council. (2021). *Global Trends 2040. A More Contested World*. https://www.dni.gov/nic/globaltrends

NATO. (2020, 25. november). *NATO 2030: United for a New Era. Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General*. Hentet 17. januar 2021 fra https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf

Nesser, P. & Stenersen, A. (2014). The Modus Operandi of Jihadi Terrorists in Europe. *Perspectives on Terrorism*, *8*(6). http://www.terrorismanalysts.com/pt/index.php/pot/article/view/388

Nesser, P., Stenersen, A. & Oftedal, E. (2016). Jihadi Terrorism in Europe: The IS-Effect. *Perspectives on Terrorism*, *10*(6), 3-24.

NHO. (2018). *Verden og oss. Næringslivets perspektivmelding 2018*. https://www.nho.no/siteassets/publikasjoner/naringslivets-perspektivmelding/pdf-er-30okt18/nho_perspektivmeldingen_hele_web_lowres.pdf

Nilsen, R. Å. (1994). *Multidimensjonalitet og Ambivalens - Max Weber og det moderne.* (ISO-rapport nr. 5, Issue. Universitetet, Institutt for sosiologi, .

Nilsen, A. A. & Tjørhom, V. (2013, 4. juli). Morsi avsatt som president – Egypts grunnlov satt til side. *NRK*. https://www.nrk.no/urix/morsi-er-ikke-lenger-president-1.11115353

Nordås, H. K. (2020, 28. september). Pandemi = økonomisk kollaps. *NUPI, Hvor hender det?*, s. nr. 12. https://www.nupi.no/Publikasjoner/Innsikt-og-kommentar/Hvor-hender-det/HHD-2020/Pandemi-oekonomisk-kollaps

NOU 1981: 35. *Politiets rolle i samfunnet. Delutredning I*. Justis- og politidepartementet.

NOU 1987: 27. *Politiets rolle i samfunnet. Delutredning II*. Justis- og politidepartementet.

NOU 2012: 14. *Rapport fra 22. juli-kommisjonen*. Justis- og beredskapsdepartementet.

NOU 2015: 13. *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden*. Justis- og beredskapsdepartementet.

NOU 2020: 4. *Straffelovrådets utredning nr. 1 — Kriminalisering av deltakelse i og rekruttering til kriminelle grupper*. Justis- og beredskapsdepartementet.

NOU 2020: 15. *Det handler om Norge. Bærekraft i hele landet. Utredning om konsekvenser av demografiutfordringer i distriktene*. Kommunal- og moderniseringsdepartementet.

NOU 2020: 16. *Levekår i byer. Gode lokalsamfunn for alle*. Kunnskapsdepartementet & Kommunal- og moderniseringsdepartementet.

NTB. (2020a, 27. mai). EU-kommisjonen vil låne 750 milliarder euro til koronagjenreising. *Aftenposten*. https://www.aftenposten.no/verden/i/LAwB9x/eu-kommisjonen-vil-laane-750-milliarder-euro-til-koronagjenreising

NTB. (2020b, 11. november). NHO-økonom: Hjemmekontoret er kommet for å bli. *Dagbladet*. https://www.dagbladet.no/nyheter/nho-okonom-hjemmekontoret-er-kommet-for-a-bli/73054184

Nyadera, I. & Bincof, M. (2019). Human security, terrorism, and counterterrorism: Boko Haram and the Taliban. *International Journal of World Peace*, *36*, 7-32.

Næss, O. H. B. (2020, 26. oktober). Professor om trusler mot lokalpolitikere: - Politiet tar det ikke alvorlig nok. *NRK*. https://www.nrk.no/norge/professor-om-trusler-mot-lokalpolitikere_-_-politiet-tar-det-ikke-alvorlig-nok-1.15092893

OECD. (2012). *OECD Environmental Outlook to 2050. The Consequences of Inaction*. https://dx.doi.org/10.1787/9789264122246-en

Olstad, F. (2017). *Den lange oppturen: norsk historie 1945-2015*. Dreyer.

Omholt, E. L. (2019). *Økonomi og levekår for lavinntektsgrupper 2019* (Rapporter 2019/33). Statistisk sentralbyrå.

