# FFI-RAPPORT

21/01026

# Ikke-statlige aktører og fremvoksende teknologi mot 2050

## – utviklingstrekk og konsekvenser for militære operasjoner

Michael Mayer
Mats Rjaanes
Harald Erik Andås
Truls Tønnessen

# Ikke-statlige aktører og fremvoksende teknologi mot 2050
## – utviklingstrekk og konsekvenser for militære operasjoner

Michael Mayer
Mats Rjaanes
Harald Erik Andås
Truls Tønnessen

Forsvarets forskningsinstitutt (FFI) 19.mai 2021

**Emneord**
Teknologiske trender
Terrorisme
Militære operasjoner

**FFI-rapport**
21/01026

**Prosjektnummer**
1521

**Elektronisk ISBN**
978-82-464-3346-2

**Engelsk tittel**
Non-state actors and emerging technology towards 2050 – developments and consequences for military operations

**Godkjennere**
Torgeir Mørkved, *forskningsleder*
Hanne Bjørk, *forskningsdirektør*

*Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.* / *The document is electronically approved and therefore has no handwritten signature.*

# Sammendrag

Ved å bruke fremvoksende og banebrytende teknologier kan voldelige ikke-statlige aktører innen 2050 ha skaffet seg evner til å forårsake skade i en grad som tidligere bare var mulig for statlige aktører. For Forsvaret vil ikke-statlige aktører som kriminelle nettverk, terrororganisasjoner, opprørsgrupper eller proxy-aktører forbli potensielle motstandere. Denne typen aktører kan være svært innovativ og voldelig, og har mindre reservasjoner mot å bruke midler som resten av samfunnet anser som uetisk eller som går på tvers av etablerte internasjonale normer.

Som et ledd i prosjektet *Teknologiske trender med konsekvenser for militære operasjoner* (TEKNO) analyserer denne rapporten sannsynlige teknologiske utviklingstrekk, mulige kapabiliteter voldelige ikke-statlige aktører kan forvente å få i tidsrommet 2030–2050, samt konsekvensene dette vil kunne få for militære operasjoner.

Gjennom workshop-aktivitet, strukturert analyse og sekundærlitteratur former rapporten et bilde av hvordan samfunnet kan komme til å bli seende ut i 2030 og 2050 og skisserer effekten teknologi vil kunne ha på ulike samfunnsdimensjoner. Dette blir deretter benyttet til å analysere den fremtidige trusselen fra ikke-statlige aktører.

Teknologiområdene som omtales og inkluderes i analysen er: digital teknologi, kunstig intelligens, ubemannede og autonome systemer, additiv tilvirkning, rombasert overvåking, bioteknologi og soldatforbedringssystemer og bruk av det elektromagnetiske spekter.

Rapporten finner at militære operasjoner kan være langt mer utfordrende for norske styrker dersom ikke-statlige aktører benytter fremvoksende teknologi til å nå sine mål. Flere aktører vil ha evnen til å ramme store deler av samfunnet ved å bruke lett tilgjengelig fremvoksende teknologi. Denne teknologien vil primært bli utviklet av sivile aktører.

Ikke-statlige aktører vil kunne ha et fortrinn i tilfeller der det oppstår etisk asymmetri mellom aktører som er villige til å ta i bruk etisk tvilsom teknologi og aktører som er mer skeptiske. Det er ikke nødvendigvis en selvfølge at norske militære styrker forblir teknologisk overlegen i møte med en ikke-statlige aktør.

Hensikten med fremtidsanalyser er å danne et beslutningsgrunnlag som kan gjøre oss bedre rustet til å håndtere fremtiden. Mulige teknologiske tiltak inkluderer å styrke evnen til elektronisk krigføring, satsning på kunstig intelligens, kompetanseheving, samt videreutvikling av mottiltak mot ubemannede systemer og biologiske trusler. Organisatoriske tiltak inkluderer å øke den teknologiske bevisstheten i Forsvaret, forbedre muligheten til å trene med ny teknologi og utvikling av nye strategier, doktriner og taktikker.

# Summary

By 2050, violent non-state groups may have an expanded capacity to cause harm using emerging technologies that were previously only accessible to state actors. For the Norwegian Armed Forces, non-state actors such as criminal networks, terrorist organizations, insurgency groups or proxy actors may be particularly relevant, especially with regard to international operations. Such actors can be very innovative, violent, and have fewer reservations about using weapons that most people consider unethical or against established international norms.

As part of a FFI-project on emerging technologies, this report seeks to understand the likely future development of technology, what kind of capabilities violent non-state actors can be expected to have within the period 2030-2050, and the implications of these trends for military operations.

The technologies included are: digital technology, artificial intelligence, unmanned and autonomous systems, additive manufacturing, space technology, biotechnology and human enhancement, and the use of the electromagnetic spectrum. Since non-state actors often use tools that are readily available, it was necessary to develop some claims about the future effects of technology on a number of societal dimensions. Through workshop activities, structured analyzes and a review of secondary literature, a future image of society was created for both 2030 and 2050, which was then used to analyze the future threat from non-state actors.

The main tendencies were clear. Military operations can be far more challenging for Norwegian forces if non-state actors use emerging technologies to become more capable and lethal. More actors will have the ability to affect large parts of society with easily accessible emerging technologies developed primarily by civilian actors. This will be especially relevant in technology areas where an ethical asymmetry arises between actors who are willing to use ethically questionable technology and others who are skeptical. Norwegian military forces in international operations cannot always count on having technological superiority in meetings with non-state groups.

The intent of future analyses is to provide a foundation for taking actions today that can make the country better equipped for the future. Possible technological measures include strengthening electronic warfare and artificial intelligence capabilities, as well as further developing countermeasures against unmanned systems and biological threats. Organizational measures include better technological awareness throughout the Armed Forces, better training opportunities with new technology, and the development of new doctrines.

# Innhold

# Forord

Denne rapporten er en delleveranse i FFIs forskningsprosjekt «Teknologiske trender med konsekvenser for militære operasjoner» (TEKNO). Formålet med dette arbeidet er å se langsiktig på de teknologiske trendene og utarbeide analyser og vurderinger knyttet til hva dette vil kunne innebære for Forsvaret. Før prosjektet kan komme med en samlet vurdering er det nødvendig å forstå hvordan trendene kan påvirke en potensiell motstander, det er med bakgrunn i dette at rapporten fokuserer på ikke-statlige aktører. Studien skal i så måte danne grunnlag for videre analyser av hvilke betydning de teknologiske trendene vil kunne ha for fremtidige militære operasjoner.

TEKNO-prosjektet og denne studien har vært avhengig av bred støtte fra FFIs teknologi-, forsvars- og totalforsvarsmiljøer. En rekke forskningsprogrammer og enkeltpersoner ved FFI har bidratt til rapporten med innspill og kommentarer. Spesielt viktig har støtten fra forskningsprogrammet TERRA og SORD vært, som har bidratt med diskusjoner, kommentarer og tekst.

En stor takk rettes til de interne og eksterne workshop deltagerne som har bidratt med kreative diskusjoner, viktige innspill og løpende tilbakemeldinger.

Michael Mayer, Mats Rjaanes og Harald Andås

Kjeller, 19. mai 2021

# 1 Innledning

I fremtidige militære operasjoner kan Forsvaret møte motstandere som benytter teknologi på helt andre måter enn i dag. Historisk sett har mange teknologiske nyvinninger – alt fra trykkpressen, forbrenningsmotoren, flyet, antibiotika, og datamaskinen –skapt ringvirkninger langt utover sitt opprinnelige formål. Flere teknologier og oppfinnelser som i utgangspunktet ble utviklet for bruk i det sivile samfunn har vist seg å ha stor innvirkning også i den militære sfæren, mens for andre nyvinninger gikk det motsatt vei, fra det militære inn i det sivile.

Flere fremvoksende teknologier – blant annet kunstig intelligens (AI), autonome systemer og robotikk, digital teknologi, og bioteknologi – vil ha en positiv innflytelse på fremtidens samfunnsliv. Samtidig vil denne typen fremvoksende teknologi kunne føre til at ikke-statlige grupper med voldelige hensikter får utvidede evner. Denne type aktør vil i fremtiden kunne utnytte ny teknologi på en måte som muliggjør angrep og gjennomføring av militære operasjoner i en skala som tidligere bare har vært mulig for statlige aktører. Som den anerkjente forskeren Audry Kurth Cronin sa: «tilgang til dødelige teknologi har gitt flere aktører evnen til å starte krig, samtidig som stormaktene har mistet evnen til å avslutte dem».[1]

For å kunne være bedre forberedt på hvordan fremtidige trusler kan bli seende ut er det essensielt å være kjent med og følge de teknologiske trendene. Samtidig som man danner seg en oversikt over hvilke teknologier som forventes å modnes i løpet av de kommende 10-30 år, er det viktig å opparbeide seg kunnskap om hvordan disse teknologiene kan komme til å bli anvendt av forskjellige aktører i en operasjonell og militær kontekst. Med bakgrunn i dette tar denne rapporten for seg hvordan ikke-statlige aktører vil kunne benytte fremvoksende teknologi i en fremtidig konfliktsituasjon. Rapporten opererer med to tidshorisonter: et kortsiktig tidsperspektiv på 10 år som ser på konsekvensene av teknologi som i dag nærmer seg modenhet frem mot 2030, og et lengre tidsperspektiv som ser på konsekvensene av fremvoksende teknologi i de kommende 30 år – det vil si mot år 2050.[2]

Analysen begrenser sitt fokus til militære operasjoner. For å konkretisere hva som kan defineres som militære operasjoner benyttes Forsvarets fellesoperative doktrine (FFOD) som utgangspunkt.[3] Ikke-statlige aktører vil kunne utgjøre en relevant trussel mot flere av oppgavene listet opp i FFOD.[4] Diskusjoner om ikke-statlige aktører og teknologi dreier seg ofte om

[1] Cronin, Audry Kurth (2020), "Power to the People: How open technological innovation is empowering tomorrow's terrorists", *Oxford: Oxford university Press.*

[2] Det er verdt å understreke tidshorisonten, særlig fra et teknologisk ståsted. For 30 år siden var to teknologier som nå preger vår hverdag – mobiltelefonen og internett, nærmest ikke i bruk på verdensbasis. Den logiske og betydningsfulle kombinasjonen av internett og mobiltelefonen i en «smartphone» som Blackberry har vært i bruk mindre enn 20 år.

[3] Forsvarsstaben (2019), "Forsvarets fellesoperative doktrine", *Oslo: Forsvaret*. ss. 38- 45.

[4] FFOD lister opp Forsvarets ni kjerneoppgaver som er til Forsvaret – *troverdig avskrekking, forsvar av Norge mot alvorlige trusler, håndtering av sikkerhetspolitiske kriser, overvåking og etterretningsansvar, suverenitetshevdelse,*

terrorangrep mot sivile mål, eller situasjoner der andre sektorer har hovedrollen i hendelseshåndteringen, gjerne med støtte fra forsvarssektoren. Denne rapporten sitt fokus er derimot hovedsakelig situasjoner der militære styrker skal nedkjempe ikke-statlige aktører, mens annet arbeid ved FFI undersøker konsekvensene av teknologisk utvikling fra et samfunnssikkerhetsperspektiv.[5]

Målet til rapporten er å kombinere aktørvurderinger med teknologiske trender, og vurdere hvordan den fremtidige trusselen fra ikke-statlige aktører kan arte seg. Rapportens vurderinger gjøres med forbehold om at det ikke er mulig å nøyaktig forutse hvordan hverken teknologiutviklingen vil bli seende ut, og heller ikke hvordan fremtidige ikke-statlige trussel-aktører kan komme til å benytte teknologi. Hvordan de ulike aktørene tilnærmer seg ny teknologi og innovasjon blir således et viktig vurderingskriterium. Analysen og rapporten inneholder derfor betydelig grad av usikkerhet og bygger på en noe utradisjonell tilnærming som integrerer kunnskap om teknologi med fantasi og kreativitet.

Samtidig er det ikke nødvendigvis konklusjonene i denne type studie som er det mest verdifulle, men heller problemstillingene som analysen belyser. Intensjonen er å undersøke muligheter og potensielle trusler fremfor å komme med bastante påstander om hvilke teknologier som vil benyttes av ikke-statlige aktører i fremtiden. Selv om fremtiden forblir ukjent, kan vi analysere atferdsmønstre og peke på indisier knyttet til hvordan ulike aktørtyper kan komme til å benytte fremvoksende teknologi. Dette bidrar til å redusere sannsynligheten for strategiske og operasjonelle overraskelser og gjør at vi kan starte utvikling av mottiltak på et tidligere tidspunkt.

## 1.1 Hvorfor ikke-statlige aktører?

Historisk har det vært store forskjeller mellom statlige og ikke-statlige aktørers evne til å utvikle og benytte avansert militærteknologi. Statlige aktører har betydelige fordeler gitt deres økonomiske ressurser og satsning på forsking og utvikling (FoU). Regulatoriske barrierer er med på å hindre tilgangen ikke-statlige aktører har til mye av denne FoU aktiviteten. Ikke-statlige aktører har dermed begrensede muligheter sammenlignet med statlige aktører og har i lang tid måtte belage seg på det åpne marked og egne ferdigheter for å få tilførsel av ny teknologi. At informasjon er globalisert bidrar derimot til at ikke-statlige aktører i større grad kan få tilgang til den samme kunnskapen som statlige aktører gjennom nye markeder og kanaler for utveksling av erfaringer og informasjon.

Ikke-statlige aktører har ofte andre bruksmønstre og behov enn de statlige aktørene. Dette påvirker hva slags teknologi de ikke-statlige aktøren anskaffer og bruker. Ikke-statlige aktører skiller seg også ut fra de statlige aktørene når det gjelder innovasjon, organisasjonslæring og

*myndighetsutøvelse, flernasjonal krisehåndtering, internasjonal sikkerhetspolitisk, forsvarspolitisk samarbeid og samfunnssikkerhet*.

[5] Sellevåg, Stig Rune & al. (2020), "Samfunnssikkerhet mot 2030 – Utviklingstrekk". *FFI-rapport 20/00530 (Kjeller: FFI).*

institusjonell hukommelse. Dette er faktorer som bidrar til at aktørene ofte belager seg på moden, gjennomprøvd teknologi med begrenset kompleksitet.

Ikke-statlige aktører utgjør i utgangspunktet ikke en eksistensiell trussel mot Norge, men er samtidig en relevant trussel i militære operasjoner. Forberedelse til statlig høyintensitetskrigføring er en stor og viktig del av Forsvarets aktivitet for å ivareta nasjonal suverenitet og sikkerhet. Likevel er det trusselen fra ikke-statlige aktører som i stor grad har preget de internasjonale operasjonene Forsvaret har vært involvert i de siste to tiår. Mange analytikere mener at den internasjonale sikkerhetspolitiske strukturen kommer til å være mer preget av stormaktrivalisering de kommende tiårene.[6] Kina presser aktivt på for å utvide sin makt og innflytelse, noe USA og NATO forsøker å forhindre på grunn av egne geopolitiske interesser. Samtidig har Russland spilt en mer aktiv rolle både i Europa og Midtøsten for å bevare sine strategiske interesser og øke sin politisk innflytelse. I flere områder har Russland motstridende interesser med USA og NATO. Dette har i flere tilfeller – blant annet i Libya og Syria – ført til situasjoner der ikke-statlige aktører støttet av Russland har kommet i direkte konflikt med lignende aktører støttet av USA.[7]

Bruk av ikke-statlige aktører som en stedfortreder eller «proxy» forventes å øke når stormaktene forfølger sine strategiske interesser. Å bruke stedfortredere fremfor å risikere kostbare konfrontasjoner som øker sannsynligheten for en ukontrollert eskalasjon, kan i flere tilfeller fremstå som mer attraktivt og innebære lavere risiko for de involverte statene.[8] En annen måte å tvinge frem politisk endring på, uten å overstige terskelen som utløser en høyintensiv mellomstatlige konflikt, har vært bruk av såkalte gråsonevirkemidler ofte omtalt som hybrid krigføring.[9] Aktører som Kina, Russland og Iran har de senere år benyttet denne tilnærmingen, ved å bruke en kombinasjon av ukonvensjonell krigføringstaktikker og informasjons- og påvirkningsoperasjoner.[10]

Ikke-statlige aktører byr på andre sikkerhetspolitiske utfordringer enn statlige aktører gitt deres uortodokse operasjonsmønstre, angrep mot sivile og manglende vilje til å følge internasjonale normer og regler. Hvordan disse aktørene ledes, er organisert og hva de ønsker å oppnå er tidvis uklart og gjør statlige militære styrkers mulighet til avskrekking vanskelig og diplomati utfordrende. For terrorgrupper er taktikkene ofte designet for å sjokkere og spre frykt. Med bakgrunn i dette er det større sannsynlighet for at disse aktørene velger å benytte våpenteknologi som er etisk tvilsomt og går på tvers av internasjonale normer.

[6] Lynch, Thomas F III (red.) (2021), "Strategic assessment 2020 – into a new era of great power competition", *National defense university press.*
[7] Frantzman, Seth J. (2020), "Libya is now the Middle East's most important proxy war", *The spectator 20. Mai 2020*; Bezhan, Frud (2020), "US vacuum: How Libya is descending into a Russia-Turkey proxy war", *RadioFreeEurope 21. Januar, 2020*; Benowitz, Brittany & Ross, Tommy (2020), "Time to get a handle on America's conduct of proxy warfare", *Lawfareblog*, 9. april 2020.
[8] Mumford, Andrew (2013), "Proxy warfare and the future of conflict", *RUSI Journal, April/May vol. 158(2).*
[9] Diesen, Sverre (2018), "Lavintensivt hybridangrep på Norge i en fremtidig konflikt", *FFI-rapport 18/00080 (Kjeller: FFI).*
[10] Bredesen, Maren & Reichborn-Kjennerud, Erik (2016), "Hybrid krigføring – hva er det?", *NUPI – Hvor hender det nr. 7, 1.*

Ikke-statlige aktører har ikke nødvendigvis de samme behovene for testing og eksperimentering med ny teknologi som statlige aktører og kan raskt benytte nye løsninger i skarpe oppdrag. Et våpen som fungerer «greit nok» kan ofte være mer enn tilstrekkelig for at ikke-statlige aktører velger å gjennomføre et angrep eller igangsette en operasjon. Disse aktørene kan tilegne seg ny kunnskap via digitale plattformer og nettverk for sosial interaksjon, på den måten vil aktørene kunne utnytte teknologi på nye måter. Dette er utviklingstrekk som kan føre til at ikke-statlige aktører i fremtiden kan gjennomføre angrep med annen teknologi enn hva man har sett til nå.

Det er med bakgrunn i disse trekkene at man bør følge nøye med på teknologiutviklingen i en kontekst av fremtidige militære operasjoner som involverer ikke-statlige aktører.

## 1.2 Metode og analytisk tilnærming

Forvarets forskningsinstitutt (FFI) har utviklet metoder for å integrere fremtidsrettede trendanalyser i støtte til langtidsplanleggingen av Forsvaret.[11] Denne studien tar sikte på å være et bidrag inn i denne type langtidsplanlegging i form av en trendstudie med et langt tidsperspektiv. Mye av arbeidet som har blitt gjort av *Globale trender*-prosjektet ved FFI utgjør et viktig analytisk grunnlag for denne rapporten.[12] Problemstillingene som søkes belyst her er imidlertid enda mer spisset mot fremvoksende teknologi og fremtidens operasjonsmiljø. Dette krever andre metodiske tilnærminger og en større fortrolighet med teoretisering om tekniske løsninger som ennå ikke eksisterer. Utgangspunktet for mye av de teknologiske beskrivelsene er derfor hentet fra tidligere publikasjoner og pågående arbeid ved FFI.[13]

Fremtidsanalyser gjennomføres jevnlig av organisasjoner som NASA, US Army Futures Command, NATO og ulike aktører innen næringslivet. Metodene innebærer ofte bruk av ulike former for strukturert idemyldring gjennom workshop aktivitet, ulike typer spill, spørreundersøkelser i gjentagende runder, eller ved bruk av science fiction og historiefortellinger som skal øke forståelsen for hvordan teknologi vil kunne anvendes i en fremtidig tenkt virkelighet.[14] Alle fremtidsanalyser som baserer seg på denne type metode vil være preget av faglig usikkerhet. Dette er også tilfelle for denne rapporten da tidshorisonten tidvis forsøker å strekke seg 30 år inn i fremtiden.

Problemstillingene som diskuteres krever kompetanse fra ulike fagmiljøer. Arbeidet har derfor helt fra starten vært en tverrfaglig forskningsaktivitet som har benyttet relevant spisskompetanse ved FFI om teknologi og aktører. Det er også gjennomført spørreundersøkelser for å innhente ytterligere perspektiv, både av teknisk og samfunnsvitenskapelig art. Noe av rapportens innhold

[11] Vatne, et.al (2020), "Norwegian long-term defence analysis – a scenario and capability based approach", *FFI-rapport 20/02367 (Kjeller:FFI).*
[12] Beadle, Alexander W. et.al (2019), "Globale trender mot 2040 – et oppdatert fremtidsbilde», *FFI-rapport 19/00045 (Kjeller:FFI).*
[13] Andås, Harald (2020), "Emerging technology trends for defense and security", *FFI-rapport 20/01050 (Kjeller:FFI).*
[14] For en oversikt over metoder for fremtidsforskning; se Mayer, Michael (2020), "Methodologies for technology forecasting – a framework for the TEKNO project", *FFI-notat 20/1243 (Kjeller:FFI).*

hviler på et bredt spekter av sekundære kilder, særlig når det gjelder egenskapene ved ulike ikke-statlige aktører, samt beskrivelsene av fremtidige teknologiske utviklingstrekk. Denne tverrfaglige tilnærmingen har skapt et bredt empirisk grunnlag, noe som er viktig gitt at analysen strekker seg mot det ukjente.

For de delene av rapporten som beskriver mulige fremtidstrekk benyttes metoder forbundet med strukturert fremtidsanalyse.[15] For å forstå hvordan fremvoksende teknologi kan anvendes som håndfaste kapabiliteter i en fremtidig konflikt med ikke-statlige aktører, ble det organisert og gjennomført flere workshoper med utvalgte eksperter innen teknologi, ikke-statlige aktører og militære operasjoner. Dette bidro til økt fagmilitær innsikt i hvordan ikke-statlige aktører vil komme til å påvirke det fremtidige operasjonsmiljøet.

Flere grunnleggende forutsetninger har vært viktig for arbeidet med rapporten. Prosjektet har primært fokusert på mulighetsrommet til fremtidsteknologi og ikke-statlige aktører. Dette er like mye en konseptualisering av teknologiutviklingen som det er en gjennomgang av hvordan aktørene vil utvikle en konkret fremtidig kapabilitet. Teoretisk mulige kapabiliteter som per i dag ikke kan realiseres har vært av spesiell interesse. Mange av ideene og beskrivelsene som skisseres vil nødvendigvis ikke bli realisert, men dette er heller ikke hensikten med denne type studie. Formålet er derimot å identifisere nyttig informasjon og beskrive mulige anvendelsesområder slik at man på et tidlig tidspunkt kan analysere og forstå konsekvenser.

En annen forutsetning er erkjennelsen om at den fremtidige utviklingen innen forsvars- og sikkerhetspolitikk vil bli viktig for selve anvendelsen av ny teknologi. Utviklingen innen enkelte teknologiområder er utfordrende nok, men det er viktig å unngå at teknologien vurderes i isolasjon. Når for eksempel den militære betydningen av autonomi for ikke-statlige aktører i 2050 skal vurderes, må dette settes i en kontekst som gjenspeiler den teknologiske utviklingen i samfunnet.

Det er heller ikke gitt at vi er i stand til å forutse slik utvikling. Som FFI-forsker Alexander Beadle og andre har påpekt, er vår evne til å unngå vanlige kognitive fallgruver i fremtidsanalyser nokså dårlig.[16] Det er særdeles utfordrende å unngå fristelsen om å ta mye som er kjent fra dagens situasjon med seg inn i en analyse av fremtiden. Like fullt er det mange teknologioptimister som har bommet grovt når de har konstatert at alt skal være annerledes i fremtiden. Vi må være realistisk med tanke på våre begrensninger samtidig som vi forsøker å stille relevante spørsmål.

[15] Heuer, Richards J. Jr. & Pherson, Randolph H. (2008), "Structured analytical techniques for intelligence analysis", *CQ Press.*

[16] Se: Beadle, Alexander W. (2016), "Å forske på Forsvaret i fremtiden: muligheter, begrensninger og kognitive fallgruver", *FFI-rapport 16/01810 (Kjeller:FFI);* Hatlebrekke, Kjetil Anders (2019), "The problem of secret intelligence", *Edinburgh University Press.*

## 1.3 Rapportens struktur

Strukturen i rapporten følger logikken skissert i innledningen. Vi begynner i kapittel to med en diskusjon om ulike ikke-statlige aktører og egenskapene til disse gruppene. Siden mange av aktørene – inkludert kriminelle nettverk, terrororganisasjoner, opprørsgrupper, og proxy-aktører – har flere fellestrekk og sammenfallende interesser, konkluderer vi med at fellesbegrepet *ikke-statlige aktører* har mer analytisk verdi enn først antatt. Til slutt lanseres et analytisk rammeverk som anvendes senere i rapporten. I kapittel tre tar rapporten for seg ulike fremvoksende teknologier som kan være både tilgjengelig og relevante for ikke-statlige aktører.

Etter at rapporten har skissert hvilke aktører og teknologier som er mest relevante, kombineres disse i kapittel fire for å vurdere hvilke kapabiliteter som vil kunne vært aktuelle i et 10 års perspektiv og i et 30 års perspektiv. Det fokuseres på fem hovedkategorier: kommunikasjon, informasjonsinnhenting, mobilitet, effekt/våpen, og logistikk. Kapabilitetskategoriene settes inn i en fremtidig samfunnskontekst for å belyse potensielle sårbarheter eller mulige løsninger på samfunnssikkerhetsutfordringer. I kapitel fem peker rapporten på hvordan de forventede endringene vil påvirke fremtidige militære operasjoner. Kapitelet tar også for seg det fremtidige operasjonsmiljøet samt redegjør for noen utvalgte teknologiske og organisatoriske tiltak som kan bidra til at Forsvaret settes i bedre stand til å håndtere disse endringene. Avslutningsvis, i kapitel seks, oppsummeres rapportens viktigste funn og kommer med forslag til videre forskning.

# 2 Ikke-statlige aktører

Historisk sett har ikke-statlige aktører vært en sentral motstander i vestlige militære operasjoner og i flere situasjoner har de skapt store utfordringer for statene de var i konflikt med. Dette har vært tilfelle når ulike opprørsgrupper, med hjelp av asymmetriske taktikker, har bekjempet langt større og teknologisk overlegne statlige militære styrker. Det har også oppstått situasjoner hvor mektige kriminelle organisasjoner utgjør en så stor trussel at statlige militære styrker må settes inn. Det er ingen grunn til å tro at dette vil forandre seg. Uavhengig av den teknologiske og globale utviklingen forventes det derfor at voldelige ikke-statlige aktører vil forbli en potensiell motstander for statlige militære styrker. I tillegg vil den teknologiske utviklingen bidra til at disse aktørene i fremtiden vil kunne ha tilgang på andre type våpen, teknologi og kapabiliteter enn i dag. Ved første øyekast virker begrepet «ikke-statlig aktør» som et litt ullent og upresist paraplybegrep. Etter en mer omfattende vurdering kan det imidlertid se ut til å være en kategori med tilstrekkelig analytisk verdi.

## 2.1 Kategorier av ikke-statlige aktører

I denne rapporten vil analysen dreie seg om fire hovedkategorier ikke-statlige aktører som er motivert til å bruke vold for å oppnå sine mål og med høyest potensiell påvirkningskraft på militære operasjoner. De ulike kategoriene er: (i) kriminelle nettverk, (ii) terrororganisasjoner, (iii) opprørsgrupper, og (iv) proxy-aktører.[17] Definisjonsmessig er disse underkategoriene ikke helt distinkte, og i mange tilfeller kan en aktør plasseres i flere kategorier samtidig. I analysen har vi derfor valgt å legge vekt på å undersøke de samlede kapabilitetsmulighetene for ikke-statlige aktører, fremfor et forsøk på å identifisere kausale sammenheng mellom ulike aktørtyper og bestemte teknologiske løsninger. Det kan likevel være konstruktivt å se nærmere på noe av forskjellene som skiller disse kategoriene fra hverandre.

Ifølge både Europol og FN har teknologi i løpet av de siste 20 årene blitt en hjørnestein i kriminalitet, særlig gjennom bruk av internett.[18] *Organiserte kriminelle nettverk* benytter teknologi med ulik modenhet i sine aktiviteter. Tradisjonell organisert kriminalitet som samarbeider på en strukturert måte for å drive ulovlig aktivitet trenger ikke nødvendigvis å ha et stort innslag av teknologi. Andre grupper har derimot hatt et cyber element som en støttefunksjon i form av en markedsplass, en kommunikasjonsplattform, eller en måte å hvitvaske penger på. Slike aktører vil i større grad kunne ha behov for teknologi for å gjennomføre kriminell aktivitet.

[17] Det eksister andre ikke-statlige aktører med potensiell stor påvirkningskraft på fremtidige militære operasjoner – blant annet internasjonale selskaper som bidrar med logistikk eller datatjenester. Næringsinteresser kan skape nye muligheter ved å tilby produkter og tjenester som statlige aktører kan benytte i en forsvarspolitisk sammenheng. I fremtiden kan enkelte bedrifter sikre sine økonomiske interesser ved å undergrave militære operasjoner med bruk av teknologiske kapabiliteter som satellitter, cyberkapabiliteter eller ved påvirkningsoperasjoner som kombinerer store datasett og sosiale medier.

[18] Fedortov, Yury (2017), "In just two decades, technology has become a cornerstone of criminality", *United Nations office on drugs and crime*, 23. oktober 2017.

Mest avansert er organisert cyberkriminalitet som primært driver internettbasert aktivitet, stort sett ulike former for vinningskriminalitet. Cyberkriminelle har de senere år blitt mer sofistikerte, avanserte og har økt sitt fokus på forretningsbasert kriminalitet eller salg av kriminelle tjenester. Disse aktørene er i økende grad integrert med annen ulovlig aktivitet på internett.[19] Bruk av teknologiske løsninger for kriminelle aktører omfatter mer enn cyberdomenet, og inkluderer også additiv tilvirkning, bruk av undervannsbåter, og ubemannede systemer.[20]

*Kriminelle nettverk* har ikke nødvendigvis et stående behov for å direkte kunne påvirke en militær operasjon eller utøve vold. Likevel kan denne aktørgruppen utøve omfattende vold i konfrontasjon med myndighetene eller andre kriminelle organisasjoner, og har ofte blitt koblet til ulike opprørsgrupper eller terrororganisasjoner. Enkelte transnasjonale kriminelle organisasjoner besitter betydelige ressurser i form av økonomi, personell og tilgang på materiell. Disse aktørene kan på den måten bli en del av verdikjeden til de andre formene for ikke-statlige aktører ved at de kan selge høyteknologiske tjenester til terroraktører eller gjennomføre avanserte cyberangrep på vegne av opprørsgrupper eller som en proxy-aktør.

*Terrororganisasjoner* er opptatt av å true eller bruke vold mot sivile mål (individer eller eiendom) for å oppnå politiske, økonomiske eller ideologiske mål ved å spre frykt eller trusler.[21] Ifølge en velkjent analyse har «moderne» terrorisme forekommet i fire distinkte bølger: anarkister (1880–1914), frigjøringsbevegelser (1920–1960), marxister og nasjonalister (1970-1990), og religiøse fundamentalister (1990–nåtid).[22] Terrorgrupper har ikke nødvendigvis bred støtte blant befolkningen og må ofte operere i det skjulte for å bevare taktisk og operasjonell sikkerhet. Denne marginaliseringen kan gjøre det vanskelig for disse aktørene å skaffe seg tilstrekkelig ressurser eller politisk støtte for å oppnå sine mål. Videre kan det skilles mellom terrorister som aktører, og terrorisme som en taktikk benyttet av kriminelle nettverk, terrororganisasjoner og opprørsgrupper. Definisjonsmakten spiller en vesentlig politisk rolle dersom «terrorist»-merkelappen kan benyttes for å svekke legitimiteten til opprørsbevegelser. [23]

*Opprørsgrupper* er organiserte bevegelser med målsetting om å velte en regjering ved bruk av subversjon og væpnet konflikt. Ubalansen i maktforholdet mellom staten og opprørsgruppen gjør at motstandsbevegelser som regel tyr til asymmetriske krigføringstaktikker for å svekke staten. Dette kan inkludere en viss grad av terrorisme-lignende angrep, men det må være et politisk rasjonale bak voldsbruken.[24] Hovedmålet til en opprørsgruppe er å overta det politiske ansvaret og kontrollen innen et gitt geografisk område. I motsetning til terror-aktører er det derfor

[19] Se: Europol (2017), "Crime in the age of technology", *EDOC #924156*; Grabosky, Peter (2007), "The internet, technology, and organized crime", *Asian Criminology 2*, ss.145-161; Leukfeldt. E. Rutger, et.al (2019), "Criminal networks in a digitized world: on the nexus of borderless opportunities and local embeddedness", *Erasmus School of Law*.
[20] Fiegel, Brenda (2017), "Narco-drones: A new way to transport drugs", *Small Wars Journal* 5. juli 2017; Sutton, H.I. (2020), "Rare Electric Narco Submarine Seized in Colombia", *US Naval Institute News, 16. november.*
[21] NATO Glossary of terms AAP-06 (2019), s. 128.
[22] Rapoport, David C. (2001), "The fourth wave: September 11 in the history of terrorism", *Current history: 100 (650).* ss. 419-424.
[23] Johnston, Nicolas (2018), "Defining terrorism and insurgency: Beyond morality", *Small Wars Journal.*
[24] United States Army (2016), "Field manual FM 3-24 Counterinsurgency", *US Army.*

avgjørende at opprørsgrupper beholder en grad av anerkjennelse og legitimitet blant befolkningen, noe som et terrorangrep mot sivilbefolkningen vil kunne undergrave.[25] For en gruppe som den Islamske stat (IS) vil begrepene terrororganisasjon og opprørsgruppe begge ha relevans. Terrorhandlinger ble blandet sammen i Syria med mer tradisjonell manøverkrigføring og i noen områder også tilbud om nokså omfattende samfunnstjenester selv om kvaliteten og omfanget varierte. Ifølge den amerikanske opprørsbekjempelsesdoktrinen kan kriminelle nettverk potensielt utvikle seg til å bli en opprørsgruppe dersom det statlige rettsvesenet forstyrrer den kriminelle virksomheten.[26]

Et *proxy*-forhold oppstår når en statlig eller ikke-statlig gruppe i en konflikt får økonomisk eller militær støtte fra en velgjører eller sponsor motivert av sin egeninteresse i utfallet av konflikten. Den eksterne tredjeparten intervenerer aldri direkte i konflikten, men ønsker å beholde en indirekte kobling gjennom en proxy-aktør eller stedfortreder. Motivasjonen for dette kan være varierende og kan inkludere kostnadsbesparelser, plausibel fornektelse eller andre innenriks- eller utenrikspolitiske årsaker.[27] De øvrige andre aktør kategoriene kan i enkelte tilfeller benyttes som ikke-statlige proxy-aktører. Proxy-aktører er også i økende grad relevant i cyberdomenet.

I proxy begrepet vil det videre være relevant å inkludere *private militære firmaer* som blir hyret inn for å gjennomføre oppdrag på vegne av andre aktører. Dette kan omfatte militære støttefunksjoner, konsulenttjenester eller militære kampenheter.[28] Mange stater – inkludert Norge – bruker sivile aktører til diverse støttefunksjoner innenfor logistikk, men det er sponsorens bruk av private militære kampenheter i en konflikt som er relevant her. Russlands bruk av private selskaper som proxy-aktører i blant annet Ukraina, Syria og Libya er godt dokumentert.[29] Det ble også rapportert om bruk av leiesoldater i konflikten i Nagorno-Karabakh høsten 2020, og noen kilder antyder at statlige aktører har bidratt med både materiell og logistikkstøtte i form av dronepiloter.[30] Ifølge forsker Philip Bobbitt vil stater antagelig benytte proxy aktører i enda større grad i fremtiden: «fremfor å kjempe med store vernepliktige kampenheter, vil stater i økende grad utkjempe fremtidige kriger ved å ta i bruk mange partnerorganisasjoner» som private militære firmaer, bedrifter og ideelle organisasjoner.[31]

Gjennomgangen av de fire ulike ikke-statlige aktørene understreker de ulike fellestrekkene og egenskapene som forener disse grupperingene. Dette gjør at fellesbegrepet «voldelig ikke-statlig aktør» kan være vel så relevant fra et analytisk ståsted. Rapportens overordnede analyse sikter

[25] Kilcullen, David (2005), "Counterinsurgency", *Oxford University Press*; Johnston (2018).
[26] United States Army (2016), "Field manual FM 3-24 Counterinsurgency", *US Army.*
[27] Fox, Amos (2019), "Conflict and the need for a theory of proxy warfare", *Journal of strategic security vol 12:3,* ss. 44-71.
[28] Mumford, Andrew (2013), "Proxy warfare and the future of conflict", *RUSI Journal, April/May vol 158(2);* Svendsen, Jahn Arvid (2009), "Forsvaret og private militære firmaer", *Institutt for forsvarsstudier (Oslo).*
[29] Saghavan, Sudarsan (2020), "As military power shifts in Libya, Turkey and Russia control country's fate", *Washington Post,* 23. mai 2020; Østensen, Åse Gilje & Bukkvoll, Tor (2018),"Russian use of private military and security companies – the implications for European and Norwegian security", *FFI rapport 18/01300* (Kjeller:FFI).
[30] Alayboubi, Mohammed & Jentoft, Morten (2020), "De dreper for barna sine", *NRK Nyheter, 25. oktober 2020.*; Urcosta, Ridvan Bari (2020), "Drones in the Nagorno-Karabakh", *Small Wars Journal*, 23. oktober 2020.
[31] Wittes, Benjamin & Blum, Gabrielle (2015), "The future of violence", *Basic books, (New York).*

såpass langt inn i fremtiden at egenskapene til spesifikke grupper ikke blir like viktige som egenskapene som kjennetegner hele aktørkategorien. Med andre ord, en fellesbeskrivelse av «terrororganisasjoner» er mer vesentlig enn de spesifikke egenskapene til Al Qaeda, spesielt når de fleste terrorgrupper regnes å ha en levetid på godt under 10 år.[32] For denne analysen er heller ikke terrororganisasjoner like vesentlig som en analytisk enhet enn «ikke-statlig aktør». Den islamske stat (IS) eksemplifiserer utfordringen med å fokusere for snevert på en bestemt kategori i en fremtidsanalyse: den hadde opphav som en opprørs- og terrorgruppe i Irak; den ble videreutviklet til en «kvasistat» med egen hær, omfattende kriminell virksomhet, territorielt kontroll, og leverandør av samfunnstjenester; til slutt ble gruppen redusert til et nivå som ligner et terrornettverk.[33] Derfor vil «ikke-statlige aktører» være mest relevant for denne analysen og resten av rapporten.

## 2.2 Organisasjonslæring og innovasjonsevne

Voldelige ikke-statlige aktører organiserer seg vanligvis på en annen og mindre strukturert måte enn statlige aktører, selv om det finnes eksempler på godt organiserte opprørsbevegelser eller kriminelle virksomheter. Siden et av hovedskillene dreier seg om utenomrettslig bruk av vold, vil ikke-statlige aktører ofte ha høyere krav til hemmelighold og operasjonell sikkerhet. Dette skaper en del utfordringer, blant annet knyttet til hvordan de er organisert og finansiert, hvordan de lærer og overfører kunnskap seg imellom, hvordan de får tilgang til teknologi, og hvorvidt de har mulighet til testing og eksperimentering. Det er ingen tvil om at ikke-statlige aktører kan være innovative når det gjelder nye taktikker, men med unntak av narkotikakartellers bruk av ubåter og droner, har de fleste ikke-statlige aktørene ofte vist seg å være nokså konservative med å ta i bruk fremvoksende teknologi. Ifølge en beregning er nesten 90 prosent av terrorangrep utført mellom 1970 og 2015 blitt gjennomført med bruk av enten skytevåpen eller eksplosiver. Det samme gjelder også for de fleste opprørsgrupper.[34] Angrepene 11. september 2001 var innovativt på et taktisk nivå, men ingen ny teknologi ble benyttet.

Det krever fantasi og kreativitet å generere nye ideer, mens innovasjon kan forstås som prosessen der ideer omgjøres til handling. Noe forskning kan tyde på at organisasjonsstrukturen i terrororganisasjoner påvirker deres kreativitet. I likhet med andre typer organisasjoner kan for mye struktur kvele kreativitet, men for lite struktur forhindrer at nye ideer realiseres. Den desentraliserte strukturen til al-Qaeda etter september 2001 virket å hemme gruppens oppfinnsomhet i jakten på masseødeleggelsesvåpen. Noen forskere har konkludert med at «ressursene til store organisasjoner kan tilrettelegge for innovasjon, men det kan også føre til tap

[32] Dolnik, Adam *(*2007), "Understanding terrorist innovation: Technology, tactics and global trends", *Routledge, (London).*
[33] Cronin, Audrey Kurth (2015), "ISIS is not a terrorist group", *Foreign Affairs* (mars-april 2015).
[34] Cronin, Audrey Kurth (2020), "Power to the people: How open technological innovation is empowering tomorrow's terrorists", *Oxford University Press.*

av fokus, som igjen fører til dårlig planlegging».[35] Mye tyder på at struktur i en organisasjon er betydningsfull for innovasjonsevnen.

Dersom slike aktører faktisk skal ta i bruk og nyttiggjøre seg av ny teknologi, må de først lære om det og bestemme seg for å integrere, og potensielt endre, måten de opererer på. Prosedyrer som sørger for at kunnskap overføres og spres i en organisasjon kan være krevende, selv for moderne og velorganiserte bedrifter i fredstid. Individer kan akkumulere kunnskap gjennom selvstudie eller erfaring, men informasjonen kan fort gå tapt for organisasjonen idet vedkommende bytter jobb eller pensjonerer seg. Dersom organisasjonen skal beholde og bygge en institusjonell hukommelse må det eksistere en bevisst og strukturert prosess for dette. Kravene til innovasjon kan være enda vanskeligere. Den institusjonelle motstanden mot å prøve nye teknikker og teknologi utover de vanlige arbeidsmetodene er et velkjent fenomen. Organisasjoner og individer foretrekker ofte å utnytte eksisterende kunnskap fremfor å utforske ny kunnskap. I tillegg kan anskaffelse og overføring av ny kunnskap være mer krevende enn vedlikehold av eksisterende kunnskap. Det er behov for motivasjon og energi fra organisasjonens ledere for å få det til.[36]

For ikke-statlige aktører i aktive konfliktområder kan dette bli mye vanskeligere. Soloterrorister eller grupper som har tilgang til friområder eller statlig beskyttelse, har rom til å trene og eksperimentere, men dette blir mer krevende i konfliktsituasjoner. Vanlige prosedyrer, taktikk og våpensystem må ofte læres i løpet av kort tid under stressende forhold, og kunnskapsrike og erfarne krigere går tapt i strid. Organisasjonen er nødt til å sørge for egen overlevelse, slik at organisasjonslæring og innovasjon blir kraftig nedprioritert. Noen ganger blir aktørene av ulike årsaker tvunget til å innovere, eller det oppstår gunstige forhold som muliggjør nettopp læring og/eller innovasjon. Krig kan også være en pådriver for innovasjon. Gamle og nye taktikker eller våpen kan testes side om side for å sammenligne resultater. Som en forlengelse av dette virker det å være en sammenheng mellom intensiteten i asymmetrisk krigføring og motivasjonen til å innovere.[37]

I slike tilfeller forekommer læring gjerne gjennom en firetrinns prosess: anskaffelse, tolkning, distribusjon, og lagring. *Anskaffelse* av kunnskap foregår blant annet gjennom observasjon av andre aktører, prøving-og-feiling, eller sanking av informasjon fra ulike databaser som skriftlige dokumenter eller internettbaserte kilder. *Tolkning* av kunnskap er særdeles viktig siden dette må tilpasses organisasjonen og de faktiske forholdene. Hvorvidt kunnskap kan nyttiggjøres kan avhenge av gruppens analytiske evner, organisasjonens kultur og fleksibilitet. *Distribusjon* av kunnskap på tvers av organisasjonen gjør at alle kan dra nytte av nyvinninger og at hele organisasjonen lærer, fremfor kun noen få individer. *Lagring* av kunnskap henger tett sammen med distribusjon, siden «lagring» i en organisasjonssammenheng ofte vil foregå muntlig eller

[35] Gill, et.al (2003), "Malevolent creativity in terrorists organizations", *Journal of creative behavior vol. 47:2,* ss. 125-151, (2003).
[36] Cronin (2020).
[37] Dolnik (2007), s. 15.

skriftlig. Etter at kunnskap har blitt integrert i en organisasjons rutiner kan det regnes som internalisert.[38]

I sum er det krevende for en ikke-statlig aktør å være innovativ. Gruppemedlemmer som tilegner seg kunnskap om fremvoksende teknologi kan forsvinne gjennom krigshandlinger eller arrestasjon, og dermed forsvinner kunnskapen, og organisasjonens evne til læring faller bort. Viljen til testing og eksperimentering kan bli nedprioritert pga. pågående kamphandlinger og styrende operasjonsmønster. Dersom ikke-statlige aktører skal ta i bruk en ny kapabilitet eller taktikk som benytter ny teknologi, må tilstrekkelig kunnskap om dette spres gjennom organisasjonen. Selv om dette er på plass er det likevel ikke gitt at aktøren evner å nyttiggjøre seg av ny teknologi.

## 2.3 Teknologiadopsjon, taktikk og våpenteknologi

I tillegg til organisasjoners evne til å tilegne seg og beholde kunnskap, er det Brian Jackson beskriver som *teknologiadopsjon* svært vesentlig. Dette definerer han som prosessen der grupper lærer om og deretter anskaffer nyttig teknologi og teknikker. Begrepet omfatter videre måten den anskaffede teknologien integreres i operasjoner, og ikke minst hvordan man øver og eksperimenterer for å kunne bruke teknologien på en effektiv måte. Veien mot effektiv bruk av teknologiske nyvinninger kan være lang. Organisasjoner kan velge å forbedre eller videreutvikle eksisterende teknisk kunnskap, eller utvikle og oppdage nye teknologiske løsninger, der sistnevnte tilnærming er mest vesentlig med tanke på fremvoksende teknologi.

Hvorvidt en ikke-statlig aktør velger å satse på teknologisk innovasjon vil være utslagsgivende for hvilke kapabiliteter som kan anvendes. Beslutningen om å forsøke å skaffe seg ny våpenteknologi fremfor finpussing av eksisterende kapabiliteter kan delvis forklares ved faktorer som organisasjonskultur. Ifølge Jackson finnes det eksempler der grupper har fått «oppskriften» på en ny teknologi, men likevel ikke har maktet å anvende den.[39] Terrororganisasjoner har ofte en pragmatisk tilnærming og anser teknologi kun som middelet som skal oppnå en målsetning. For statlige aktører vil det derimot kunne være forbundet mye prestisje og verdi i selve innovasjonsprosessen. For disse aktørene blir utviklingen i seg selv et mål, mens de ikke-statlige aktørene i større grad benytter det som er mest egnet til å oppnå et ønsket resultat – uavhengig av om dette er med bruk av enkel eller avansert teknologi.[40]

Tilgang til militærteknologi vil variere blant de ulike ikke-statlige aktørene. En kombinasjon av ulike årsaker kan stå i veien for at disse aktørene får tilgang til avansert våpenteknologi. Noe forskning tyder på at det er mer sannsynlig at større organisasjoner med god økonomi, eksterne

[38] Gartenstein-Ross, et.al (2019), "Virtual plotters. Drones. Weaponized AI? Violent non-state actors as deadly early adopters", *Valens Global (Washington D.C)*; Jackson et.al. *(*2005), "Aptitude for destruction, Volume 1: Organized learning in terrorist groups and its implications for combating terrorism", *Rand Corporation (Santa Monica CA).*
[39] Jackson, et.al 2005, s. 9.
[40] Cornish, Paul (2010), "Technology, strategy and counterterrorism", *International Affairs 86:4, ss.* 875-888.

sponsorer, og selektiv medlemskap er mer tilbøyelig til taktisk og teknologisk innovasjon.[41] Ifølge en akademisk studie var det først når statlige aktører hadde interesse av å støtte aktivitetene til ikke-statlig aktører at slike grupper evnet å opparbeide seg nye kapabiliteter. Dette var enten fordi aktørene fikk økonomisk støtte som kunne benyttes til å kjøpe ny våpenteknologi, eller at aktørene fikk direkte overført våpen og utstyr fra en statlig sponsor.[42]

Noen fremvoksende teknologiområder som bioteknologi eller additiv tilvirkning har utbredte «gjør-det-selv» miljø bestående av amatørteknologer og forskere som utvikler avanserte produkter og løsninger ved å benytte informasjon og utstyr som er lett tilgjengelig. Slike «maker-space» grupper eller «prosumers» utnytter åpne kilder og komponenter som kan bestilles eller lages med additiv tilvirkning for å drive fremoverlent anvendt forskning.[43]

Uavhengig av hvilke våpenteknologi som anskaffes, så vil læringsprosessen for å benytte teknologien variere. Dette kan inkludere uorganiserte forsøk på «learning by doing» under operasjoner eller angrep, eller det kan være mer strukturert øvingsbasert læring, forskningsbaserte tilnærminger, eller gjennom observasjonsbasert læring fra lignende grupper. Aktive læringsmetoder kan være fordelaktig siden eksplisitt kunnskap om teknologi og prosedyrer kan tilegnes sammen med mer subtile teknikker.[44] Et estimat fra 2004 anslo at opp mot en tredjedel av de som har blitt drept av improviserte eksplosiver (IED) var selve bombefabrikantene. Forsøkslæring med dødelige våpenteknologi innebærer betydelig risiko og krever eksplisitt kunnskap i form av en oppskrift, men også subtile teknikker for å blande og konstruere eksplosivene på en trygg og effektiv måte.[45]

Forskjellige ikke-statlige aktører har ulike tilnærminger når det kommer til valg av våpen og taktikk. Noen foretrekker en stor portefølje og et bredt utvalg. Dette skal bidra til at de vil kunne være forberedt på å gjennomføre ulike typer angrep, dermed øker sannsynligheten for at de vil ha et egnet våpen klar for bruk når muligheten dukker opp. Andre grupper velger å spesialisere seg på bestemte våpentyper som kan være allsidige, slik at et våpen kan fungere for flere ulike oppdrag. Her er skytevåpen og eksplosiver mest vanlig – skytevåpen kan brukes til blant annet attentatforsøk og til gisseltaking. En tredje og mindre vanlig variant er grupper som bygger opp en selvstendig kapasitet for produksjon av spesialtilpassede våpen. Dette kan gi aktøren større grad av fleksibilitet ved at de selv kan forme våpenkarakteristikk basert på operasjonelle behov

[41] Dolnik (2007), s. 20.
[42] DeVore, Marc R. (2012), "Exploring the Iran-Hezbollah relationship: A case study of how state sponsorship affects terror groups decision-making", *Perspectives on terrorism vol. 6:4-5,* ss. 85-107.
[43] Tsanni Abdullahi (2020), "African scientists leverage open hardware", *Nature vol. 582*, 4. juni 2020.
[44] Da testing av det amerikanske missilforsvarssystemet intensiverte mot slutten av 1990-tallet opplevde programmet en rekke mislykkede prøveoppskytinger. En del av forklaringen viste seg å være feil i produksjonen av avskjæringsmissiler. Siden missilproduksjonen etter den kalde krigen stoppet opp på en ganske dramatisk måte, var det mange missilteknikere som hadde pensjonert seg. Dermed forsvant mye av den institusjonelle hukommelsen om de teknikkene og tilpasningene som var nødvendig i tillegg til de skriftlige manualene, som hadde gjort fabrikasjonen vellykket. Se blant annet Independent Working Group, "Missile Defense, the Space Relationship, & the Twenty-First Century" *(Cambridge, MA: Institute for Foreign Policy Analysis, 2009).*
[45] Jackson (2004), s. 16.

og ønskende utfall.[46] Noen terrorgrupper har blitt såpass glad i spesifikke våpen eller taktikker at det har blitt en del av gruppens identitet, da blir det vanskeligere å være innovativ og å ta i bruk ny teknologi.[47]

Å tilegne seg ny kunnskap om våpenteknologi er krevende og forbundet med risiko. Noen faktorer kan forhindre innovasjon hos ikke-statlige aktører. Innovasjon krever ekstra kapasitet og energi av en organisasjon – noe som ofte er en knapp ressurs blant aktører i konfliktområder som kjemper for sin overlevelse. I tillegg kan spesialisering føre til intern motstand mot innovasjon. Individer som har blitt eksperter har gjerne økt status innad i organisasjonen. Dette er noe de helst vil beholde. Nye metoder eller teknologiske løsninger trenger modningstid før det kan benyttes på en effektiv måte, og dette fører ofte til dårligere resultater i begynnelsen, sammenlignet med mer etablerte metoder.[48] Utilstrekkelig tilgang til treningsområder kan også hindre introduksjon av nye taktikker eller teknologi. Dette er særlig tilfelle for terrorgrupper som ikke har en vertsnasjon som beskytter dem. Ifølge FFI-forsker Truls Tønnessen er kontroll over territorium en vesentlig faktor som delvis forklarer hvorvidt en ikke-statlig aktør benytter seg av teknologiske nyvinninger som droner.[49]

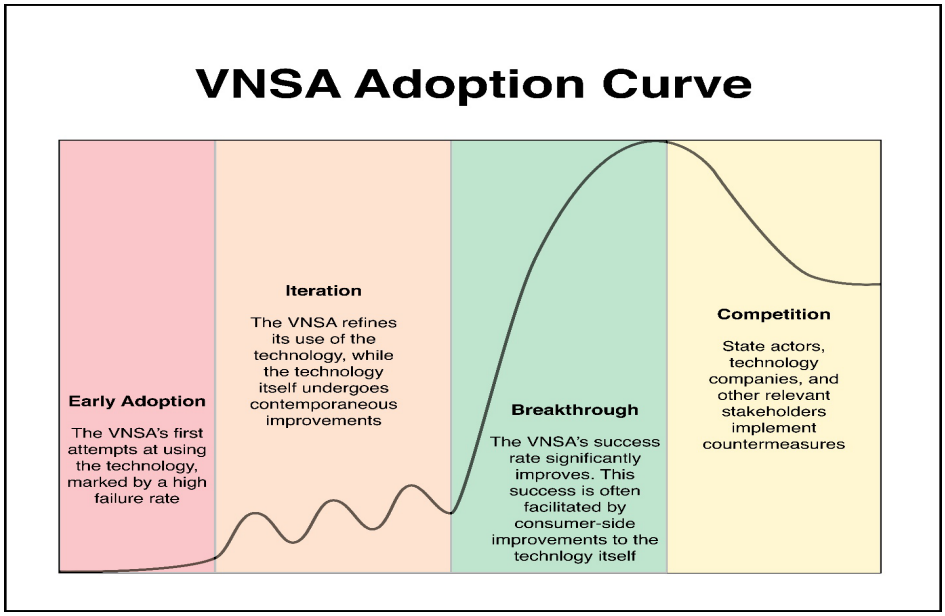
Videre kan selve karakteren og strukturen til en ikke-statlig aktør være et hinder for at kunnskap og innovasjon spres gjennom organisasjonen. Noen grupper – eksempelvis kriminelle nettverk eller terrororganisasjoner – kan ofte være nødt til å operere på en mer klandestin måte enn opprørsgrupper eller et privat militært selskap som fungerer som en proxy-aktør. Behovet for operasjonell sikkerhet og hemmelighold gjør at slike aktører organiserer seg for å forhindre omfattende konsekvenser dersom en del av organisasjonen blir infiltrert. Disse barrierene kan også begrense kunnskapsspredning og etablering av institusjonell hukommelse.

Teknologiadopsjonen til en ikke-statlig aktør kan utvikle seg i fire faser: *tidlig adopsjon*, *iterasjon*, *gjennombrudd* og *konkurranse*. I den første fasen vil ikke-statlige aktører oppleve mange mislykkede forsøk med den nye teknologien. Deretter vil bruk av teknologien forbedres gjennom en periode av *iterasjon* der organisasjonen lærer fra sine feil. I den tredje fasen vil aktøren få et *gjennombrudd* der teknologien begynner å fungere slik den var ment å gjøre og brukes hyppig. I den siste fasen vil andre aktører reagerer på suksessen ved å utvikle mottiltak som *konkurrerer* med og begrenser effektiviteten til teknologien.[50]

Selv om det er en konseptuell fremstilling er denne modellen likevel et nyttig analytisk verktøy. Noen aktører vil sannsynligvis klare å nesten umiddelbart tilpasse teknologiske nyvinninger på en effektiv måte og dermed hoppe over tidligere faser. Andre grupper vil aldri komme frem til «gjennombruddsfasen» i teknologibruk. Noen aktører vil muligens følge modellens utviklingskurve helt nøyaktig. Det gir oss et fint referansepunkt for å vurdere fremtidig utvikling

[46] Jackson, Brian A. & Frelinger, David R. (2008), "Rifling through the terrorist arsenal: Exploring groups, weapon choice and technology strategies", *Studies in conflict and terrorism Vol. 31*, ss. 583-604.
[47] Dolnik (2007), s. 17.
[48] Jackson (2004), s. 18-19.
[49] Tønnessen, Truls H. (2017), "Islamic state and technology – A literature review", *Perspectives on terrorism 11:6,* ss. 101-111.
[50] Gartenstein-Ross, et.al (2019), s. 8.

når en bestemt teknologi først brukes av en ikke-statlig aktør. Det kan anses som et «tidlig varsel» for det som kan komme senere.




*Figur 2.1 Innovasjonsmodell for voldelig ikke-statlige aktører. Gartenstein-Ross, Shear & Jones, (2019).*

Modellen er også en påminnelse om at kapabiliteter ofte blir møtt med mottiltak. Selv om en gruppe utvikler en kapabilitet ved bruk av fremvoksende teknologi, er det ikke gitt at teknologien vil forbli effektiv over tid. Like fullt er det en fare for at mottiltak kan være såpass kostbare og krevende i implementering at det i denne fasen svekker de operasjonelle evnene til statlige aktører. Et godt eksempel på dette er USA og NATOs erfaringer med veibomber. Relativt enkle bomber lagt ved og under veien i Afghanistan og Irak ble ekstremt kostbart for intervensjonsstyrkene med tanke på tap av personell og materiell. Tiltak for å oppdage eller ufarliggjøre bombene krevde ofte avansert teknologi og involverte kompliserte løsninger. Opprørerne viste seg å være svært kreative og innovative i form av å finne opp nye og enkle løsninger for hvert av de nye tiltakene som ble utviklet av amerikanske Joint Improvised Explosive Device Defeat Organization (JIEDDO).[51]

[51] Cronin (2020), s. 50-51.

## 2.4 Ikke-statlige aktører, samfunnsteknologi og fremtiden

Det forventes at ikke-statlige aktører vil fortsette å bruke et bredt utvalg kapabiliteter i sine aktiviteter også i fremtiden og at aktørene vil være opptatt av nye kapabiliteter som kan realiseres ved bruk av teknologiske nyvinninger. Det er i tillegg viktig å huske at det generelle teknologinivået i samfunnet også videreutvikles over tid. Innen 2050 vil teknologi som i dag virker usannsynlig være dagligdags. Veibomber i Afghanistan ble ofte detonert ved bruk av billige mobiltelefoner, noe som var lett tilgjengelig selv i en krigssone og som ble sett på som en lav-teknologisk løsning i 2005. Ser man derimot på mobilteknologi med et 1985-perspektiv ville dette virket nokså avansert for en ikke-statlig aktør. Når vi ser langt inn i fremtiden, er det derfor viktig å huske at samfunnet også utvikler seg. I 2050 vil derfor ikke-statlige aktører kunne anvende helt annen teknologi enn det vi ser for oss i dag.

I større grad enn statlig militærmakt er valgmulighetene til voldelige ikke-statlige aktører begrenset av teknologiene som befinner seg i samfunnet. Dette er særlig tilfelle for de ikke-statlige aktørene som pragmatisk velger midler, våpen og taktikk basert på tilgjengelige ressurser og teknologi. For disse aktørene er ikke teknologisk eller taktisk innovasjon en prioritet, og de benytter verktøy som allerede finnes rundt dem. Når slike grupper anser sivile som legitime mål blir teknologien som preger samfunnet relevant av en annen grunn. Teknologi påvirker hvilke angrepsmuligheter som finnes – enten det er kollektivtransport, flykapring, eller et mer avansert angrep i det digitale rom.

For å vurdere ikke-statlige aktørers fremtidige kapabiliteter må vi forøke å forestille oss hvordan teknologi benyttes i og preger samfunnet i fremtiden, som i det følgende vil omtales med begrepet *samfunnsteknologi*. Fremtidsanalyse er en krevende oppgave hvor det må tas hensyn til mange komplekse og usikre geopolitiske, demografiske, og økonomiske variabler. Selv en begrenset analyse av teknologiens rolle i fremtidens samfunn hviler på et stort antall ukjente faktorer. Denne studien har derfor valgt å fokusere på fem områder som historisk har blitt særlig påvirket av fremvoksende teknologi og teknologiske nyvinninger. Disse områdene forventes derfor å få stor innvirkning i menneskers dagligliv også i fremtiden, både på individnivå og i samfunnet som helhet. Dimensjonene er: (i) *mellommenneskelig kommunikasjon, (ii) informasjon og nyheter, (iii) helse og bioteknologi, (iv) handel og produksjon* og (v) *transport.*

Den første dimensjonen er *mellommenneskelig kommunikasjon*. Dette omfatter utviklingen fra skriftlige brev til bruk av telegraf, muntlig kommunikasjon gjennom fasttelefon, mobiltelefon og satellittforbindelser, og til slutt elektronisk kommunikasjon gjennom ulik internett-teknologi som epost, VoIP eller videochat. I løpet av det siste århundret har kommunikasjon blitt raskere, rimeligere, og mer lettvint. Infrastrukturen er blitt mer rettet mot det elektromagnetiske spekteret med mobiltelefoni og satellittkommunikasjon. Utviklingen har hatt omfattende konsekvenser for individer og familier, samtidig som industrien og næringslivet har dratt nytte av gode kommunikasjonsforbindelser som del av økonomisk globalisering.