OPCW. (2018). *Summary of the report on activities carried out in support of a request for technical as-sistance by the United Kingdom of Great Britain and Northern Ireland* (S/1612/20128). https://www.opcw.org/sites/default/files/documents/S_series/2018/en/s-1612-2018_e___1_.pdf

opprør. (u.å.). Store norske leksikon. Hentet 4. september 2020 fra https://snl.no/oppr%C3%B8r

Oslo politidistrikt. (2019a). *Barne- og ungdomskriminaliteten i Oslo. Rapport basert på data fra 2019*. https://kriminalitetsforebygging.no/wp-content/uploads/2020/10/Barne-og-ungd.krim-Oslo_2019_SaLTo.pdf

Oslo politidistrikt. (2019b). *Hatkriminalitet. Anmeldt hatkriminalitet 2019*. https://www.politiet.no/globalassets/dokumenter/oslo/rapporter/anmeldt-hatkriminalitet-oslo/Anmeldt-hatkriminalitet-i-Oslo-2019

Oughton, E. J., Usher, W., Tyler, P. & Hall, J. W. (2018). Infrastructure as a Complex Adaptive System. *Complexity*, *2018*, 3427826. https://doi.org/10.1155/2018/3427826

Oye, K., Bubela, T. & Lawson, C. H. (2015). Regulate 'home-brew' opiates. *Nature*, *521*, 281-283.

Palmer, D. A. R. (2015). *Back to the future? Russia's hybrid warfare, revolutions in military affairs, and Cold War comparisons* (Research Paper No. 120). Research Division – NATO Defense College. https://www.files.ethz.ch/isn/194718/rp_120.pdf

Parker, T. (2014). *Avoiding the Terrorist Trap. Why Respect for Human Rights is the Key to Defeating Terrorism* (Bd. Volume 12) [doi:10.1142/p995]. World Scientific. https://doi.org/doi:10.1142/p995

pogrom. (u.å.). Store norske leksikon. Hentet 9. april 2021 fra https://snl.no/pogrom

Politidirektoratet. (2015). *Politiets omverdensanalyse 2015*. https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/omverdensanalyse/politiets-omverdensanalyse-2015.pdf

Politidirektoratet. (2020). *PBS I. Politiets beredskapssystem del I. Retningslinjer for politiets beredskap*.

Politiet. (2021). *Politiets trusselvurdering 2021*.

Politiets sikkerhetstjeneste. (2017). *Rapport om soloaktører*. https://www.pst.no/globalassets/artikler/utgivelser/temarapport-om-soloaktorer.pdf

Politiets sikkerhetstjeneste. (2021). *Nasjonal trusselvurdering 2021*. https://pst.no/globalassets/artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/ntv_2021_final_web_1802-1.pdf

Powell, J. M. & Thyne, C. L. (2011). Global instances of coups from 1950 to 2010: A new dataset. *Journal of Peace Research*, *48*, 249-259.

Prop. 1 S (2019-2020). *For budsjettåret 2020*. Justis- og beredskapsdepartementet.

Prop. 1 S (2020-2021). *For budsjettåret 2021*. Justis- og beredskapsdepartementet.

Prop. 14 S (2020-2021). *Vilje til beredskap – evne til forsvar. Langtidsplan for forsvarssektoren* Forsvarsdepartementet.

Prop. 61 LS (2014-2015). *Endringer i politiloven mv. (nærpolitireformen)*. Justis- og beredskapsdepartementet.

Pörtner, H.-O., Roberts, D. C., Masson-Delmotte, V., Zhai, P., Tignor, M., Poloczanska, E., Mintenbeck, K., Nicolai, M., Okem, A., Petzold, J., Rama, B. & Weyer, N. (Red.).

(2019). *Summary for Policymakers, IPCC Special Report on the Ocean and Cryosphere in a Changing Climate*. Intergovernmental Panel on Climate Change (IPCC).

Rácz, A. (2015). *Russia's Hybrid War in Ukraine* (FIIA Report 43). The Finnish Institute of International Affairs. https://stratcomcoe.org/andras-racz-russias-hybrid-war-ukraine-breaking-enemys-ability-resist

Rantala, R. R. (2008). *Cybercrime against Businesses, 2005* (Bureau of Justice Statistics Special Report, Revised 10/27/08). U.S. Department of Justice.