Den andre dimensjonen, som er beslektet med den første, er teknologisk utvikling knyttet til spredning og innhenting av *informasjon og nyheter*. I likhet med mellommenneskelig

kommunikasjon har mediebransjen utviklet seg fra aviser og radiosendinger til å inkludere nyhetssendinger på fjernsyn og til slutt via digitale eller internett-baserte informasjonskilder. Evolusjonen innen nyheter og informasjonsflyt har økt hastigheten på nyhetsbildet med nesten umiddelbar mediedekning av hendelser i sanntid. Den lave terskelen for tilgang til internettbaserte nyhetsplattformer har i tillegg svekket den dominerende posisjonen store medieselskap har i å filtrere og formidle nyheter til befolkningen.

Den tredje dimensjonen er de teknologiske nyvinningene innen *helse og bioteknologi* man har sett det siste århundret. Den vestlige befolkningens forventede levealder økte betraktelig i perioden 1900-2000. Dette var godt hjulpet av trygge blodoverføringsteknikker, bedre kirurgiske prosedyrer, og utvikling av medisin som antibiotika og nye vaksiner. Årsakene til bedre levekår er sammensatt, men teknologi har utvilsomt spilt en viktig rolle.[52] Gjennom forskningsbasert sykdomsbekjempelse har utviklingen blant annet muliggjort gjennomføring av store infrastrukturprosjekter som Panamakanalen (1881-1914).[53] I tillegg til en generell økning av samfunnshelsen har teknologisk fremgang innen de helsefaglige dimensjonene positivt påvirket overlevelsesstatistikken i krigssoner.

Den fjerde dimensjonen omfatter trender innen *handel og produksjon* av varer. Dette er en utvikling som er svært fremtredende i samfunnet. Industrialisering har gjennomgått flere perioder med teknologisk fremvekst. Sentralt i disse industrielle revolusjonene var energikilder som damp eller elektrisitet, samt fremveksten av mekaniserte og etter hvert automatiserte produksjonsmetoder. Tilgangen på masseproduserte varer påvirket handelsmønsteret til befolkningen som i økende grad kunne finne et stort utvalg av varer i kataloger, deretter i større kjøpesentre og etter hvert via internett.

Den femte og siste dimensjonen omhandler *transportsektoren.* Deler av denne sektoren har gjennomgått store forandringer i løpet av det siste århundret, mens andre områder har forblitt uforandret. Introduksjonen av motoriserte kjøretøy og fly har økt samfunnets mobilitet og betraktelig redusert tiden det tar å reise. Frakt av gods har vært mest kosteffektiv til sjøs og effektiviteten økte enda mer med fremvekst av containerskip og shipping etter andre verdenskrig. Rimelige transportløsninger for gods har vært en viktig faktor i globaliseringen og har muliggjort produksjon av varer og tjenester i land med billigere arbeidskraft.

Teknologisk fremgang innen hvert av disse områdene vil være betydningsfullt for samfunnet i fremtiden. Flere dimensjoner ville gitt et bedre og mer nyansert fremtidsbilde, samtidig som det øker analysens kompleksitet og dermed risiko for feiltolkning. Disse fem dimensjonene vurderes derimot som tilstrekkelig for å danne et grunnleggende bilde av det fremtidige samfunnet.

[52] Roser, Max, Ortiz-Ospina, Esteban & Ritchie, Hannah (2019), "Life expectancy: Our world in data", University of Oxford.
[53] McCullough, David (1978), "The path between the seas", *Simon & Schuster (New York).*

## 2.5 Fire fremtidige aktørtyper

Mange kloke mennesker har begått grove prediksjonsfeil, til og med når det dreier seg om spesifikk teknologi og korte tidshorisonter. Nøyaktige prediksjoner er krevende når det gjelder utviklingstrender innenfor et teknologiområde eller hvorvidt en teknologisk nyvinning vil bli adoptert og tatt i bruk i samfunnet.[54] Fallhøyden og feilmarginene er derfor store, men vi er likevel nødt til å skissere et grovkornet bilde for å vurdere de fremtidige kapabilitetene som ikke-statlige aktører vil kunne benytte i samfunnet mot 2050. Det forventes at trusselen fra ikke-statlige aktører vil fortsette å eksistere i fremtiden, uavhengig av den teknologiske utviklingen. Fokuset i denne rapporten er derimot å vurdere i hvilken grad fremvoksende teknologi vil kunne påvirke denne trusselen. For denne vurderingen legges to hovedfaktorer til grunn: (i) *teknologiens tilgjengelighet* for ikke-statlige aktører og (ii) *aktørens vilje til å adoptere ny teknologi*.

Noen teknologiområder kan være vanskelig for ikke-statlige aktører å få tilgang til, enten grunnet egenskapene til selve teknologien eller med bakgrunn i samfunnsmessige forhold. Videre så vil enkelte teknologier være fysisk vanskelig å få tak i, enten på grunn av regelverk (som med spaltbare materialer), innebygde sikkerhetstiltak som forhindrer uautorisert bruk (som «geofencing» for droner), eller fysiske egenskaper ved teknologien (som biologiske stoffer som krever spesialtilpassede oppbevaring). Annen teknologi kan være en økonomisk utfordring for ikke-statlige aktører. Videre så eksisterer det teknologi som krever spesialisert kompetanse for at den kan anvendes på en effektiv måte, eller at teknologien må tilpasses for å anvendes på en måte som er nyttig for aktøren. Disse utfordringene gjør at mange ikke-statlige aktører lar vær å ta i bruk ny teknologi.[55]

Flere fremvoksende teknologier vil likevel være flerbruksteknologi, og dermed vil de kunne være lovlig tilgjengelig for ikke-statlige aktører. Dersom aktøren allikevel forsøker å gjennomføre et angrep eller igangsette en operasjon, er det deres innovasjonsevne og risikovillighet som blir avgjørende. Videre vil aktørens evne til opplæring innad i organisasjonen og tilpasning av planlagte angrepsmønstre og metoder også være viktig.

[54] Szczerba, Robert J. (2015), "15 worst tech predictions of all time", *Forbes*, 5. januar 2015.
[55] En mer omfattende diskusjon av disse utfordringer finnes i kapittel tre sammen med en gjennomgang av spesifikke fremvoksende teknologiområder.

| | | Aktørens adopsjonsvilje | |
|---|---|---|---|
| | | **Lav** | **Høy** |
| **Teknologi tilgjengelig i samfunnet** | **Høy** | **Umotivert aktør**<br>*Nye avanserte teknologier kan være tilgjengelige, men benyttes ikke av aktørene* | **Hypertrussel-aktør**<br>*Nye avanserte teknologier er tilgjengelig og aktøren er motivert til å utvikle og anvende dem* |
| | **Lav** | **Status quo-aktør**<br>*Den teknologiske tilgangen er lavere enn forventet og aktørinnovasjon forblir lav* | **Innovativ aktør**<br>*Tilgang til teknologi er lav, men innovative aktører finner nye løsninger med fremvoksende teknologi* |

*Figur 2.2 Fire kategorier av aktører basert på tilgang til teknologi i samfunnet og aktørenes vilje til å adoptere teknologien for bruk i egne operasjoner.*

Ved å bruke graden av tilgang til teknologi på den ene aksen og aktørenes grad av teknologiadopsjon på den andre, kan vi lage en tabell som skisserer fire alternative ikke-statlige framtidstrusler. Dersom aktørene i hovedsak ikke er interessert i innovasjon og den teknologiske adopsjonsviljen er lav, så vil en *status quo-aktør* hverken ha interesse av, eller ha tilgang til teknologisk avanserte løsninger. På den andre siden kan en *umotivert aktør* ha tilgang til relevant teknologi men mangle tilstrekkelig interesse for å benytte teknologien. Noen terrorgrupper og kriminelle nettverk havner i en av disse to kategoriene.

Dersom aktørens interesse for innovasjon og teknologiadopsjon er høy, kan langt farligere situasjoner utvikle seg. Når innovative aktører, med begrenset tilgang til avansert teknologi ønsker å gjennomføre et angrep må de i større grad gjøre seg avhengig av kreative løsninger ved å benytte seg av den dagligdagse teknologien som finnes i fremtiden. Dette omtales i denne rapporten som en *innovative aktør* eksemplifisert av blant annet opprørsgrupper og terrorister i Afghanistan, Irak eller Syria. Noen kriminelle nettverk har også vist seg å være svært innovativ i sin bruk av fremvoksende teknologi. Ved å bruke teknologi som var lettere tilgjengelig i samfunnet, utviklet slike grupper kreative løsninger som en asymmetrisk respons mot en teknologisk overlegen statlig motstander. Den siste trussel-kategorien har de mest omfattende implikasjonene: en høyt motivert ikke-statlige aktør med tilgang til avansert teknologi utover det som vanligvis finnes i samfunnet og som grenser mot statlige kapabiliteter. Disse aktørene, omtalt i denne rapporten som *hypertrussel-aktør,* og vil sannsynligvis være en form for proxy-aktør som den paramilitære aktøren Wagner Group eller en svært innovativ opprørsgruppe.

Innenfor disse fire aktørkategoriene finner man de fleste ikke-statlige aktører som kan bli en potensiell motstander i fremtidige militære operasjoner. Avhengig av hvordan teknologien utvikler seg og integreres i samfunnet, vil aktørene komme til å benytte teknologi på ulike

måter. Hvorvidt de anvendes hviler i stor grad på teknologiens tilgjengelighet og innovasjonsviljen til den enkelte aktør.

# 3 Fremvoksende teknologi

Teknologi kan defineres som praktisk anvendt vitenskap eller kunnskap for å løse problemer eller utvikling av nye redskaper, som maskiner, materiell, teknikker eller prosesser. I denne rapportens sammenheng er teknologi simpelthen middelet som skal sørge for at ikke-statlige aktører når sine mål. Det forventes at teknologiområdene som diskuteres i dette kapittelet i fremtiden vil få høy relevans for forsvars- og sikkerhetssektoren. Flere av teknologiene har både sivile og militære bruksområder, men fokuset er primært rettet mot teknologi som kan skape nye muligheter for voldelige ikke-statlige aktører og dermed en konsekvens for militære operasjoner.

Flere av områdene er *fremvoksende,* som innebærer at teknologien er i begynnelsen av sin livssyklus og under utvikling. Tidspunktet teknologien vil kunne få den forespeilede effekten er derimot forbundet med usikkerhet. Flere av de fremvoksende teknologiene vil forårsake *inkrementelle* endringer, mens andre teknologier er *banebrytende* og har potensialet til å skape *disruptive* effekter. Dette er teknologier som vil kunne endre helt hvordan man løser en konkret oppgave. [56] I en forsvars- og sikkerhetssammenheng vil dette være teknologi som ikke passer inn i dagens praksis og prosess. Denne typen teknologi har potensiale til drastisk å endre måten krig og konflikt utkjempes på.

I mange tilfeller vil flere teknologier kunne skape *konvergens.* Dette vil si at ulik teknologi samvirker for på den måten å løse nye, ikke tidligere planlagte oppgaver. Siden ikke-statlige aktører ofte befinner seg i et asymmetrisk maktforhold med ønske om å gjennomføre operasjoner eller angrep mot statlige aktører, vil disruptiv bruk av banebrytende teknologi kunne være svært attraktivt sett fra den ikke-statlige aktørens ståsted. Ved slik disruptiv bruk av teknologi vil det nødvendigvis ikke foreligge opplagte måter å benytte den på, hverken i angrep eller forsvar. Ny teknologi har således potensialet til å utnytte tidligere uidentifiserte sårbarheter.

## 3.1 Tilgang på ny teknologi

Til tross for at det forventes at ny teknologi kan ha stor effekt i en forsvars- og sikkerhetssammenheng, så er ikke alt av fremvoksende forsvarsteknologi nødvendigvis like relevant for ikke-statlige aktører. For å avgjøre hvilke teknologiområder som i størst grad vil bli tatt i bruk av denne typen aktør de kommende 10-30 år, diskuterer rapporten noen spesifikke faktorer: (i) *tilgjengelighet*, (ii) *investeringskrav*, (iii) *kompetansebehov* og (iv) *tilpasningsbehov*.

Disse fire faktorene relateres direkte til aktørkategoriene omtalt i rapportens kapitel 2.5. Faktorene gjenspeiler aspekter som på ulikt vis påvirker hvorvidt en konkret teknologi forventes å være tilgjengelig for ikke-statlige aktører. De første to beskriver egenskaper som har med anskaffelsen av teknologi å gjøre. De resterende faktorene sier noe om teknologiens krav til aktørenes

[56] Bower, Joseph & Christensen, Clayton (1995), "Disruptive technologies; catching the wave", *Harvard Business Review*, January-February 1995.

innovasjonsevne og hvorvidt ikke-statlige aktører evner å adoptere og integrere teknologien i operasjonene sine.

Teknologi som benyttes av ikke-statlige aktører er i stor grad preget av hva som er *tilgjengelig* på et gitt tidspunkt. Tilgang på den mest attraktive og høyteknologiske forsvarsteknologien er som regel begrenset gjennom et strengt eksportregime og sikkerhetsmekanismer som skal forhindre at uvedkommende får tak i den. Allikevel finnes det flere tilfeller hvor ikke-statlige aktører har tilegnet seg teknologisk avanserte løsninger og benyttet dette til gjennomføring av terrorangrep eller militære operasjoner. Hvordan aktøren har forbigått sikkerhetsmekanismene og fått tilgang kan variere, men ofte er dette forbundet med korrupsjon, kriminalitet og utnyttelse av kaoset som oppstår i en konfliktsituasjon. Samtidig kan aktørene få tilgang på teknologi på lovlige måter, blant annet gjennom overføringer fra en statlig aktør til en proxy.

Noen av de viktigste komponentene i ny militærteknologi er ikke bare hardware og fysiske plattformer, men også selve programvaren (software). For eksempel er nye kampfly, missiler, fartøy eller luftvernsensorer avhengig av mange linjer med kode for mye av funksjonaliteten sin. Skalerbar programvare kan være relevant for ikke-statlige aktører for å øke ytelsen til mindre avanserte plattformer. I stridshandlingene i Nagorno-Karabakh høsten 2020, utstyrte Aserbajdsjan et utdatert fly med fjernstyring for å bruke det som narremiddel for armensk luftvern.[57] Når det avgjørende elementet i et forsvarssystem er programvaren like mye som det fysiske systemet, har dette betydning for spredningen av militærteknologi siden programvare kan overføres lettere enn fysiske kampsystemer.

Videre vil såkalt flerbruksteknologi som selges i det sivile markedet, og som lett kan tilpasses militære formål være lett tilgjengelig for ikke-statlige aktører. Enkelte husholdningsartikler og kjemiske stoffer kan benyttes til å produsere hjemmelaget sprengstoff eller kjemiske våpen som kan benyttes i terrorangrep. Når teknologien er ny og det potensielle bruksområdet ukjent så vil innovative aktører kunne skaffe seg tilgang på teknologi før eventuelle spredningsbegrensninger og reguleringer iverksettes. At leverandørkjeder og marked er globale har gjort at ikke-statlige aktører vil kunne skaffe seg teknologiske nyvinninger på en helt annen måte i dag enn hva som var tilfelle for 10-20 år siden.

Hvorvidt aktøren forsøker å tilegne seg en spesifikk teknologi vil samtidig avgjøres av *kompetansebehovet* som kreves for effektiv bruk av teknologien. Historisk sett er det mange ikke-statlige aktører som har belaget seg på løsninger og teknologi som har krevd lite forkunnskap og lav kompetanse for å bli tatt i bruk. Angrep og operasjoner kan ofte være spontane og intensjonsdrevet, noe som gjør at det ikke er tid til nøye planlegging eller kompetansebygging. Blant annet vil aktivitetene til kriminelle nettverk eller terrororganisasjoner ofte være under kontinuerlig overvåking av relevante påtalemyndigheter som forsøker å forebygge og eliminere eventuell angrepsforsøk. Dette kan være med på å gi denne type aktør begrenset mulighet til å finne ut hvordan ny og fremvoksende teknologi kan tas i bruk.

[57] Roblin, Sebastien (2020), "What Open Source Evidence Tells Us About The Nagorno-Karabakh War", *Forbes*, 23. oktober 2020.

I tillegg til teknologi med kinetisk effekt, har ikke-statlige aktører benyttet teknologi som krever liten kompetanse for å sikre eller forbedre egen kommunikasjon, få økt situasjonsoversikt, eller som bidrar til å spre aktørens ønskede budskap og narrativ. Med den forventede utviklingen innen automatisert styring og kontroll, er det mange avanserte plattformer og systemer som i fremtiden vil kunne benyttes uten mye teknisk forkunnskap. Der hvor integrasjonen mellom maskin og menneske er lett, brukervennligheten er høy, eller der kompetanse kan bygges raskt, vil terskelen for bruk være lavere. Samtidig vil det eksistere løsninger og teknologi som vil kreve såpass spesialisert kompetanse at en ikke-statlig aktør vil ha begrensede muligheter til å tilegne seg nødvendig kompetanse på egenhånd.

For flere fremvoksende og nye teknologier vil kostnaden eller *investeringskravet* være en begrensende faktor for hva en ikke-statlig aktør vil komme til å benytte i et fremtidig angrep eller operasjon. Prislappen på avansert militærteknologi utfordrer i enkelte tilfeller kjøpekraften til selv mindre stater. For ikke-statlige aktører som ikke har en sponsor eller tilgang på store økonomisk midler, vil derfor enkelte teknologier forbli utilgjengelig. Når investeringskostnaden er høy bør det derfor forventes at ikke-statlige aktører ser etter andre løsninger og alternativ som kan gi tilsvarende ønsket effekt.

At teknologi kan tas i bruk uten store *tilpasningsbehov* gjør at den ikke-statlige aktøren kan oppnå sine mål med å bruke den aktuelle teknologien uten tid- og ressurskrevende tilrettelegning. Når moden teknologi kan kjøpes og benyttes, såkalt hyllevare, vil dette være en viktig faktor aktøren vil ta høyde for. Når teknologien derimot må bli spesialtilpasset og integrert med eksisterende løsninger og plattformer, vil det kunne være mindre fristende for aktøren å ta dette i bruk. Om aktørene er villige til å tilpasse teknologien vil videre avhenge av dens intensjoner. Terrororganisasjoners fremste intensjon vil ofte være å gjennomføre angrep og operasjoner som trekker oppmerksomhet, er dramatiske, oppsiktsvekkende og som sprer frykt. Derfor kan teknologi som ikke genererer åpenbare eller umiddelbare effekter tenkes å være mindre interessante. Angrep som benytter teknologi hvor attribusjon er usikker vil også kunne komme til å bli nedprioritert av aktører med intensjon om å generere oppmerksomhet og frykt.

En ikke-statlig aktørs vurdering av disse faktorene vil være med på å avgjøre hvorvidt en spesifikk teknologi blir tatt i bruk. Aktørens organisering, antall medlemmer, ressurser, ideologi, intensjoner og mål påvirker videre faktorenes betydning. Samtidig vil dette raskt kunne endres. Tilgang på teknologi, kompetanse og muligheten til å benytte spesialtilpassede løsninger kan fort endres dersom en terrororganisasjon oppnår territoriell kontroll og beveger seg i retning av å bli en opprørsgruppe. Den samme gruppen kan i tillegg få tilgang på statlig støtte og dermed fungere som en proxy. Dette vil igjen ha en positiv virkning på aktørens evne til å rekruttere nytt personell, samle ressurser, og øke den generelle tilgangen de har på teknologi og avanserte kapabiliteter. På den andre siden vil en ikke-statlig aktør kunne redusere mulighetene sine til å tilegne seg ny teknologi ved eventuell tilspisning av en konflikt, ved strengere eksportreguleringer eller ved bortfall av territoriell kontroll.

## 3.2 Relevante teknologiområder

For å gjøre en kvalitativ sortering av hvilke fremvoksende teknologiområder det vil være aktuelt at ikke-statlig aktører tilegner seg i løpet av de kommende 10-30 år, tar rapporten utgangspunkt i tilgjengelig fremtidslitteratur om teknologi. Noen viktige kilder i dette arbeidet har blant annet vært FFI-rapporten *«Emerging technology trends for defence and security»* og NATO-STO rapporten *«Science and Technology Trends 2020-2040: Exploring the S&T Edge».*[58] Områdene som løftes frem i disse rapportene forventes å kunne forårsake disruptive effekter på militære operasjoner i fremtiden. Blant disse teknologiområdene finner man paraplybegrepet *digital teknologi* som inkluderer stordata og analytiske verktøy, cyberteknologi, «edge»-prosessering, og Tingenes internett (IoT). Videre peker disse rapportene på ubemannede systemer, kunstig intelligens, autonomi, additiv tilvirkning, romteknologi, bioteknologi, og teknologi som omfatter bruken av det elektromagnetiske spekteret.

Noen teknologiområder tas ikke med i rapportens beskrivelser. Dette med bakgrunn i at noen områder anses som utilgjengelig for ikke-statlige aktører. Blant disse er hypersoniske farkoster – missiler, kryssermissiler eller såkalte «glide vehicles» – som kan oppnå hastighet langt over fem ganger lydens hastighet. I motsetning til ballistiske missiler, som oppnår lignende hastighet gjennom atmosfæren mot målet, vil hypersoniske farkoster kunne manøvrere underveis og vanskeliggjøre deteksjon og avskjæring med luftvern. Kostnaden til systemene og våpenets potensielt strategiske funksjon antyder at kun stater med avanserte forsknings- og utviklingsevner vil kunne utvikle og benytte slike våpen.

Teknologi for energiproduksjon og –lagring vil i det vesentlig bidra indirekte til ikke-statlige aktørers bruk av andre teknologier. Utvikling av batterier og brenselceller vil f.eks. muliggjøre enklere og mer effektiv bruk av autonome systemer og generelt øke bruken av denne teknologien i samfunnet. Slike systemer for lagring og utvinning av elektrisk energi vil også være sterkt knyttet til en forventet økning i utnyttelsen av fornybare energikilder, som sol- og vindkraft. Andre, mer esoteriske former for energiproduksjon, som nedskalerte fisjonsreaktorer eller fusjonsreaktorer (varm eller kald)[59], kan anses å bli for utfordrende å håndtere for ikke-statlige aktører eller være for umodne til å vurderes her («wildcards»). Samlet vil derfor teknologier for energiproduksjon og –lagring ikke vurderes selvstendig i denne analysen, men integreres i behandlingen av andre teknologiområder.

Kvanteteknologi er det siste område som i det vesentligste uteblir fra analysen. Teknologiutvikling basert på kunnskap om kvantefysikk – som beskriver materien og vekselvirkninger på atomært og subatomært nivå – vil på sikt føre til flere oppsiktsvekkende framskritt. Dette inkluderer GNSS-uavhengig måling av posisjon og tid for navigasjonsformål med ultrapresise atomur og sensorer for registrering av akselerasjon og tyngde- og magnetfelt. «Kvantekameraer» og «-radarer» vil kunne bruke sammenfiltret belysning for avbildning og

[58] Andås (2020); Reding, D.F. & Eaton, J (2020), "Science and technology trends 2020-2040: Exploring the S&T Edge", *NATO Science and Technology Organization,* Brussels.
[59] Andås (2020), s. 31-32; Allison, Peter Ray, (2020), "The UK's quest for affordable fusion by 2040", *BBC Future,* 15. desember 2020.

deteksjon av objekter med flere størrelsesordener og høyere oppløsning enn dagens standarder. Kvantedatamaskiner vil kunne prosessere svært komplekse beregninger utenfor rekkevidden til konvensjonelle supercomputere med konsekvenser bl.a. for dagens asymmetriske krypteringsmetoder. Konsekvensene av kvanteteknologiene vil dermed på sikt være både oppsiktsvekkende og omfattende, men tidshorisonten og omfanget er inntil videre svært usikre. En løsning for sikre kommunikasjonsnettverk basert på optiske systemer for distribusjon av kvantenøkler (QKD) vil kunne være en anvendelse av kvanteteknologi med et mer umiddelbart potensiale for ikke-statlige aktører, spesielt for dem med en «sponsor». Ellers vil tilgjengeligheten til flere av disse nyvinningene i første omgang trolig være begrenset, til dels også på grunn av kostnadsaspektet.

De resterende teknologiene som diskuteres i dette kapitelet ansees å være de mest tilgjengelige områdene for bruk av ikke-statlige aktører i fremtiden. Analysen fokuserer utelukkende på ny og fremvoksende teknologi. Modne og kjente teknologier som håndvåpen, eksplosiver og kjøretøy holdes derfor utenfor vurderingen. Slik teknologi vil fortsatt eksistere og vil ha stor effekt i lang tid fremover. Videre vil ny teknologi kunne påvirke moden teknologi på en måte som gjør at bruken av den reduseres. Sannsynligheten og terskelen for at de fremvoksende teknologiene tas i bruk av ikke-statlige aktører vil henge tett sammen med teknologienes modenhetsnivå og løpende utvikling. På generelt grunnlag vil bruk av en spesifikk teknologi øke med graden av dens modenhet. Dette innebærer at tidshorisonten blir viktig når man vurderer hvorvidt teknologien kan forventes å bli tatt i bruk av ikke-statlige aktører. Teknologiene som diskuteres vurderes som realistisk for bruk av ikke-statlige aktører i løpet av de kommende 10-30 år.

### 3.2.1 Digital teknologi og tingenes internett

At samfunnet i dag er avhengig av digital teknologi for å fungere er en veldokumentert sannhet. Digital teknologi forstås i denne sammenheng som en samlekategori bestående av teknologier som *edge prosessering, cyberteknologi, dataanalyse og tingenes internett (IoT).* Utviklingen har gjort at også fysiske *ting* nå kan kobles sammen i nettverk og aksesseres via digitale og internettbaserte løsninger. Resultatet er at det produseres stadig større datamengder. At data og informasjon kan behandles i distribuerte nettverk eller i skyløsninger er både kostnads- og tidsbesparende. Denne digitale revolusjonen har allerede hatt store konsekvenser og ringvirkninger for hvordan konflikter og moderne forsvar og sikkerhet forstås.

For ikke-statlige aktører har man sett at digital teknologi har blitt benyttet til å organisere egen aktivitet, for å tilrettelegge kommunikasjon mellom medlemmer, til gjennomføring av kommando og kontroll, gjennomføring av logiske angrep, eller som en viktig arena for rekruttering og propaganda. På denne måten fungerer internett som en viktig ressurs for ikke-statlig aktører. De får tilgang til pålitelige tjenester med høy brukervennlighet, samt de kan opprettholde en viss form for anonymitet og kommunisere på en sikker måte.[60] Internett ble en uvurderlig ressurs for terrororganisasjonen IS i 2014, både for å kunne radikalisere og rekrutterer nye medlemmer, men

[60] Singer, Peter W. (2012), "The cyber terror bogeyman", *Brookings*, 1. november 2012.

også som et verktøy for planlegging og gjennomføring av angrep. Terrororganisasjoner og opprørsgrupper kommuniserte seg imellom via ulike krypterte meldingstjenester og applikasjoner som har forhindret myndigheter i å detektere og avverge terrorplot.[61] IS utnyttet i tillegg mulighetsrommet internett ga dem som en propagandakanal. Dette gjorde at nye potensielle medlemmer strømmet til, men også at teknologien fungerte som et middel for å spre frykt og sinne blant organisasjonens fiender.[62]

I tillegg til at digitale verktøy og internett gir ikke-statlige aktører mulighet til kommunikasjon, kompetansebygging og planlegging, så har utviklingen også ledet til at antallet potensielle digitale angrepsmål har økt. Veksten i bruk av digital teknologi gjør derfor at nettverksangrep og cyberoperasjoner i dag har svært stor effekt. Å utnytte digitale sårbarheter for å spre skadevare på målets IKT-system med den hensikt å overvåke, kompromittere, sabotere, utpresse eller ødelegge, er derfor å anse som et betydelig samfunnsproblem. De ikke-statlige aktørene bak denne type aktivitet vil kunne være kriminelle nettverk, individer og grupper med statlige støtte.[63]

I løpet av de kommende 10-30 år forventes det at digital teknologi som cyber og IoT vil øke i relevans og viktighet. Digitale tvillinger – eksakte digitale representasjoner av systemer og nettverk – kan i fremtiden brukes for testing og simuleringer av angrep og operasjoner.[64] Nye tekniske løsninger og materialer for produksjon av databrikker – blant annet karbonnanorør, grafén og neuromorfiske databrikker –forventes å øke den mulige prosesseringskraften og dermed utbredelsen av digital teknologi og objekter tilknyttet internett.[65] I samspill med utviklingen innen kunstig intelligens vil utvidet virkelighet (AR) og virtuell virkelighet (VR) videreutvikles slik at disse til sammen blir et vanlig grensesnitt mellom mennesker og den digitale sfæren. Parallelt vil fremveksten av eksempelvis haptiske drakter eller hologramteknologi også bidra til forbedring av dette grensesnittet. Fremstilling og bearbeiding av digital data kan i fremtiden se svært annerledes ut enn dagens skjermbaserte løsninger.[66]

### 3.2.2 Kunstig intelligens (AI)

En konsekvens av pågående digital transformasjon er en enorm vekst i data og informasjon. Mye av dataen som genereres vil derimot bare kunne nyttiggjøres dersom den kan analyseres og bearbeides tilstrekkelig. Dette er ofte en krevende prosess som involverer mange maskiner, høy prosesseringskraft og menneskelige analytikere. Kunstig intelligens (AI) er en teknologi som drar nytte av data og muliggjør analyse.

[61] Graham, Robert (2016), "How terrorists use encryption", *CTC Sentinal vol 9:6 (juni 2016), ss. 20-25.*
[62] Lakomy, Miron (2017), "Cracks in the online "Caliphate": How the Islamic state is losing ground in the battle for cyberspace", *Perspectives on terrorism Vol. 11:3.*
[63] PST (2021), "Nasjonal trusselvurdering 2021", *Politiets sikkerhetstjeneste.*
[64] Marr, Bernard (2020), "How Are Digital Twins Used In Practice: 5 Real-World Examples Beyond Manufacturing", *Forbes*, 28. august 2020.
[65] European Commission (2019), "100 radical innovation breakthroughs for the future", *Directorate General for Research and Innovation.*
[66] European Commission (2019) s. 27-61.

AI forstås som et dataprograms evne til å gjennomføre menneskelignende kognitive funksjoner, deriblant å kunne forstå og reagere på sine omgivelser.[67] En spesifikk retning innen AI hvor det de siste 20 år er gjort store fremskritt, er maskinlæring. Med maskinlæring kan systemene trenes opp til å lære og gjenkjenne mønstre og «riktige svar». En maskinlæringsmetode som er hyppig omtalt er bruk av såkalte *nevrale nettverk.* Dette er et elektronisk nettverk modellert etter menneskets hjerne som består av lag med nevroner. Disse nevronene «trenes» opp til å gjenkjenne mønstre i data. Et nettverk med mange lag kalles gjerne et «dypt» nettverk, og omtales som «dyp læring». Teknikken har vært kjent lenge, men utviklingen har skutt fart de siste par år på grunn av teknologisk utvikling som har muliggjort bedre prosesseringskraft, økt tilgang til store datasett, og datanettverktilgang som AI er avhengig av.[68]

Mye av styrken i AI ligger i at den kan lære på egenhånd, og at den med tid og tilgang til data vil kunne bli bedre og mer effektiv. Utviklingen innen AI algoritmer har forårsaket en kraftig reduksjon i tiden det tar å trene nye datasett.[69] Likevel kan AI oppleves som nokså snevert fordi suksess i ett område ikke nødvendigvis er overførbart til et annet.[70] I dette ser vi litt av paradokset til AI: teknologien er overlegen mennesker innenfor spesifikke oppgaver som krever stor analyse- og prosesseringskraft, men i andre oppgaver som mennesker klarer intuitivt, er AI «skjør» og langt under menneskers kognitive evner.

I cybersfæren har AI til en viss grad allerede blitt benyttet av ikke-statlige aktører, både defensivt og offensivt. Cyberhendelser som benytter AI til å koordinere skadevare og botnet dataangrep har blitt oppdaget av virksomheter som blant annet Nokia og Instagram.[71] Utholdenheten til AI systemer, kombinert med deres evne til læring og tilpasning, gjør at digitale angrep kan skje kontinuerlig med økt kompleksitet, og uten at et menneske styrer angrepet. Andre kriminelle bruksområder hvor AI har blitt benyttet er gjennom såkalte «deep fake» bilderedigering hvor aktøren imiterer eller påtar seg en annen persons identitet, og på den måten svindler eller manipulerer målet sitt. Denne type AI teknologi er også blitt benyttet for å narre ansiktsgjenkjennelsesutstyr.[72]

I de senere år har utviklingen innen AI har foregått i en voldsom fart. Det er forventet at utviklingen innen maskinlæring vil fortsette og at teknologien får et stadig utvidet bruksområde. Nye teknikker for å trene AI uten store datasett utvikles blant annet ved bruk teknikkene «reinforcement learning», og «generative adversarial networks» (eller GAN) som benytter to separate nevrale nettverk som trenes i tandem og utnytter forskjellene i treningsdata slik at

[67] Stanford University (2016), "Artificial Intelligence and life in 2030: One hundred year study on artificial intelligence", *Stanford, Stanford University.*
[68] Lewis-Kraus, Gideon (2016), "The great AI awakening", *New York Times Magazine*, 14. desember 2014; Ilachinski, Andrew (2017), "AI, Robots, and Swarms: Issues, Questions, and Recommended Studies", *Alexandria VA: CAN,* 2017.
[69] Standford University (2019), "The 2019 AI Index report", *Stanford Center for Human-centered Intelligence.*
[70] ibid.
[71] Kaloudi, Nektaria & Li, Jingyue (2020), "The AI-based cyber threat landscape: A survey", *ACM Computing Surveys 53.1.*
[72] Caldwell, et.al (2020), "AI-enabled future crime", *Crime Science Vol 9:14.*

nettverkene lærer raskere.[73] Når AI gjennom dataanalyse og mønstergjenkjennelse kan øke en maskins situasjonsforståelse, er handlinger og beslutningsevnen til maskinene ansett å være neste steg. Da er det viktig med metoder som øker forståelse og innsikt i hvordan nevrale nettverk finner frem til svarene sine. Annen forskning satser på utvikling av *artificial general intelligence* – dette innebærer å gi maskiner evnen til å vurdere omgivelsene sine og koble sammen situasjonsforståelse med resonneringsevne på en måte som ligner menneskelig «sunn fornuft».[74] Til tross for fremgangen innen dyplæringsteknikker er det lett å overvurdere det fremtidige bruksområde for AI og hvorvidt teknologien etter hvert kan sammenlignes med menneskelig intelligens.

Selv om noen AI eksperter er skeptiske til at nevrale nettverk kan «vite» ting på lik linje med et menneske, er det mange bruksområder for teknologien – særlig innen militærteknologi – som ikke krever et høyt kognitivt nivå. Den fremtidige utviklingskurven til AI er likevel uklar. De store gjennombruddene som har funnet sted skjedde da velkjente teknikker endelig fikk tilgang på tilstrekkelig dataprosesseringskraft og store datasett. Det har tidligere vært lange perioder der utviklingen stagnerte. Derfor er flere eksperter usikre på om vi er på randen av en AI-revolusjon eller egentlig ved slutten av en slik epoke.[75]

### 3.2.3 Ubemannende og autonome systemer

Bruk av maskiner og system som erstatning for menneskelig arbeidskraft har eksistert i lang tid. Å kunne skape fysisk avstand mellom maskin og operatør ved bruk av ubemannede system er i dag svært utbredt innen blant annet industriell robotikk, romteknologi og forsvarssektoren. Både fjernstyrte og delvis autonome systemer kan brukes i alle domener til målsøking, overvåking, og situasjoner der det er langt mer forsvarlig å risikere en maskin fremfor eget personell. Enkelte av de ubemannende systemene er plattformer som bærer våpenlast og kan returnere til start etter at lasten er levert, mens andre system som kryssermissiler eller enkelte flyvende droner treffer målet sitt og destrueres.

I dag er de fleste slike systemer fjernstyrte eller delvis automatiserte – dette innebærer at man kan forhåndsprogrammere flybanen til systemet og eventuelt hvordan det skal reagere dersom de mister link til operatøren eller møter uforutsette hindringer. Trenden peker mot en økende grad av autonomi. Ifølge en FFI rapport kan autonomi forstås *som «et systems evne til å tolke sine omgivelser, planlegge, ta beslutninger og handle slik at det kan utføre oppgavene sine».*[76] Autonomi kan kategoriseres i flere nivåer av menneskelig innblanding: fjernstyrte systemer der mennesker har direkte kontroll; fjernopererte systemer som kan bevege seg selvstendig fra punkt A til punkt B men som krever at mennesker bidra når problemer oppstår; fjernovervåkede systemer som kan operere mer eller mindre selvstendig men som må ha mennesker som passer på

[73] National Security Commission on AI (2019), «Interim report», *NSCAI (November 2019).*
[74] Berruti, et.al (2020), "An executive primer on artificial general intelligence", *McKinsey,* 29. pril 2020.
[75] John Horgan (2020), "Will Artificial Intelligence Ever Live Up to Its Hype?", *Scientific American, 4. desember 2020*; Richbourg, Richard (2018), "It's either a panda or a gibbon: AI winters and the limits of deep learning", *War on the Rocks*, 10 mai 2018.
[76] Bruvoll, Solveig et al. (2019), *"*Den autonome framtid*", FFI-Viten 19/00906 (Kjeller:FFI).*

at systemet opererer som den skal; og helt autonome systemer som kan gjennomføre oppdrag uten menneskelig innblanding.

Bruken av kommersielt tilgjengelige fjernstyrte droner som del av en militær operasjon har i løpet av de siste 5-10 år vært en vedvarende trussel fra ikke-statlige aktører. Dette henger delvis sammen med at flere kommersielle virksomheter nå tilbyr svært avanserte systemer, men også at den teknologiske utviklingen har muliggjort at systemene evner å fly lengre og kan bære tyngre og ulik last som f.eks. våpen, sprengstoff, kamera og andre typer sensorer. Terrororganisasjonen IS benyttet seg flittig av droneteknologi i perioden 2014-2018 og opprettet på et tidspunkt et eget droneprogram for å utvikle nye måter teknologien kunne benyttes på i terrorangrep og militære operasjoner.[77]

I 2018 gjennomførte en ikke-statlig aktør et angrep mot en russisk-drevet base i Syria med hjelp av en primitiv sverm bestående av 13 bevæpnede GPS-styrte droner.[78] Ubemannede systemer har også blitt tatt i bruk av kriminelle grupper. I 2017 brukte en kriminell gruppe droner for å plage agentene av det amerikanske etterforskningsbyrået FBI mens de overvåket gruppens aktivitet. Aktøren benyttet dronene til egen overvåking av agentene og lyktes med å forstyrre FBIs operasjon ved å fly mange droner over hodene til agentene samtidig.[79]

I løpet av de kommende 10-30 år forventes det at denne teknologien vil bli videreutviklet og enda mer utbredt. Fremtidig utvikling av programvaren, batterikapasiteten og designet til disse systemene vil muliggjøre større og mer effektive dronesvermer med reell autonomi og «intelligent» koordinering, oppførsel og målfatning. Økt prosesseringskraft i mindre enheter gjennom «edge»-prosessering vil bidra til å gjøre beslutningssystemene skalerbare, slik at enheter kan koordinere bevegelsene sine og operere samlet mot et felles mål. På denne måten kan en sverm med små enheter oppnå stor effekt til tross for begrenset lastekapasitet. Nøkkelen til suksess med autonome system ligger i programvaren og kontrollsystemet fremfor selve dronen, som lett vil kunne produseres gjennom additiv tilvirkning eller andre mer tradisjonelle metoder.

### 3.2.4 Additiv tilvirkning

Additiv tilvirkning (også kjent som 3D-printing eller additive manufacturing (AM)) er et fellesbegrep for en gruppe produksjonsteknikker der et objekt lages ved å påføre byggemateriale lagvis på en veldig presis måte. Prosessen med å lage et produkt starter med at det lages en digital tredimensjonal modell av objektet man ønsker, deretter oversettes dette til todimensjonale mønstre som skrives ut lag for lag. Siden produksjonsmetoden først ble kommersialisert på slutten av 1980-tallet har additiv tilvirkning utviklet seg fra en nisjeteknikk til å være en viktig teknologi i den globale produksjonskjeden. Additiv tilvirkning brukes særlig når individuelt tilpassede

[77] For en gjennomgang, se Tønnessen (2017).
[78] Trevithick, Joseph (2018), "Russia Offers New Details About Syrian Mass Drone Attack, Now Implies Ukrainian Connection", *The Drive*, 11. januar 2018.
[79] Tucker, Patrick (2018), "A Criminal Gang Used a Drone Swarm To Obstruct an FBI Hostage Raid", *DefenseOne*, 3. mai 2018.

objekter eller deler må produseres, fordi dette kan gjøres på en lettvint måte uten at utstyr eller verktøy må skiftes ut. Det er mulig å lage svært komplekse objekter med slike teknikker som erstatter flere deler som før måtte settes sammen med blant annet sveising eller liming. Dette sparer tid, materialer og ekstra verktøy, og kan i flere tilfeller effektiviserer hele produksjonsprosessen. Noen produksjonsmetoder tillater at elektronikk som ledninger eller antenner legges inn mellom de ulike lagene slik at det blir en integrert del av objektets struktur.[80]

Det finnes allerede noen få eksempler hvor ikke-statlige aktører benytter additive tilvirkningsteknikker. Et av de første forsøkene var en 9mm pistol kalt «Liberator», der alle delene unntatt tennstempelet kunne lages med en 3D-skriver. Siden den gang har digitale filer for mange våpentyper havnet på internett. Med tilgang til en skriver som kan produsere objekter av metall kan det lages mer avansert våpen.[81] Additiv tilvirkning muliggjør også ulovlige modifikasjoner av eksisterende materiell, selv med enkle plastbaserte printere.[82]

Kriminelle miljø har eksperimentert med metoder for additiv tilvirkning for å produsere alt fra nøkler og håndjern til deler av minibankkortskimmere.[83] Det nødvendige utstyret kan gjøres nokså flyttbart, som kan være fordelaktig for aktører med skiftende territoriell kontroll. Et kontainerbasert verksted basert på additiv tilvirkning har blitt testet i felt både av den amerikanske hæren og Forsvaret. En slik løsning vil kunne gi ikke-statlige aktører en begrenset evne til produksjon av kritiske komponenter, med redusert risiko for å bli sporet, og gjør dem mindre avhengig av robuste forsyningslinjer.[84]

Innen 2050 forventes det at additiv tilvirkning vil være en integrert del av den globale produksjonskjeden og at relevant utstyr vil være tilgjengelig selv i områder med begrenset fremkommelighet.[85] Utviklingen går i retning av at teknikker basert på additiv tilvirkning i fremtiden vil kunne produsere større og/eller mer avanserte objekter med økt effektivitet. Litt avhengig av hvilken teknikk som benyttes, vil en printer kunne produsere egne deler for å lage en ny 3D-skriver. Dette vil gjøre det lettere å øke produksjonsevnen samtidig som produktene som lages ikke kan identifiseres eller spores.[86]

Bruk av utvidet virkelighet (AR/VR) i designprosessen kan benyttes for å foreta endringer underveis. Kombinasjonen av utvidet tilgang til digitale filer, AI-støtte og AR-briller kan utgjøre

[80] Grimstvedt, Eirik Skjelbreid, et. al (2015), "LINE EW-UAS: an experimental unmanned system for coastal surveillance using ESM technology", *FFI-Rapport 15/02442 (Kjeller:FFI)*.
[81] Fey, Marco (2017), "3D printing and international security: PRIF report no. 144", *Frankfurt: Peace Research Institute Frankfurt.*
[82] Greenberg, Andy (2020), "The FBI Says 'Boogaloo' Extremists Bought 3D-Printed Machine Gun Parts", *Wired*, 4. november 2020
[83] O'Neal, Bridgett (2014), "Authorities Bust European Crime Network Taking Advantage of 3D Printing Technology for Credit Card Fraud", *3Dprint.com*, 6. oktober 2014
[84] Flathagen, Joakim et.al (2016), "Additiv produksjon av prototyper og reservedeler i felt", *FFI-rapport 16/01008 (Kjeller:FFI).*
[85] Freund, Caroline, Mulabdic, Alen & Ruta Michele (2019), "Is 3D Printing a Threat to Global Trade? The Trade Effects You Didn't Hear About", *Policy research working paper 9024*, *World Bank Group*.
[86] Hummel, Stephen & Burpo, F. John (2020), "Small groups, big weapons: The nexus of emerging technologies and weapons of mass destruction", *West Point: United States Military Academy*.

en verdifull støttefunksjon for individer uten fagkunnskap som ønsker å produsere avanserte produkter eller våpen. Utbredelsen av digitale oppskrifter kan føre til at enkelte ikke-statlige aktører vil forsøke å manipulere disse filene med den hensikt å kompromittere eller ødelegge en produksjonsprosess.

Når additiv tilvirkningsteknologi blir mer utbredt, vil tilgangen til maskiner og råmaterialer som metallpulver være mindre problematisk. Det forventes at flere maskiner til hjemmebruk blir tilgjengelige, noe som vil redusere behov for dybdekunnskap om ulike produksjonsteknikker.[87] Bruken av additiv tilvirkning innen bioteknologi forventes også å øke. Allerede i dag er det mulig å produsere menneskelig vev ved å bruke «bioblekk» laget av celler og annet organisk materiale. Indre organer og kroppsdeler har mikrostrukturer med egenskaper som er utfordrende å gjenskape med «bio-printing», men det er enighet blant eksperter om at dette vil kunne løses innen et par tiår.[88]

### 3.2.5 Rombasert overvåking

Romsegmentet, primært satellitter og ulike sensorsystemer, har i lengre tid vært sentralt for kapasiteter relatert til overvåking, kommunikasjon, navigasjon og dataoverføring og romteknologi spiller derfor en sentral rolle i militære operasjoner. Satellitter kommer i flere størrelser og kan veie alt fra flere tonn helt ned til noen få kilograms nanosatellitter, avhengig av tiltenkt funksjonalitet. De kan operere enkeltvis, eller i konstellasjoner av flere satellitter, noe som utvider deres potensielle bruksområde og betydning. Satellittene opererer i ulik avstander fra jorden og vil avhengig av dette kunne levere ulike tjenester. Evnen til å skyte opp satellitter krever betydelig ressurser og kunnskap, men å benytte seg av mulighetene teknologien gir er mer overkommelig.

At stater og samfunnet i dag er avhengig av rombaserte tjenester, gjør denne infrastrukturen til et potensielt mål for ikke-statlige aktører. Mye av teknologien som er benyttet i eldre satellitter er sårbar, siden disse ble tatt i bruk før trusselen fra cyberdomenet slo inn for fullt. Dette kan utnyttes av ondsinnete aktører. I 2007 hacket den Sri-Lanka-baserte opprørsgruppen *Tamiltigrene* kommunikasjonssystemene til det amerikanske firmaet *Intelsat* og aksesserte en satellitt de benyttet til å sende sin egen TV-sending. Sendingen pågikk opp mot 1 time før man greide å kutte den, dette ga aktøren god tid til å spre sitt budskap. En lignende hendelse skjedde noen år tidligere i 2002 da aktøren *Falun Gong* tok over TV-sendingen til en TV-kanal ved at de hacket en satellitt eid av den kinesiske staten.[89]

Satellittmarkedet, og romsegmentet generelt, har over det siste drøye tiåret blitt revitalisert og transformert via oppblomstringen av ny teknologi for småsatellitter (mikro- og nano-) og betydelige kommersielle investeringer, hovedsakelig med fokus på kommunikasjons- og jordobservasjonsløsninger. Transformasjonen har blitt hjulpet frem av miniatyrisering av

[87] Johnston, Trevor, Smith, Troy D. & Irwin, J. Luke, (2018), "Additive Manufacturing in 2040", *RAND Corporation, Santa Monica.*
[88] Dahal,Sahas (2016), "Printing the future: 3D bioprinters and their uses", *Medium*, 29. februar 2016
[89] Jill Stuart, (2015), "Comment: Satellite industry must invest in cyber security", *Financial Times*, 10. april 2015.

nyttelast, nye produksjonsmetoder, «plug-and-play»-teknologi og stadig mer kostnadseffektive satellittoppskytinger. SpaceX har blitt den viktigste kommersielle leverandøren av oppskytingskapasitet i dette «new space». De aktuelle teknologitrendene mot økt automatisering, samarbeidende nettverk og konstellasjoner, kunstig intelligens for beslutningsstøtte og distribuert beregningskapasitet, vil utvilsomt også i fremtiden øke effektiviteten ytterligere og fremme nye bruksområder for satellitteknologi. Med videre utvikling av nye tilpassede sensorsystemer vil bruken av rommet og romrelaterte tjenester øke, ikke minst drevet av kommersielle interesser basert på utnyttelse av data generert via disse sensorene.[90]

Med betydelig kostnadsreduksjon, ikke minst basert på kommersialiseringen av oppskytingstjenester, kan selv små stater, private selskaper eller til og med ressurssterke privatpersoner få tilgang til data med kvalitet og oppløsning som tidligere var forbeholdt stormakter. Dette vil drastisk utvide hvem som har tilgang på tjenestene denne teknologien tilbyr og dermed vil rommet raskt kunne bli et overbelastet og omstridt miljø. I 2020 fantes det mer en 2000 satellitter i verdensrommet. I løpet av de kommende 10-20 år forventes det å bli skutt opp 1100 satellitter per år[91] med en forventet pris ned mot 10 USD pr. kg nyttelast, en reduksjon på to størrelsesordener fra dagens kostnad[92].

Satellittbasert overvåking med bruk av sensorer for det visuelle eller infrarøde spekteret (EO/IR) har lenge levert bilder av utvalgte områder på bakken. Detaljeringsnivået og kvaliteten på bildene avgjør hvor effektiv denne type overvåking er. En økning av antallet tilgjengelige satellitter innebærer at det på et tidspunkt vil være mulig med en kontinuerlig global satellittbasert overvåking, ettersom det til enhver tid vil være mulig å navigere en satellitt inn i riktig område slik at man får dekket dette. Slik informasjon vil dermed også kunne bli tilgjengelig for ikke-statlige aktører. [93]

Videre vil mindre satellitter kunne utstyres med en rekke sensorer og kommunikasjonssystemer. I tillegg til EO/IR-sensorer, er passive radarer mulig. Aktive radarer kan også implementeres, men med redusert driftssyklus for å spare strøm. Det kan derfor forventes at svært avanserte småsatellitter kan anskaffes og skreddersys for å støtte avanserte nyttelaster for applikasjoner som[94]: sikker telekommunikasjon, AIS[95]-skipssporing og maritim redning (M-SAR[96]), ADS-B[97] flysporing for neste generasjons lufttransportsystem (NGATS[98]), konstellasjon for forbedret satellittnavigasjon i nordområdene (GNSS[99]-basert), jordobservasjon (visuell, radar og hyper-

[90] D.F. Reding og J. Eaton, (2020), s. 17.
[91] D.F. Reding og J. Eaton, (2020), s. 81.
[92] Jones, Harry W. (2018), "The Recent Large Reduction in Space Launch Cost", *48th International Conference on Environmental Systems*, 8.-12. juli 2018, Albuquerque, New Mexico.
[93] Planet Labs Inc. (2021), "Using Space to Help Life on Earth", *planet.com*, 5. mai 2021;
Bold, Michael (2018), "Very Small Satellites, Very Big Deal", *Army AL&T Magazine,* January - March 2018.
[94] Andås (2020), ss. 47-48.
[95] Automatic Identification System.
[96] Maritime Search-And-Rescue.
[97] Automatic Dependent Surveillance/Broadcast.
[98] Next Generation Air Transportation System.
[99] Global Navigation Satellite System.

spektral), kommunikasjonsetterretning og elektronisk etterretning (COMINT/ELINT/ MASINT[100]). Disse tjenestene vil dermed være tilgjengelig mange ulike interessenter i fremtiden.

### 3.2.6 Bioteknologi og soldatforbedringssystem

Raskere og kraftigere dataprosessering samt nye verktøy som kunstig intelligens, har gitt oss banebrytende kunnskap og oppsiktsvekkende nyvinninger innen biovitenskap. Gjennom teknologiske løsninger kan den menneskelige kroppen måles, overvåkes, forbedres og forandres på måter som tidligere har vært svært vanskelig eller helt umulig. Dette området er en del av fagfeltet bioteknologi. Fagfeltet deles gjerne i fire hovedkategorier: (i) *bioinformatikk og biosensorer*; (ii) *menneskelig forbedring*; (iii) *biomedisinske teknologier*; og (iv) *syntetisk biologi*.[101]

Bioinformatikk dreier seg om lagring, innhenting, organisering og analyse av biologiske data, og særlig menneskelig aktivitet. Biosensorer måler biologiske eller biokjemiske prosesser og forandrer dette til et elektrisk signal. Det kan blant annet brukes i små sensorer integrert i klesplagg for å oppdage og varsle kontakt med farlige radioaktive eller kjemiske substanser i luften, overvåke pasienter som behandles for sykdom, eller bruk av midlertidige tatoveringer som måler fysiologisk eller kognitiv stress. Menneskelig forbedring kan dreie seg om bedre ernæring eller farmaka som øker den fysiske eller kognitive ytelsen, forbedret menneske-maskin integrasjon eller eksoskjeletter. Biomedisinske teknologier ligger tett opp mot bioinformatikk, biosensorer og teknologi for menneskelig forbedring, og bruker disse fagfeltene til å diagnostisere, overvåke og behandle mennesker med sykdom og skader.

Syntetisk biologi – definert som design og utbygging av modifiserte eller nye biologiske systemer – er et felt som i skrivende stund opplever en særdeles bemerkelsesverdig fremgang. En viktig del av dette er knyttet til utviklingen av genredigeringsmetoden *Clustered Regularly Interspaced Short Palindromic Repeats-assosiert med proteinet-9* (CRISPR-Cas9) og videreutviklinger av denne. Dette er metoder som fungerer som en «gensaks». Kartlegging av DNA åpner for syntetisk produksjon av organismer med egenskaper som ikke forekommer naturlig. Potensialet for å kunne avvikle arvelig sykdom eller utvikle robuste plantearter er stort, men det er også risikoen for at teknologien misbrukes. Kombinasjonen av økende kunnskap om funksjonen til gensekvenser, nye redigeringsverktøy som CRISPR-Cas9, og nye laboratorieteknikker har bidratt til å utvide tilgangen til både eksplisitt og stilltiende kunnskap om syntetisk biologi, samt bioteknologi generelt, til et bredere sett av aktører. Kostnadene ved anvendelsen av denne teknologien – både programvaren og laboratorieutstyret – er blitt tilstrekkelige lave slik at «gjør-det-selv»-miljøer og såkalte «bio-hackers» nå eksperimentere med å modifisere DNA.[102]

[100] Communication Intelligence / Electronic Intelligence / Measurement and Signature Intelligence.
[101] Oppsummering og kategorisering baseres på Reding, D.F. & Eaton, J (2020), ss. 94-103.
[102] Frinking, Erik et al. (2016), "The increasing threat of biological weapons*", Hague Center for Strategic Studies*; Sandeep, Ravindran (2020), "How DIY technologies are democratizing science", *Nature 587, ss. 509-511 (2020)*; iGEM Foundation (2020), *International Genetically Engineered Machine.*

Genmodifiseringsteknologi kan brukes for å øke menneskers fysiske eller kognitive ytelser, men kan også brukes i utviklingen av biologiske våpen. Ved å anvende kommersielt tilgjengelig genetisk materiale klarte en kanadisk forsker å lage en utryddet variant av koppeviruset i løpet av seks måneder.[103] Prosedyren kan brukes til å finne nye vaksiner for koppeviruset men demonstrerer også hvordan farlige sykdommer kan genmodifiseres for å brukes som våpen gjennom «bio-hacking».[104]

Ikke-statlige aktører har sjelden benyttet biologiske våpen og de fleste tilfellene har både vært primitive og mislykkede. Det mest omfattende vellykkete angrepet – men også det minst farlige – fant sted da en religiøs kult spredde salmonellabakterier blant spisestedene i en liten landsby i Oregon i USA, med over 750 tilfeller av matforgiftning, men ingen dødsfall. Den japanske religiøse gruppen Aum Shinrikyo er kjent som aktøren bak et alvorlig giftgassangrep med sarin som drepte 13 mennesker og skadet nesten 6000. Den samme aktøren forsøkte ved flere anledninger i 1995 å spre ebola og miltbrann, uten at dette ledet til dødsfall. I 2001 sendte en amerikaner miltbrannbakterier gjennom posten til flere embetsmenn og personer i diverse media, og forårsaket fem dødsfall, mens over 20 ble skadet.[105]

Konvergensprosesser vil akselerere fremveksten av bioteknologifeltet. Nye trender innen nanoteknologi, robotikk, informasjonsteknologi, og kunstig intelligens påvirker allerede bioteknologiens utvikling, slik som automatiserte laboratorieprosesser og produksjons-plattformer, eller fremstillingen av nanopartikler for testing og vektorering av medisiner.[106] AI-verktøy som utvikles for kjemisk industri kan komme til å bli benyttet som støtte til ikke-statlige «amatører» for fremstilling av farlige kjemiske stoffer eller biologiske agenter (syntetiske eller modifiserte). Videre har syntetisk biologi i senere år blitt tettere koblet til additiv tilvirkning innen det voksende feltet bioprinting. Frem mot 2030 er det sannsynlig at 3D-bioprinting vil kunne kobles til cellefri syntetisk biologi for å skape utstyr som enkelt kan syntetisere komplekse proteiner, både naturlig forekommende og nye proteiner bestående av ikke-naturlige aminosyrer.

### 3.2.7 Bruk av det elektromagnetiske spekteret

Vi har i dag blitt vant til den dramatiske økningen og tilgangen på trådløs teknologi som muliggjør kommunikasjon og datautveksling gjennom objektene i Tingenes internett, inkludert mobiltelefoner, smartklokker og wi-fi. I tillegg har mange bilfabrikanter installert avanserte sensorer i nye kjøretøy som muliggjør delvis autonom kjøring. Fellesnevneren for disse teknologiene er utnyttelsen av det elektromagnetiske spekteret, som utgjør fundamentet eller er et understøttende element for mange nye digitale løsninger.

Kombinasjonen av økt dataprosesseringskraft og miniatyriseringen av databrikker har ført til en skarp økning av tilgjengelige objekter som kan benyttes som sensorer i samfunnet. Mobiltelefoner

[103] Hummel og Burpo (2020) s. 4.
[104] Frinking (2016) s. 13.
[105] Frinking (2016) s. 37-38.
[106] Bajema, Natasha & DiEuliis, Diane (2017), "Peril and promise: Emerging technologies and WMD", *National Defense University Press, (Washington DC).*

er et åpenbart eksempel, men dette gjelder også mindre droner med optiske kamera, navigasjonsutstyr som mottar signaler fra satellitter, ansiktsgjenkjennelsesprogramvare integrert med overvåkningskameraer, nanosatellitter som gjør overvåkningsdata fra rommet tilgjengelig for private aktører eller radiofrekvensidentifikasjonsbrikker (RFID) for å følge varestrømmer. Det elektromagnetiske spekteret utnyttes til å generere data på en helt annen måte enn før, og flere har tilgang til langt mer informasjon enn tidligere.

Det finnes flere eksempler på at ikke-statlige aktører har utnyttet disse mulighetene. Under konfliktene i Irak og Afghanistan på 2000-tallet lagde opprørsgrupper improviserte bomber (også kjent som *improvised explosive devices,* eller IED) og benyttet radiofrekvensene for å utløse dem ved bruk av dagligdags teknologi som mobiltelefoner, garasjeportåpnere eller fjernkontroller for radiobiler. En enkel måte å forstyrre kommunikasjon på – enten radio- eller GPS-signaler – er å fylle frekvensen med støy («jamming»). Når den eksakte frekvensen som IED-utløseren bruker er ukjent, må man forstyrre en større del av frekvensbåndet for å sette den ut av spill. Dette skapte utfordringer for amerikanske styrker og deres allierte når kraftig jammeutstyr, som skulle ufarliggjøre IEDene, også forstyrret egne kommunikasjonsfrekvenser.[107]

I tillegg til å forstyrres kan kommunikasjon også fanges opp – slik irakiske opprører gjorde med amerikanske droner i 2009. Ved å benytte den kommersielt tilgjengelige programvaren «SkyGrabber» klarte opprørerne å fange opp videofiler fra dronene.[108] Med kraftig nok utstyr kan signalene til droner også «jammes» og lede til at det krasjer. For å overta kontroll av dronen kan falske GPS-signaler genereres, såkalt «spoofing». Ved å bruke enkel teknologi og programvare gjennomførte en universitetsstudent i Texas i 2012 et vellykket eksperiment der han tok kontroll over en stor RQ-1 drone operert av den amerikanske grensevakten.[109]

I løpet av de neste 30 år vil veksten i sensormengden fortsette og inkludere flere små sensorer som dekker både bymiljøet og slagmarken. I en NATO-rapport er dette beskrevet som «nye, distribuerte systemer, med lavt strømbruk og følsomme sensorer med evne til storskala «mesh»-atferd og selvorganisering».[110] Dette inkluderer biologisk nedbrytbare sensorer – såkalte «smart dust» – som brukes i kroppen eller som kan ligge strødd på slagmarken. Slike sensorer vil emittere elektromagnetisk stråling som kan detekteres, men vil brytes ned og forsvinne gjennom biokjemiske prosesser.[111] Andre nyvinninger vil kunne bruke elektromagnetisk stråling til å skjule identitet eller bevegelser. En del ansiktsgjenkjennelsesteknologi, som Apple FaceID, anvender infrarødt lys til å kartlegge ansiktet. Dette kan motvirkes ved å sende forstyrrende stråling mot systemet for å forhindre nøyaktig avlesning.[112]

[107] Koerner, Brendan (2014), "Inside the new arms race to control bandwidth on the battlefield", *Wired*, 18. februar 2014.
[108] Ibid.
[109] Goodman, Marc (2015), "How terrorists are turning robots into weapons", *DefenseOne*, 16. april 2015.
[110] Reding, D. F. & Eaton, J. (2020).
[111] European Commission (2019) ss.125-127.
[112] Thomas, Elise (2019), "How to hack your face to dodge the rise of facial recognition tech", *Wired*, 1. februar 2019.