Rapoport, D. C. (2004). The Four Waves of Modern Terrorism. I A. K. Cronin & J. M. Ludes (Red.), *Attacking Terrorism. Elements of a Grand Strategy* (s. 46-73). Georgetown University Press.

Rassler, D. (2016). *Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology*. Combating Terrorism Center at West Point, United States Military Academy. https://ctc.usma.edu/wp-content/uploads/2016/10/Drones-Report.pdf

Ray, T. (2018, 30. november). Google's image recognition AI fooled by new tricks. *ZDNet*. https://www.zdnet.com/article/googles-best-image-recognition-system-flummoxed-by-fakes/

Rege, M., Skardhamar, T., Telle, K. & Votruba, M. (2019). Job displacement and crime: Evidence from Norwegian register data. *Labour Economics*, *61*, 101761.

Riddervold, M. & Trondal, J. (2020, 28. september). Hvorfor EU vil komme styrket ut av koronakrisen. *NUPI*. https://www.nupi.no/Nyheter/Hvorfor-EU-vil-komme-styrket-ut-av-koronakrisen

Riksrevisjonen. (2021a). *Riksrevisjonens undersøkelse av myndighetenes arbeid med eksportkontroll av strategiske varer* (Dokument 3:4 (2020-2021)). https://www.riksrevisjonen.no/globalassets/rapporter/no-2020-2021/myndighetenes-arbeid-med-eksportkontroll-av-strategiske-varer.pdf

Riksrevisjonen. (2021b). *Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT* (Dokument 3:5 (2020-2021)). https://www.riksrevisjonen.no/globalassets/rapporter/no-2020-2021/politiets-innsats-mot-kriminalitet-ved-bruk-av-ikt.pdf

Rolandsen, E. (2021, 9. februar). Vi elsker sosiale medier. *Kapital*. . https://kapital.no/reportasjer/2021/02/09/7611561/antall-brukere-av-sosiale-medier-globalt-har-na-bikket-3-5-milliarder

Rosten, M. G. (2017). Territoriell stigmatisering og gutter som «leker getto» i Groruddalen. *Norsk sosiologisk tidsskrift*, *1*(1), 53-70. https://doi.org/10.18261/issn.2535-2512-2017-01-04

Schneier, B. (1999). *A plea for simplicity*. Hentet 26. februar 2021 fra https://www.schneier.com/essays/archives/1999/11/a_plea_for_simplicit.html

Sellevåg, S. R. (2021). *Morfologisk analyse av trusler mot Norges sikkerhet – utfordringskategorier for politiet, PST og påtalemyndigheten* (FFI-rapport 20/03171; Unntatt offentlighet). Forsvarets forskningsinstitutt.

Sellevåg, S. R., Brattekås, K., Bruvoll, J. A., Buvarp, P. M. H., Fardal, H., Farsund, B., Fykse, E. M., Gisnås, H., Hellesø-Knutsen, K., Kirkhorn, S., Nystuen, K. O., Olsen, R. & Seehuus, R. A. (2020). *Samfunnssikkerhet mot 2030 – utviklingstrekk* (FFI-rapport 20/00530). Forsvarets forskningsinstitutt.

Sellevåg, S. R. & Buvarp, P. M. H. (2021). *Tilsiktede handlinger som kan true Norges sikkerhet - scenarioer for politiet, PST og påtalemyndigheten* (FFI-rapport 21/00415; BEGRENSET). Forsvarets forskningsinstitutt.

Sellevåg, S. R., Stenersen, A., Hoelsæter, Ø. T., Olafsen, H. K., Fykse, E. M., Kippe, H., Tørnes, J. A., Dullum, O. & Bjerkeseth, L. H. (2017). *Assessment of the possible use of unmanned aerial vehicles for terrorism in Western Europe* (FFI-rapport 17/00078; BEGRENSET). Forsvarets forskningsinstitutt.

Sikkerhetsloven. (2019). *Lov om nasjonal sikkerhet* (LOV-2018-06-01-24). Lovdata. https://lovdata.no/dokument/NL/lov/2018-06-01-24

Simonsen, K. B. (2020, 6. mai). *Sions vises protokoller*. Store norske leksikon. Hentet 1. februar 2021 fra https://snl.no/Sions_vises_protokoller

Skule, S. & Grytli, T. (1997). *Teknologisk utvikling og samfunnsendring. Eksempler fra oljehistorien og bankhistorien* (Fafo-rapport 217). Forskningsstiftelsen Fafo.

Statistisk sentralbyrå. (2020a). *Dette er Norge 2020*. Hentet 27. februar 2020 fra https://www.ssb.no/befolkning/artikler-og-publikasjoner/_attachment/430969?_ts=1756a0b4970

Statistisk sentralbyrå. (2020b). *Konjunkturtendensene med nasjonalregnskap for 2. kvartal og juli 2020* (Tall som forteller 2020/3). Statistisk sentralbyrå.

statskupp. (u.å.). Store norske leksikon. Hentet 8. april 2021 fra https://snl.no/statskupp

Stenersen, A. (2017). Thirty years after its foundation - Where is al-Qaida going? *Perspectives on Terrorism*, *11*, 5-16.

Stone, P., Brooks, R., Brynjolfsson, E., Calo, R., Etzioni, O., Hager, G., Hirschberg, J., Kalyanakrishnan, S., Kamar, E., Kraus, S., Leyton-Brown, K., Parkes, D., Press, W., Saxenian, A., Shah, J., Tambe, M. & Teller, A. (2016). *Artificial Intelligence and Life in 2030. One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel*. Stanford University.

Stortinget. (2014, 14. oktober). – *En varig endring i forholdet til Russland*. Hentet 1. mars 2021 fra https://www.stortinget.no/no/Hva-skjer-pa-Stortinget/Nyhetsarkiv/Hva-skjer-nyheter/2014-2015/--En-varig-endring-i-forholdet-til-Russland/

Sverdrup-Thygeson, B. & Mathy, E. (2020). Norges debatt om kinesiske investeringer: Fra velvillig til varsom. *Internasjonal Politikk*, *78*(1), 79-92.

Sverdrup, U. (2020, 6. september). Kronikk: Europeisk solidaritet kan bli en bombe i norsk politikk. *Dagens næringsliv*. https://www.dn.no/globalt/eu/koronakrisen/koronadebatt/kronikk-europeisk-solidaritet-kan-bli-en-bombe-i-norsk-politikk/2-1-868805

SySS. (2018, 18. desember). *SYSS-2017-027: BIOMETRICKS: Bypassing an enterprise-grade biometric face authentication system*. Hentet 19. november 2020 fra https://www.syss.de/pentest-blog/2017/syss-2017-027-biometricks-bypassing-an-enterprise-grade-biometric-face-authentication-system/

Sætre, M., Hofseth, C. & Kjenn, B. L. (2018). *Trender i kriminalitet 2018-2021. Digitale og globale utfordringer*. Oslo politidistrikt. http://www.forebygging.no/Global/trendrapport-oslo-2018---2021.pdf

Teknologi for bærekraftig bevegelsesfrihet og mobilitet. (2019). Rapport fra Ekspertutvalget – teknologi og fremtidens transportinfrastruktur. Hentet 30. september 2019 fra https://www.regjeringen.no/contentassets/ccdc68196014468696acac6e5cc4f0e7/rapport-teknologiutvalget_web.pdf

Telenor. (2020). *De lange linjene. Digital sikkerhet 2020*. https://www.telenor.no/binaries/om/digital-sikkerhet/Telenor_Digital_Sikkerhet_2020_1.pdf

Turkmen, Z. & Kuloglu, M. (2018). A New Era for Drug Trafficking: Drones. *Forensic Science & Addiction Research*, *2*, 114-118.

Turner, B. S. (2008). *The body & society: explorations in social theory*. Sage.

Tønnessen, T. H. (2017). Islamic State and Technology – A Literature Review. *Perspectives on Terrorism*, *11*, 101-111.