Den økende mengden sensorer vil også drive frem nye måter å kamuflere sårbart utstyr og personell på. Et eksempel på dette er nanomaterialer som absorberer infrarød stråling slik at de kan skjule selv større konstruksjoner mot deteksjon fra IR-sensorer.[113] Andre metamaterialer kan, teoretisk sett, skjule eller redusere synligheten av objekter også i den synlige delen av spekteret og gjøre dem vanskeligere å detektere med optiske sensorer.[114] Rettet elektromagnetisk stråling kan også benyttes til å kontrollere folkemengder, deaktivere maskiner/systemer eller forstyrre ulike sensorsystemer.[115]

Laserteknologi har lenge vært under utvikling, og bruksområdene forventes å bli enda flere fremover. Bredbåndet («hvit») elektromagnetisk stråling generert av kortpulsert laser kan være et svært effektivt virkemiddel mot elektro-optiske sensorer. På samme måte kan videre utvikling av kaskadelasere gi grunnlag for neste generasjons mottiltak mot IR-sensorer (IRCM) for å redusere sårbarheter mot varmesøkende missiler. Teknologisk fremgang har også bidratt til at størrelsen på enhetene som genererer laserstråler har blitt redusert. USA har nå ambisjoner om å utvikle et laservåpen for nærforsvar mot missiler som kan plasseres under vingene til et kampfly.[116] I tillegg til våpensystemer kan laserteknologi også brukes til kommunikasjon, blant annet i verdensrommet for å oppnå hurtigere og mer effektive forbindelser mellom satellitter. [117]

## 3.3 Oppsummering

Disse syv teknologiområdene utgjør et bredt nedslagsfelt for bruksområder og kapabiliteter som kan benyttes av ikke-statlige aktører i fremtiden. Noen av områdene er velkjente og har modnet over tid. Det er imidlertid forventet at mange av teknologiene vil videreutvikles og finne nye bruksmåter. Konvergens av fremvoksende teknologier vil fortsette å være en vesentlig usikkerhetsfaktor. Det er i tillegg viktig å legge merke til at de fleste teknologiområdene diskutert i dette kapittelet primært har sivile anvendelser, og at forskningen derfor drives frem av kommersielle aktører i langt større grad enn forskning og utvikling direkte for militære formål.

Derfor er det et viktig poeng å forstå hvordan teknologiske nyvinninger adopteres av befolkningen i et fremtidig samfunn. Dette er særlig relevant med tanke på hvorvidt fremvoksende teknologi vil være tilgjengelig for ikke-statlige aktører. For noen aktørtyper vil kommersiell tilgjengelig teknologi som er i vanlig bruk i samfunnet være lettere å tilpasse til egne behov. Tilgjengeligheten av samfunnsteknologi påvirker også sikkerheten da økt bruk av nye teknologiske løsninger kan gi et endret risikobilde. Den omfattende digitaliseringen har i mange tilfeller økt effektiveten og gjort nyttig informasjon lettere tilgjengelig, samtidig som den har gjort funksjonaliteten til mange samfunnstjenester og kommersielle aktiviteter avhengig av et fungerende internett. Dette gir ikke-

[113] The Week magazine (2018), "Hiding from infrared cameras is now possible", *theweek.in, 10.* desember 2018; Yount, Jordan (2020), "New Cloaking Material Could Protect Buildings, Soldiers", *University of Missouri College of Engineering,* 21. mai 2020.
[114] Calderone, Julia (2015), "Scientists have developed a super-thin, skin-like invisibility cloak", *Business Insider*, 18. september 2015.
[115] Akerman, Spencer (2012), "I got blasted by the Pentagon's pain ray: twice" *Wired, 12.* Mars 2012.
[116] Mayfield, Mandy (2020), "Air Force Wants Lasers on Fighter Jets by 2025", *National Defense*, 9. november 2020.
[117] Chen, Sophia (2017), "Tiny, Laser-Beaming Satellites Could Communicate With Mars", *Wired*, 10. juli 2017.

statlige aktører med høy teknologiadopsjonsvilje utvidete muligheter til å ramme militære og sivile mål.

Samfunnsteknologi utgjør en viktig faktor i det fremtidige militære operasjonsmiljøet, særlig når det gjelder fredsbevarende styrker, stabilitetsoppdrag, opprørsbekjempelse, eller kontraterror-operasjoner. Slike operasjoner foregår ofte tett på lokalbefolkningen. I fremtiden er det forventet at tettbefolkede storbyer eller «megacities» vil være enda mer vanlig og at militære operasjoner vil kunne foregå innenfor disse storbyene. Da kommer samfunnsteknologi til å være en viktig faktor for å forstå sårbarheter og identifisere mulighetene som kan øke effektiviteten til operasjonene.

Kartlegging av relevante aktører og teknologier danner det empiriske grunnlaget for rapportens neste analytiske steg som består av å konstruere et fremtidsbilde der aktørene og teknologiene settes inn i samfunnsbeskrivelser mot henholdsvis år 2030 og 2050. Utarbeidingen av disse fremtidsbildene er nødt til å være spekulative, men tar likevel utgangspunkt i eksisterende kunnskap om den forventede utviklingen til hvert teknologiområde. Kun når samfunnsutviklingen, aktørene og teknologien settes sammen, er det mulig å se konturene av operasjonsmiljøet og hvordan dette vil påvirke fremtidige norske militære operasjoner.

# 4 Anvendelse av fremvoksende teknologi

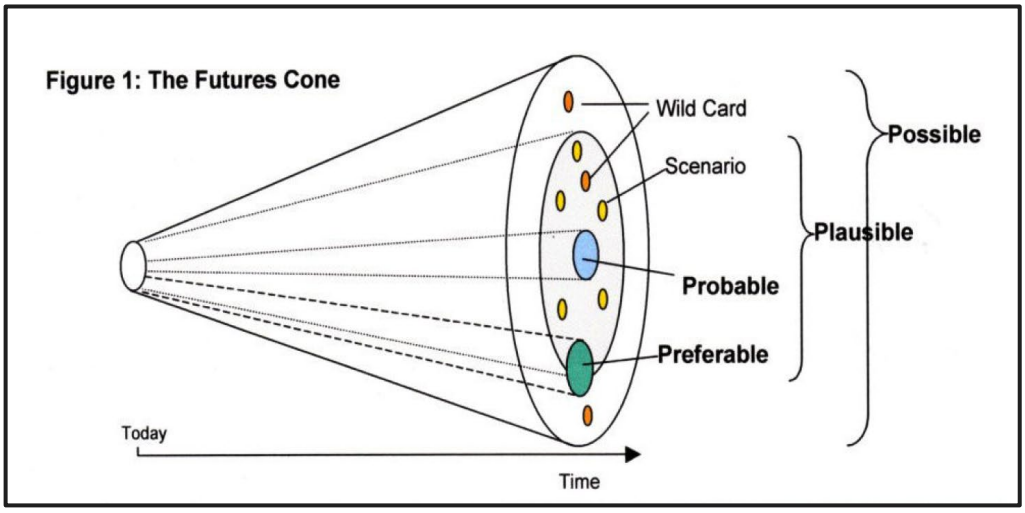
I en omdiskutert bok fra 2015 lanserte Klaus Schwab ideen om at verden var på randen av en fjerde industriell revolusjon.[118] Ifølge Schwab har verden opplevd tre store industrielle epoker kjennetegnet av teknologisk fremgang: den første revolusjonen benyttet vann og damp til å drive maskiner, den andre brukte strøm til å muliggjøre masseproduksjon, og den tredje revolusjonen var preget av automatisert produksjon ved bruk av elektronikk og informasjonsteknologi. Schwab argumenterte for at verden nå var i gang med en ny revolusjon som representerte et klart brudd med den forrige.

Den fjerde industrielle revolusjonen drives frem ved at milliarder av mennesker kobles sammen gjennom små mobile enheter med stor prosesseringskraft og får tilgang til store mengder kunnskap og evne til kommunikasjon. Videre drives endringene av fremvoksende teknologi som kunstig intelligens, robotikk, Tingenes internett, autonome kjøretøy, additiv tilvirkning, nanoteknologi, bioteknologi, og andre områder. Schwab mente at disse teknologiene utgjorde en ny industriell epoke og at hastigheten og bredden i endringene ville skje på tvers av ulike sektorer og påvirke omtrent alle sosioøkonomiske lag i samfunnet.

De mulige fremtidsbildene som beskrives i dette kapitelet går strukturert gjennom hvordan fremvoksende teknologi vil kunne påvirke samfunnsdimensjonene beskrevet i rapportens kapittel 2.4. Fremtidsanalyser vil alltid være forbundet med usikkerhet. Samtidig er intensjonen at en delvis strukturert metodisk tilnærming vil sørge for et nyansert og bredt bilde som forhåpentligvis reduserer sannsynligheten for at forfatterne blir offer for egne kognitive biaser. Fremtidsbildene er rettet mot to tidshorisonter: 2030 og 2050. Et tidsperspektiv på 30 år er spesielt krevende, særlig når teknologiutviklingen, menneskelig atferd og preferanser sees under ett.

Fremtidsanalyser deles gjerne inn i fire kategorier. *Mulig fremtid* inkluderer alle mulige kjente og ukjente teknologiske utviklinger, dette er en analyse som kan ligne science-fiction. *Plausibel fremtid* er basert på kjent kunnskap og kjente teknologier slik at fremtiden som skisseres er «rimelig». *Sannsynlig fremtid* baserer seg på en nesten-lineær framskriving av nåværende teknologi. Den siste kategorien er *foretrukket fremtid* og er en normativ vurdering av hvordan vi ønsker at fremtiden blir seende ut.[119] I denne rapporten sikter vi først og fremst mot en blanding av en *plausibel* og *sannsynlig* fremtidsanalyse basert på eksisterende teknologier og mulig samfunnsutvikling. Andre usikkerhetsmomenter inkluderes i analysen som såkalte jokere eller «wildcards» som kan få uvanlig stor påvirkningskraft på fremtiden.

[118] Schwab, Klaus (2015), "The fourth industrial revolution: What it means and how to respond", *Foreign Affairs*, desember 2015.
[119] Voros, Joseph (2001), "A primer on future studies, foresight and the use of scenarios", *Foresight Bulletin*, desember 2001.




*Figur 4.1 Fremtidsanalyser kan deles i fire ulike kategorier: mulig, plausibel, sannsynlig og foretrukket fremtid. (Voros 2001).*

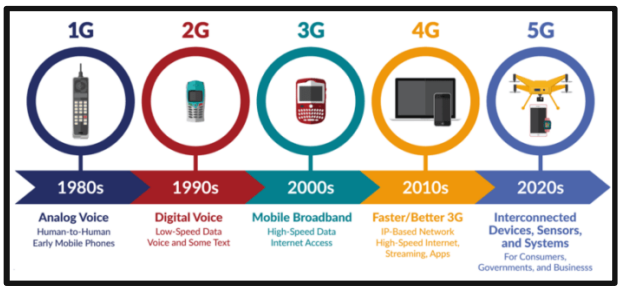
## 4.1 Samfunnsutvikling mot 2030

En fremtidsanalyse av samfunnet i 2030 kan, til en viss grad, gjennomføres ved å identifisere teknologi og trender som allerede er under utvikling og tatt i bruk. I et 10 års perspektiv anses det som mindre sannsynlig at nye og helt ukjente teknologiske løsninger vil vokse frem. Da er det som oftest mer verdifullt å se på hvordan samfunnet kan bli påvirket av eksisterende teknologi som modnes og gradvis blir integrert og brukt av næringslivet, statlige etater, og resten av befolkningen.

Samfunnet i 2030 forventes å være ganske likt slik det er i dag, men med noen vesentlige endringer forårsaket av hurtigheten som preger teknologisk utvikling. Akkurat som i dagens samfunn vil vi se vesentlige forskjeller i ulike verdensdeler, selv om det er fullt mulig at utviklingsland vil kunne avstå fra å benytte en teknologi og gå direkte til anvendelse av neste generasjons teknologi. Eksempler på dette kan være at en stat velger å bygge ut et robust 5G-nett fremfor et krevende og kostbart prosjekt for å grave ned fiberoptiske kabler. På denne måten «hopper de bukk over» en teknologi og går direkte til anvendelse av en nyere teknologi.[120]

[120] Hairsine, Kate (2019), "Is Africa ready for 5G?", *Deutsche Welle*, 29. november 2019.

***Mellommenneskelig kommunikasjon*** forventes å bli videreutviklet i løpet av det neste tiåret. Vi har sett en dramatisk utvikling i måten mennesker kommuniserer med hverandre, noe som kommer som et direkte resultat av samfunnsmessig digitalisering og digital transformasjon. Muntlig kommunikasjon gjennom telefoni og skriftlig kommunikasjon via post og epost har blitt supplert med korte tekstbeskjeder og video-chat, gjerne med innebygd kryptering. Den mest betydningsfulle utviklingen har imidlertid vært sosiale medier som har gitt individer evnen til å kommunisere med mange på en svært enkel måte. Sosiale medier har hatt innvirkning på sosiale, økonomiske og politiske prosesser som ville vært vanskelig å forutse. Forretningsmodellen til flere av disse kommunikasjonsplattformene baserer seg på reklameinntekter og benytter mønstergjenkjennelsesalgoritmer for å sortere og kanaliserer innhold som pirrer den enkelte brukers interesse, slik at plattformen benyttes hyppig. Teknologiutvikling har vært sentral for å kunne gjøre dette sosiale fenomenet mulig – særlig viktig er smarttelefonen som består av en sammensmelting av ulike teknologiske løsninger: telefon, datamaskin, kamera, internettportal osv.




*Figur 4.2 Evolusjonen av trådløs teknologi har hittil nærmest vært lineær.*

Det er nyttig å reflektere over utviklingen av den teknologiske konvergensen som førte til smarttelefonen og miniatyriseringen av databrikker og prosesseringskraft. Da elektroniske datamaskiner først ble en realitet på 1940-tallet så fylte de store rom, deretter krympet de til å passe inn på en skrivepult, en laptop på fanget, og til slutt som en del av de mobile enhetene og nettbrettene vi kjenner i dag. Med bakgrunn i forventet teknologisk utvikling så vil grensesnittet for slike enheter innen 2030 bli benyttet virtuelt og med hjelp av blandet virkelighet. Store teknologiselskap som *Microsoft*, *Google* og *Facebook* har vært sentrale i utviklingen av både VR- og AR-briller, teknologier de mener vil bli den foretrukne løsningen for neste generasjons kommunikasjons- og internettverktøy.[121] Virtuell virkelighet brukes allerede i dag i forbindelse med trening og tilvenning, eksempelvis av sykehusansatte som virtuelt kan teste og blir vant med nye løsninger før sykehuset er ferdigbygget.[122]

Fremgangen i talegjenkjennelsesteknologi gjør det nærliggende å tro at bruk av tastaturer – selv digitale – snart vil anes å være tungvint. Kombinert med utvidet tilgang til 5G-nettverk, kan AR-baserte grensesnitt bli et logisk neste skritt som integrerer menneskets fysiske oppfatning av verden med en digital tilstedeværelse. Som det fremkommer av figur 4.2 har kapasiteten og hurtigheten i trådløs infrastruktur opplevd et generasjonshopp stort sett hvert tiår. Det er derfor

[121] Condon, Stephanie (2020), "Facebook previews smart glasses and the future of work in VR", *ZDNet*, 16. September 2020; Facebook (2020), «Announcing project Aria: A research project on the future of wearable AR», *fb.com*, 16. september 2020.
[122] Se for eksempel: Helse Nord-Trøndelag (2019), "Sikker pasientsikkerheten med VR teknologi", 8. oktober 2019; Braaten, Frøydis (2016), "Sykepleiere vandrer rundt på sykehuset - før det er bygget", *Aftenposten* 27. januar, 2016.

ikke urimelig å forvente at enkelte IT-selskap vil starte forberedelser til neste generasjon og en overgang til 6G-nettverk innen 2030.[123]

Måten mennesker får ***informasjon og nyheter*** på i 2030 henger tett sammen med utviklingen beskrevet over. Informasjon forventes å bli enda mer skreddersydd til den enkelte brukeren og fremtidens AR system. Internettbaserte nyhetskilder har gjennom 2000-tallet bidratt til et svært variert informasjonsmiljø der ulike kilder konkurrerer om brukere og relevans. Overgangsfasen fra den tidligere informasjonssituasjonen, som besto av et fåtall allment aksepterte aviser og nyhetssendinger som bidro til å etablere et felles faktagrunnlag for samfunnet, til et internettbasert miljø, har vært preget av mediapolarisering og en ekkokammereffekt som har forsterket eksisterende sosiale og politiske splittelser i samfunnet. Gitt de nåværende trendene er det vanskelig å se hvordan man kan unngå at digitale virkemidler forsterker disse effektene og fører til en enda mer skreddersydd eksistens i fremtiden.[124]

I en bredere kontekst vil den massive veksten av satellitter komme til å gi oss enda bedre personlig, lokal og global situasjonsforståelse. Fra nettbaserte tjenester som *Bellingcat* kan man allerede i dag få geolokaliserte Twitter-meldinger om begivenheter fra et spesifisert område – supplert med ferske satellittbilder – alt sortert og sveiset sammen av kommersielt tilgjengelig analyseverktøy bygget på stordata og kunstig intelligens. Dette gir enkeltindivid tilgang på avanserte etterretningsverktøy som vil forbedres og bli mer tilgjengelig innen 2030.[125]

Noe som får mindre oppmerksomhet, men som vil ha stor innvirkning på menneskers daglige liv er nyvinninger innen ***helse og bioteknologi***. En rekke biometriske sensorer som Apple-klokker og Fitbit er allerede i bruk. Nytt fleksibelt sensormateriale kombinert med utviklingen innen nanoteknologi vil redusere størrelsen på disse sensorene og øke datafangsten, noe som gir flere mennesker tilgang til mer omfattende biometriske data om seg selv. Dette kan bidra til å forebygge sykdom, sørge for tilpasset kosthold og trening, samt overvåke personers helsemessige tilstand. Økt dataprosesseringskraft kombinert med AI har fått fortgang i DNA kartleggingsarbeidet, og CRISPR-lignende genredigeringsverktøy vil innen 2030 kunne tilby mulige løsninger på genetiske sykdommer med såkalte DNA-vaksiner.[126] De samfunnsmessige fordelene med denne teknologien, som ble demonstrert i den hittil vellykkede bruken av mRNA vaksiner for COVID-19, vil antagelig presse forskningsfronten til tross for den reelle risikoen for uintendert bruk.

Videreutviklingen av grensesnittet mellom menneske og maskin vil fortsette i tiden frem mot 2030. Arbeidet med å tolke hjernebølger vil med tiden utvikles fra å være på det eksperimentelle stadiet til praktisk anvendelse, eksempelvis i form av manipulering av mekaniske proteser og

[123] Johnson, Dexter (2020), "With 5G Rollout Lagging, Research Looks Ahead to 6G", *IEEE Spectrum*, 29. juli 2020.
[124] Perl, Peter (2019), "What is the future of truth?", *Pew Research*, 4. februar 2019.
[125] Izadi, Elahe & Farhi, Paul (2021), "Bellingcat breaks stories that newsrooms envy — using methods newsrooms avoid", *Washington Post*, 9. januar 2021.
[126] I 2020 lanserte Pfizer en COVID vaksine som benyttet genredigeringsteknologi. Se Isaacson, Walter (2020), "I was part of a trial for Pfizer's covid-19 vaccine. It's a miracle for genetic medicine", *Washington Post*, 9. november 2020.

andre funksjoner Selv om Elon Musks Neuralink skapte flere overskrifter enn praktiske resultater i 2020, kan integrerte «databrikker-i-hodet» på sikt komme til å tilby en tettere og mer smidig overgang mellom menneske og maskin.[127]

Teknologi i form av robotikk vil bli mer brukernært i løpet av perioden mot 2030. Dette kan komme i form av eksoskjelett som benyttes i varehus for å effektivisere flytting av tung last. Neste generasjons smarthøyttalere og digitale assistenter som Amazons Alexa eller Apples Siri vil kunne kombineres med neste generasjons robotikk for å løse oppgaver i hjemmet eller i eldreomsorgen i en overvåkings- og støttefunksjon. AI-systemer benyttes allerede i dag til å overvåke og vurderer arbeidernes produktivitet, utviklingen forventes å fortsette.[128]

| **Teknologi i samfunnet: 2030** | |
|---|---|
| Kommunikasjon | Mobiltelefon, 5G+ utbredt<br>Første gen utvidet-virkelighet briller |
| Informasjon/nyheter | Skreddersydd info-strøm<br>Massiv økning personlig data<br>Økende antall satellitter: data/bilder |
| Helse/bioteknologi | Biosensorer<br>Genmodifisering (begrenset)<br>Hjerne-datamaskin grensesnitt (begrenset) |
| Handel og produksjon | Videre automatisering/autonome systemer<br>Heldigital bank/valuta |
| Transport | Autonome kjøretøy<br>Overflatefartøy (begrenset) |
| Konsekvenser for samfunnet | Økende fokus på digital virkelighet<br>Skreddersydd og tilpasset virkelighet<br>Data omfang øker i takt med AI analytikk |

*Figur 4.3: Bruksområdene til teknologi i samfunnet mot 2030*

***Handel og produksjon*** av varer er et område som blir spesielt påvirket av den fjerde industrielle revolusjonen. I perioden mot 2030 vil det vokse frem nye bruksområder for AI og autonomi som vil integreres i produksjonskjedene. Smarte fabrikker som kombinerer additiv tilvirkning og automatisering vil kunne oppnå svært fleksible produksjonsløsninger. Konsumenter vil bli tilbudt individuelt tilpassede produkter – anbefalt av en AI-styrt digital salgsassistent som kjenner kjøpshistorikk og priser på tilsvarende varer. Autonome systemer som koordinerer sine bevegelser vil benyttes til jordbruk eller overvåking av skogsområder. Utstillingsplattformer basert på blandet virkelighet vil gjøre det mulig for kunder å prøve klær og andre produkter digitalt før det bestilles på nettet. Digitale banktjenester og pengeapplikasjoner som Vipps har ført til en kraftig reduksjon av kontanter i omløp, denne trenden forventes å fortsette frem mot 2030. Aktiviteter i verdensrommet vil intensiveres med fremvekst av flere statlige og kommersielle aktører som benytter satellitter

[127] Neil Harbisson er anerkjent som verdens første «cyborg»: se: Veløy, Chris (2019), "Vil la folk velge hvilken art de vil være", *NRK.no*. 18 Juni 2019.
[128] Dzieza, Josh (2020), "How hard will the robots make us work?", *The Verge*, 17. februar 2020.

eller utplasserer egne rombaserte installasjoner og tilbyr nye og avanserte kommersielt tilgjengelige rombaserte tjenester.[129]

I ***transportsektoren*** vil autonome kjøretøy og fartøy være den største pådriveren for forandring. I løpet av det neste tiåret vil autonomi – i kombinasjon med AI bli bedre til å observere og predikere menneskelig atferd – dette vil løse dagens utfordringer med førerløse kjøretøy. Teknologien vil være særlig utbredt innen områdene logistikk og offentlig transport, med lastebiler i logistikk-kolonner som kjører lengre avstander og rutebusser på dedikerte traséer. Menneskelig kontroll av disse systemene kan sannsynligvis bli redusert til overvåkende støttefunksjoner. Fergetrafikk og tog med korte og faste ruter kan i større grad bli autonome, med mennesker i en støttefunksjon slik man allerede ser i dagens kommersielle luftfart der pilotene hovedsakelig passer på autopiloten.

Noen stater kan allerede i 2030 ha startet planlegging av neste generasjons samferdselsnett med en betydelig grad av tilrettelegging for autonome systemer. Ny batteriteknologi basert på materialer som grafén kan gjøre det mulig for materialstrukturer som bilrammer og båt- eller flyskrog å lagre energi og fungere som store, hurtigladende batterier. Elektriske motorer har færre bevegelige deler som krever overvåking og vedlikehold, og vil bidra til at autonomiprosessene akselerer.[130]

Konsekvensene av den forespeilede utviklingen innenfor disse fem samfunnsområdene vil være omfattende. Videre vil samspillet mellom dem kunne føre til enda større forandring. Med større innslag av virtuell virkelighet og smidig brukergrensesnitt, kan mennesker i fremtiden skape sine egne tilpassede virkeligheter. Man vil kunne gjennomføre videosamtaler med venner i en del av synsfeltet, samtidig som data og objekter «tagges» og gir brukeren informasjon om omverdenen i sanntid. Samtidig vil man i andre deler av synsfeltet kunne motta informasjon fra både sosiale og «tradisjonelle» medier som kjemper om brukerens oppmerksomheten. I en slik hverdag kan det være enda mer krevende å etablere en felles forståelse når folk, bokstavelig talt, ser ulikt på verden. Falske nyheter og meldinger skapt for å vekke sterke reaksjoner hos enkelte sosiale grupper kan komme til å bli langt mer effektive.

Tilgjengelig datamengde vil i 2030 ha økt som følge av ekspansjonen av Tingenes internett, 5G, en rekke nye smarte AI-styrte objekter og tilstedeværelsen av biosensorer. Data er muligens ikke «den nye oljen», men kan likevel være svært verdifullt, særlig når analytiske verktøy utvikles parallelt med den massive økningen av tilgjengelig data. Informasjon som kan samles fra og analysere individer – alt fra arvemateriale, helsetilstand, handlemønstre, og daglige vaner – vil kunne spores, lagres og havne på avveie. Dersom digitale plattformer tilbyr rike interaktive opplevelser kan det bli fristende for flere enn «gamere» å tilbringe mange timer hjemme fremfor å omgås mennesker i «den virkelige verden».

[129] Wall, Mike (2020), "What's next after the International Space Station? Plans afoot for more off-Earth outposts", *Space.com*, 3. november 2020.
[130] Katwala, Amit (2018), "A graphene breakthrough hints at the future of battery power", *Wired*, 16. august 2018.

### 4.1.1 Wildcards 2030

Å predikere fremtidig teknologisk utvikling og mulige bruksområder er krevende nok, men når menneskelige preferanser inkluderes øker usikkerheten betraktelig. Individuelle og samfunnsmessige reaksjoner på teknologi forblir en konstant utfordring for fremtidsanalyser.

Videreutviklingen av autonome systemer og økt AI-kapasitet vil redusere behovet for arbeidskraft i mange sektorer, også innen yrker som tradisjonelt har vært skånet for automatisering. Et av de største usikkerhetsmomentene i denne fremtidsanalysen blir derfor graden av teknologiadopsjon i samfunnet. Vil mennesker føle behov for fysisk kontakt fremfor å leve heldigitalt? Vil de velge bort AR-briller fordi produktene blir avvist av moteverden? Vil familier være villig til å akseptere at AI-drevne robotassistenter passer på besteforeldre fremfor sykepleiere på aldershjemmet?

Dagens barn og ungdom har i stor grad vokst opp som «digitale innfødte» og er blitt vant til smarttelefoner og nettbrett fra en tidlig alder. Allerede i dag har disse et rikt sosialt liv via digitale plattformer. Innen 2030 vil barn være vant med en digital hverdag og være komfortabel med robotikk på en helt annen måte enn i dag. Dersom robotikk og autonomi blir mer akseptert i samfunnet kan den pågående økonomiske polariseringen akselerere. Dette kan føre til at høytlønnede arbeidstagere vil ha andre preferanser og holdninger enn lavtlønnede arbeidere med arbeidsoppgaver som likevel er for kompliserte for roboter å gjennomføre.[131] Hvordan demokratiske stater håndterer utfordringen med informasjonsflyt og felles faktaforståelse i et digitalisert samfunn kan påvirke både hvilke teknologier som tas i bruk og hvorvidt disse bidrar til økt radikalisering blant sårbare befolkningsgrupper, særlig når verktøy for å manipulere informasjon blir mer avansert og tilgjengelig.[132]

En annen utvikling som er relevant for den digitale sfæren i dette tidsperspektivet er modningen av teknologi for krypterte kommunikasjonsløsninger som er sikker fra trusselen mot asymmetriske krypteringsalgoritmer som vil kunne komme fra kvantedatamaskiner. Bruken av kvantenøkkeldistribusjon (QKD) gjør det mulig å oppdage dersom noen avlytter kommunikasjonskanaler og dermed hindre at informasjon kommer på avveie. Fremveksten av slik teknologi virker for tiden å være drevet av kommersielle interesser, og teknologien er foreløpig i liten grad utbredt. I første omgang fokuseres den videre utviklingen på å raffinere dagens laserbaserte systemer for sikker punkt-til-punkt-kobling (med begrenset rekkevidde og båndbredde) som et forsvar mot avlytting og jamming, slik at nettverk for kvantekommunikasjon mellom sentral og fjerntliggende infrastruktur muliggjøres.[133]

---

[131] Qureshi, Zia (2020), "Inequality in the digital era", *Brookings Institution*, 14 februar 2020; Sterling Amy (2019), "Millions of Jobs have been lost to automation. Economists weigh in on what to do about it", *Forbes*, 15. juni 2019; West, Darrell M. (2018), "Will robots and AI take your job? The economic and political consequences of automation", *Brookings Institution*, 18. april 2018.

[132] Paul, Christopher & Posard, Marek (2020), "AI and the manufacturing of reality", *RAND Corporation*; Hwang, Tim (2020), "Deep fakes: A grounded threat assessment", *Center for Security and Emerging Technology*, *Georgetown University, Washington DC, juli 2020.*

[133] Lin, Jeffery, Singer, P. W. & Costello, John (2016), "China's Quantum Satellite Could Change Cryptography Forever", *Popular Science,* 3. mars 2016.

## 4.2 Ikke-statlige aktører mot 2030

Skillelinjene mellom kriminelle nettverk, terrororganisasjoner, opprørsgrupper og proxy-aktører er, og vil forbli uklare, med bakgrunn i dette konkluderte kapittel 2.5 med at det vil være hensiktsmessig å sortere aktørene basert på deres vilje til å adoptere fremvoksende teknologi. Når denne variabelen kombineres med hvorvidt avansert teknologi er tilgjengelig i samfunnet, skapes det fire ulike aktørtyper. Når teknologinivået i samfunnet er lavt og aktørens adopsjonsviljen også er lav, forblir aktørens evner stort sett uforandret av teknologisk fremgang og dermed blir *status quo* opprettholdt. Kategorien *innovativ* aktør oppstår når tilgang til avansert teknologi i samfunnet er lav men aktøren er motivert til å finne kreative løsninger med «hverdagslig» samfunnsteknologi. Når tilgangen til avansert samfunnsteknologi er høy men aktøren forblir uinteressert – noe som beskriver mange terrororganisasjoners forhold til teknologi – vil den *umotiverte* aktøren likevel nyte godt av den teknologiske utviklingen i samfunnet. Den farligste kombinasjonen – høy teknologitilgang og høy innovasjonsevne – fører til en innovativ, velfinansiert *hypertrussel-aktør*, eksempelvis en ny type terrorgruppe eller en statlig støttet proxy-aktør.

For å forstå hvordan disse aktørtypene kan benytte fremvoksende teknologi frem mot 2030 fokuserer rapporten på fem ulike oppgaver eller funksjoner som aktørene vanligvis er interessert i å løse: (i) kommunikasjon, (ii) informasjonsinnhenting, (iii) mobilitet, (iv) angrepsmidler, og (v) logistikkløsninger. Innenfor hvert av oppgavesettene beskrives mulige teknologiske løsninger for fremtidige ikke-statlige aktører frem mot 2030.

**Kommunikasjon** blant ikke-statlige aktører vil i likhet med dagens situasjon foregå på mange ulike plattformer. Den videre utviklingen av kryptering og anonymiseringsverktøy som TOR («The Onion Router») eller applikasjoner som *Signal,* vil føre til at aktører med lav teknologiadopsjonsvilje vil ha gode muligheter for skjult kommunikasjon i 2030.[134] Fremtidige kriminelle aktører, terrorister eller opprørsgrupper som klassifiseres som «umotiverte» med hensyn til teknologisk adopsjon, vil anonymt kunne planlegge kriminell atferd, eller voldelige handlinger uten frykt for å bli oppdaget. Innovative opprørsgrupper i konflikt med statlige aktører kan evne å operere mer smidig og oppnå kommando- og kontroll på nye og bedre måter gitt den teknologiske utviklingen innen kommunikasjonsteknologi. Algoritmer og kunstig intelligens vil bistå nasjonale myndigheter i å sortere tilgjengelig informasjon og detektere disse aktørene, men utviklingen av ulike applikasjoner og nye krypterte nettverksmuligheter vil gjøre det lettere for disse aktørene å operere med lav signatur.

Dataproduksjon fra tingenes internett fortsetter å øke og informasjonsmengden på nettet vil passere 175 milliarder GB allerede innen 2025.[135] Uten å måtte anstrenge seg mye, vil disse aktørene evne å kommunisere med likesinnede, rekruttere og radikalisere nye medlemmer via digitale plattformer. Informasjons- og nyhetsboblene som allerede har blitt skapt vil forsterkes

[134] Harrison, Seth (2018), "Evolving tech, evolving terror", *New Perspectives in Foreign Policy*, *vol 15*, *Center for Strategic and International Studies, Washington DC* .
[135] Reinsel, David, Gantz, John & Rydning, John (2018), "The Digitization of the World
From Edge to Core", *IDC White Paper*.

innen 2030. Dette vil gjøre det lettere for terrororganisasjoner og opprørsgrupper å appellere til nye medlemmer og tilpasse egne nyheter og propaganda på en enda mer finurlig måte.

I motsetning til mindre ambisiøse *status quo*- eller *umotiverte* aktører som kun benytter kommersielt tilgjengelige produkter, vil innovative og velfinansierte *hypertrussel-aktører* utvikle og benytte mer avanserte kommunikasjonsplattformer. For enkelte innovasjonsvillige kriminelle organisasjoner eller terrorgrupper kan kommunikasjon foregå via virtuelle møteplasser, bruk av kryptert internett og sikker mobilkommunikasjon. De kan komme til å ha tilgang til kommunikasjonsnettverk bygget på sikker utveksling av kvantenøkler (QKD). Gitt at fredsbevarende styrker eller stabiliseringssoperasjoner vil overvåke lokale sosiale medier, kan ikke-statlige aktører med høy teknologiadopsjonsvilje søke å benytte seg av disse kanalene for spredning av desinformasjon og propaganda.

*Hypertrussel-aktører* vil innen 2030 kunne benytte AI til å produsere falske videoer, bilder eller lydspor som er vanskelig å identifisere som falske. Denne formen for «deep-fakes» kan brukes for å utnytte ekkokammereffekter og eksisterende splittelser i samfunnet. Dette sørger for at aktørene fremmer egne synspunkt til utvidede og nye publikum slik at de kan rekrutterer nye medlemmer. Denne teknologien kan også bidra til at aktørene sprer falske videoklipp eller bilder som del av et ønsket narrativ. Til tross for at denne typen «deep-fakes» lar seg avkrefte ved bruk av andre kilder, så vil gjentatte tilfeller være med på å skape en uoversiktlig situasjon som vanskeliggjør pågående militære operasjoner.

**Informasjonsinnhenting** om mulige terrormål eller militære angrep mot statlige motstandere blir lettere ved bruk av kommersiell tilgjengelig teknologi. Det som omtales som «åpne kilder» innen etterretningsfaget kan komme til å inkludere satellittbilder, data fra sosiale medier, eller annen lett tilgjengelig data om motstanderens bevegelser. Datamengden vil være såpass omfattende på grunn av antallet objekter i Tingenes internett at ikke-statlige aktører med lav teknologiadopsjonsvilje i 2030 vil ha økte evner til å gjennomføre egen etterretning, overvåking, og rekognoseringsaktivitet. Dagens VR løsninger for trening og simulering forventes å utvikles ytterlig slik at selv *umotiverte* aktører vil ha gode muligheter til å øve virtuelt på angrep for å perfeksjonere taktikkene sine.[136]

Informasjonsinnhenting kan gjennomføres med avanserte system og verktøy for ikke-statlige aktører med høy teknologiadopsjonsvilje. Kommersielle satellittbaserte bildetjenester og kartfunksjoner vil innen 2030 være videreutviklet og kan gi detaljert overvåkingsdata over et bestemt geografisk område, noe som er nyttig i operasjonsplanleggingen til enkelte *hypertrussel-aktører*. Tilgangen på små og mellomstome rimeligere flyvende ubemannede sensorer vil utvide innhentingskapasitetene til disse aktørene og gir dem økte etterretnings- og rekognoserings-muligheter.

[136] Teknologiene som nå utvikles blant statlige aktører vil innen 2030 være tilgjengelig også for ikke-statlige aktører. Se Wilson, Clay (2018), "Avatars, Virtual Reality Technology, and the U.S. Military: Emerging Policy Issues", *Congressional Research Service, (Washington DC*); Shubsda Brian (2019), "SOCOM Must Tie Operational Data to Virtual Reality Training", *National Defense Magazine*, 2. mai 2019.

Videre må det forventes at innovasjonsvillige aktører innen 2030 evner å nyttiggjøre seg av data fra objekter i Tingenes internett. Muligheten til å identifisere og spore individer og grupper – for eksempel medlemmer av en folkeforsamling – kan gjøre det lettere for disse aktørene å gjennomføre presisjonsangrep i komplekse situasjoner. Dette kan eksempelvis gjennomføres med GPS-sporing i populære applikasjoner på en mobiltelefon. Samfunnet har over veldig kort tid blitt vant til å dele mye personlig informasjon i det digitale rom – enten bevisst via sosiale medier, men også ubevisst gjennom applikasjoner og annet utstyr tilkoblet Tingenes internett. Dette kan utnyttes av disse aktørene og muliggjør kartlegging av mål gjennom innhenting og analyse av metadata. På den måten kan planlegging av angrep gjennomføres med enkle digitale ferdigheter via kommersielt tilgjengelige tjenester.

Ikke-statlige *umotiverte* aktører kan innen 2030 oppleve økt **mobilitet**, enten i et bymiljø eller på slagmarken. Det vil være mulig for aktørene å finne gode logistikkløsninger ved å benytte autonome lastebiler, skip eller godstog som har minimal med menneskelig bemanning. I slike situasjoner er det muligheter for ikke-statlige grupper å kunne bruke lignende kjøretøy uten å vekke oppmerksomhet. Dette slår begge veier: sensornettverk som blir nødvendig for å operere slike autonome systemer vil kunne detektere uønskede passasjerer og vil sannsynligvis ha sikkerhetstiltak på plass for å unngå uautorisert bruk. Dermed er det mindre sannsynlig at dette prioriteres av aktører med lav teknologiadopsjonsvilje. Sensorteknologi på slagmarken vil bære preg av et større antall lavkostandssensorer som kan dekke et større område og gjør det vanskeligere for ikke-statlige grupper å bevege seg uten å bli oppdaget og overvåket. For *umotiverte* aktører vil statlige sensornettverk være et betydelig hinder for planlagt aktivitet og operasjoner.

Mobiliteten til *hypertrussel-aktører* kan også påvirkes av tilgangen på autonom transport. Innen 2030 vil det være mulig med automatisk sporing av mistenkelige aktører i veinettet med hjelp av kameraovervåking og scanning av bilskilt. Gjennom utnyttelse av dronetrafikk, kan *innovative* aktører tenkes å kunne anonymt transportere både personell og materiell gjennom å benytte seg av en 2030-versjon av et «Uber»-lignende kjøretøydelingsprogram. Dette fordrer at enkeltindividene forblir anonyme slik at de ikke identifiseres på andre måter, noe som er vanskelig allerede i dag. Autonomi og droner vil også påvirke aktørers evne til etterforsyning, evakuering av sårende o.l. På den måten kan operasjonshastigheten til aktører i konflikt med statlige styrker øke.

Ansiktsgjenkjenning og tilstedeværelsen av overvåkningskameraer vil i mange land være et viktig verktøy for myndighetene i å begrense mobiliteten til denne type aktør. Når det ikke er mulig å gjemme seg, kan *innovative* eller *hypertrussel-aktører* derfor forsøke å skjule identiteten sin ved å benytte teknologi som briller som emitterer lys, infrarød stråling som forstyrre overvåkningskameraer, kosmetikk som forhindrer dyplæringsalgoritmene til AI i å kjenne igjen ansiktet, eller ved å bruke små jammere for å slå ut det lokale 5G-nettverket.

Det forventes at sensornettverket til statlige aktører vil være omfattende og utbredt innen 2030, derfor vil ikke-statlige aktører måtte finne mottiltak for å kunne operere med lav signatur på en effektiv måte. Elektronisk krigføring vil i den sammenheng få en viktig og fremtredende rolle.

Tiltak for å skjule eller justere emittering av elektromagnetiske signaler– enten det er varmestråling, samband, eller radar – vil være avgjørende. I noen situasjoner, særlig i strid som foregår i bebyggede områder og bymiljø, kan *innovative* aktører komme til å måtte benytte seg av eksisterende underjordiske tunnelsystem for å gjøre deteksjon vanskelig og mobilitet mulig.

**Angrepsmåten** som aktører med lav teknologiadopsjonsvilje velger å benytte i 2030 kan vise seg å være nokså uforandret fra dagens situasjon og vil i stor grad forbli fokusert på eksplosiver, stikkvåpen og skytevåpen. Angrepsmulighetene til ikke-statlige aktører med høy teknologiadopsjonsvilje forventes derimot å øke som et resultat av den teknologiske utviklingen frem mot 2030. Et bredt utvalg rimelige ubemannede systemer – både som sensor og effektor – vil øke angrepsmulighetene til disse aktørene. Med bedre informasjon om motstanderens posisjon, hentet inn ved bruk av ubemannede system, kan *hypertrussel-aktører* mer presist benytte lavkostnadsartilleri eller raketter i angrep mot pansrede kjøretøy. Disse aktørene kan i noen tilfeller benytte store mengder droner, kombinert med hjemmelagde eksplosiver og predefinerte flymønster, i angrip mot bakkebasert infrastruktur og militære anlegg. Dronene trenger ikke nødvendigvis å være hverken koordinerte eller bevæpnet for å utgjøre en reel trussel – dersom et tilstrekkelig antall droner treffer et passasjerfly vil dette kunne være nok for at det styrter. Denne formen for droneangrep kan også skape betydelig effekt i møte med statlige militære styrker.

En *hypertrussel-aktør* kan innen 2030 komme til å benytte syntetisk biologi for å gjennomføre terrorangrep med bruk av biologiske våpen og syntetiske stoffer. Aktørene kan med hjelp av ny teknologi og innovative teknikker fremstille syntetiske og biologiske stoffer som vanskelig lar seg detektere. Om aktøren har vilje og kompetanse kan det også oppstå forsøk på å syntetisk manipulere arvestoffet til sykdommer som ebola eller miltbrann, slik at dødeligheten eller smittsomheten økes betraktelig. Ved å kombinere additiv tilvirkning, CRISPR-teknologi og ubemannede systemer kan ikke-statlige aktører med høy teknologiadopsjonsvilje forsøke å gjennomføre biologiske eller kjemiske angrep med hjemmeproduserte droner som leveringsmiddelet.[137]

Godt finansierte proxy-aktører eller opprørsgrupper klassifisert som *hypertrussel-aktører* kan i 2030 komme til å gjennomføre avanserte cyberoperasjoner rettet mot både sivil og militær infrastruktur. At store deler av samfunnet har blitt digitalt må sees på i et samfunnssikkerhetsperspektiv. Allerede i dag er det mulig for ikke-statlige aktører å angripe digital infrastruktur fra hvor som helst i verden uten behov for bruk av militærmakt eller store investeringer. Slik utviklingen går vil disse aktørene innen 2030 ha økt evne til å forårsake skade ved at samfunnsutviklingen muliggjør en bredere angrepsflate.

Digitale mottiltak kan føre til at enkelte mål vil være svært utfordrende for disse aktørene å gjennomføre et angrep mot, mens mål med mindre sikringstiltak vil være mer utsatt. Samfunnsteknologi gir aktørene muligheter, men kan også lede til at de i større grad retter aktiviteten mot samfunnsmessige tjenester og teknologi med svak IKT-sikkerhet fremfor forsøk på angrep mot militær infrastruktur og IKT-systemer med høy grad av sikring. Hendelsene kan

[137] Hummel og Burpo (2020) s. 3.

rettes mot alt fra havner, veinettet, kraft, logistikk, helsesektoren osv. Et omdiskutert scenario er et cyberangrep mot det nasjonale strømnettet på et svært ubeleilig tidspunkt, som for eksempel vinterstid når mange er avhengig av elektrisk oppvarming. Denne type angrep vil være utfordrende for militære operasjoner hvor styrker gjør seg avhengig av sivil infrastruktur til blant annet kommunikasjon, mobilitet, kraft og logistikk.

Aktører med høy teknologiadopsjonsvilje kan i 2030 forsøke å kompromittere og hacke satellitter med hensikt å ødelegge eller manipulere tjenestene de leverer. Dette kan utvide handlingsrommet for aktørene på bakken ved at deres statlige motstandere mister evne til overvåking. Et scenario beskriver hvordan ikke-statlige aktører kan forsøke å krasje en satellitt for å forårsake en kjedereaksjon – den såkalte Kessler-effekten. Denne romversjonen av en «IED» vil kunne lage så mye romsøppel at det vil være tilnærmet umulig å sende opp nye satellitter på flere år. Gjennomføringen av et slikt type angrep – selv om det regnes som usannsynlig – vil ha globale konsekvenser.

Med tilgang på økt prosesseringskraft kan det være lettere for ikke-statlige aktører å både analysere og forstyrre elektromagnetiske signaler som binder kritiske samfunnsfunksjoner som kommunikasjon eller nettverk sammen. Med avansert og kompakt «jamming» eller narring kan *innovative* aktører benytte kommersielle løsninger for å forstyrre og manipulere GPS signaler, kommunikasjonsforbindelsen i flytrafikken eller autonome kjøretøy. Autonom transport blir på denne måten sårbar for sensormanipulasjon. Kameraene på Tesla-biler ble i 2020 manipulert til å feiltolke et fartsgrenseskilt ved at det ble satt opp teip over tallet på skiltet, noe som gjorde at bilens autopilot øke farten i en 50 km/t sone til 130 km/t. Slike enkle grep kan gjennomføres av en oppfinnsom innovativ aktør som ønsker å skape kaos på en taktisk hensiktsmessig måte.

**Logistikkløsninger** for ikke-statlige aktører med lav teknologiadopsjonsvilje vil være tilsvarende lik som dagens situasjon i 2030. Den største endringen er forbundet med additiv tilvirkning som muliggjør at selv *umotiverte* aktører kan produsere utstyr og våpen, inkludert objekter som kan benyttes i terrorangrep eller skjulte operasjoner. Aktørene kan videre komme til å benytte kommersielt tilgjengelige autonome systemer i utvidet grad, både i vann og i luften for å etterforsyne egne styrker eller til transport av illegalt gods. For *hypertrussel-aktører* kan det være aktuelt å benytte autonome transportløsninger i 2030 til egne formål gjennom å manipulere programvaren til systemene. Selv uten manipulasjon, kan autonome kjøretøy eller fartøy tilby anonymitet for logistikkoperasjoner.

Oppsummert vil ikke-statlige aktører innen 2030 effektivt kunne utnytte tilgjengelige samfunnsteknologiske løsninger for å øke sine operative evner. Aktørenes evner og mulighet til kommunikasjon og situasjonsforståelse vil øke i takt med den samfunnsmessige digitaliseringen. Det samme gjelder aktørenes mobilitet og evne til å påvirke flere mål gjennom midler som biologiske våpen eller avanserte cyberangrep. Logistikk vil forenkles ved at autonome systemer og additiv tilvirkning blir mer tilgjengelig. De fremtidige angrepsmulighetene til terrororganisasjoner og opprørsgrupper har en tendens til å fange all oppmerksomhet, men denne gjennomgangen har vist at teknologiske støttefunksjoner vil være vel så avgjørende i et tiårsperspektiv.

## 4.3 Samfunnsutvikling mot 2050

En beskrivelse av hvilke fremvoksende teknologier som kommer til å prege samfunnet i 2050 innebærer en utvidet grad av usikkerhet sammenlignet med 2030-perspektivet. Det eksisterer svært mange ukjente faktorer som kan påvirke hurtighet, retning, og graden av teknologiadopsjon på langsikt. Det er verdt å minne om at denne gjennomgangen må tolkes som et tankeeksperiment for å trekke ut delkonklusjoner om hvordan vi kan forberede oss på en mulig fremtid. I likhet med innledningen til samfunnsbeskrivelsen mot 2030 er det verdt å legge merke til at teknologiadopsjon vil skje ujevn globalt, regionalt, og lokalt.

| Teknologi i samfunnet: 2050 | |
|---|---|
| Kommunikasjon | Avanserte linser for virtuell/blandet virkelighet<br>Omfattende digitalisert verden – hologram<br>Satellitt-internett og neste generasjon trådløst nett |
| Informasjon/nyheter | Nyheter og underholdning i VR/AR<br>Kommunikasjonsnettverk bygd på kvanteteknologi (QKD) |
| Helse/bioteknologi | Utbredt genredigering – samfunnsskiller<br>Utbredt hjerne-maskin-grensesnitt<br>Bioprinting av kroppsdeler/organer |
| Handel og produksjon | Helautonom produksjon – utbredt robotikk<br>Lokal produksjon basert på additiv tilvirkning<br>Avanserte materialer for batterier o.l.<br>Betydelig kommersiell aktivitet i verdensrommet |
| Transport | Autonome kjøretøy og fartøy<br>Romtransport |
| Konsekvenser for samfunnet | Store forandringer i samfunnet<br>Enda større sosioøkonomiske forskjeller<br>Etiske/moralske/filosofiske utfordringer |

*Figur 4.4: Bruksområdene til teknologi i samfunnet mot 2050*

Analyser av fremtiden har ofte overvurdert de kortsiktige konsekvensene av teknologiutviklingen og samtidig undervurdert de langsiktige konsekvensene. Fascinasjonen med atomkraft på 1950-tallet førte til en rekke spådommer om ulike oppfinnelser som skulle bruke denne energikilden. Det samme gjelder datamaskinen og internett.[138] Vi bør likevel være forsiktig med slike historiske sammenligninger. Flere av teknologiområdene vi nå begynner å se konturene av – inkludert kunstig intelligens, autonomi, og gen-redigering – virker å være av en annen art enn tidligere oppfinnelser.

Som AI-forsker Stuart Russell har påpekt, så vil verktøyene som springer ut av disse teknologiene ha evnen til å påvirke, forandre eller erstatte grunnleggende menneskelige egenskaper og karakteristikker på en måte vi aldri har sett før.[139]

[138] Siedensticker, Bob (2006), "Future Hype: Myths of Technological Change", *Berrett-Koehler Publishers, Oakland*.
[139] Russell, Stuart (2020), "Human Compatible: Artificial Intelligence and the problem of control"*, Penguin Books, New York*; Landsend, & al. (2020), "Genome Editing for Soldier Enhancement – trends and implications" – *FFI-notat 20/02378 (Kjeller:FFI).*

***Mellommenneskelig kommunikasjon*** i 2050 vil preges av at befolkningen har omfavnet digitale plattformer på en mer helhetlig måte enn i dag og i 2030. Med blandet-virkelighetsbriller i en innføringsfase fra 2030, vil teknologien modnes innen 2050 og vil kunne føre til en kompleks og overbevisende virtuell opplevelse. Istedenfor briller eller eksterne enheter for utvidet virkelighet, vil man innen 2050 kunne benytte smarte kontaktlinser som gir en sømløs visualisering av det fysiske og digitale.[140] Dette vil også forandre hvordan kommunikasjon foregår. Mobiltelefoner vil for lengst blitt erstattet med kroppsnære systemer eller implantater som kobles til kontaktlinsene, og andre tilpasninger vil øke det allerede flytende grensesnittet mellom menneske, datamaskin og robotikk.[141] Distinksjoner mellom menneske og maskin vil i 2050 være mindre klare.

Godt hjulpet av satellittbasert internett og neste generasjons trådløsteknologi, så vil utvidet eller virtuell virkelighet tilby virtuelle samtaler i form av en avatar eller et hologram. Smarte materialer brukt i ringer eller armbånd vil tilrettelegge for håndbevegelser som kontrollerer valgmulighetene i det digitale rom. Kommunikasjon mellom grupper eller individer vil foregå virtuelt og gjennom kvantenettverk sikret med QKD.

***Informasjon og nyheter*** vil gradvis tilpasse seg de teknologiske mulighetene i samfunnet. Heldigitale virtuelle nyheter der seerne får en 360-graders opplevelse av journalistens reportasje vil være en mulighet i 2050. Underholdningsbransjen vil for lengst ha laget filmer og særlig videospill som fungerer i kombinasjon med denne teknologien. Bruken av heldekkende drakter med berøringsaktivatorer vil være dagligdags. Denne teknologien kan bidra til at man fysisk kjenner vannet når man svømmer i et virtuelt hav og at man blir kjølig av vinden når man forlater vannet på en øde virtuell strand. Slike opplevelser vil tilpasses enhver smak – både til unge og voksne – og kan fort bli avhengighetsskapende. Flere vil velge å tilbringe mye tid i en virtuell verden fremfor den fysiske virkeligheten, og for noen blir det vanskeligere å definere hva som er ekte.

Selv med mindre fysisk bevegelse kan den teknologiske fremgangen innen ***helse- og bioteknologi*** bidra til å holde samfunnet friskere. Genredigering vil være utbredt og vil øke de fysiske og kognitive funksjonene til enkeltindivid og redusere risikoen for genetiske sykdommer. Potensialet eksisterer for å utvikle et sorteringssamfunn som skiller velstående familier som investerer i genmodifiserte barn, fra lavinntektsfamilier som må ta til takke med genmaterialet de har fra naturen. Avanserte biosensorer og midlertidige tatoveringer som sender data om biologiske funksjoner vil bidra til økt forståelse av den menneskelige kroppen. Additiv tilvirkning vil innen 2050 løse utfordringene med bioprinting av kroppsdeler og indre organer, noe som vil kunne erstatte organtransplantasjoner fra donorer. «Myke roboter» basert på nanoteknologi vil bevege seg inn i menneskekroppen som små sensorer eller aktivatorer for å redusere behovet for kompleks kirurgi. Utbredt bruk av hjerne-datamaskin-grensesnitt vil forenkle og utvide menneskelig kontroll over robotikk og andre maskiner.

[140] Stein, Scott (2020), "A single contact lens could give your entire life a head-up display", *CNET*, 24. januar 2020.
[141] Irving, Doug (2021), "Are we ready for the internet of bodies?" *Rand Review*, 8 januar 2021.

Innen ***handel og produksjon*** vil avanserte materialer og robotikk stå sentralt. Flere typer to-dimensjonale materialer kan øke dataprosesseringskraften eller forbedre fremtidige batterier. AI-baserte enheter vil utvikle kunstig intelligens-programvare, godt hjulpet av kvantedatamaskiner som tillater raskere maskinlæring og dataprosessering, på måter som menneskehjernen ikke klarer, og kan nærme seg det som kalles for «artificial general intelligence» (eller AGI).

De fleste roboter vil prestere bedre enn mennesker innen mange områder og oppgaver, noe som vil gi oss mer tid til andre aktiviteter. Additiv tilvirkning kan bli hovedleverandør av mange produkter. Produkter vil kunne bestilles digitalt, lages autonomt i lokale fasiliteter for additiv tilvirkning og bli tilsendt kunden via autonom transport. For noen produkter, vil disse kunne produseres via kundens egne printere. Autonome fabrikker vil ved bruk av additiv tilvirkning produsere roboter som kan bevege seg vekk fra 3D-skriverne for egen maskin.[142]

Autonome systemer vil støtte ytterligere aktivitet i verdensrommet, som vil benyttes av statlige og kommersielle aktører for transport, kommunikasjon og utvinning av råvarer.[143] Dette vil utfordre statlige og globale reguleringer, gitt at Romtraktaten fra 1967 vil være utilstrekkelig for å håndtere de nye utfordringene som kommer med den økte aktiviteten.[144] Motstridende statlige interesser vil kunne forhindre ratifisering av et effektivt og oppdatert rettslig fundament. Kombinasjonen av uklart myndighetsansvar og store verdier vil tiltrekke ikke-statlige aktører som benytter romteknologi fra kommersielle aktører for å få tilgang til både satellitter og gruvedriftsaktivitet på månen eller asteroider.

***Transportsektoren*** vil være totalt forvandlet innen 2050 med utbredt bruk av autonome systemer. Langdistanseskipstrafikk vil være helelektrisk og autonom, og romfart vil ha blitt vanlig. Reiser fra en side av jordkloden til den andre vil kunne gjennomføres i løpet av et par timer via verdensrommet – et begrenset men kostbart tilbud, tilsvarende Concorde-flyene som var i operasjon fra 1976 til 2003. Samtidig vil det være jevnlig kommersiell transport til månen, muligens som en mellomstasjon mot Mars eller andre destinasjoner i solsystemet.

Tilbake på jorden vil mennesker migrere for å unngå, men også utnytte, regionale effekter av klimaendringer. Teknologiske løsninger som kan påvirke atmosfæren for å bremse eller reversere effektene av klimaendring kan være på plass innen 2050.[145] Det vil også kunne eksistere teknologiske løsninger som avanserte avsaltingsanlegg eller fasiliteter for lokal atmosfærisk manipulasjon som kan dempe de verste konsekvensene av klimaendringene. Nye transportmønstre vil for lengst ha etablert seg, særlig rundt de arktiske regioner. Et isfritt Arktisk vil kunne gjøre byer som Kirkenes til sentrale havner for autonom skipstrafikk.

Fremgangen innen mange teknologiområder som i dag er under utvikling, men til dels har en lav modenhetsgrad vil endre samfunnet rundt oss. Noen av disse forandringene vil utfordre dagens

[142] University of California San Diego (2019), "Get up and go bots getting closer", *Iconnect007*, 16. juli 2019.
[143] Aerospace Corp (2020), "Aerospace presents: Pathfinders guide to the space enterprise", *Aerospace.org*, februar 2020.
[144] Bratberg, Kathinka Louise Rinvik (2020), "Militærisering av verdensrommet", *Folk og Forsvar*, 12. januar 2020.
[145] Temple, James (2019), "What is geo-engineering and why should you care", *MIT Technology Review*, august 2019.

måter å tenke på. Tanker om alt fra demokrati, statlig organisering, rådende ideer om arbeid og verdien av enkeltindividet vil kunne være annerledes og i noen tilfeller ikke gjenkjennbart fra dagens situasjon i 2050.

Intelligente maskiner vil utføre langt flere arbeidsoppgaver slik at også kunnskapsbaserte stillinger forsvinner. Hvorvidt teknologisk fremgang vil skape nye arbeidsplasser, som i tidligere generasjoner, er fortsatt usikkert. Dette vil kunne endre samfunnets sosioøkonomiske grupper. Teknologiutviklingen kan dermed tvinge frem strukturelle forandringer som har potensial til å påvirke samfunnet på en såpass grunnleggende måte at det utfordrer oss på et dypere moralfilosofisk plan, og i ytterste konsekvens fører til spørsmål om hva det betyr å være et menneske.

### 4.3.1 Wildcards 2050

Usikkerhetsmomentene øker i både antall og effekt jo lenger inn i fremtiden man forsøker å se. Derfor finnes det mange gode kandidater til rollen som «joker» i denne fremtidsanalysen. Likevel er det to ukjente faktorer som er særdeles interessante og som har potensiale til å forårsake nokså store forandringer i samfunnsbildet som skisseres her.

Den første er de nye kvanteteknologiene – kvantekommunikasjon, kvantedatamaskiner og kvantesensorer. Dette er teknologi som i ulik grad er på terskelen til betydelige gjennombrudd og som på noe sikt vil få banebrytende konsekvenser[146]. For eksempel vil evnen til å prosessere svært mye data på kort tid få betydelige konvergenseffekter og muliggjøre store framskritt innen blant annet kunstig intelligens, robotikk, autonomi og utgjøre en trussel mot dagens asymmetriske krypteringsløsninger. Konsekvensene av kvanteteknologiene vil dermed på sikt være både banebrytende og omfattende, men tidshorisonten og omfanget er inntil videre svært usikkert og tilgjengeligheten kan forbli begrenset en tid, til dels også på grunn av kostnader.

Et annet «wildcard» er knyttet til politiske beslutninger som regulerer bruk og anvendelse av ny teknologi. Som gjennomgangen av samfunnsutviklingen antyder, vil felt som autonomi, kunstig intelligens, robotikk, bioteknologi og digital teknologi få stor innvirkning på samfunnet og individet. Hvordan stater reagerer på disse nyvinningene vil ha mye å si for hvordan det globale samfunnet formes av teknologiutviklingen. Mange av disse teknologiene kan potensielt generere store spenninger i befolkningen dersom utviklingen skjer uten nødvendige reguleringstiltak. Ulike etiske og reguleringstekniske synspunkter på tvers av stater vil gjøre utviklingen av normer og standardisering av regelverk svært utfordrende. I likhet med tiltak mot globale klimaendringer, er noe av utfordringen knyttet til at kostnadene må fordeles og restriksjoner fastsettes før konsekvensene av utviklingen blir åpenbar.[147] Dette øker presset på stater som i utgangspunktet

[146] UK Government Office for Science (2016), "The Quantum Age: technological opportunities", *The UK Government office for science.*

[147] Dette er kjent som *Collingridge's dilemma*: «The dilemma of control may be summarized: attempting to control a technology is difficult and not rarely impossible, because during its early stages, when it can be controlled, not enough can be known about its harmful social consequences to warrant controlling its development; but by the time these consequences are apparent, control has become costly and slow» sitat fra, kapittel 3(ss. 52-70.) i Zaschary S.

er tilbøyelig til å være mer restriktive i bruk av ny teknologi, men som ikke vil miste de økonomiske, strategiske og operative gevinstene som følger med noen av de mer kontroversielle teknologiområdene.

## 4.4 Ikke-statlige aktører mot 2050

Teknologisk fremgang kan påvirke samfunnet på måter som forandrer konfliktlinjene. Statlige samfunnsstrukturer kan lede til skiftende oppfatninger av tilhørighet eller tilknytning, og krav om lojalitet til andre aktører eller stater kan vokse frem. Flere av teknologiene utfordrer eksisterende normer og etiske grenser, noe som kan føre til krav om at forskning og utvikling innen noen områder stanses før konsekvensene av teknologien materialiseres. Teknologidrevne endringer i samfunnet vil føre til nye atferdsmønstre og sårbarheter, samt et nytt grunnlag for verdisetting av aktiva knyttet til digitalisering av samfunnet og kommersialisering av verdensrommet. For aktører som ønsker å skape uro og gjennomføre voldelige handlinger, kan teknologi som finnes i 2050 potensielt gi små grupper og enkeltindivid evner som kan klassifiseres som masseødeleggelsesvåpen.

I likhet med den antatte situasjonen i 2030, vil teknologisk innovasjon i 2050 drives frem hovedsakelig av kommersielle interesser. Dermed vil mye avansert teknologi være tilgjengelig for de fleste ikke-statlige aktører med lav teknologiadopsjonsvilje. Varierende global utvikling vil begrense tilgjengeligheten av de nyeste teknologisatsningene i noen geografiske områder. Det er et kjent fenomen at økonomisk vekst korrelerer med teknologiadopsjon og at stater i den lavere enden av FNs utviklingskala ofte opplever en forsinkelse i omfattende bruk av teknologiske nyvinninger.[148]

Likevel er det rimelig å anta at selv *umotiverte* aktører i 2050 vil ha tilgang til produkter og tjenester i alle deler av verden som tilsvarer den mest avanserte teknologien fra 2030. Det kan også være tilfelle at noen teknologiløsninger – blant annet neste generasjon trådløse dataforbindelser eller autonom transport – vil være såpass innarbeidet i samfunnet at de til en viss grad kan være tilgjengelig selv i konfliktsoner. Ikke-statlige aktører med høy teknologiadopsjonsvilje vil i 2050 fleksibelt og effektivt kunne utnytte seg av mulighetene som finnes i ny og moderne teknologi. Det vil være et suksesskriterium for disse aktørene å følge utviklingen og gradvis tilpasse seg. Det vil være et gjennomgående behov for å holde aktiviteten skjult og den teknologiske signaturen lav – slik at aktøren selv kan avgjøre når de velger å engasjere de militære styrkene til motstanderne sine.