UNESCO. (2021, 25. januar). *UNESCO figures show two thirds of an academic year lost on average worldwide due to Covid-19 school closu-res*. Hentet 27. februar 2021 fra https://en.unesco.org/news/unesco-figures-show-two-thirds-academic-year-lost-average-worldwide-due-covid-19-school

United Kingdom National Cyber Security Centre. (2020). *Advisory: APT29 targets COVID-19 vaccine development* (version 1.1). https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf

United Nations. (2020). *The Sustainable Development Goals Report 2020*. https://unstats.un.org/sdgs/report/2020/The-Sustainable-Development-Goals-Report-2020.pdf

United Nations Department of Economic and Social Affairs. (2019, juni). *World Population Prospects 2019: Highlights*. Hentet 6. oktober 2020 fra https://population.un.org/wpp/Publications/Files/WPP2019_10KeyFindings.pdf

Wallace, E., Stern, M. & Song, D. (2020). Imitation attacks and defenses for black-box machine translation systems. https://arxiv.org/abs/2004.15015

Wang, F.-Y. (2010). The emergence of intelligent enterprises: From CPS to CPSS. *IEEE Intelligent Systems*, *25*, 85-88.

Wiik, J. H. (2020). *Cybersecurity and cryptographic methods in unmanned systems – a study of the current state in unmanned aerial vehicles and similar systems* (FFI-rapport 20/01289). Forsvarets forskningsinstitutt.

Wikipedia. (u.å.-a). *Catalan independence movement*. Hentet 5. oktober 2020 fra https://en.wikipedia.org/wiki/Catalan_independence_movement

Wikipedia. (u.å.-b). *Facebook-Cambridge Analytica data scandal*. Hentet 20. oktober 2019 fra https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal

Waage, K., Kvalvik, S. N. & Lindgren, P. Y. (2021). *Utenlandske investeringer og andre økonomiske virkemidler - når truer de nasjonal sikkerhet?* (FFI-rapport 20/03149). Forsvarets forskningsinstitutt.

Yampolskiy, M., King, W. E., Gatlin, J., Belikovetsky, S., Brown, A., Skjellum, A. & Elovici, Y. (2017). Security of additive manufacturing: Attack taxonomy and survey. *Additive Manufacturing*, *21*, 431-457.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books Ltd.

Økokrim. (2017, 29. juni). *Økonomisk kriminalitet og miljøkriminalitet*. Hentet 10. april 2021 fra https://www.okokrim.no/kriminalitetsomraader.422249.no.html

Økokrim. (2020). *Trusselvurdering 2020*. https://www.okokrim.no/trusselvurdering-2020.540514.no.html

Økokrim. (2021, 6. januar). *Statistikk 2019*. Hentet 10. januar 2021 fra https://www.okokrim.no/statistikk.417074.no.html

Aaberge, R., Modalsli, J. H. & Vestad, O. L. (2020, 24. september). *Ulikheten – betydelig større enn statistikken viser*. Hentet 7. mars 2021 fra https://www.ssb.no/inntekt-og-forbruk/artikler-og-publikasjoner/ulikheten-betydelig-storre-enn-statistikken-viser

Aamaas, B., Aaheim, H. A., Alnes, K., Oort, B. V., Dannevig, H. & Hønsi, T. (2018). *Oppdatering av kunnskap om konsekvenser av klimaendringer i Norge* (Report 2018:14). CICERO Center for International Climate Research og Vestlandsforskning.

A Sentrale begreper

I rapporten benyttes følgende begreper (Meld. St. 5 (2020-2021); Sellevåg *et al.*, 2020; Sikkerhetsloven, 2019):

- *Trend/utviklingstrekk:* Generell tendens eller retning til en endring over tid.
- *Driver/drivkraft/endringsdriver:* Faktor som forårsaker endring eller som kan påvirke eller forme fremtiden.
- *Trussel:* En trussel er relatert til faren for at en tilsiktet uønsket handling kan oppstå, hvor aktøren bak handlingen både har intensjon og kapabilitet (evne) til å gjennomføre handlingen.
- *Fare:* Fare er en risikokilde som er knyttet til fysisk eller psykologisk skade eller tap.
- *Risikokilde:* En risikokilde er et element som alene eller sammen med andre elementer har i seg et potensial for å gi konsekvenser for noe som er av verdi for mennesker.
- *Utfordring:* En handling eller hendelse som krever innsats for å håndtere.
- *Utfordringskategori:* Gruppe av utfordringer med fellestrekk.
- *Statssikkerhet:* Ivareta statens eksistens, suverenitet, territorielle integritet og politiske handlefrihet.
- *Samfunnssikkerhet:* Samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare. Slike hendelser kan være utløst av naturen, være et utslag av tekniske eller menneskelige feil eller bevisste handlinger.
- *Nasjonal sikkerhet:* Er definert som statssikkerhetsområdet og en avgrenset del av samfunnssikkerhetsområdet som er av vesentlig betydning for statens evne til å ivareta nasjonale sikkerhetsinteresser.
- *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.
- *Sikkerhetstruende virksomhet:* Tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser.

- *Samfunnsfunksjon:* Et system eller et sett av systemer som ivaretar en eller flere funksjonsevner som har til hensikt å dekke befolkningens og samfunnets behov.

- *Kritisk samfunnsfunksjon:* Er de samfunnsfunksjoner som er nødvendige for å ivareta befolkningens og samfunnets grunnleggende behov (mat, vann, varme, trygghet og lignende) og befolkningens trygghetsfølelse.

B Metodisk tilnærming

I hovedsak er to metodiske tilnærminger benyttet i denne rapporten for å beskrive samfunnsutviklingens betydning for politiet, PST og påtalemyndigheten. Først og fremst er denne rapporten en dokumentanalyse av publiserte utviklingstrekk som kan være av betydning for utfordringsbildet for politiet, PST og påtalemyndigheten frem mot 2030. Dernest er konsekvenser av samfunnsutviklingen vurdert basert på kvalitative intervjuer av eksperter i justis- og beredskapssektoren, samt egne analyser. I det følgende beskrives de metodiske aspektene i større detalj.

B.1 Omverdensanalyse

Kapittel 4 er en omverdensanalyse av den sosiale, teknologiske, økonomiske, miljømessige og politiske konteksten som kriminalitet, terrorisme og trusler mot nasjonal sikkerhet utvikler seg i. Variabler innenfor de ulike dimensjonene som blir drøftet er blant annet:

- **Politisk dimensjon:** Trender som berører aktører, maktforhold og det generelle konfliktnivået
- **Sosial dimensjon:** Trender innen demografi, migrasjon og innvandring
- **Økonomisk dimensjon:** Trender innen globalisering, økonomisk utvikling og fattigdomsutvikling
- **Miljødimensjonen:** Klimaendringer, klimatiltak og klimatilpasninger
- **Teknologisk dimensjon:** Teknologiutviklingens betydning for kriminalitetsutviklingen, ikke-spredning og trusler mot nasjonal sikkerhet

Omverdensanalysen forsøker å belyse generelle utviklingstrekk fra ulike sider i den grad det er mulig ut fra litteraturen som er tilgjengelig. Således forsøker omverdensanalysen både å peke på forhold som representerer utfordringer for politiet, PST og påtalemyndigheten, og på forhold som kan innebære en positiv utvikling. Imidlertid vurderes verken faktorer knyttet til juridiske forhold eller hvilke konsekvenser potensielle enkelthendelser kan gi. Konsekvenser som følge av covid-19-pandemien er forsøkt vurdert i den utstrekning det underbygges av troverdig publisert litteratur.

Med bakgrunn i omverdensanalysen, diskuteres utviklingen innen tematiske utfordringsområder i kapittel 5. Utfordringsområdene er identifisert ut fra en morfologisk analyse av trusler mot Norges sikkerhet (Sellevåg, 2021).

Datagrunnlaget for omverdensanalysen er først og fremst basert på følgende kilder:

- Globale trender mot 2040 – et oppdatert fremtidsbilde (Beadle *et al.*, 2019)
- Samfunnssikkerhet mot 2030 – utviklingstrekk (Sellevåg *et al.*, 2020)

- Trussel- og risikovurderinger til politiet, PST, Etterretningstjenesten og Nasjonal sikkerhetsmyndighet
- Trusselvurderinger fra Europol
- Politiets omverdensanalyse (Politidirektoratet, 2015)
- Offentlig statistikk fra Statistisk sentralbyrå og tilsvarende byråer internasjonalt
- Norges offentlige utredninger
- Stortingsmeldinger og proposisjoner til Stortinget

I tillegg er det gjort søk i publisert litteratur ved hjelp av søkemotorene Google, Google Scholar og Web of Science. Utvalgskriteriene for valg av litteratur er (fra høyest til lavest rangering):

1. Oversiktsartikler («reviews») i høyt rangerte internasjonale vitenskapelige tidsskrifter med fagfellevurdering
2. Vitenskapelige artikler i høyt rangerte internasjonale vitenskapelige tidsskrifter med fagfellevurdering
3. Vitenskapelige artikler i vitenskapelige tidsskrifter med fagfellevurdering
4. Fagbøker
5. Analyser og rapporter fra anerkjente akademiske institusjoner og forskningsinstitutter
6. Analyser og rapporter fra tenketanker og lignende organisasjoner
7. Artikler fra nyhetsmedier med redaktøransvar
8. Store norske leksikon / Wikipedia
9. Andre internettkilder

B.2 Kvalitative intervjuer

For å styrke forståelsen og kunnskapsgrunnlaget om sammenhengen mellom samfunnsutviklingen og politiets fremtidige oppgaver, ble det gjennomført intervjuer med relevante eksperter i justis- og beredskapssektoren. Ekspertene var tilknyttet JDs faggruppe for delutredningen «Beredskap og nasjonal sikkerhet». Totalt ble syv eksperter intervjuet. To av intervjuene ble gjennomført via Microsoft Teams, mens de resterende fikk tilsendt spørsmålene for skriftlig besvarelse. Det ble benyttet samme intervjuguide for alle intervjuene. Intervjuguiden var strukturert, som vil si at spørsmålene og rekkefølgen på disse var utviklet og arrangert på forhånd. Intervjuguiden var inspirert av «7 questions»-tilnærmingen presentert av det britiske Government Office for Science (2017), som er et verktøy for å innhente kunnskap om fremtiden.

About FFI

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

FFI's MISSION

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

FFI's VISION

FFI turns knowledge and ideas into an efficient defence.

FFI's CHARACTERISTICS

Creative, daring, broad-minded and responsible.

Om FFI

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

FFIs FORMÅL

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

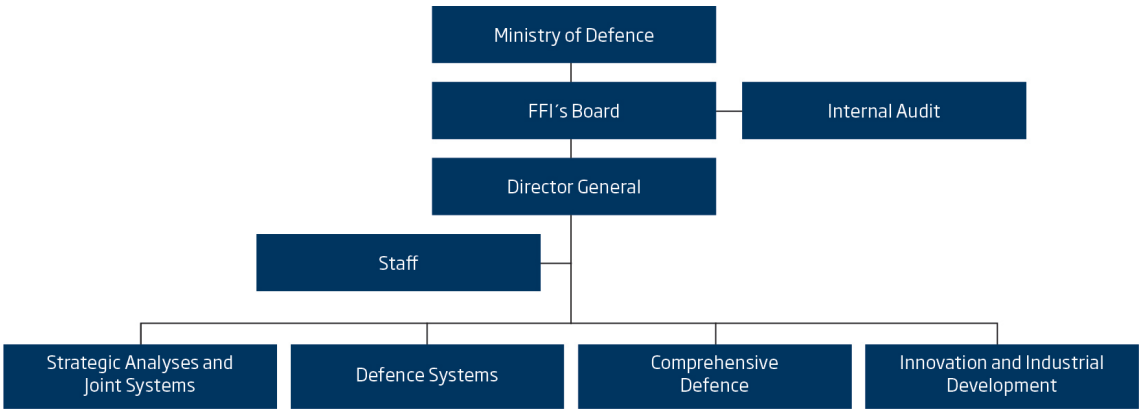
FFIs VISJON

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs VERDIER

Skapende, drivende, vidsynt og ansvarlig.

FFI's organisation



Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

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

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

Office address:
Instituttveien 20
N-2007 Kjeller

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

FFI Forsvarets forskningsinstitutt