***Kommunikasjon*** mellom gruppemedlemmer vil i 2050 foregå virtuelt og via sikre kvantenettverk. Ved at mesteparten av sosial aktivitet foregår med hjelp av digitale plattformer vil det være lettere selv for *umotiverte* aktører å gjemme seg i digitale folkemengder, og man vil kunne forbli anonym

Davis & Nacht Michael, red. (2018), "Strategic latency: Managing the national and international security consequences of disruptive technologies*", Lawrence Livermore National Laboratory (Livermore, CA: 2018).*

[148] Nobel, Carmen (2012), "How Technology Adoption Affects Global Economies", *Harvard Business School*, 30 juli 2012.

ved å benytte krypteringsløsninger og digitale avatarer. Kommunikasjon vil være lettere for grupper som kan benytte seg av vanlige samfunnstjenester og mer utfordrende for aktører som ikke har denne muligheten. Fremtidens *hypertrussel-aktører*, i form av opprørsgrupper er proxy aktører, kan i 2050 ha økte evner til sikker kommunikasjon og vil benytte digital infrastruktur til både propaganda og hybrid krigføring. Disse aktørene kan ende opp med å tilby egne plattformer, sikre nettverk og sosiale interaksjonsmuligheter som del av deres kommunikasjon og operasjonsplanlegging. Samfunnets bruk av skreddersydde informasjonsbobler vil gi slike aktører økte muligheter til å konkurrere og forme det dominerende narrativ knyttet til konflikter eller hendelser – på den måten kan deres bruk av falske historier og desinformasjon skape reelle utfordringer for statlige militære styrker og sørge for å forme opinionen.

***Informasjonsinnhenting*** vil foregå omtrent på samme måte som situasjonsbeskrivelsen i 2030 med omfattende bruk av åpne kilder. Også aktører med lav teknologiadopsjonsvilje vil evne å utnytte AI-drevne innhentingsplattformer og kan gjennomføre cyberkriminalitet og operasjoner for å lure individer og skaffe seg nyttig informasjon. For aktører med høy adopsjonsvilje vil informasjonsinnhenting henge tett sammen med behovet for å operere skjult, da de fleste sensorer og teknologisk avansert plattformer vil innebære emittering av signaler som kan fanges opp av statlige militære styrker. Det forventes derfor at *hypertrussel-aktører* vil utvikle og belage seg på innhenting med lav signatur som skjuler deres posisjon, bevegelse og kommunikasjonsforbindelse. De vil i så måte gjøre seg avhengig av å kunne manipulere det elektromagnetiske spekteret, eller ved å kunne opptre anonymt i det digitale rom, gjennom elektronisk krigføring og offensive cyberoperasjoner.

Med utviklingen av nanoteknologi og «smart-dust» konsepter som muliggjør store mengder svært små sensorer, kan *hypertrussel-aktører* deployere et distribuert innhentingsnettverk som bidrar til økt situasjonsforståelse over et bestemt geografisk område. I kombinasjon med fremtidens åpne-kilder og avansert AI-drevet analyse vil aktørene i 2050 ha en oversikt over stridsfeltet som i dag er begrenset til statlige aktører.

Som en motreaksjon på statlige evner til deteksjon av teknologisk avanserte innhentingsplattformer kan ikke-statlige aktører komme til å belage seg på «lavteknologi» i et forsøk på å «gå under radaren» til motstanderne. Aktørene kan derfor komme til å avvise teknologiske nyvinninger som kroppslige implantater og tettere grensesnitt mellom menneske og maskin i frykt for at aktiviteten deres skal bli avdekket.

***Mobiliteten*** til *umotiverte* aktører med lav teknologiadopsjonsvilje kan i 2050 bli utfordrende og det kan bli vanskelig å forflytte seg uten å bli oppdaget, siden myndighetenes evne til overvåkning antas å være svært avansert. Utbredt bruk av programvare for ansiktsgjenkjenning og annen overvåkingsteknologi vil derfor skape store utfordringer for *umotiverte* aktører som må belage seg på kommersielle tilgjengelige mottiltak i form av ulik kamuflasje eller forstyrrelser av elektromagnetiske sensorer. Det vil foregå en kontinuerlig kamp mellom «hiders vs. seekers», der «hiders» må være svært oppfinnsomme for å skjule seg. Her kan det forventes at *innovative* aktører vil finne kreative løsninger med de teknologiske løsningene som de har tilgjengelig.

Ved å bruke biosensorer og andre nyvinninger innen helseteknologi, vil fremtidige opprørsgrupper kunne holde soldatene sine friske og veltrente over lengre perioder. Denne type løsninger kan bidra til økt kampkraft, utvidet operasjonell fleksibilitet og evne til bedre mobilitet.[149] Teknologiens forventede tilgjengelighet gjør at også *umotiverte* aktører vil ha disse muligheten i 2050. For *hypertrussel-aktører* vil bruk av genredigering og mulighetene innenfor bioteknologi, bidra til å endre de fysiske attributtene til aktørens enkeltsoldater og på den måten redusere behovet for restitusjon. Dette kan gi aktøren mulighet til å forflytte seg over lengre avstander med tyngre last til fots, slik at mobiliteten til bakkestyrkene utvides sammenlignet med dagens situasjon og 2030-perspektivet.

***Angrepsmulighetene*** til aktører med lav teknologiadopsjonsvilje kan i 2050 være omfattende, selv uten bruk av avansert teknologi. Samfunnet kan ha endret oppfatningen av hva som er verdifullt i fremtiden, på den måten vil også målene til *umotiverte* aktørene justeres sammenlignet med dagens situasjon. Allerede i dag er verdien av metadata høy, og forretningsmodellen til flere virksomheter innebærer å tilby gratistjenester til brukere mot «betaling» i form av brukerdata. Med den omfattende digitale transformasjon som har tatt plass innen 2050, vil digital kriminalitet kunne ta helt nye former. Ulovlig innsamling av store datavolum som kan benyttes som digital valuta kan være en viktig inntektskilde for disse aktørene. Videre vil samfunnets verdsettelse av «avatarer» og digital eiendom være enda mer utbredt i 2050 sammenlignet med dagens situasjon og 2030 – bortføring, utpressing og phishing mot denne type verdier kan således bli et nisjemarked for enkelte *hypertrussel-aktører*.

Angrep vil fortsatt være rettet mot digitaliserte samfunnstjenester, i en økonomi fri for bruk av kontanter. Ved å bevege seg vekk fra fysisk infrastruktur mot det digitale, vil angrep i cyberdomenet ha mer omfattende ringvirkninger. Selv om det i dag er lettere å foreta angrep mot fysisk infrastruktur, er det langt fra sikkert at dette vil fortsette dersom befolkningen i økende grad gjør seg avhengig av aktivitet og tjenester i det digitale domenet. Mindre åpenbare sårbarheter kan fremkomme, eksempelvis et cyberangrep mot digitale plantegninger som benyttes i additiv tilvirkning, som gjør sluttproduktet defekt uten at det er synlig før det tas i bruk. Graden av IKT-sikkerhet vil avgjøre hvorvidt *umotiverte* aktører evner å gjennomføre denne type digitale angrep.

I det fysiske domene vil også aktører med lav teknologiadopsjonsvilje ha tilgang på avansert våpenteknologi, inkludert autonome våpensystemer. Uten evnen eller tilbøyeligheten til å foreta tilpasninger eller manipulasjon av disse systemene, vil *umotiverte* aktører være avhengig av kommersiell tilgjengelig teknologi. Akkurat som i dag vil det i 2050 eksistere aktører som vil selge avansert våpenteknologi videre til slike grupper. Forsvarsindustrien vil innen 2050 kunne levere GNSS-uavhengige autonome dronesvermer utstyrt med eksplosiver og ansiktsgjenkjenningsprogramvare som aktører med lav teknologiadopsjonsvilje kan benytte. Dersom aktørene får tilgang til denne typen systemer, vil dette utgjøre en betydelig trussel for deres motstandere. Nye våpentyper som strålevåpen, enten laservåpen eller en fremtidig versjon

[149] Landsend & al., (2020).

av et EMP-våpen, kan ha blitt mer tilgjengelig innen 2050, graden av behov for tilpasning og kompetanse vil avgjøre hvorvidt aktører med lav teknologiadopsjonsvilje evner å benytte dette.

Angrepsmulighetene til *hypertrussel-aktører* vil i 2050 være svært avansert og kan i noen tilfeller utfordre de statlige aktørene. Den teknologiske utviklingen innen AI, autonomi, romteknologi og bioteknologi vil skape nye avanserte militære systemer og kapabiliteter – dette er løsninger som også kan havne i hendene på enkelte ikke-statlige aktører med høy teknologiadopsjonsvilje, spesielt dersom aktøren har en statlig sponsor og fungerer som en proxy.

Biologiske våpen kan utgjøre en reell trussel mot militære styrker, særlig dersom aktøren selv evner å produserer eget utstyr, biologisk materiale og har tilgang på et sikkert produksjonsområde f.eks. i form av en militærleir. De syntetiske egenskapene til disse stoffene kan gjøre de svært vanskelig å detektere for militære styrker. Disse aktørene kan også komme til å gjennomføre eksperimenter med soldatforbedringsteknologi og genredigering for å øke enkeltsoldatens styrke, utholdenhet eller kognitive evner. Noen *hypertrussel-aktører* kan komme til å benytte modifiserte versjoner av eksoskjellet og forsøk på hjerne-datamaskin grensesnitt for å muliggjøre menneskelig kontroll over robotikk via tankekraft f.eks. i form av. en dronesverm eller en våpenplattform.

*Hypertrussel-aktører* som opprørsgrupper eller proxy-aktører med tilgang på betydelige ressurser kan komme til å satse på en kombinasjon av ubemannede systemer, autonomi, additiv tilvirkning og AI for å oppnå større effekt og intensitet i sine operasjoner og sin krigføring. På denne måten kan aktørene komme til å benytte hjemmeproduserte droner med små effektorer, side og side med større autonome system og konvensjonelle midler. Utviklingen vil føre til at disse aktørene opparbeider seg kapabiliteter på tvers av luft-, sjø- og land- domene. Angrep og operasjoner kan derfor foregå på tvers av domener samtidig. Ved å utnytte mulighetene som finnes i AI vil mye av dette kunne foregå delvis eller helt autonomt slik at den kognitive byrden på enkeltsoldaten reduseres. Ved å ta i bruk ansiktsgjenkjenningsalgoritmer kan slike *hypertrussel-aktører* angripe bestemte individer eller befolkningsgrupper med distinktive ansiktstrekk. Bruk av dronesvermer kan bidra til å sette de større plattformene til statlige aktører ut av drift og redusere motstandernes operative fleksibilitet. Resultatet vil være at disse aktørene kan gjennomføre mer effektive, og presise operasjoner med økt kvantitet og intensitet.

***Logistikken*** til *umotiverte aktører* vil i 2050 være avansert sammenlignet med 2030-perspektivet og inkluderer omfattende bruk av additiv tilvirkning for produksjon av objekter og substanser. For å redusere behovet for anskaffelser og reparasjoner, vil aktørene kunne fremskaffe komplekse reservedeler kun ved innkjøp av råmaterialer – eksempelvis i pulverform – tilpasset denne typen produksjon. Gjennom additiv tilvirkning kan aktørene også produsere nye våpen eller våpendeler som kan testes i kampsituasjoner. Dette vil neppe være en løsning for storskala produksjon, men noe som kan være en erstatning for vanlige forsyningslinjer.

Logistikken til *hypertrussel-aktører* vil være lettere i 2050 ved at de får utvidede muligheter til produksjon og transport av nødvendig utstyr og materiell via additiv tilvirkning og globale transportnettverk. Disse aktørene kan evne å masseprodusere alle delene brukt i en dronesverm,

energetiske eksplosiver samt biologiske og kjemiske våpen. Dette vil redusere behovet for forhåndslagring og gjør at de kan opprettholde en lavere signatur ved at behovet for forflytning av materiell reduseres.

Sett i helhet vil mange av disse potensielle bruksmulighetene representere en markant økning av ikke-statlige aktørers evner. Til tross for usikkerheten som legges til grunn er det likevel plausibelt at noen av teknologiene som nevnes her vil utvikles og tas i bruk både i sivilsamfunnet og blant voldelige ikke-statlige aktører. Det er fortsatt uklart hvordan og hvorvidt kappløpet mellom ikke-statlige kapabiliteter og statlige evner til å oppdage, spore og forhindre angrep vil utarte seg.

# 5 Konsekvenser for militære operasjoner

I løpet av de siste 20 år har Norge vært involvert i en rekke internasjonale militære operasjoner. Felles for disse operasjonene er at den innsatsen Forsvaret har bidratt med i stor grad har vært rettet mot ikke-statlige aktører, primært terrororganisasjoner eller opprørsgrupper. Denne type aktør vil forbli en aktuell motstander for Forsvaret også i fremtiden. Hvem aktørene er, hvor de befinner seg og eventuelt hvem som finansierer dem vil med tid endres. Det samme vil gjelde hva slags midler og teknologi disse aktørene kan komme til å benytte i møte med norske militære styrker. Dette innebærer at etablerte sannheter om hvordan disse motstanderne opererer vil bli utfordret og at måten Forsvaret bekjemper dem på vil endres i takt med utviklingen. Dette vil være tilfellet både for nasjonale operasjoner og i alliansesammenheng.

Beskrivelsene av fremtidig teknologi og ikke-statlige kapabiliteter er spekulative tanke-eksperiment basert på teknologiske trender. Dersom denne øvelsen skal ha ønsket analytisk verdi bør to hovedspørsmål besvares. For det første, hva kan denne analysen fortelle oss om den fremtidige trusselen fra ikke-statlige aktører? For det andre, hva bør norske beslutningstagere gjøre i dag som forberedelser på en slik utvikling?

## 5.1 Den fremtidige trusselen fra ikke-statlige aktører

I nyere tid har voldelige ikke-statlige aktører ofte operert i samfunn med lav grad av teknologisk utvikling. Denne type aktør vil utgjøre en trussel mot norske interesser også i fremtiden, men det er ikke gitt at samfunnet de opererer i vil se likt ut som i dag. Aktører med andre politiske eller ideologiske motiv kan også danne grunnlag for fremtidige militære operasjoner, enten det er radikale miljøaktivister, voldelige motstandere av teknologi, høyreradikale terrorister, eller opprørsgrupper med statlige sponsorer som opererer i et teknologisk avansert samfunn.

Ikke-statlige aktører i 2021 har tilgang på betydelig mer avanserte teknologiske verktøy enn tilsvarende grupper hadde i 1990, særlig når det gjelder teknologi for digital kommunikasjon og overvåking. Som beskrevet i tidligere kapitler har ikke-statlige aktører ofte unnlatt å benytte avansert teknologi. Med et såpass stort spenn i aktørtyper som må inkluderes i en fremtidsanalyse – alt fra kriminelle grupper til proxy-aktører – er det utfordrende å identifisere hvilke grupper som kommer til å være mest relevant eller hva slags tilnærming de vil ha til teknologi. Derfor er det hensiktsmessig med en bred tilnærming til hvilke muligheter og trusler som kan oppstå som følge av fremvoksende teknologi.

***Ikke-statlige aktører med økt innovasjonsevne.*** Den teknologiske utviklingen i samfunnet forventes å fortsette langs de kurvene vi ser i dag. For statlige aktører vil dette innebære utvikling innen svært mange områder. Her vil det kunne oppstå nye sårbarheter. Ikke-statlige aktører med høy teknologiadopsjonsvilje kan utnytte dette og konsentrere seg om bruk av nisjeteknologi som fokuserer på de teknologiske gapene og sårbarhetene som vil eksistere i samfunnet. Teknologiutviklingen vil dermed føre til at innovative ikke-statlige aktører kan komme til å utgjøre en større trussel i fremtiden.

***Ikke-statlige aktører med utvidet operativ evne***. Alle aktørkategoriene, uavhengig av deres interesse for teknologisk innovasjon, vil oppleve forbedret evne til å gjennomføre operasjoner eller angrep på grunn av den generelle teknologiske utviklingen i samfunnet frem mot 2050. Selv om aktører med høy teknologiadopsjonsvilje får økt kapasitet til voldsanvendelse, så vil også aktører med lav vilje oppleve store løft. Dette er særlig tilfelle for områdene informasjonsinnhenting, kommunikasjon og logistikk. Ikke-statlige aktører vil lettere kunne kommunisere, planlegge oppdrag, drive propagandavirksomhet ovenfor sårbare grupper i samfunnet, samt produsere nødvendig utstyr og våpen.

Noen teknologiområder må forventes å være lettere tilgjengelig for ikke-statlige aktører på grunn av deres kommersielle anvendelsesområde og den utbredte bruken i samfunnet. Autonome droner, bioteknologi, og avansert cyberteknologi er blant teknologiområdene som kan ha svært ødeleggende effekt dersom de brukes med voldelige hensikter. Innen noen områder vil ikke-statlige aktører kunne nærme seg statlige evner. Ikke-statlige aktører som evner å drive teknologisk innovasjon på et høyt nivå, vil i noen tilfeller kunne anvende særdeles dødelige våpen med effekter som ligner masseødeleggelsesvåpen.

Informasjonstilgangen til ikke-statlige aktører vil være utvidet betraktelig i 2050 sammenlignet med i dag. Aktørene vil kunne tilegne seg større datamengder av bedre kvalitet via blant annet biometriske sensorer, kommunikasjonsutstyr, tingenes internett og satellittbaserte sensorer. Videre vil nye kommersielt tilgjengelige analyseverktøy bidra til at data lettere kan sveises sammen og danne et bedre situasjonsbilde som aktørene kan benytte i planlegging og gjennomføring av militære operasjoner.

***Flere og nye domener blir tilgjengelig for ikke-statlige aktører***. Teknologisk konvergens øker ikke-statlige aktørers tilgang til teknologi som f.eks. autonome systemer, kunstig intelligens, additiv tilvirkning, nye materialer og batteriteknologi. Utviklingen gjør at disse aktørene fremover vil kunne gjennomføre operasjoner samtidig og på tvers av krigføringsdomener. En fremtidig ikke-statlige aktør forventes å kunne bruke land-, sjø-, luft-, og cyberdomenet på en mer effektiv og måte enn i dag.

Et domene som ikke-statlige aktører i liten grad har benyttet til nå er verdensrommet. Med bakgrunn i den voldsomme kommersielle aktiviteten som pågår forventes det derimot at romdomenet blir stadig viktigere i årene fremover. Dette vil tiltrekke voldelige ikke-statlige aktører som fristes av uklar lovgivning og myndighetsutøvelse. Utfordringen forventes å være større i 2050 enn i 2030.

***Etisk asymmetri.*** Det har alltid vært tilfelle at noen aktører, særlig den svake aktøren i en asymmetrisk konflikt, finner det fordelaktig å benytte uetiske og mindre aksepterte midler og metoder. For noen av teknologiområdene som forventes å bli tilgjengelig i innen 2050, vil etiske og moralske føringer kunne forhindre Forsvaret fra å benytte dem. Dette kan gjelde autonome våpensystem uten tilstrekkelig menneskelige kontroll, soldatforbedring som innebærer genmodifisering av personell, eller biologiske våpen som syntetisk eller modifiserte virus og bakterier som spres i befolkningen. Det vil med bakgrunn i dette kunne oppstå en form for etisk

asymmetri mellom ikke-statlige aktører som er villig til å benytte seg av denne type teknologi, og statlige aktører som bestemmer seg for å ikke utvikle og benytte slike løsninger. I en konflikt der en statlig aktør med bestemte etiske føringer møter en ikke-statlig opprørsgruppe eller proxy-aktør som anvender autonome våpensystem og genmodifiserte soldater, vil den statlige aktøren, fra et taktisk ståsted, kunne være på feil side av asymmetrikalkylen.

***Globaliserte aktører og uberegnelige nettverk.*** Ikke-statlige aktører vil i fremtiden evne å kommunisere seg imellom og utveksle informasjon, ideer og angrepsplaner på en lettere måte enn i dag. Tilgangen på krypterte kommunikasjonsplattformer øker aktørenes operasjonelle sikkerhet og reduserer risikoen for å bli oppdaget av myndighetene. Aktører vil lettere evne å hente inspirasjon fra sammenlignbare grupper, uavhengig av geografisk og kulturell avstand. Ikke-statlige aktører i et område kan komme til å støtte en aktør et annet sted slik at trusselen oppfattes som både global og uberegnelig.

***Ikke-statlige aktører med kvalitative eller kvantitative fortrinn.*** Aktørene vil i fremtiden ha tilgang på kostnadseffektive ubemannede systemer, som kan angripe *en masse* på en koordinert måte. Hver enhet utgjør nødvendigvis ikke en betydelig trussel mot større plattformer som stridsvogner eller fregatter, men den samlede effekten kan være plagsom nok til å redusere effektiviteten og til dels ufarliggjøre denne type kampsystem. På denne måten kan den ikke-statlige aktøren oppnå en kvantitativ fordel.

På lengre sikt vil teknologi som bidrar til fysisk eller kognitiv forbedring av enkeltindividet, bidra til at ikke-statlige aktører kan tilegne seg evner som er overlegen en eventuell motstander som frastår fra å benytte denne teknologien. Dette kan gi en ikke-statlige aktør taktiske fordeler som f.eks. evne til raskere forflytning, økte kognitive evner eller utvidet utholdenhet. Utviklingen kan i så måte lede til et kvalitativt fortrinn.

Disse utviklingstrekkene fører til at den fremtidige trusselen fra ikke-statlige aktører kan beskrives som potensielt mer farlig enn i dag. I militære operasjoner som involverer kontraterrorisme eller opprørsbekjempelse er Forsvaret vant til å operere med stor grad av teknologisk overlegenhet sammenlignet med sine motstandere. Dette vil ikke nødvendigvis være tilfelle i fremtiden. Ikke-statlige aktører kan komme til å anvende teknologiske løsninger som i noen tilfeller vil være like avanserte som materiellet som benyttes av Forsvaret. Ikke-statlige aktører kan være mer kapabel til å forstyrre eller utnytte sårbarheter forbundet med de teknologiske løsningene som norske militære styrker bruker.

## 5.2 Hva bør Forsvaret gjøre?

Å utforme spesifikke råd og anbefalinger basert på fremtidsanalyser er krevende. Vanlige utfordringer med forsvarsplanlegging må tas hensyn til, inkludert strategisk usikkerhet skapt av uoversiktlige geopolitiske forhold, uberegnelige aktører, og økonomisk utvikling. Samtidig preges analysen av den lange tidshorisonten som reduserer dens nøyaktighet. Analysen og anbefalingene alene danner dermed ikke grunnlag for omfattende endringer i Forsvaret, men utgjør en av mange indikatorer som kan benyttes til å fatte beslutninger.

Til tross for usikkerhetsmomentene pekes det på noen tiltak som kan bidra til at Forsvaret vil være bedre rustet til å møte den teknologiske fremtiden og potensielle trusler fra ikke-statlige aktører. Anbefalingene holdes på et overordnet nivå for å ivareta Forsvaret sitt behov for fleksibilitet. Mulige tiltak deles i to hovedkategorier: teknologiske muligheter og organisatoriske tilpasninger.

### 5.2.1 Teknologiske muligheter

Det er naturlig å lete etter teknologiske løsninger som svar på teknologiske utfordringer. For Forsvaret blir det å holde tritt med den teknologiske utviklingen i samfunnet en løpende utfordring. Dersom ikke-statlige aktører ikke har de samme institusjonelle kravene til interoperabilitet og etisk bruk, kan de oppnå en grad av fleksibilitet i sin adopsjon av ny teknologi. Fordi ikke-statlige aktører kan komme til å være mer kapabel i fremtiden og i noen tilfeller kan anvende kapabiliteter på et nivå som ligner statlige aktører, vil de fleste teknologiske mottiltak være verdifulle, også mot en eventuell statlige motstander. Mulige tiltak for å imøtegå den fremtidige ikke-statlige trusselen kan derfor innebære lavere risiko for feilinvestering og økt operativ evne.

***Økt robusthet i samband og sensorteknologi.*** For å motvirke den forventede økningen av ikke-statlige aktørers evner innen digital teknologi og manipulasjon av det elektromagnetiske spekteret, må fremtidens IKT-system og datanettverk ment for sammenkobling av sensorer, våpenplattformer, og personell forsterkes. Samtidig bør teknologi som øker Forsvarets evne til å skille narrekilder fra ekte objekter forbedres. Forsvaret bør prioritere redundans og tilstrekkelige reserveløsninger for kommunikasjon, navigasjon, målsøking, og andre rombaserte kapabiliteter.

***Deteksjon og beskyttelse mot biologiske trusler.*** Utviklingene innen bioteknologi øker risikoen for at farlige og muligens ukjente biologiske stoffer blir brukt i operasjoner av ikke-statlige aktører. Forsvaret bør sørge for evnen til tidlig varsling og deteksjon av nye syntetiske og biologiske stoffer, f.eks. ved bruk av smarte materialer og biosensorer. Mulige mottiltak og behandlingsmuligheter for biologiske våpen bør videreutvikles.

***Satsning på kunstig intelligens.*** Å kunne tolke, bearbeide og forstå den økte mengden data som blir tilgjengelig i fremtiden vil være kritisk for Forsvarets evne til forebygging, deteksjon og koordinert innsats mot fremtidige trusler, uavhengig av aktørens tilhørighet eller teknologiadopsjonsvilje. Kunstig intelligens vil være navet som muliggjør dette og vil utvide Forsvarets analysekapasitet, bidra til økt situasjonsforståelse, raskere kommando- og kontroll og

utnyttelse av morgendagens smarte våpenplattformer. Forsvaret bør derfor prioritere kompetansebygging på dette teknologiområde og sørge for at eksisterende data kan integreres med fremtidige AI-drevne kapabiliteter.

***Mottiltak mot ubemannede systemer.*** Ikke-statlige aktørers bruk av ubemannede og autonome systemer vil utgjøre en betydelig trussel i fremtiden. Systemene utvikles raskt og mottiltak blir stadig utdatert. Forsvaret bør opparbeide seg kunnskap og tilgang til effektive system som kan kontre denne forventede trusselen. Dette vil innebære økte evner til deteksjon og uskadeliggjøring. Forsvaret må blant annet evne å benytte elektromagnetiske og kinetiske angrep, samt kapring av motstanderes dronesvermer med bruk av egne droner eller offensive cyberoperasjoner.

***Etterretning i det digitale domenet.*** Det forventes at fremtidens ikke-statlige aktører i enda større grad vil benytte seg av digital teknologi til kommunikasjon, planlegging, trening samt gjennomføring av cyberoperasjoner mot virksomheter og kritisk infrastruktur. Å kunne spore, overvåke og følge de ikke-statlige aktørene i dette domenet vil derfor forbli kritisk. Forsvaret bør videreutvikle sine evner til digital etterretningsinnhenting, signaturgjenkjenning og attribusjon av ikke-statlige aktørers digitale aktivitet. Utviklingen vil føre til at større deler av Forsvaret må forvente å kunne håndtere motstandere i det digitale domene. Forsvaret bør opparbeide og videreutvikle defensive og offensive digitale kapabiliteter.

### 5.2.2 Organisatoriske tilpasninger

Som organisasjon kan tiltak som ikke direkte omhandler teknologi være vel så viktig. Dersom teknologiområdene diskutert i denne rapporten modnes og utvikles som forventet, vil nye produkter og system dukke opp. En viktig grep vil være å følge denne utviklingen og vurdere eventuelle endringer i motstanderens tilgang.

For Forsvaret vil måten ny teknologi integreres, anvendes og tas i bruk avgjøre ens egne evner til håndteringen av fremtidige trusler. Dette kan innebære utvikling eller oppdatering av eksisterende doktriner, prosedyrer eller strategi.

***Teknologisk kompetanse og ny kunnskap.*** Forsvarets behov for økt og ny kunnskap om teknologi har ved flere anledninger, både innenfor og utenfor forsvarssektoren, blitt løftet frem som et viktig punkt som vil øke og påvirke operative evner.[150] Fremtidig styrkeproduksjon bør ta høyde for hvordan teknologisk utvikling påvirker Forsvarets behov for ny kompetanse. Teknologisk forståelse og innsikt i forventet utvikling vil gi Forsvaret et bedre utgangspunkt for å vurdere fremtidige trusler og effekten av teknologiske tiltak. Behovet for kompetanse vil strekke seg fra det subtaktiske nivået til strategisk nivå og krever dermed en helhetlig innsats på tvers av forsvarsgrenene.

[150] Svendsen, Berit & al. (2020), "Økt evne til å kombinere menneske og teknologi: Veier mot et høyteknologisk forsvar ", *Regjeringen.no.*

***Evne til hurtig teknologiadopsjon.*** Den teknologiske utviklingen vil føre til at ikke-statlige motstandere i fremtiden vil benytte et større utvalg teknologi og at de raskere kan komme til å bytte ut sine kapabiliteter og endre sine operasjonsmønstre. Kjennskap til hvordan trusselaktøren benytter teknologi på stridsfeltet må derfor avgjøre hvilke midler Forsvaret selv benytter. Det er også viktig å erkjenne at det er forskjell på teknologi som skal brukes i en krig mot stater og en krig mot ikke-statlige aktører. Mot ikke-statlige aktører trenger ikke Forsvaret beskytte teknologien mot de mulige mottiltakene en avansert stat har, og kan dermed gå fra ide til innovasjon hurtigere. Forsvaret må evne å tilpasse seg denne utviklingen og raskt integrere og benytte nye løsninger sammen med eksisterende materiell, når trusselen endres.

***Treningsmuligheter med fremvoksende teknologi.*** For å avgjøre den faktiske effekten av ny og fremvoksende teknologi er det avgjørende at Forsvaret tester og eksperimenterer med nye løsninger. Dette vil muliggjøre at Forsvaret raskere blir kjent med ny teknologi og at de lettere kan videreutvikle taktiske og operasjonelle tilpasninger som tar høyde for morgendagens systemer. Forsvaret bør etterstrebe å teste denne nye teknologien både på øvelser og i skarpe oppdrag for å opparbeide seg tilstrekkelig bestillerkompetanse. Eksperimentering vil videre sørge for at Forsvaret bygger tillit til ny teknologi og at de raskere kan vurdere nytteverdien.

Denne formen for *prototypetesting* innebærer at man gradvis integrerer ny teknologi i strukturen, og at man tilpasser operasjonsmønsteret sitt basert på hvor suksessfull teknologien er. På denne måten vil løsninger og teknologi som fortsatt er under utvikling, benyttes side om side med eksisterende materiell.

***Økt bevissthet rundt verdien av egne data***. Forsvaret må ta hensyn til at ikke-statlige aktører gradvis vil få utvidete muligheter og økte evner til innhenting fra nye datastrømmer, deriblant kommersielle og åpne kilder. Aktørene vil i større grad kunne analysere og forstå denne informasjonen ved hjelp av digitale analyseverktøy og AI. For at Forsvaret skal kunne opprettholde sitt behov for sikkerhet og skjerming vil denne utviklingen gjøre det nødvendig å videreutvikle eksisterende retningslinjer knyttet til eget personells bruk av åpne kilder, sosiale medier o.l. Dette kan inkludere alt fra biometriske sensorer, personlig kommunikasjonsutstyr, sosiale medier og andre datarike kilder som kan komme til å gi en potensiell motstander verdifull informasjon om Forsvarets metoder, kapasiteter og personell.

***Forstyrre ikke-statlige aktørers teknologiske adopsjonsmuligheter.*** Ikke-statlige aktørers bruk og adopsjon av ny teknologi vil foregå i faser som ligner adopsjonsmodellen fra kapittel to: tidlig adopsjon, iterasjon, gjennombrudd og konkurranse. For Forsvaret vil det være viktig å være bevisst på dette slik at man planlegger egen utvikling og ivaretar et fortinn. Forsvaret må evne å forstyrre ikke-statlig aktørs adopsjon av ny teknologi for å unngå at perioden med iterasjon og gjennombrudd trekker ut i tid og gir aktørene mulighet til å unytte teknologien. Overvåking og etterretning som ledd i å identifisere endringer i hvordan ikke-statlige aktører bruker teknologi vil være et suksesskriterium og vil løfte Forsvarets evner til å sette gruppene under press. Dersom motstandere adopterer ny teknologi må Forsvaret samtidig evne å hurtig tilpasse seg dette gjennom konsekvensanalyser og utvikling av effektive mottiltak. Dersom man ikke mester dette vil teknologien ikke-statlige aktører benytter kunne overraske og overrumple Forsvaret. Med

bakgrunn i dette må Forsvaret ha innsikt i ikke-statlige aktørers teknologibruk slik at man enten direkte kan forhindre og forebygge adopsjon, eller gjennom utvikling av egne kapabiliteter som indirekte kontrer mulighetene til den ikke-statlige aktøren. På denne måten vil Forsvaret evne å ligge et steg foran teknologiadopsjonsprosessen til sine motstandere.

# 6 Konklusjon

Fremtidsanalyser er usikre. Likevel finnes det momenter og nyanser man allerede i dag ser konturene av som kan gi et oss hint om hvordan morgendagen vil bli. Denne rapporten har sett nærmere på hvordan fremvoksende teknologi i løpet av de kommende 10-30 år vil kunne bli benyttet av ikke-statlige aktører, og ikke minst hvilke konsekvenser dette vil kunne få for militære operasjoner. Målet har vært å tegne et bilde av hvordan fremtiden kan komme til å bli seende ut, basert på det som er tilgjengelig av åpne kilder. Ved å gjøre dette er håpet at rapporten skal bidra til diskusjoner knyttet til den videre utviklingen av Forsvaret. Formålet har ikke vært å komme med nøyaktige prognoser om fremtiden, men å sette i gang tanker og prosesser knyttet til hva utviklingen vil kunne innebære. Rapportens viktigste funn kan oppsummeres på følgende vis:

De særskilte fellestrekkene til ikke-statlige aktører innebærer at teknologisk tilgjengelighet er med på å avgjøre om en aktør vil komme til å anvende ny teknologi eller ikke. Derfor er det viktig at den teknologiske utviklingen i samfunnet tas med i betraktningen når de fremtidige kapabilitetene til ikke-statlige aktører vurderes. Aktører med lav teknologiadopsjonsvilje vil allikevel være mer kapable i et 10-30 års perspektiv enn de er i dag. Aktører med høy teknologiadopsjonsvilje kan forvente å øke sine operative evner betydelig.

Det er utfordrende å indentifisere spesifikke utviklingstrekk og det fremtidige bruksområde til konkrete teknologier. Det samme gjelder hvordan ulike teknologier vil konvergere. Ved å se på den samfunnsmessige dimensjonen beskriver rapporten mulighetene til ikke-statlige aktører i fremtiden. Det forventes at teknologi vil påvirke samfunnet på ulikt vis, men at den største virkningen vil skje innen dimensjonene kommunikasjon, informasjonsdeling, produksjon, helse, og transport.

Teknologien som preger samfunnet i 2030 vil i stor grad bestå av mer utviklede versjoner av teknologi som allerede eksisterer. Derimot forventes det at samfunnet innen 2050 har adoptert teknologi som i dag er helt eller delvis ukjent. Trender innen digital teknologi vil fortsette, både i et 10 og 30 års- perspektiv, noe som vil bidra til fremvekst av nyvinninger innen kommunikasjon og informasjonsteknologi. Det digitale domene vil bli tilnærmet like viktig for menneskelig sosial interaksjon som det fysiske.

Oppfinnelser innen bioteknologi preger allerede samfunnet vårt i dag. Dette vil øke i omfang, spesielt i forbindelse med genredigering og fremvekst av nye grensesnitt mellom menneske og maskin. Effektene av den pågående utviklingen i kommersiell romfart vil bli mer synlig. I første omgang vil dette resultere i nye globale nettverk og avanserte sensorsystem. Innen 2050 vil utviklingen kunne innebære romturisme, gruvedrift og raskere transport. Autonome system for produksjon og transport vil være viktig allerede i 2030, men vil ha enda større samfunnsmessig innvirkning i 2050.

Ikke-statlige aktører vil få utvidede muligheter til kryptert kommunikasjon. Kunstig intelligens vil gi aktørene mulighet til å bearbeide og analysere store datasett og utvider deres situasjonsforståelse. Denne teknologien kan også benyttes til vinningskriminalitet samt trening

og øvelse. Additiv tilvirkning vil muliggjøre produksjon av usporbare våpen og spesialtilpasset utstyr. ikke-statlige aktører med høy teknologiadopsjonsvilje vil kunne benytte avanserte cyberkapabiliteter, de vil kunne innhente informasjon fra sensorer tilknyttet Tingenes internett og rombaserte tjenester, utvikle biologiske våpen, anvende autonome våpensystem, manipulere det elektromagnetiske spekteret, og gjennomføre angrep mot rombasert infrastruktur.

Dette er utviklingstrekk som vil påvirke Forsvarets mulighet til gjennomføring av operasjoner. I noen tilfeller kan ikke-statlige aktører ha evner på høyde med statlige aktører. Dette er særlig tilfelle for teknologi som autonome systemer, biologiske trusler eller avanserte cyberkapabiliteter. Ikke-statlige aktører vil med bruk av slik teknologi kunne operere på tvers av krigføringsdomenene. Teknologi som utfordrer juridiske og etiske vurderinger kan gi ikke-statlige aktører nye muligheter.

Betraktninger av denne typen tilkjennegir et behov for videre forskning og analyse knyttet til flere av de diskuterte problemstillingene og foreslåtte tiltakene. Teknologien og de mulige bruksområdene som har blitt diskutert er ikke uttømmende og vil bli beriket dersom flere teknologiske detaljer inkluderes. Videre vil det være behov for å se nærmere på hvordan teknologisk utvikling påvirker statlige aktører og hvilke konsekvenser dette har for Forsvaret og fremtidens operasjonsmiljø. Dette er problemstillinger som vil bli belyst i det videre arbeidet til TEKNO-prosjektet.

# Referanser

For kilder og referanser som er fritt tilgjengelig på internett, er klikkbare lenker inkludert i alle referansene. Alle lenker ble besøkt og var fungerende per mai 2021.

**Bøker og bokkapitler**


Barno, David & Bensehel, Nora (2020), "Adaptation under fire: How militaries change in wartime", *Oxford University Press*.

Creveld, Martin van (1989), "Technology and war: From 2000 BC to the present*", Free Press*, New York.

Cronin, Audry Kurth (2020), *"Power to the People: How open technological innovation is empowering tomorrow's terrorists", Oxford: Oxford University Press*.

Davis, Zaschary S. & Nacht, Michael (2018), "Strategic latency: Managing the national and international security consequences of disruptive technologies*"*, *Lawrence Livermore National Laboratory*, Livermore, CA.

Dolnik, Adam (2007), "Understanding terrorist innovation: Technology, tactics and global trends"*, Routledge*, London.

Hatlebrekke, Kjetil Anders (2019), "The problem of secret intelligence", *Edinburgh University Press.*

Heuer, Richards. J. Jr & Pherson, Randolph H. (2008), "Structured analytic techniques for intelligence analysis"*, CQ Press.*

Kilcullen, David (2005), "Counterinsurgency", *Oxford: Oxford University Press*

Lynch, Thomas F III (red.), (2021), "Strategic assessment 2020 – into a new era of great power competition", *National defense university Press.*

McCullough, David (1978), "The path between the seas", *Simon & Schuster*, New York.

NATO (2019), NATO glossary of terms and definitions, *NATO AAP-06:2019.*

Russell, Stuart (2020), "Human Compatible: Artificial Intelligence and the problem of control*"*, *Penguin Books,* New York.

Schwab, Klaus (2015), "The fourth industrial revolution: What it means and how to respond", *Foreign Affairs*.

Siedensticker, Bob (2006), "Future Hype: Myths of Technological Change", *Berrett-Koehler Publishers*, Oakland CA.

Wittes, Benjamin & Blum, Gabrielle (2015), “The future of violence”, *Basic Books*, New York.

**Forskningsartikler, rapporter, fremtidsstudier og kronikker**

Allen, T.S., Brown, Kyle & Askonas, Jonathan (2020), “How the Army out-innovated the Islamic States drones”, *War on the Rocks*.

American Bar Association (2019), “The legal framework regulating proxy warfare”, *American Bar Association’s Center for Human Rights & Rule of Law Initiative.*

Andås, Harald (2020), "Emerging technology trends for defense and security", *FFI-rapport 20/01050* (Kjeller: FFI).

Bajema, Natasha & DiEuliis, Diane (2017), “Peril and promise: Emerging technologies and WMD”, *National Defense University Press*, Washington DC.

Beadle Alexander William (2016), "Å forske på Forsvaret i fremtiden: muligheter, begrensninger og kognitive fallgruver"*, FFI-rapport 16/01810* (Kjeller: FFI).

Beadle, Alexander William, Diesen, Sverre, Nyhamar, Tore, & Bostad, Eline Knarrum (2019), "Globale trender mot 2040 – Et oppdatert fremtidsbilde"*, FFI-rapport 19/00045* (Kjeller: FFI).

Berruti, Frederico, Nel, Pieter & Whiteman, Rob (2020), “An executive primer on artificial general intelligence”, *McKinsey*, 29. april 2020.

Bruvoll Solveig et al. (2019), “Den autonome framtid“, *FFI Viten 19/00906* (Kjeller: FFI).

Caldwell, M., Andrews, J.T.A., Tanay, T. *et al.* (2020), “AI-enabled future crime”. *Crime Science Vol* 9:14.

Cronin, Audrey Kurth (2015), “ISIS is not a terrorist group”, *Foreign Affairs*, 2015-02-18.

Cornish, Paul (2010), “Technology, strategy and counterterrorism”, *International Affairs* 86:4 pp. 875-888.

DeVore, Marc R. (2012), “Exploring the Iran-Hezbollah relationship: A case study of how state sponsorship affects terror group decision-making”, *Perspectives on terrorism* vol. 6:4-5 pp. 85-107.

Diesen, Sverre (2018), "Lavintensivt hybridangrep på Norge i en fremtidig konflikt"*, FFI-rapport 18/00080* (Kjeller: FFI).

European Commission (2019), “100 radical innovation breakthroughs for the future”, *Directorate General for Research and Innovation.*

EUROPOL (2017), “Crime in the age of technology”, *Europol: EDOC# 924156 v7,* The Hauge.

Fey, Marco (2017), "3D printing and international security: *PRIF report no. 144", Peace Research Institute Frankfurt*.

Fiegel, Brenda (2017), "Narco-drones: A new way to transport drugs", *Small Wars Journal* 5. juli 2017

Flathagen, Joakim et.al (2016), "Additiv produksjon av prototyper og reservedeler i felt"*, FFI-rapport 16/01008* (Kjeller: FFI).

Forsvarsstaben (2019), "Forsvarets fellesoperative doktrine"*, Oslo: Forsvaret*.

Fox, Amos (2019), "Conflict and the need for a theory of proxy warfare", *Journal of Strategic Security vol. 12:3 pp. 44-71.*

Freund, Caroline, Mulabdic, Alen & Ruta, Michele (2019), "Is 3D Printing a Threat to Global Trade? The Trade Effects You Didn't Hear About", *Policy research working paper 9024*, *World Bank Group*.

Frinking, Erik et al. (2016), "The increasing threat of biological weapons": *Hague Center for Strategic Studies*, The Hague.

Gabriel, Rachel & Koven, Barnett (2018), "Malicious non-state actors and contested space operations", *National Consortium for the Study of Terrorism and Responses to Terrorism (START).*

Gartenstein-Ross, Daveed, Shear, Matt & Jones, David (2019), "Virtual plotters. Drones. Weaponised AI?: Violent non-state actors as deadly early adopters*"*, *Valens Global,* Washington DC.

Ghafur, S., Kristensen, S., Honeyford, K. *et al. (2019),* "A retrospective impact analysis of the WannaCry cyberattack on the NHS", *Digital Medicine* 2**,** 98 (2019).

Gill, Paul, Horgan, John, Hunter, Samuel T. & Chushenbery, Lily D. (2003), "Malevolent creativity in terrorist organizations", *Journal of Creative Behavior*, *vol. 47:2 (2003), ss. 125-151.*

Grabosky, Peter (2007), "The internet, technology, and organized crime", *Asian Criminology Vol 2: pp 145-161*

Graham Robert (2016), "How terrorists use encryption", *CTC Sentinal vol 9:6 pp. 20-25.*

Grimstvedt, Eirik Skjelbreid, et. al, (2015), "LINE EW-UAS: an experimental unmanned system for coastal surveillance using ESM technology." *FFI-Rapport 15/02442* (Kjeller: FFI).

Harrison, Seth (2018), "Evolving tech, evolving terror", *New Perspectives in Foreign Policy*, *vol 15, Center for Strategic and International Studies*, Washington DC.

Horgan, John (2020), "Will Artificial Intelligence Ever Live Up to Its Hype? ", *Scientific American*, *4. December 2020.*

Hummel, Stephen & Burpo, John F. (2020), "Small groups, big weapons: The nexus of emerging technologies and weapons of mass destruction", *West Point: United States Military Academy*.

Hwang, Tim (2020), "Deep fakes: A grounded threat assessment", *Center for Security and Emerging Technology*, *Georgetown University,* Washington DC.

Ilachinski, Andrew (2017), "AI, Robots, and Swarms: Issues, Questions, and Recommended Studies", *CNA analysis & Solutions,* Alexandria VA: CAN.

Independent Working Group (2009), "Missile Defense, the Space Relationship, & the Twenty-First Century", *Institute for Foreign Policy Analysis*, Cambridge, MA

Irving, Doug (2021), "Are we ready for the internet of bodies?" *Rand Review, 8 januar 2021.*

Jackson, Brian A., John C. Baker, Kim Cragin, John Parachini, Horacio R. Trujillo, and Peter Chalk. (2005), "Aptitude for Destruction, Volume 1: Organizational Learning in Terrorist Groups and Its Implications for Combating Terrorism", *Rand Corporation,* Santa Monica CA.

Jackson, Brian A. & Frelinger, David R (2008), "Rifling through the terrorists arsenal: Exploring groups' weapon choices and technology strategies", *Studies in Conflict and Terrorism Vol. 31 pp. 583-604.*

Johnston, Nicolas (2018), "Defining terrorism and insurgency: Beyond morality", *Small Wars Journal.*

Johnston, Trevor, Smith, Troy D. & Irwin, Luke J. (2018), "Additive Manufacturing in 2040 ", *Rand Corporation, Santa Monica.*

Kallenborn, Zachary (2020), "In defense of WMD: A war of words and the challenge of swarms", *War on the Rocks*.

Kaloudi, Nektaria & Li, Jingyue (2020), "The AI-Based Cyber Threat Landscape: A Survey". *ACM Computing Surveys* 53, 1.

Lakomy Miron (2017), "Cracks in the Online "Caliphate": How the Islamic State is Losing Ground in the Battle for Cyberspace", *Perspectives on Terrorism*, *vol. 11:3.*

Leukfeldt, E. Rutger, Kleemans, Edward R., Kruisbergen, Edwin W. & Roks, Robert A (2019), "Criminal networks in a digitized world: on the nexus of borderless opportunities and local embeddedness", T*rends Organ Crim* 22**,** 324–345, Rotterdam.

Livingston, David & Lewis, Patricia (2016), "Space: The final frontier for cybersecurity?", *Chatham House*.

Mayer, Michael (2020), "Methodologies for technology forecasting – a framework for the TEKNO project", *FFI-notat 20/1243*, (Kjeller: FFI).

Mumford, Andrew (2013), "Proxy warfare and the future of conflict", *RUSI Journal, april/mai vol. 158(2).*

Monsen, Ingunn Helene Landsend, Glenna, Susanne & Rjaanes, Mats (2020), "Genome Editing for Soldier Enhancement – trends and implications*", FFI-notat 20/02378* (Kjeller: FFI).

National Security Commission on AI (2019), "Interim report", *NSCAI*, *November 2019*.

Paul, Christopher & Posard, Marek (2020), "AI and the manufacturing of reality", *RAND Corporation*.

Perl, Peter (2019), "What is the future of truth?", *Pew Research*.

PST (2021), "Nasjonal trusselvurdering 2021", *Politiets sikkerhetstjeneste.*

Qureshi, Zia (2020), "Inequality in the digital era", *Brookings Institution*, *14 Februar 2020*.

Rapoport, David C. (2001), "The fourth wave: September 11 in the history of terrorism", *Current History*: 100 (650): 419-424.

Reding D.F. & Eaton, J. (2020), *"Science and technology trends 2020-2040: Exploring the S&T Edge"*, *NATO Science and Technology Organization*, Brussels.

Reinsel, David, Gantz, John & Rydning, John (2018), "The Digitization of the World From Edge to Core", *IDC White Paper*.

Richbourg, Richard (2018), "'It's either a panda or a gibbon: AI winters and the limits of deep learning", *War on the Rocks*.

Roser, Max, Ortiz-Ospina, Esteban & Ritchie, Hannah (2019), "Life expectancy" *Our world in data*, *University of Oxford*.

Sellevåg, Stig Rune et.al, (2020), "Samfunnssikkerhet mot 2030 – Utviklingstrekk". *FFI-rapport 20/00530* (Kjeller: FFI).

Singer, Peter.W (2012), "The cyber terror bogeyman", *Brookings*, *1. November*

Stanford University (2016), "Artificial Intelligence and life in 2030: One hundred year study on artificial intelligence", *Stanford University.*

Stanford University (2019), "The 2019 AI Index report", *Stanford Center for Human-centered Intelligence*.

Svendsen, Berit et. al. (2020), "Økt evne til å kombinere menneske og teknologi: Veier mot et høyteknologisk forsvar ", *Regjeringen.no*

Svendsen, Jahn Arvid (2009), "Forsvaret og private militære firmaer"*, Institutt for forsvarsstudier* (Oslo).

Tønnessen, Truls Hallberg (2017), "Islamic state and technology – A literature review" *Perspectives on Terrorism 11:6 pp. 101-111*.

UK Government Office for Science (2016), "The Quantum Age: technological opportunities*", The UK Government, Office for Science.*

United States Army (2016), "Field manual FM 3-24 Counterinsurgency", *US Army.*

Urcosta, Ridvan Bari (2020), "Drones in the Nagorno-Karabakh", *Small Wars Journal*.

Vatne, Dagfinn Furnes, Køber, Petter Kristian, Guttlevik, Mona Sagsveen, Arnfinnsson, Brynjar & Rise, Ørjan Rogne (2020), "Norwegian long-term defence analysis – a scenario and capability-based approach", *FFI-rapport 20/02367* (Kjeller: FFI).

West, Darrell M. (2018), "Will robots and AI take your job? The economic and political consequences of automation", *Brookings Institution*, 18. april 2018.

Wilson, Clay (2018), "Avatars, Virtual Reality Technology, and the U.S. Military: Emerging Policy Issues*"*, *Congressional Research Service*, Washington D.C.

Østensen, Åse Gilje & Bukkvoll,Tor (2018), "Russian use of private military and security companies – the implications for European and Norwegian security", *FFI rapport 18/01300* (Kjeller: FFI).

**Nyhetsartikler, intervjuer, pressemeldinger og taler**

Aerospace Corp (2020), "Aerospace presents: Pathfinders guide to the space enterprise", *Aerospace.org, Februar 2020*.

Akerman, Spencer (2012), "I got blasted by the Pentagon's pain ray: twice", *Wired, 12. Mars 2012*.

Alayboubi, Mohammed & Jentoft, Morten (2020), "De dreper for barna sine", *NRK Nyheter*, 25. oktober 2020.

Allison, Peter Ray (2020), "The UK's quest for affordable fusion by 2040", *BBC Future*, 15. desember 2020.

BBC (2017), "Drone collisions 'worse than bird strikes for planes'", *BBC News*, 5. desember 2017.

Beene, Ryan (2020), "Electrical Tape on Sign Fooled a Tesla Into Speeding in Test", *Bloomberg*, 19. februar 2020.

Benowitz, Brittany & Ross, Tommy (2020), "Time to get a handle on America's conduct of proxy warfare", *Lawfareblog*, 9. april 2020.

Bezhan, Frud (2020), "US vacuum: How Libya is descending into a Russia-Turkey proxy war", *RadioFreeEurope/Radio Liberty*, 21. januar 2020.

Bold, Michael (2018), "Very small satellites, very big deal", *Army AL&T Magazine,* January-March 2018.

Bower, Joseph L. & Christensen, Clayton (1995), "Disruptive technologies; catching the wave", *Harvard Business Review*., January-February 1995.

Braaten, Frøydis (2016), "Sykepleiere vandrer rundt på sykehuset - før det er bygget", *Aftenposten*, 27. januar 2016.

Bratberg, Kathinka Louise Rinvik (2020), "Militarisering av verdensrommet", *Folk og Forsvar*, 12. januar 2020.

Bredesen, Maren Garberg & Reichborn-Kjennerud, Erik (2016), "Hybrid krigføring– hva er det?", *NUPI – Hvor hender det* nr. 7, 14. mars 2016.

Calderone, Julia (2015), "Scientists have developed a super-thin, skin-like invisibility cloak", *Business Insider*, 18. september 2015.

Chen, Sophia (2017), "Tiny, Laser-Beaming Satellites Could Communicate With Mars", *Wired*, 10. juli 2017.

Condon, Stephanie (2020), "Facebook previews smart glasses and the future of work in VR", *ZDNet*, 16. September 2020.

Dahal, Sahas (2016), "Printing the future: 3D bioprinters and their uses", *Medium*, 29. februar 2016.

Dzieza, Josh (2020), "How hard will the robots make us work?" *The Verge*, 27. februar 2020.

Facebook *(*2020*)*, "Announcing project Aria: a research project on the future of wearable AR", *Tech@facebook*,16. september 2020.

Fedortov, Yury (2017), "In Just Two Decades, Technology Has Become A Cornerstone Of Criminality", *United Nations Office on Drugs and Crime*, 23. oktober 2017**.**

Frantzman, Seth J. (2020), "Libya is now the Middle East's most important proxy war", *The Spectator*, 20. mai 2020.

Garfield, Leanna (2016), "Scientists just got closer to creating a real-life 'invisibility cloak'", *Business Insider*, 16. mars 2016.

Goodman, Marc (2015), "How Terrorists Are Turning Robots Into Weapons", *DefenseOne*, 16. april 2015.

Greenberg, Andy (2016), "Tesla Responds to Chinese Hack With a Major Security Upgrade", *Wired*, 27. september 2016.

Greenberg, Andy (2020), "The FBI Says 'Boogaloo' Extremists Bought 3D-Printed Machine Gun Parts", *Wired*, 4. november 2020.

Hairsine, Kate (2019), "Is Africa ready for 5G?", *Deutsche Welle*, 29. november 2019.

Helse Nord-Trøndelag (2019), "Styrker pasientsikkerheten med VR-teknologi", *hnt.no*, 8. oktober 2019.

iGEM Foundation (2020), "International Genetically Engineered Machine", *igem.org*, 4. juni 2020.

Isaacson, Walter (2020), "I was part of a trial for Pfizer's covid-19 vaccine. It's a miracle for genetic medicine", *The Washington Post*, 9. november 2020.

Izadi, Elahe & Farhi, Paul (2021), "Bellingcat breaks stories that newsrooms envy — using methods newsrooms avoid", *The Washington Post*, 9. januar 2021.

Jill, Stuart, (2015), "Comment: Satellite industry must invest in cyber security", *Financial Times,* 10 april 2015.

Johnson, Dexter (2020), "With 5G Rollout Lagging, Research Looks Ahead to 6G", *IEEE Spectrum*, 29. juli 2020.

Jones, Harry W. (2018), "The recent large reduction in space launch cost", *48th International Conference on Environmental Systems,* 8-12 July, Albuquerque, New Mexico.

Katwala, Amit (2018), "A graphene breakthrough hints at the future of battery power", *Wired*, 16 august 2018.

Koerner, Brendan I. (2014), "Inside the New Arms Race to Control Bandwidth on the Battlefield", *Wired*, 18. februar 2014.

Lewis-Kraus, Gideon (2016), "The Great AI Awakening", *The New York Times Magazine*, 14. desember 2016**.**

Lin, Jeffery, Singer, P. W. & Costello, John (2016), "China's Quantum Satellite Could Change Cryptography Forever", Popular Science, Mars 3 2016

Manea, Octavian (2020), "The Need to Compete on Multiple Battlegrounds: An Interview with Lt. Gen. H.R. McMaster", *Small Wars Journal*, 17. november 2020.

Marr, Bernard (2020), "How Are Digital Twins Used In Practice: 5 Real-World Examples Beyond Manufacturing", *Forbes*, 28. August 2020.

Mayfield, Mandy (2020), "Air Force Wants Lasers on Fighter Jets by 2025", *National DEFENSE*, 9. november 2020.

Nobel, Carmen (2012), "How Technology Adoption Affects Global Economies", *Harvard Business School*, 30. juli 2012.

O'Neal, Bridgett (2014), "Authorities Bust European Crime Network Taking Advantage of 3D Printing Technology for Credit Card Fraud", *3dprint.com*, 6. oktober 2014.

Planet Labs Inc. (2021), "Using space to help life on earth", *planets.com,* 5 mai 2021.

Ravindran, Sandeep (2020), "How DIY technologies are democratizing science", *nature,*, 17. november 2020.

Reuters *(2010)*, "U.S. successfully tests airborne laser on missile", *Reuters*, 12. februar 2010.

Roblin, Sebastien (2020), "What Open Source Evidence Tells Us About The Nagorno-Karabakh War", *Forbes*, 23. oktober 2020.

Rogoway, Tyler (2016), "This Bird Strike Reminds Us it Doesn't Take a Missile to Down a Fighter", *The Drive*, 7. november 2016.

Saghavan, Sudarsan (2020), "As military power shifts in Libya, Turkey and Russia control country's fate", *The Washington Post*, 23. mai 2020

Shubsda, Brian (2019), "SOCOM Must Tie Operational Data to Virtual Reality Training", *National DEFENSE*, 2. mai 2019.

Stein, Scott (2020), "A single contact lens could give your entire life a head-up display", *CNET*, 24. januar 2020.

Sterling, Amy (2019), "Millions Of Jobs Have Been Lost To Automation. Economists Weigh In On What To Do About It", *Forbes*, 15. juni 2019.

Stuart, Jill (2015), "Comment: Satellite industry must invest in cyber security", *Financial Times*, 10. april 2015.

Sutton, H.I. (2020), "Rare Electric Narco Submarine Seized in Colombia", *US Naval Institute News, 16. november.*

Szczerba, Robert J. (2015), "15 Worst Tech Predictions Of All Time" *Forbes*, 5. Januar 2015.

Temple, James (2019), "What is geo-engineering and why should you care", *MIT Technology Review*, august 2019.

Thales Group (2021), “Facial recognition: top 7 trends (tech, vendors, markets, use cases & latest news)”, *thalesgroup.com*, 30. mars 2021.

The Week *Magazine (2018)*, “Hiding from infrared cameras is now possible”, *theweek.in*, 10. desember 2018.

Thomas, Elise (2019), “How to hack your face to dodge the rise of facial recognition tech”, *Wired*, 1. februar 2019.

Trevithick, Joseph (2018), “Russia Offers New Details About Syrian Mass Drone Attack, Now Implies Ukrainian Connection” *The Drive*. 11. januar 2018.

Tsanni, Abdullahi (2020), “African scientists leverage open hardware”, *nature*, 1. juni 2020.

Tucker, Patrick (2018), “A Criminal Gang Used a Drone Swarm To Obstruct an FBI Hostage Raid”, *DefenseOne*, 3. mai 2018.

University of California San Diego (2019), “Get Up and Go Bots Getting Closer”, *IConnect007*, 16. juli 2019.

Veløy, Chris (2019), “Vil la folk velge hvilken art de vil være”, *NRK.no 18 Juni 2019*

Voros, Joseph (2001), “A primer on Futures Studies, Foresight and the Use of Scenarios”, *Foresight bulletin*, desember 2001.

Wall, Mike (2020), “What's next after the International Space Station? Plans afoot for more off-Earth outposts”, *Space.com*, 3. november 2020.

Yount, Jordan (2020), “New Cloaking Material Could Protect Buildings, Soldiers”, *University of Missouri College of Engineering*, 21. mai 2020.

## About FFI

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

### FFI's MISSION

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

### FFI's VISION

FFI turns knowledge and ideas into an efficient defence.

### FFI's CHARACTERISTICS

Creative, daring, broad-minded and responsible.

## Om FFI

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

### FFIs FORMÅL

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

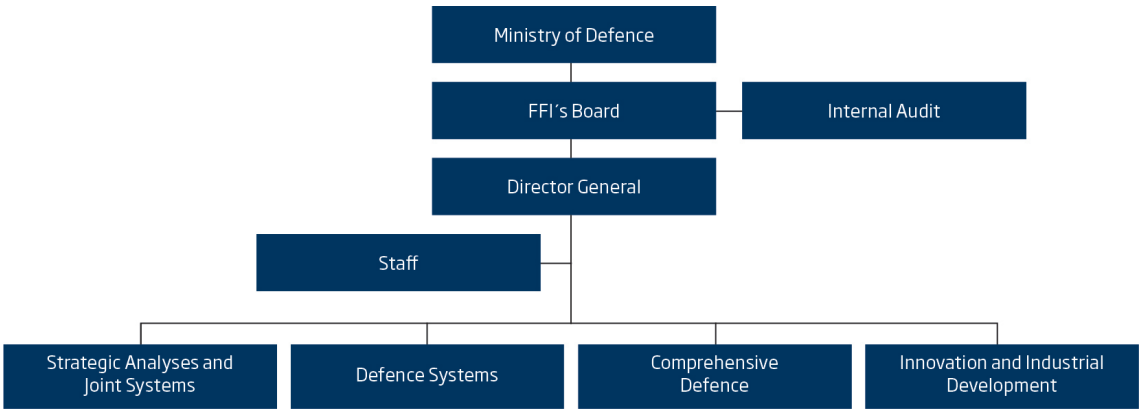
### FFIs VISJON

FFI gjør kunnskap og ideer til et effektivt forsvar.

### FFIs VERDIER

Skapende, drivende, vidsynt og ansvarlig.

## FFI's organisation



**Forsvarets forskningsinstitutt**
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

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

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

Office address:
Instituttveien 20
N-2007 Kjeller

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

FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment