FFI Forsvarets forskningsinstitutt

23/00879

FFI-RAPPORT

Teknologiske og samfunnsmessige utviklingstrekk av betydning for nasjonale sikkerhetsinteresser i et 2030-perspektiv

Karina Barnholt Klepper
Ole Ingar Bentstuen
Arild Bergh
Torgeir Broen
Torbjørn Kveberg
Petter Y. Lindgren
Eskil Sivertsen
Øyvind Sjøvik
Knut Svenes
Kristin Waage
Ronny Windvik

Teknologiske og samfunnsmessige utviklingstrekk av betydning for nasjonale sikkerhetsinteresser i et 2030-perspektiv

Karina Barnholt Klepper
Ole Ingar Bentstuen
Arild Bergh
Torgeir Broen
Torbjørn Kveberg
Petter Y. Lindgren
Eskil Sivertsen
Øyvind Sjøvik
Knut Svenes
Kristin Waage
Ronny Windvik

Forsvarets forskningsinstitutt (FFI) 9. mai 2023

Emneord
Nasjonal sikkerhet
Samfunn og sikkerhet
Trusler
Teknologisk utvikling
Klimaendringer
Hybridkrigføring

FFI-rapport
23/00879

Prosjektnummer
5807

Elektronisk ISBN
978-82-464-3470-4

Engelsk tittel
Technological and societal developments of importance for national security interests towards 2030

Godkjennere
Stig Rune Sellevåg, *forskningsleder*
Janet M. Blatny, *forskningsdirektør*

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Sammendrag

Nasjonal sikkerhetsmyndighet (NSM) har gitt Forsvarets forskningsinstitutt (FFI) i oppdrag å belyse teknologiske og samfunnsmessige utviklingstrekk av særskilt betydning for nasjonal sikkerhet. Dette skal bidra til utdypende kunnskap for NSMs sikkerhetsfaglige råd for 2025-2028. Rapporten tar opp forventet utvikling innenfor teknologi, klima og energisikkerhet og sammensatte trusler i et 2030-perspektiv, og hva dette kan bety for nasjonale sikkerhetsinteresser.

Utviklingen av 5G har mye å si for stordata, kunstig intelligens og elektroniske kommunikasjonstjenester (EKOM). 5G vil danne basis for de aller fleste kommunikasjonstjenester. Det betyr mye for våre nasjonale sikkerhetsinteresser fram mot 2030. 5G vil få andre og nye sårbarheter sammenliknet med tidligere generasjoner. NATO forventer at kvanteteknologiske produkter vil ha operativ nytte om 5-15 år. Dette medfører store endringer for militære og sivile systemer innenfor autonomi, sensorer for etterretning, overvåkning og målfatning, kommunikasjon/krypto og dataprosessering (kvantedatamaskiner). Forsvarets og sivilsamfunnets sentrale kapabiliteter og kapasiteter må utvikles basert på dette.

Klimaendringer en av de største utfordringene samfunnet står overfor. Variable energikilder, økt ekstremvær, automatisering, transnasjonale avhengigheter og økt potensiale for cyberhendelser og kaskadefeil øker kompleksiteten i energisystemet. Det kan gi økt sårbarhet, redusert pålitelighet og motstandsdyktighet i systemet. Hyppigere, langvarige strømbrudd og bortfall av samfunnskritiske tjenester over store områder er en risiko.

Samfunnet blir mer avhengig av rombaserte tjenester. Stadig bedre tjenester utvikles innen kommunikasjon, observasjon og etterretning som følge av romvirksomheten. Militært tap av satellittkommunikasjon kan føre til degradering av kommando og kontroll og distribusjon av etterretningsinformasjon. Sivilt tap kan føre til bortfall av mange samfunnskritiske tjenester.

Digitalisering av samfunnet øker angrepsflaten for datakriminalitet og offensive cyberoperasjoner. Digital sikkerhet må derfor inkludere norm- og sanksjonsarbeid, økt vekt på personellsikkerhet, kontinuerlig utvikling av maskinlæringsteknikker for deteksjon og kommunikasjon rundt egne cyberkapasiteter.

Digitalisering, internett og sosiale medier har gitt nye muligheter og større effekt av påvirkningsoperasjoner med lav risiko. Forebygging og forsvar mot slike operasjoner krever god og omforent situasjons- og sikkerhetspolitisk forståelse i alle sektorer. Det krever kunnskap om truslene, virkemidlene, aktørene og deres hensikter. Det krever hurtig koordinerte responstiltak.

Kina og Russland kan utøve økonomisk statshåndverk mot Norge. Fram mot 2030 kan økonomiske virkemidler ha stort potensial for å true norsk sikkerhet. Den teknologiske utviklingen gjør det vanskeligere å identifisere og ha kontroll over hvilke selskaper, leverandører og data kan utnyttes til formål som kan true Norges nasjonale sikkerhetsinteresser.

Summary

The Norwegian Defense Research Institute (FFI) has been commissioned by the National Security Authority (NSM) to shed light on technological and societal developments of particular importance to national security. This will contribute to an in-depth knowledge base for the preparation of the chief NSM's Advise on National security (SFR) for 2025-2028. The report addresses expected developments in technology, climate and energy security and hybrid interference activities in a 2030 perspective and the significance for national security interests.

The development of 5G is of great importance for big data, artificial intelligence and electronic communication services (ECOM). 5G will form the basis for the majority of communication services. It is highly important for our national security interests until 2030. 5G will have different and new vulnerabilities compared to previous generations. NATO expects that quantum technology products will be operationally useful in 5-15 years. This entails major changes for military and civilian systems within autonomy, sensors for intelligence, surveillance and targeting, communication/crypto and data processing (quantum computers). The central capabilities and capacities of the armed forces and civil society must adapt to the development.

Climate change is one of the biggest challenges society faces. Variable energy sources, extreme weather, automation, transnational dependencies and increases in cyber incidents and cascading failures increase the complexity of the energy system. This may result in increased vulnerability, reduced reliability and resilience in the system and more frequent, long-lasting power outages and the loss of critical services over large areas.

Society is increasingly dependent on space-based services. Ever better services are developed within communication, observation and intelligence as a result of space activities. Military loss of satellite communications can lead to the degradation of command and control and the distribution of intelligence information. Civil loss can lead to the loss of many critical services.

Digitization of society increases the attack surface for computer crime and offensive cyber operations. Digital security must therefore include norm and sanction work, increased focus on personnel security, continuous development of machine learning techniques for detection and communication around own cyber capabilities.

Digitization, the internet and social media gives new opportunities and greater effect to influence operations with low risk. Prevention and defence against such operations require a good and coordinated situational understanding and security policy in all sectors, knowledge of the threats, the means, actors and their intentions, and rapid coordination of response measures.

China and Russia can exercise economic statecraft against Norway. Until 2030, economic instruments may have great potential to threaten Norwegian security. Technological developments make it more difficult to identify which companies, suppliers and data that can be used for purposes that may threaten Norway's national security interests.

Innhold

Sammendrag **3**

Summary **4**

1 Innledning **7**

2 Teknologiutviklingens betydning **8**

2.1 Generelt om teknologisk utvikling fram mot 2030 8

2.2 Stordata, kunstig intelligens, samarbeid og risiko 10

2.3 Teknologisk utvikling innen EKOM-tjenester 13

2.4 Utvikling innen kvanteteknologier 17

2.5 Utvikling innen romteknologi og rombaserte tjenester 23

3 Klima og energisikkerhet **37**

3.1 Klimamål og forpliktelser 37

3.2 Utslippskutt i et nordisk energisystem 38

3.3 Elektrifisering av samfunnet 39

3.4 Drift av kritiske samfunnsfunksjoner 40

3.5 Energisikkerhet og transnasjonale avhengigheter 43

4 Sammensatte trusler **46**

4.1 Cyberoperasjoner 46

4.2 Påvirkningsoperasjoner i informasjonsmiljøet 57

4.3 Økonomisk virkemiddelbruk 69

5 Betydning for nasjonale sikkerhetsinteresser **89**

5.1 Teknologibruk, verdiskapning og 5G 89

5.2 Kvanteteknologi 90

5.3 Romvirksomhet 90

5.4 Klima og energisikkerhet 90

5.5 Sammensatte trusler 91

Referanser **95**

1 Innledning

Etterretningstjenesten, Politiets sikkerhetstjeneste (PST) og Nasjonal sikkerhetsmyndighet (NSM) sine åpne trussel- og risikovurderinger for 2022, samt FFIs egne studier,[1,2,3,4] peker på en rekke viktige utviklingstrekk i samfunnet som kan påvirke Norge. Dette inkluderer blant annet erodering av den liberale verdensorden, intensivert global konkurranse, globaliseringsskepsis og populisme, tvil om demokratiets evne til å håndtere problemene som skapes på grunn av mindre tro på flernasjonale løsninger, Kinas økende tilstedeværelse i flere domener, klima- og miljøutfordringer og økonomisk utvikling. I tillegg har stormaktsrivaliseringen mellom USA, Kina og Russland blitt forsterket av koronapandemien i 2020-2022 og av Russlands invasjon av Ukraina 24. februar 2022.

Denne rapporten beskriver utvalgte utviklingstrekk fram mot 2030 som er av særlig betydning for nasjonale sikkerhetsinteresser. Rapporten er skrevet på oppdrag for NSM for å understøtte NSMs arbeid med Sikkerhetsfaglig råd (SFR). SFR fremlegges våren 2023. Rapporten danner et bredt kunnskapsgrunnlag for SFR og gir derfor ikke konkrete anbefalinger. Utviklingstrekk og tidshorisont er valgt i samarbeid med NSM. Utviklingstrekkene som beskrives, er knyttet til følgende temaer:

1) Teknologiutviklingens betydning
2) Klima og sikkerhet
3) Sammensatte trusler

Første del omhandler teknologisk utvikling generelt, utnyttelse av data, samarbeid, elektronisk kommunikasjon (5G), kvanteteknologier og romvirksomhet, med hovedfokus på militære anvendelser. Andre del beskriver klimaendringer og framtidige endringer i kraftsystemet. Til slutt tar tredje del for seg sammensatte trusler med fokus på cyberoperasjoner, påvirkningsoperasjoner og økonomisk virkemiddelbruk.

Denne studien benytter definisjonen av nasjonale sikkerhetsinteresser (NSI-er) hentet fra Lov om nasjonal sikkerhet (sikkerhetsloven). I sikkerhetsloven er nasjonale sikkerhetsinteresser definert som (§ 1-5): «landets suverenitet, territorielle integritet, demokratiske styreform og overordnede sikkerhetspolitiske interesser knyttet til:

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

[1] Beadle et al. (19/00045), 2019

[2] Skjelland et al. (22/00659), 2022

[3] Sellevåg et al. (20/00530), 2020

[4] Sellevåg et al. (21/01132), 2021

2 Teknologiutviklingens betydning

Kommersielle behov og utsikter i samfunnet styrer mye av teknologiutviklingen. Teknologi vil kunne benyttes til flere ulike formål og på helt andre måter enn opprinnelig tiltenkt. I det følgende vil vi se nærmere på hvilken betydning det kan ha for nasjonale sikkerhetsinteresser i et 2030-perspektiv.

2.1 Generelt om teknologisk utvikling fram mot 2030

Det er mange forskjellige aktører og organisasjoner som analyserer teknologiutviklingen og hvilke konsekvenser utviklingen vil ha for samfunnet, bedrifter og militære operasjoner i fremtiden. Mange kommersielle trendanalyser beskriver i dag i stor grad konsekvenser av teknologiutviklingen og ikke lenger enkeltteknologier. Gartner sine årsrapporter fra 2018[5] til 2021[6] viser for eksempel en merkbar dreining fra å beskrive enkeltteknologier og teknologitrender til å beskrive anvendelse og nyttegjøring av teknologiutviklingen. Tilsvarende rapporter fra Deloitte[7] og Future Technology Institute[8] viser tilsvarende utvikling i deres beskrivelser av teknologiutviklingen.

Teknologiutviklingens betydning for NATOs fremtid har vært diskutert på øverste nivå i alliansen.[9] NATO, med NATO Science and Technology Organization (STO) i spissen, har publisert flere dokumenter som beskriver teknologiutviklings potensielle effekt på alliansen fremover. I disse dokumentene beskrives teknologier de kaller *Emerging and Disruptive Technologies* (EDT). Det er fire generelle utviklingstrekk som beskrives som drivende framover – intelligent, sammenkoblet, distribuert og digitalt.[10] Følgende åtte hovedtrender listes opp som EDT-er:

- stordata og avansert analyse
- kunstig intelligens (KI)
- autonomi
- kvanteteknologier
- romteknologier
- hypersoniske våpensystemer
- bioteknologi og menneskelig forbedring («human enhancement»)
- nye materialer og framstilling

[5] Gartner; *Top 10 Strategic Technology Trends for 2019*, 2018

[6] Gartner; *Top Strategic Technology Trends for 2022*, 2021

[7] Deloitte; *Deloitte Tech Trends for 2021*, 2021

[8] Future Today Institute; *2021 Tech Trends report*, 2021

[9] NATO; *Emerging and disruptive technologies*, 2022

[10] NATO STO; *Science & Technology Trends 2020-2040*, 2020

Med unntak av hypersoniske våpensystemer, vil de samme EDT-ene har stor betydning for sivil næringsutvikling og samfunnssikkerhet.[11] Flerbrukspotensialet til EDT-ene blir derfor viktig framover. Dette kan gi både muligheter og utfordringer for norske myndigheters ivaretagelse av nasjonale sikkerhetsinteresser.

NATO STO-rapporten er klar på at selv om det er disse åtte trendene som driver utviklingen, så vil innovasjon oppstå i krysningspunkter mellom teknologitrendene, for eksempel i krysningen mellom stordata og autonomi. Det er i slike tilfeller at multiple bruksområder og nye, ikke-tiltenkte områder der teknologien tas i bruk oppstår.

Imidlertid har det vist seg vanskelig å kople teknologiutvikling til konkrete konsekvenser for militære operasjoner og Forsvaret. Dette har NATO STO erkjent i sin *Disruptive Technologies Table-Top Exercise*-rapport.[12] Sjefsforsker Sverre Diesen beskriver dette slik i FFI-rapporten *Fra teknologi til strategi og operasjoner – teknologiutviklingens påvirkning på militære styrker og bruken av militærmakt* (s. 7-8):[13]

> «Mangelen på en entydig eller deterministisk sammenheng mellom teknologi og militære forhold fører til at tolkningsrommet for å bedømme teknologiens betydning i fremtidige konflikter blir tilsvarende stort. Denne usikkerheten kommer i tillegg til annen uenighet om hvorledes fremtidige konflikter vil arte seg som følge av andre drivere, som politisk, sosial eller økonomisk utvikling. Så vel organisering og utrustning som bruk av militære styrker påvirkes med andre ord av samfunnsutviklingen i bred forstand, der teknologiutviklingen bare er én av flere dimensjoner.»

Beskrivelsene av NATO EDT og utviklingen i beskrivelsene i Gartners rapporter leder til en hypotese om at utviklingen innen enkeltteknologier (særlig innen IKT-området) ikke lenger er det som styrer innovasjon generelt. Dette er oppsummert i FFI-rapporten *Trender innen IKT – relatert til militærmakt*.[14] Nye anvendelser og innovasjon skjer ofte gjennom å sette sammen teknologier på nye måter. Den begrensende faktoren er vår fantasi og våre evner til å utføre oppgaver på nye måter, som for eksempel militære operasjoner. Mulighetsrommet gitt av teknologiutviklingen er så stort at det er vanskelig å peke på konkrete militære kapabiliteter. Dette betyr også at det i enda større grad enn tidligere vil være kommersielle muligheter som styrer hvilke teknologier som vil bli tatt fram. Med dagens teknologiutvikling er det mulig å få til ganske mye funksjonalitet. Det er en prioriteringssak hva de kommersielle aktørene vil implementere av teknologi i sine produkter. Dersom norske myndigheter og offentlige virksomheter ikke signaliserer tidlig og klart nok hva behovene er og legger til rette for et stort nok «kommersielt marked», kan potensielt interessante teknologimuligheter ikke bli implementert av de kommersielle aktørene. Da kan det bli langt mer kostbart, i form av både tid og penger, for offentlige virksomheter å utvikle og implementere nødvendige løsninger, for

[11] Sellevåg et al. (20/00530), 2020

[12] NATO STO; *Disruptive Technologies Table-Top Exercise (D3TX) - Summary Report*, 2021

[13] Diesen (22/01682), 2022

[14] Bentstuen (22/00544), 2022

eksempel innen beredskap og samfunnssikkerhet. 5G-utviklingen er et godt eksempel på dette (omtales nærmere i kapittel 2.3.1).

2.2 Stordata, kunstig intelligens, samarbeid og risiko

En egenskap med moderne verdiskapning er at virksomheter i mindre grad kan oppnå suksess alene. Det er derfor ofte behov for utstrakt samarbeid.[15,16] Samarbeidet kan være alt fra langsiktige, strategiske samarbeid, som Forsvarets virksomhetsprogram *militær anvendelse av skytjenester* (MAST),[17] til dynamiske og spontane samarbeid med utenlandske konsulenter og universiteter. Samarbeid er nødvendig for blant annet å få tilgang til kompetanse, utvikle produkter og tjenester sammen med kunden, utvikle komplementære produkter, gjøre innovasjon i nettverk, mobilisere desentraliserte ressurser, dele data og raskt kunne ta i bruk ny teknologi. Samarbeid er også grunnlaget for å kunne skape nettverkseffekter i markeder. Dette krever trygghet og tillit internt i virksomheten og mellom virksomheter.[18]

Nåtidens og framtidens virksomheter har gjerne mål om å bli mer datadrevne, slik at beslutninger baseres på data og at man i større grad også leverer tilknyttede tjenester («value-added services») sammen med produktene. Dette skjer i form av at data samles inn fra kunden og tjenesten eller produktet forbedres for kunden basert på de innsamlede dataene.[19] Produktene og miljøet rundt utstyres dermed med sensorer koblet til leverandørene (og andre aktører). Sensorene måler over tid og bidrar til å forbedre produktet.[20]

Norge har en ambisjon om å kunne utnytte mulighetene som ligger i stordata i overgangen til et bærekraftig samfunn. Dette vil kunne gi økt verdiskaping, grønnere økonomi, nye arbeidsplasser og en effektiv offentlig sektor.[21] Det ligger således en forventning om en digital transformasjon som vil endre produkter, tjenester, prosesser og hvordan mennesker arbeider. Dette vil kunne påvirke både en virksomhets bredde av produkter og tjenester («scope») og volum/salg («scale»). En viktig forutsetning i et datadrevet samfunn er at data deles i næringslivet og mellom privat og offentlig sektor. For å kunne nyttiggjøre seg av informasjonen, må dataene være merket og kategorisert på en hensiktsmessig måte. Hensiktsmessig deling av data vil kreve

[15] Gupta, 2018

[16] Snow et al., 2017

[17] Forsvarsmateriell, 2023

[18] Lange, Gausdal, 2020

[19] Iansiti, Lakhani, 2014

[20] Jotun leverer for eksempel maling til båter (produkt) sammen med tjenesten drivstoffsparing. Drivstoffsparingen er basert på/beregnes på grunnlag av data fra mange forskjellige sensorer utplassert på skipene (https://www.jotun.com/ww-en/industries/solutions-and-brands/hull-performance-solutions/overview/). Et annet eksempel er John Deeres presisjonslandbruk. I dette tilfellet utstyres landbruksutstyr med sensorer, data samles inn og stedsspesifikke analyser gjennomføres slik at bonden blant annet kan redusere gjødsels-, såings- og sprøytemiddelkostnader (https://www.deere.no/no/agricultural-management-solutions/).

[21] Meld. St. 22 (2020–2021), 2021

standardisering av både funksjonalitet og sikkerhet. Merking av data (for eksempel om en epost er fakturasvindel, datapakkene var del av et datainnbrudd eller om en annonse førte til flere enn 100 klikk)[22] krever at personer med domenekunnskap jobber sammen med personer som kan jobbe med store datamengder.[23] For å utvikle kapabiliteter som kan utnytte store mengder data trenges en kombinasjon av ekspertise på datavitenskap, domenekunnskap (merking og evaluering) samt programvareutvikling for å implementere verktøy som gjør dette. Forskjellige nasjoner har forskjellig tilnærminger rundt tilgang til og bruk av disse dataene. Dette kan skape store forskjeller i utnyttelse av teknologi og utvikling av kompetanse. Over tid vil andre nasjoners overlegne utnyttelse av og tilgang på stordata potensielt kunne påvirke våre nasjonale sikkerhetsinteresser negativt som følge av at de dermed har bedre situasjonsforståelse og bedre datadrevne beslutninger.

Innsamling, deling, analyse og merking av data er forenklet sagt grunnlaget for kunstig intelligens. I henhold til EU sine retningslinjer for etisk kunstig intelligens (Ethics Guidelines for Trustworthy Artficial Inteligence (EGTAI)[24]), bør systemer som bruker kunstig intelligens være lovlige, etiske og robuste. I tillegg kan det settes krav om at algoritmene skal være etterprøvbare. Etiske betyr at systemene er i henholde til våre etiske verdier og prinsipper, og robuste betyr at systemer fra et teknisk og sosialt perspektiv ikke forårsaker utilsiktet skade. Siden det er forskjell mellom for eksempel norske og kinesiske lover, verdier og prinsipper, vil kunstig intelligens i kinesiske systemer ikke nødvendigvis fremme norske verdier.[25] I *Nasjonal strategi for kunstig intelligens* er det et eget kapittel om ansvarlig og pålitelig kunstig intelligens. Her legges det til grunn at kunstig intelligens som utvikles og brukes i Norge skal respektere menneskerettighetene og demokratiet. Videre skal digital sikkerhet bygges inn i utvikling, drift og forvaltning av løsninger for kunstig intelligens.[26] Dette setter høye krav til kompetanse om blant annet personvern og forklarbarhet (Explainable AI -XAI) i de fleste virksomheter som utvikler og utnytter kunstig intelligens.

Mange oppkjøp begrunnes i tilgang på data. Dette gir utfordringer innen både personvern generelt og for eksempel i bruk og etikk rundt stordata og algoritmer.[27] Typisk vil forutsetningene, som ble kommunisert når data ble samlet inn, kunne endres av ny eier. For eksempel kan et kunderegister utnyttes på en helt annen måte, ved at det sendes rettet reklame som bevisst utnytter svakheter hos kundene.

---

[22] Merking er ikke alltid nødvending. Man kan for eksempel bruke ikke-veiledede metoder, anomalideteksjon, simulere angrep hvor merking kan automatiseres, eller delautomatisere merkingen hvor for eksempel en domeneekspert kan gi ulike heuristikker som bruker i verktøy for mer automatisert merking. FFI erfarer innen digital sikkerhet at gode merker dog krever enda mer manuell innsats og at mange av de bedre metodene også krever merket data.

[23] Voldhaug et al. (21/01819), 2021

[24] EC; *Shaping Europe's digital future*, 2022

[25] Bergsjø, 2022

[26] KMD; *Nasjonal strategi for kunstig intelligens*, 2020

[27] Farsund (22/00631), 2022

Datadreven verdiskaping gjennom samarbeid er avhengig av tett integrerte IKT-systemer i nettverk (gjerne i form av skytjenester). IKT er altså integratoren i dagens og framtidens verdiskapning. Mange av de grunnleggende nasjonale funksjonene (GNF-ene)[28] vil sannsynligvis også realiseres gjennom datadrevne aktiviteter og ressurser i dynamiske nettverk på tvers av nasjonale grenser. Dette gir både utfordringer og muligheter for sikkerhetsarbeidet. En utfordring er økt kompleksitet og usikkerhet, der blant annet hver virksomhet har økende problemer med å beskrive sin plass i nettverket sett opp mot egen og andres verdiskaping. En annen utfordring er makten skyleverandørene og deres moderstater potensielt erverver over tid. I dag domineres skyleverandørmarkedet av amerikanske (Google, Amazon og Microsoft) og kinesiske (Alibaba og Huawei) aktører. Disse fem aktørene står for over 80 % av «infrastruktur som tjeneste (IaaS)»-markedet.[29] En mulighet med for eksempel skytjenester er at de kan skaleres etter behov og datalagring og prosessering kan «evakueres» ved uønskede hendelser.[30]

Et datadrevet samfunn der verdiskaping skjer i dynamiske samarbeidsformer kan også være et sårbart samfunn om ikke sikkerheten ivaretas. Især er IKT sin rolle som integrator i all verdiskapning viktig å beskytte mot sikkerhetstruende virksomhet som cyberoperasjoner eller økonomisk virkemiddelbruk. I tillegg må brukerne har tillit til IKT-systemene og derfor kommer blant annet beskyttelse mot fiendtlig påvirkning inn som en sentral evne i samfunnet. Cyberoperasjoner, økonomisk virkemiddelbruk og påvirkning omhandles i kapittel 4.

Sentralt i sikkerhetsarbeidet er opprettholdelse av et forsvarlig sikkerhetsnivå. Dette er nært knyttet til forståelsen av risiko. Risikobildet er komplekst. Det skyldes blant annet stadig tettere og dynamiske avhengigheter og koblinger, lange verdikjeder og rask innføring av teknologi. Det skyldes også at verdiene som skal beskyttes varierer i viktighet i forskjellige kontekster.[31]

[28] Tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser (sikkerhetsloven)

[29] Gartner; *Gartner Says Worldwide IaaS Public Cloud Services Market Grew 41.4% in 2021*
Top Five IaaS Providers Account for Over 80% of Total Market, 2022

[30] I Ukraina har myndighetene ved flere anledninger takket Google, Microsoft og Amazon for deres bidrag til å holde kritisk infrastruktur oppe (https://www.businessinsider.com/zelenskyy-amazon-ukraine-peace-prize-digital-war-support-aws-2022-7?r=US&IR=T).

[31] Eksempler på forskjellige typer verdier kan være gradering, militær evne og HMS/bærekraft.

Hva er kompleksitet?

Med kompleksitet i for eksempel et IKT-system, menes at man ikke klarer å etablere en nøyaktig helhetlig prediksjonsmodell for et system på grunnlag av kunnskap om de spesifikke funksjonene og tilstandene for systemets enkeltkomponenter.

Eksempler på forskjellige typer kompleksitet:

- Samspillskompleksitet
- Koblings-kompleksitet
- Organisatorisk kompleksitet
- Verdikompleksitet
- Dynamisk kompleksitet

Det at produkter stadig forbedres/oppdateres basert på innsamlede data, er et eksempel på dynamisk kompleksitet. Kompleksitet fører til behov for et tydeligere bevisst forhold til usikkerhet i virksomhetenes søken etter et forsvarlig sikkerhetsnivå. Med andre ord, et forsvarlig sikkerhetsnivå handler mye om å ha et kunnskapsbasert forhold til forskjellige typer usikkerheter knyttet til forskjellige typer kompleksiteter og å balansere risikohåndteringen og sikkerhetstiltakene opp mot dette. Dette vil også kunne involvere ulike avveininger, der for eksempel sikkerhetstiltak knyttet til konfidensialitet (kryptering) forringer sikkerhetstiltak knyttet til tilgjengelighet/militær evne (rask tilgang til data).

Slike vurderinger er krevende. Derfor vil alle virksomheter som er underlagt sikkerhetsloven kunne ha behov for rådgivning innen forsvarlig sikkerhetsnivå i forskjellige kontekster. Krav til kompetanse og sikkerhetstiltak vil også kunne påføre virksomhetene kostnader. For kommersielle virksomheter kan kravene i ytterste konsekvens føre til mindre evne til konkurranse og innovasjon, for eksempel begrensninger på samarbeid og deling av informasjon.

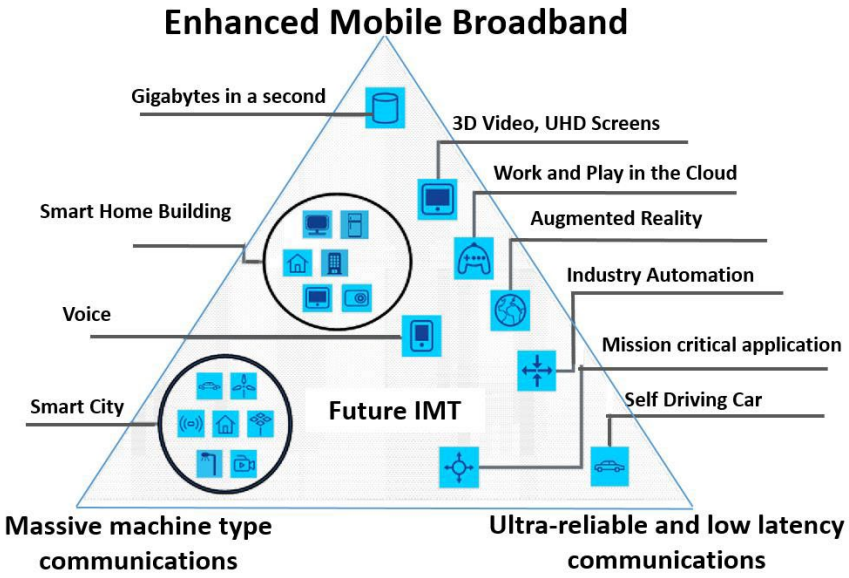
Evne til helhetlig sikkerhetsstyring vil derfor ha en svært sentral rolle i utviklingen av forsvarlig sikkerhet i en virkelighet der funksjoner i militære og sivile virksomheter vil bli stadig mer sammenvevd og kompleksitet vil øke dramatisk.

2.3 Teknologisk utvikling innen EKOM-tjenester

Den videre teknologiske utviklingen innen elektroniske kommunikasjons (EKOM)-tjenester vil relateres til innføring av femte generasjons mobilteknologi (5G). I den daglige medieomtalen om 5G er det et nytt radiogrensesnitt – 5G New Radio (5G NR) – som har størst fokus, naturlig nok siden det er 5G NR som gir bedre kapasitet til mobile enheter. Det skjer også store endringer i de delene av infrastrukturen som ikke er synlig for den vanlige bruker, så som hvordan kommunikasjonsinfrastrukturer bygges, driftes og forvaltes både nasjonalt og internasjonalt. Nøkkelord for den teknologiske utviklingen er virtualisering og

programmerbarhet for å lage EKOM-infrastrukturer som understøtter dynamiske applikasjoner og brukere.

Figur 2.1 viser ITU sitt målbilde for mobiltjenester for 2020 og som 5G-utviklingen generelt strekker seg etter. Som figuren viser, vil 5G dekke et stort antall forskjellige typer tjenester. Tjenester som nevnes ofte er selvkjørende biler, smarte byer, fjernoperasjoner og virtuell virksomhet. I tillegg vil 5G tilby mye høyere overføringskapasitet enn i dag.



Figur 2.1 Tjenester i 5G. Illustrasjon: International Telecommunication Union (ITU), ITU-R International Mobile Telecommunications (IMT) Vision 2020

Det er ingen enkeltteknologier som vil evne å tilby alle de forskjellige tjenestene samtidig. 5G må sette sammen et stort antall forskjellige teknologier for å understøtte målbildet til ITU. Det er denne understøttelsen av et meget stort antall forskjellige tjenester, og dermed også et stort antall forskjellige teknologier, som er den store teknologiske endringen mellom 4G og 5G.

Samtidig som behovet for nye mobiltjenester øker, har det skjedd store endringer i de underliggende teknologiene som kommunikasjonsnettverk bygges på de siste fem til ti årene. Istedenfor mange forskjellige "svarte bokser" fra et stort antall forskjellige leverandører, vil fremtidens kommunikasjonsnettverk bestå av mye programvare som kjøres som virtuelle prosesser i et datasenter. Dette er til dels samme teknologiutvikling som står bak veksten innen skytjenester og datasentra.

Den tredje store teknologiske endringen innen kommunikasjonsnettverk begrunnes med optimalising for dagens trafikkmønster. Dagens trafikkmønster, særlig på internett, medfører en konsentrasjon av datatrafikk inn mot sentrale aktører som søkemotorer, sosiale medier og film- og underholdningsbransjen (såkalte innholdsleverandører). Teleoperatørene har et behov for å optimalisere sine kommunikasjonsnettverk for dette trafikkmønsteret. Det gjennomføres flere

endringer i infrastrukturen for å håndtere dette. Innholdsleverandører vil møte kundene lenger ut i «kanten» av infrastrukturen og det vil også bli bedre muligheter for dataprosessering i kanten. Samtidig skjer den en forenkling av den underliggende transportinfrastrukturen mellom kanten og sentrale deler av nettverket.

Å gjøre endringer i nasjonale og internasjonale kommunikasjonsnettverk (EKOM-infrastrukturer) medfører stor risiko. Teleoperatørene vil derfor gjøre store endringer i hele sin infrastruktur samtidig med innføringen av 5G, da 5G uansett vil kreve endringer i tilstøtende infrastrukturer. Resultatet er en konsolidering av teknologi på tvers av kommunikasjonstjenester. 5G, med tilstøtende infrastrukturer, vil derfor ikke kun utnyttes for mobiltelefoni. 5G vil derimot være basis for alle eller de aller fleste kommunikasjonstjenester som blir levert av de store aktørene. ITU og 3GPP omtaler dette som *fixed-mobile convergence*. I fremtiden vil samme infrastruktur levere kommunikasjonstjenester uavhengig av tilkoblingsmetode (kablet eller trådløst) og tilby felles funksjonalitet. Det første som kommer er antagelig sømløs sammenkopling av Wifi (Wifi6+) og 5G med for eksempel sømløs overgang mellom tilkoblingsteknologiene.[32]

Følgende teknologiske endringer kommer sammen eller samtidig med 5G-utviklingen:

i. Programmerbarhet og virtualisering

Kommunikasjonsnettverk gjennomgår nå en stor endring ved at mye funksjonalitet som tidligere var implementert i flere separate, ofte lukkede, bokser blir implementert som programvare som kjører på en generell dataserver. Det er to aspekter ved dette; at funksjonalitet blir virtualisert og at nettverk blir programmerbare. Virtualisering medfører at funksjonalitet kan flyttes rundt og skaleres etter behov på samme måte som skytjenester og virtuelle datamaskiner. Programmerbarhet tilsier at nettverksfunksjonalitet blir programvare på lik linje med andre typer applikasjoner. Det er mange fordeler med denne utviklingen. Nettverksfunksjonalitet kan enkelt tilpasses behov. Det er lett å legge til nye tjenester og funksjoner og kommunikasjonsnettverk kan kontinuerlig oppdateres. Den store ulempen er at risiko- og sårbarhetsbildet endrer seg. Kommunikasjonsnettverk vil få mange av de samme sårbarhetene som andre typer dataprogrammer. I tillegg blir infrastrukturen mye mer kompleks og det blir vanskeligere å gjennomføre gode risikoanalyser. Det blir riktignok enklere å håndtere mange typer sårbarheter da det er enklere og billigere å endre programvare enn maskinvare.

ii. Edge datasenter

En del eksisterende telefonsentraler blir bygd om til små datasentre. Mye funksjonalitet som tidligere befant seg på hver enkelt basestasjon i mobilnettene vil nå flyttes inn i lokale datasentre. Disse vil betjene flere basestasjoner og etter hvert andre tilkoplingsteknologier. Det er fortsatt usikkert hvordan disse små datasentrene vil

[32] Denne funksjonaliteten eksisterer til dels i dag for noen spesifikke tjenester eller løst via «over the top»-tjenester.

utvikle seg. Noen vil kun være tilpasset behovet til hver enkelt teleoperatør mens andre vil være del av systemene til en større skyleverandør. De siste vil dermed også betjene kunder utover teleoperatørene. Slike lokale datasentra tillater teleoperatørene å flytte funksjonalitet nærmere brukerne. Dette er nødvendig for å kunne tilby en del av tjenestene i målbildet til IMT (Figur 2.2). Spesielt tjenesten «Ultralav og robust kommunikasjon» samt til dels private 5G-nett vil kreve lokale datasentre. I byene vil hver teleoperatør mest sannsynlig ha sine egne dedikerte datasentre. Det vil være konseptuelt mulig at flere teleoperatører deler på et datasenter med tilhørende basestasjoner, som kan være aktuelt i spredt bebygde områder, men det er for tidlig å si hva som faktisk vil bli implementert og hvilke løsninger teleoperatørene velger. Programvare som kontrollerer disse små datasentrene, særlig de som også brukes til andre tjenester enn 5G og i datasentre som brukes av flere teleoperatører samtidig, blir veldig viktige komponenter.

iii. Virtualiserte ende-til-ende tjenester

Det er ikke lenger slik at endepunkter for en kommunikasjonstjeneste er faste lokasjoner. Både tjenesteproduksjon og plassering av konsumenten (brukere) er nå veldig mobile/dynamiske. Med moderne datasenterteknologi vil plassering av tjenesteproduksjon bli kontinuerlig optimalisert basert på en rekke parametere så som lastbalansering, krav til robusthet og kostnader for strøm, datakraft og transporttjenester. Endepunkter er heller ikke lenger nødvendigvis fysiske komponenter. Ende-til-ende-tjenester må kunne kople sammen virtuelle servere med både andre virtuelle servere og fysiske endepunkter. Det blir dermed vanskeligere å se sammenhengen mellom en tilbudt tjeneste og den fysiske infrastrukturen. De som eier den underliggende fysiske infrastrukturen mister kontroll på trafikk som går gjennom deres utstyr. Dette fører igjen til at det blir vanskeligere å gjennomføre risikoanalyser for en bruker av en kommunikasjonstjeneste. Det vil derimot oppstå fordeler innen skalerbarhet og dynamiske tjenester.

2.3.1 5G som basis for det smarte samfunnet

5G få en sentral rolle i den fremtidige samfunnsutviklingen (se delkapittel 2.3). Mye modernisering av samfunnet vil både kreve og utnytte teknologiske muligheter som kommer med 5G-utviklingen.

Siden 5G vil medføre en konsolidering av infrastrukturer, vil svært mange samfunnsfunksjoner være avhengig av en fungerende 5G-infrastruktur. Dette gjelder blant annet nødetater, energiforsyning, transportsektoren, vann og avløp og betalingstjenester. Regjeringen bestemte i 2017[33] at neste generasjons nødnett skal baseres på kommersiell mobilteknologi. I skrivende stund er arbeidet med konseptvalgutredning av nytt nødnett fortsatt unntatt offentlighet, men

[33] Abrahamsen; *Nødnett - veien videre*, 2021

hvis nytt nødnett skal på plass innen utgangen av 2026 så vil, og bør, nytt nødnett baserer seg på 5G.

Utvikling av smarte byer og velferdstjenester som tillater eldre å bo hjemme i lengre tid enn i dag vil også være veldig avhengig av 5G. 5G vil muliggjøre kommunikasjon til et meget stort antall IoT-enheter samtidig, noe som utviklingen av smarte byer vil være avhengig av. 5G, med etterfølgere, vil være teknologien som binder alle disse sensorene sammen og som danner grunnmuren i smarte byer. Dette gjelder også alle andre samfunnsområder hvor sanntids utveksling av informasjon blir utnyttet for å lage bedre tjenester.

5G vil være en viktig forutsetning for det fremtidige energimarkedet og «det grønne skiftet» innen elektrisitetsforsyning (jf. kapittel 3).[34] En trend er at dagens konsumenter også blir produsenter av strøm gjennom solcellepaneler og andre energikilder.[35] Dette krever en helt annen styring av strømnettet som kan bli muliggjort via tjenester levert av 5G. 5G kan få lav nok transmisjonsforsinkelse til å kunne brukes til slike situasjoner istedenfor kostbar utrulling av fiber i strømnettet.[36] I tillegg kan autonomi, muliggjort via 5G, gi store innsparinger og effektivisering av inspeksjon og overvåking av installasjoner og distribusjonsnett.

2.4 Utvikling innen kvanteteknologier

2.4.1 Hva er kvanteteknologi?

Det meste av det som skjer i naturen og i omgivelsene rundt oss til daglig kan forklares med det vi omtaler som klassisk fysikk. Her er blant annet Newtons lover for bevegelse sentrale og kjent for de fleste.

Dersom man derimot begynner å studere partikler inne i molekyler (for eksempel atomer, elektroner og fotoner) svært nøyaktig, finner man at oppførselen deres ikke kan forklares tilstrekkelig med den klassiske fysikken. På 1920-tallet arbeidet kjente forskere som blant annet Niels Bohr, Max Planck og Albert Einstein med å forklare dette og kvantefysikken tok form.

For å kunne forklare det man observerer (kvanteeffekter) tildeler kvantefysikken disse partiklene (kvanteobjektene) helt spesielle egenskaper. Disse er langt fra intuitive som for eksempel;

- Energien til kvanteobjekter er kvantifisert slik at energien kun kan endres i sprang
- Ett kvanteobjekt kan være på to steder samtidig inntil man gjør målinger av objektet (superposisjon)
- Egenskapene til to kvanteobjekter kan være sammenkoblet selv om de fysisk er adskilte (sammenfiltring)

[34] Deloitte; *5G Empowers the future of Electricity*, 2021

[35] Ericsson; *Bringing 5G to power*, 2020

[36] Smart Energy International; Smart5Grid – the 5G smart grid use cases, 2022

Kvanteteknologi er teknologi som aktivt utnytter disse spesielle kvanteeffektene. Det har vært forsket på kvanteeffekter i ulike materialer i mange år. De utnyttes i flere produkter vi omgir oss med til daglig som for eksempel lasere og transistorer/dataprosessorer.

De siste årene har det derimot vært en betydelig framgang i vår evne til å kunne aktivt utnytte de kjente kvantefysiske egenskapene. I laboratorier kan man nå lage enkeltvise kvanteobjekter (for eksempel atomer, elektroner eller fotoner), endre/påvirke tilstanden til disse kvanteobjektene og lese ut tilstanden/informasjonen de representerer. Dette krever ofte svært spesialisert utstyr som også må utvikles.

2.4.2 Hvilke konsekvenser kan utviklingen av kvanteteknologi få?

Dersom vi klarer å dra nytte av de kvantefysiske egenskapene, vil dette kunne medføre kraftig forbedret ytelse i en rekke teknologier som blant annet sensorer, avbildning, posisjonering, navigasjon, tidsangivelse, kommunikasjon og dataprosessering. Systemer basert på kvanteteknologi vil være spesialiserte. For at kvanteteknologien skal ende opp i anvendbare produkter, er man ofte avhengig av at disse kan integreres med klassisk teknologi på en robust måte. Lykkes man med dette, vil utviklingen kunne medføre betydelige endringer i hvordan både det sivile samfunnet og Forsvaret fungerer i overskuelig framtid. Det er forventet at disse endringene vil påvirke systemer vi har i dag og/eller de systemene vi nå er i ferd med å anskaffe. Innen enkelte områder vil endringen også kunne være disruptiv.

Det kreves store ressurser for å drive fram forskning, utvikling og industrialisering av anvendelser basert på kvanteteknologi. Man må forvente at aktører som er tidlig ute med moden teknologi vil kunne få store fordeler både militært og sivilt/kommersielt. Som en naturlig konsekvens av dette, må man også forvente at kunnskap og moden teknologi blir underlagt spredningsbegrensinger.

Med unntak av et fåtalls anvendelsesområder, er kvanteteknologi fortsatt en umoden teknologi. Det betyr at det gjenstår betydelig utvikling/industrialisering før man har produkter som faktisk kan selges kommersielt og/eller benyttes militært. Parallelt med vurderingene av hva kvanteteknologien kan gi, pågår det derfor også en livlig diskusjon rundt hva som er oversolgt og ikke vil kunne realiseres i praktiske anvendelser.

2.4.3 Anvendelsesområder sivilt og militært

Både for sivilsamfunnet og Forsvaret vil utviklingen kunne påvirke mange kapabiliteter, både egne og en motstanders kapabiliteter. For enkelte kapabiliteter vil dette gi helt nye muligheter, mens for andre vil utviklingen sørge for at man unngår å redusere/miste den kapabiliteten man har i dag. Eksempler på anvendelser som vil kunne bli påvirket av utviklingen er:

- Autonomi - herunder posisjon, navigasjon og tid (PNT)
- Etterretning, overvåkning og målfatning
- Kommunikasjon
- Kvantedatamaskiner

Autonomi - herunder posisjon, navigasjon og tid (PNT)

En rekke autonome farkoster er i dag avhengig av «Global Navigation and Satellite Systems» (GNSS) eller andre eksterne navigasjonskilder for å kunne operere trygt. Disse farkostene er dermed sårbare for forstyrrelser/jamming av disse signalene. Både for militære og sivile anvendelser medfører dette en utfordring for operativ ytelse. Det er forespeilet at utviklingen innen kvanteteknologi vil frambringe sensorer som, i kombinasjon med klassiske sensorer, vil kunne gi betydelig bedre navigasjon uten ekstern støtte og bedre robusthet mot forstyrrelser. Det finnes i dag allerede fungerende systemer, men som er fysisk store og mindre anvendelige. På lang sikt ser man for seg at slike sensorer kan bli veldig små (kanskje chip-størrelse) og få plass på de fleste plattformer.

Etterretning, overvåkning og målfatning

Det er forventet at utviklingen innen kvanteteknologi vil frambringe sensorer med betydelig bedre ytelse innen mange anvendelsesområder. I tillegg til sensorer som detekterer elektromagnetisk stråling, så som synlig lys, termisk stråling, radiobølger, radarsignaler, er utviklingen allerede kommet langt innen kvantesensorer som detekterer magnet- og gravitasjonsfelt. I tillegg til økt følsomhet, vil flere nye sensorkonsepter gi redusert størrelse, økt båndbredde, lavere effektforbruk og i enkelte tilfeller være vanskeligere å oppdage som følge av lavere signatur. Utviklingen vil påvirke militære kapasiteter blant annet innen etterretning, overvåking og målfatning. Tilsvarende vil teknologien gi en rekke sivile nye anvendelser, og sensorer for magnetisme og gravitasjon er allerede tatt i bruk til kartlegging. På lang sikt ønsker man å kunne koble enkeltvise kvantesensorer sammen i tilpassede nettverk. Dette kan gi en ytterligere betydelig økt samlet ytelse.

Kommunikasjon

Utviklingen innen kvanteteknologi påvirker allerede hvordan framtidens kommunikasjons- og kryptoløsninger utformes. Ved bruk av kvanteteknologi for blant annet deling av kryptonøkler, forventer man å kunne kommunisere sikrere enn tidligere. Kvante-kommunikasjonsnettverk har foreløpig en begrenset rekkevidde på grunn av problemer med å bevare kvanteegenskapene til signalet over lang nok tid/avstand. Det legges derfor stor innsats i å lage komponenter som kan forsterke signalet og samtidig bevare kvanteegenskapene, såkalte «quantum repeaters». Flere land tester nå ut kommunikasjonslinker basert på kvanteteknologi i verdensrommet hvor det ikke er demping av signalet. Kommunikasjonsnettverk basert på kvanteteknologi med lang/global rekkevidde vil kunne forsterke den ytelsen vi kan få fra enkeltsystemer/sensorer («quantum internet», «quantum internet of things»).

Kvantedatamaskiner

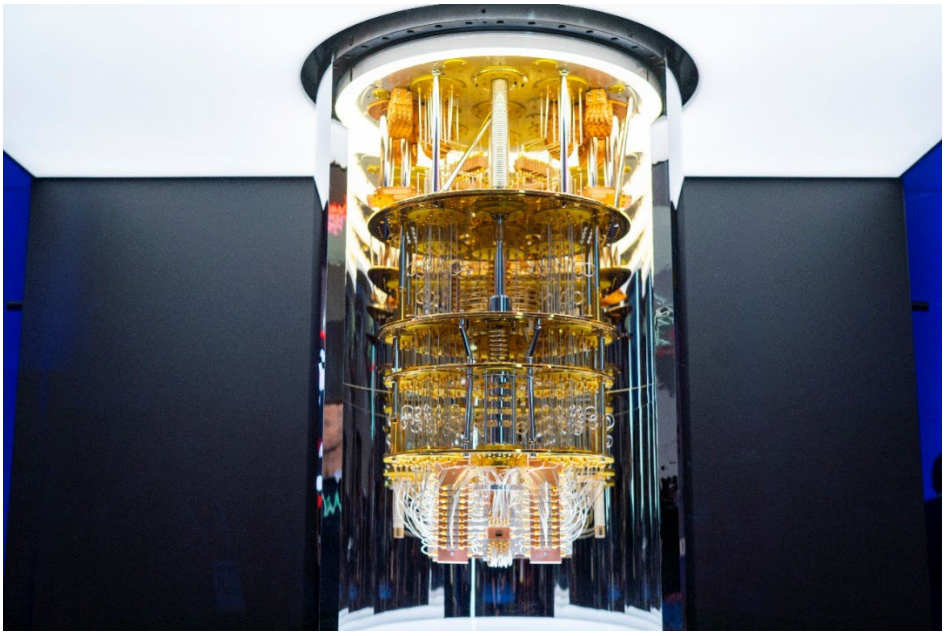
En kvantedatamaskin utnytter kvanteeffektene i et kvanteobjekt til å lage de miste byggeklossene i kvantedatamaskinen, såkalte «quantum bits» eller «qubits». I motsetning til et bit i en vanlig datamaskin, som kan være enten 0 eller 1, kan en qubits være 0, 1 eller en superposisjon av 0 og 1. Dersom man lykkes med å lage en datamaskin med tilstrekkelig mange

slike qubits, vil denne kunne utføre spesialiserte oppgaver ekstremt mye raskere (kanskje en faktor 100 millioner) enn dagens klassiske datamaskiner.

Kvantedatamaskiner vil høyst sannsynlig ikke erstatte vanlige datamaskiner, men komme i tillegg. Kvantedatamaskiner kan derfor betraktes som avanserte problemløsere som kan anvendes på områder hvor vanlige datamaskiner ikke kan benyttes.[37]

En kvantedatamaskin vil blant annet kunne analysere veldig store mengder data på kort tid. Dette vil øke ytelsen til systemer som benytter kunstig intelligens/maskinlæring eller ønsker å foreta beslutninger raskt basert på en stor mengde informasjon, som for eksempel innen finans eller militær strid. Kvantedatamaskiner vil trolig kunne knekke asymmetriske krypteringsalgoritmer. På bakgrunn av dette pågår det en stor innsats nå innen utvikling av post-quantum krypteringsalgoritmer. Kvantemaskiner vil også utføre komplekse simuleringer betydelig raskere enn dagens klassiske datamaskiner, noe som for eksempel kan gi oss oppskrifter til nye og mer avanserte materialer.

Det forskes på et stort antall ulike teknologier for å lage kvantedatamaskiner, og det er ikke opplagt hvilken teknologi som kommer til å lykkes. Figur 2.2 viser IBMs System One kvanteprosessor. Programmene (software) som skal kjøres på kvantedatamaskiner vil være spesialiserte og skreddersydd til teknologien i kvantedatamaskinen. Som for annen kvanteteknologi er det forventet at kvantedatamaskiner må brukes sammen med klassiske datamaskiner.



Figur 2.2 IBMs System One kvanteprosessor, IBM Quantum at CES 2020. Her kjøles kvanteobjektene/prosessoren nesten ned til det absolutte nullpunkt, -273 °C. Foto: IBM, Andrew Lindemann

[37] Government Office for Science, 2016

Tilgang til kvantedatamaskiner med høy ytelse (> 1 mill. qubits) vil udiskutabelt medføre disruptive endringer innenfor en rekke fagområder både sivilt og militært. Dette vil medføre stor verdiskapning for de involverte aktørene. Det vil også framskynde utviklingen innen andre EDT-er. Det er stor usikkerhet knyttet til når vi får kvantedatamaskiner med høy ytelse. I dag har de største kvantedatamaskinene i overkant av 100 qubits. Noen forventer at det vil finnes kvantedatamaskiner som overgår dagens datamaskiner innen ti år, mens andre mener det fortsatt vil gå flere tiår.

2.4.4 Kvanteteknologi i NATO

NATO følger utviklingen innen kvanteteknologi tett.[38] De har definert dette fagområdet som en av åtte såkalte EDT-er som vil kunne påvirke våre og en motstanders militære kapabiliteter. NATO sine vurderinger av når teknologien vil være moden nok for anvendelser er usikre og spriker noe, men grovt sett anslås det at kvanteteknologi vil bli introdusert og gi militær operativ nytte fra om 5-15 år.[39] Dette er innenfor levetiden til de kapasitetene vi har eller planlegger for nå i Forsvaret. En tilsvarende utvikling skjer også hos våre motstandere og i noen tilfeller i et raskere tempo. Dette medfører økt trussel mot oss og våre allierte i samme tidsperiode. NATO Science and Technology Organization (STO) har flere aktiviteter som følger opp forskningen innen kvanteteknologi. Tilsvarende vurderer NATO Conference of National Armament Directors (CNAD) konsekvenser av utviklingen for NATOs kapabiliteter og utformer strategier for implementasjon av teknologien. CNADs undergruppe for industri (National Industrial Advisory Group, NIAG) følger tilsvarende opp status for industrialiseringen av teknologien.

NATO STO satte sammen en ekspertgruppe i 2018 for å gi status for utviklingen innen kvanteteknologi. Gruppen kom med anbefalinger om videre aktiviteter for medlemslandene. Blant disse anbefalingene er:

- Etablere koordinert utviklingssamarbeid med finansiering
- Ha systemfokus på utviklingen – integrasjon klassisk og kvante
- Utvikling av utvalgte teknologikomponenter
- Forfølge kvantesikker kryptering
- Følge spesielt utviklingen internasjonalt innen
  - Logiske qubit (muliggjør kvantedatamaskiner)
  - Quantum repeaters (muliggjør kvanteteknologi i nettverk)

2.4.5 Kvanteteknologi internasjonalt

Det satses betydelige ressurser på forskning og utvikling av kvanteteknologi i mange land. Sentrale aktører som USA, Storbritannia,[40] Tyskland, Frankrike og EU/EDF har myndighetsfinansierte satsinger til flere milliarder kroner.[41] Felles for mange av disse

[38] NATO STO, 2023

[39] NATO STO, 2023

[40] UK National Quantum Technology; *UK National Quantum Technology Programme*, 2023

[41] Himsworth; *Quantum Sensing* and *Quantum Sensing in Defense and Security* (topical briefing), 2020

initiativene er at de forsøker å etablere tett samarbeid mellom myndigheter (sivile og militære), akademia og industrien. Målet er å generere verdiskapning i hele næringskjeden knyttet til kvanteteknologi. Samtidig satser internasjonale selskaper, som for eksempel IBM, Intel, Google, Amazon, Honeywell, store beløp innen utviklingen av kvantedatamaskiner og framtidig utnyttelse av disse innen stordata og kunstig intelligens.

Blant våre potensielle militære motstandere, utmerker Kina seg spesielt med store investeringer innen kvanteteknologi. De har etablert et koordinert samarbeid mellom myndigheter, akademia, mindre bedrifter og de store statlige konglomeratene. Dette samarbeidet inkluderer et stort antall studenter utdannet ved vestlige universiteter. Det er antatt at vestlige land ligger i forkant av utviklingen innen kvantedatamaskiner, mens Kina leder an innen kvantekommunikasjon. Kina rapporterer god ytelse på ulike kvantesensorer for etterretning, overvåkning og målfatning. Samtidig spekuleres det i om at noe av ytelsen er overdreven.

I Norden er det betydelig aktivitet innen kvanteteknologi blant annet gjennom The Wallenberg Centre for Quantum Technology i Sverige, Niels Bohr Institute i Danmark og National Centre of Excellence - Quantum Technology i Finland.

2.4.6 Kvanteteknologi i Norge

Norske universiteter og forskningsinstitutter har inntil nylig ikke flagget kvanteteknologi særlig sterkt som et eget satsningsområde. Flere grupper har fokusert på isolerte problemstillinger som tangerer kvanteteknologi, men uten å dekke større deler av teknologiområdet. FFI gjennomførte høsten 2021 en undersøkelse for å identifisere norske aktører og deres aktiviteter relevant for kvanteteknologi. Noen av disse er:

- Simula Research Labs
- Quantum Technology Research Group at University of South-Eastern Norway, USN
- Center for Quantum Spintronics (QuSpin) - Center of Excellence at the Department of Physics at NTNU
- The Hylleraas Centre - Centre of Excellence shared equally between UiO and UiT
- Gemini Center on Quantum Computing (UiO, NTNU and Sintef)
- Department of Physics at UiO
- Quantum AI at NordSTAR - Nordic Centre for Sustainable and Trustworthy Artificial Intelligence Research
- Centre of Research Excellence situated at OsloMet (2020)
- IBM Q Network
- Justervesenet
- FFI

Basert på denne undersøkelsen framstår norske aktiviteter innen kvanteteknologi som små og dårlig koordinerte. Det er en overvekt av teoretiske arbeider, også når det gjelder utvikling av programvare, framfor eksperimentelle arbeider og ingen har fokus på militær utnyttelse av teknologien. Norge framstår å ligge betydelig etter våre allierte partnere, inkludert våre nordiske naboland. I løpet av 2021–22 er det kommet flere initiativer til å koordinere innsatsen i Norge blant annet fra Norges forskningsråd (NFR), UiO, Simula, Sintef og enkeltpersoner.

2.5 Utvikling innen romteknologi og rombaserte tjenester

I et moderne høyteknologisk samfunn vil mange viktige tjenester inneholde et romsegment, ikke minst fordi et nært altomfattende kommunikasjonsbehov ofte dekkes via nettverk som er avhengig av satellittkommunikasjon. Imidlertid er også rombaserte tjenester utover dette blitt et stadig viktigere aspekt av samfunnslivet. Dette har sammenheng med den generelle utviklingen av industriell elektronikk med tilhørende programvare. Det sterkt fallende prisnivået innen dette området har gjort det mulig å kommersialisere rommet på en svært gjennomgripende måte.

2.5.1 Tematiske områder innen rombaserte tjenester

Satellittkommunikasjon (Satcom): De første kommersielle rombaserte tjenestene bestod i formidling av telefoni ved hjelp av geostasjonære satellitter. Fra disse første smalbåndtjenestene har det foregått en eksplosiv vekst med hovedvekt på bredbåndskommunikasjon for TV og Internett. Inntil relativt nylig har dette bygget på geostasjonære satellitter. Etter hvert har det likevel vokst fram en erkjennelse av at virkelig globale systemer forutsetter bruk av andre baner både for dekning og forenkling av bakkesegmentet.

Nasjonalt kan dette illustreres ved Telenor Satellite (tidligere Telenor Satellite Broadcasting) som har operert Thor-satellitter i geostasjonær bane i tjue år. Framover kommer også nye initiativ som demonstrasjonssatellitten Arcsat (polar lavbane) skutt opp våren 2022 og Arctic Satellite Broadband Mission (høyelliptisk bane) med planlagt oppskytning i slutten av 2022. Internasjonalt er vel de mest kjente eksemplene kjempekonstellasjonene Starlink (SpaceX), med over tusen satellitter allerede i bane, og OneWeb (i konkursbeskyttelse) med planer om over 600 satellitter i bane. Begge disse systemene består av lavbanesatellitter som skal gi full global internettdekning.

Posisjonering, Navigasjon og Tidsangivelse (PNT): Dette er systemer som gir autonom og presis geolokalisert posisjonsbestemmelse ved hjelp av mottak av tidssignaler fra satellitter med fri siktelinje til brukeren. Denne tjenesten baserer seg på mottak av ytterst presise tidssignaler fra en konstellasjon av globale navigasjonssatellittsystemer (GNSS). Mottagerne bruker så denne tidsinformasjon til å regne ut posisjon i et jordfast koordinatsystem. Opprinnelig ble systemet hovedsakelig anvendt nettopp som navigasjonssystem. I det senere har systemet blitt mer og mer brukt som tjeneste for posisjonsangivelse gjennom at mottageren har blitt så liten at den kan integreres i håndholdte enheter. Etter hvert har også den globale tilgjengeligheten av den meget presise tidsangivelsen blitt viktig i seg selv til kontroll av nettverkssystemer. I dag finnes fire uavhengige slike GNSS-systemer nemlig GPS (amerikansk), Galileo (europeisk), Glonass (russisk) og BeiDou (kinesisk).

Jordobservasjon: Satellitters mulighet for å observere planeten selv på regional og global skala, det være seg menneskelig aktivitet, land sjø eller atmosfære, bidrar til en betydelig forbedret situasjonsforståelse på en rekke områder. Blant disser finner vi:

- *Søk og redning*: Videreformidling av nødsignaler (for eksempel Inmarsat) og trafikkinformasjon (AIS) samt observasjon av hendelser (radar og optisk).
- *Værmelding*: Satellittobservasjoner (f. eks. Eumetsat og NOAA) utgjør et uvurderlig bidrag til alle moderne metrologiske modeller.
- *Maritimt bilde*: Nasjonalt har det vært fokusert på kooperativ overvåkning ved hjelp av AIS. De fem norske satellittene med AIS-mottagere (samt ytterligere data fra internasjonale kilder) har gitt helt nye muligheter for kontroll av de store havområder nasjonen er ansvarlig for.[42]
- *Ressursovervåkning*: Dette kan spenne over alt fra oppdagelse av ulovlig fiske til uttømning av grunnvannsreservoarer. Satellittobservasjoner gjøres med en mengde forskjellige sensorer og er i realiteten eneste måten å skaffe global oversikt.
- *Miljøovervåkning*: Mye av det samme gjelder her. I tillegg utgjør satellittobservasjoner også gjerne den eneste måten å utøve tilstrekkelig kontroll med at internasjonale avtaler faktisk overholdes.
- *Klimaovervåkning*: I tillegg til å verifisere faktiske endringer ved lange måleserier, vil også satellittobservasjoner blir sentrale for å kontrollere overholdelse av forpliktende tiltak under Paris-avtalen.

Mye arbeid på disse siste områdene er avhengig av internasjonalt samarbeid både med bygging og operasjoner av plattformer og sensorer, men i særdeles også deling av data. På europeisk side organiseres utvikling gjerne gjennom ESA, mens operasjon og analyse foregår innen det EU-drevne Copernicus-programmet. Tilsvarende på amerikanske side gjøres ofte utvikling av NASA mens NOAA står for operasjon.

Etterretning: Satellitter har lenge vært et viktig verktøy for innsamling av etterretningsinformasjon på grunn av den globale rekkevidden. I tillegg operer de utenfor det tradisjonelle domenet for luftkontroll og kan således betraktes som særlig robust verktøy for informasjonsinnsamling. Den teknologiske utviklingen har også medført at mindre satellitter kan brukes til innsamling av svært nyttig informasjon. De kan dermed også være et relevant verktøy for små nasjonalstater.

2.5.2 Risiko og trusler

Den delen av romsystemene som er lettest tilgjengelig og følgelig mest utsatt for trusler er bakkesegmentet. Dette segmentet består igjen av tre hovedkomponenter. Kontrollsenteret hvor satellitten styres fra. Dette vil si generering av kommandoer til satellitten og overvåkning av helseparametere fra satellitten. Den fysiske kontakten med satellittene skjer via bakkestasjoner. Siden disse kan være nokså ubeskyttet, er de alltid sårbare for sabotasje. Imidlertid er dette sjelden permanent, og redundans er et effektivt risikoreduserende tiltak her. Disse to elementene

[42] Skauen, 2019; FFI, *Kongsberg-gruppen og FFI samarbeider om maritime overvåkningssatelitter*, 2022

kobles sammen via en nettverksforbindelse enten med dedikerte linjer eller på det åpne nettet. Uansett må kryptering av signalene her sees på som en nødvendighet.

Generelt kan vi si at det er tre hovedtyper av generelle trusler mot romsegmentet. Disse blir kort oppsummert her.

Tjenestetap beror som regel på tap av signal mellom romsegment og bakkesegment av naturlige eller kunstige årsaker. Dette er en regional eller lokal trussel som påvirker både satellittkommunikasjon og PNT-systemer.

Naturlige årsaker er først og fremst forstyrrelser i mediet signalet må krysse. Dette kan bero på både atmosfæriske- og romværforstyrrelser. Effekten på signalet vil arte seg på forskjellig vis alt etter hvilke frekvenser som er i bruk. Dette kan medføre både en forvrengning og fullstendig tap av signalet.

Kunstige årsaker omfatter både jamming og spoofing. Jamming hindrer mottak av informasjon, men det er som regel klart at man er utsatt for det. Spoofing hindrer også mottak av informasjon, men siden man i stedet mottar falsk informasjon kan det være vanskelig å avsløre dette mens det pågår.

Tjenestetap av denne typen er som regel av midlertidig karakter. Romværforstyrrelser er begrensete i tid og både jamming og spoofing kan motvirkes. Normalsituasjonen vil da kunne gjenopprettes.

Kontrolltap skyldes først og fremst cyberoperasjoner. Dette kan for så vidt ramme hvor som helst i systemet. Det blir likevel mest prekært ved tap av kontroll av romsegmentet (satellitten).

Satellitter kontrolleres naturlig nok via radiosamband. Dette kan brytes både gjennom cyberoperasjoner mot kontrollsenteret eller selve satellitten direkte. I siste tilfellet må man eventuelt ha egen sender med større effekt enn den regulære. I begge tilfeller må man ha kjennskap til sårbarheter, kommandoprotokoller og, for noen satellitter, krypteringsmetoder. Dette gjør at slike typer operasjoner gjerne er langsiktige og klandestine etterretningsoperasjoner før en mulig disruptiv fase (oppnå en effekt) iverksettes (jf. kapittel 4.1).

Siden det kan være krevende eller umulig å gjenvinne kontrollen over satellitten, kan det bli svært vanskelig å gjenopprette normalsituasjonen. Ved en fiendtlig overtagelse av satellitten vil denne i tillegg kunne tapes fullstendig ved at det for eksempel gis kommandoer som tømmer batteriene helt.

Ressurstap kan enten skje via naturlige årsaker eller ved fysisk angrep. Naturlig årsaker er knyttet til strålingsskader på selve satellitten. Fysiske angrep på plattformen kan gjennomføres både med strålingsvåpen og kinetiske våpen.

Naturlige risikoer for satellitter har sitt opphav i prosesser i det nære verdensrom. Det naturlige strålingsmiljøet i det nære verdensrom vil alltid utgjøre en mulig risiko, men i forskjellig grad alt etter som hvilke baner som benyttes. I tillegg vil strålingsmiljøet i sterk grad påvirkes av solaktiviteten. Det er tre hovedtyper av satellittbaner. De banene som hele tiden krysser strålingsbeltene, hvor blant annet GPS- og Galileo-satellittene befinner seg, har de største utfordringene med høyenergetiske partikler. Satellitter i geostasjonær bane er fremdeles utsatt for høyenergetiske partikler, men i noe mindre grad. I lav jordbane er strålingsmiljøet atskillig mildere, men ved høy solaktivitet kan det også her være en fare.

Fysiske angrep kan gjennomføres både med laser (størst trussel mot sensorer), EMP-våpen og kinetiske våpen. I det siste tilfellet vil selv et lite prosjektil kunne utrette stor skade ved å utnytte den høye banehastigheten. Kunstige trusler mot satellitter kan deles opp i fire hovedgrupper:

Elektromagnetiske pulser (EMP): Tilstrekkelig sterke elektromagnetiske felt kan ødelegge elektronikk. Til en viss grad kan man beskytte seg mot dette, men i prinsippet vil det alltid foreligge en sårbarhet her. Den handlingen med størst konsekvens vil i så måte være en sprengning av atomvåpen i rommet. Imidlertid vil en slik handling også ødelegge for den som utfører den. I praksis er dette dermed en nokså begrenset trussel. Det går også an å tenke seg mer rettete pulsvåpen. Disse vil kreve så mye energi at det sannsynligvis ikke er veldig aktuelt å velge hvis man først har en aggressiv hensikt.

Kinetiske våpen: Dette er våpen som utgjør en trussel i kraft av sin energi. Siden relative hastigheter i rommet kan være meget store, vil selv et legeme med liten masse utgjøre en anselig trussel. Slike legemer kan lett spres som en sverm. De vil derfor måtte regnes som en reell trussel som det er meget vanskelig å beskytte seg mot. USA, Russland og Kina har også demonstrert egen evne til missilangrep fra bakken mot satellitter.

Romsøppel: Dette består av utrangerte rakett-trinn, døde satellitter samt deler fra tidligere kollisjoner. Som nevnt vil også slike små deler utgjøre en fare på grunn av de høye hastighetene involvert. Romsøppel har egentlig mye av de samme egenskapene som kinetiske våpen bortsett fra manglende intensjon. Et stort problem her er at dette gjerne fører til eksponentiell vekst av deler siden flere biter fra en kollisjon kan føre til mange nye. Denne risikoen har lenge vært prediktert (Kessler-syndromet) og har ytterligere steget ved anvendelsen av de nye mega-konstellasjonene.

Manøvrerbare satellitter: En ny mulig trussel vil være den nye klassen av manøvrerbare satellitter som er i ferd med å vokse frem. Disse brukes egentlig til serviceaktiviteter som Mission Extension Vehicle eller Orbital Removal Vehicle. Imidlertid kan det også være en fordekt måte å nærme seg satellitter på i den hensikt å sette dem ut av spill.

2.5.3 Samfunnseffekter

Som allerede påpekt vil romsystemer kunne forstyrres av både naturfenomen (romvær) og tilsiktete teknologiske angrep. I det følgende vil vi se nærmere på hvilke samfunnseffekter dette kan gi.

Romvær

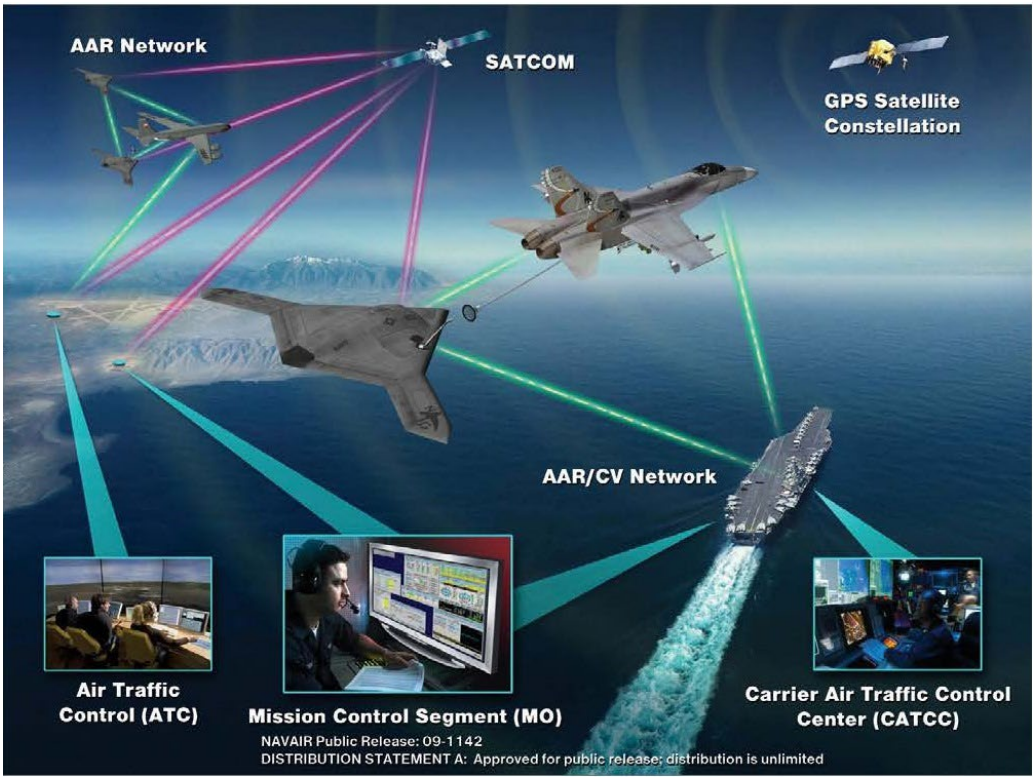
Romvær er et begrep som dekker en rekke prosesser i jordens nære verdensrom. Felles for disse er at de alle er knyttet til vekselvirkningen mellom solen og jorden, og at de kan innvirke på en rekke teknologiske systemer som er av vital interesse i en moderne samfunnsstruktur.

Solstormer ble innlemmet i Direktoratet for samfunnssikkerhet og beredskap (DSB) sitt nasjonale risikobilde første gang i 2012. Den gang ble solstormer ansett som en nokså sannsynlig naturkatastrofe med middels økonomiske konsekvenser for samfunnet. Siden den gang har nok den sterke veksten i bruk av rommet medført at en tilsvarende hendelse vil ha mye større økonomiske konsekvenser. Imidlertid er det sprikende oppfatninger om langtidskonsekvenser. Dette beror mye på hvilke antagelser man gjør om alvorlige skader på strømnettet og tidsperspektivet på nødvendige reparasjoner.

Kommunikasjonssystemer

Utviklingen mot en stadig mer globalisert verden fordrer også globaliserte kommunikasjonssystemer. Dette betyr at satellittkommunikasjon blir en sentral del av mange samfunnsfunksjoner både militært og sivilt.

Militært vil konsekvensene av tapt satellittkommunikasjon først og fremst føre til degradering av kommando og kontroll. I tillegg hindres distribusjon av etterretningsinformasjon samt annen kommunikasjon utover direkte siktlinje. I et nettverksbasert forsvar vil dette kunne medføre et stort tap av slagkraft, særlig i regionale eller globale konfliktsituasjoner. Figur 2.3 illustrerer nettverksforbindelsene i et nettverksbasert forsvar og tydeliggjør de store konsekvensene bortfall av kommunikasjon vil få i et slikt nettverk.



Figur 2.3 Illustrasjon av nettverksforbindelser i et moderne forsvarsoppsett. Illustrasjon: Naval Air Systems Command (NAVAIR)

Tap av tilgang til overvåkningssatellitter vil naturligvis føre til en betydelig redusert situasjonsforståelse. Dette gjelder både for den umiddelbare situasjonen så vel som vurdering av fremtidige hendelser. Dermed vil taktiske planlegging bli vanskeliggjort.

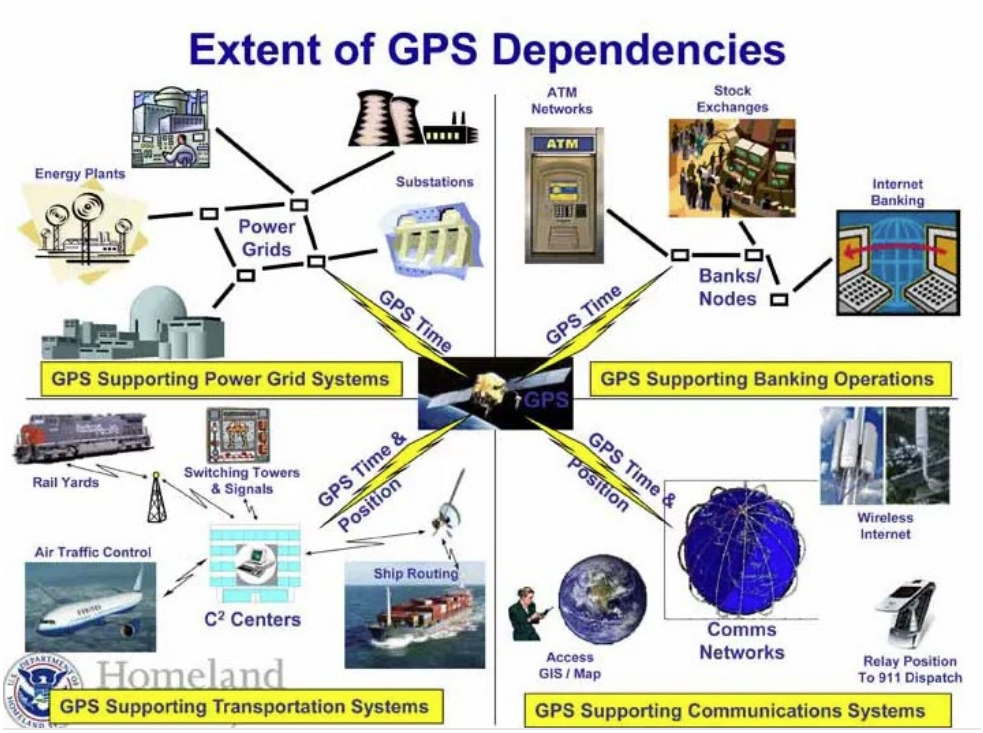
Sivilt vil tap av satellittkommunikasjon vil medføre at et vidt spekter av tjenester i blant annet samfunnskritiske funksjoner, forretningsdrift, underholdning og andre segmenter som er en integrert del av forventede samfunnsfunksjoner faller bort. Dette vil følgelig kunne få store og til dels uoversiktlige økonomiske og sikkerhetsmessige ringvirkninger.

Tap av tilgang til jordobservasjonssatellitter vil kunne degradere både statlige og private tjenester som er avhengig av den innsamlede informasjonen.

PNT-systemer

Signaltap fra romsegmentet, for eksempel ved sterke jonosfæriske forstyrrelser knyttet til kraftige solstormer, kan også påvirke en rekke systemer og prosesser i samfunnet på andre måter. Dette er i realiteten en konsekvens av kommersialisering og miniatyrisering av GPS-mottagere. Miniatyriseringen av disse mottakerne har gjort at de har kunnet integreres i en vid rekke enheter, også håndholdte, som vist i Figur 2.4. Alle disse tjenestene baserer seg på at GPS-signalet er fritt tilgjengelig til enhver tid. Hvis ikke, vil naturligvis moderne

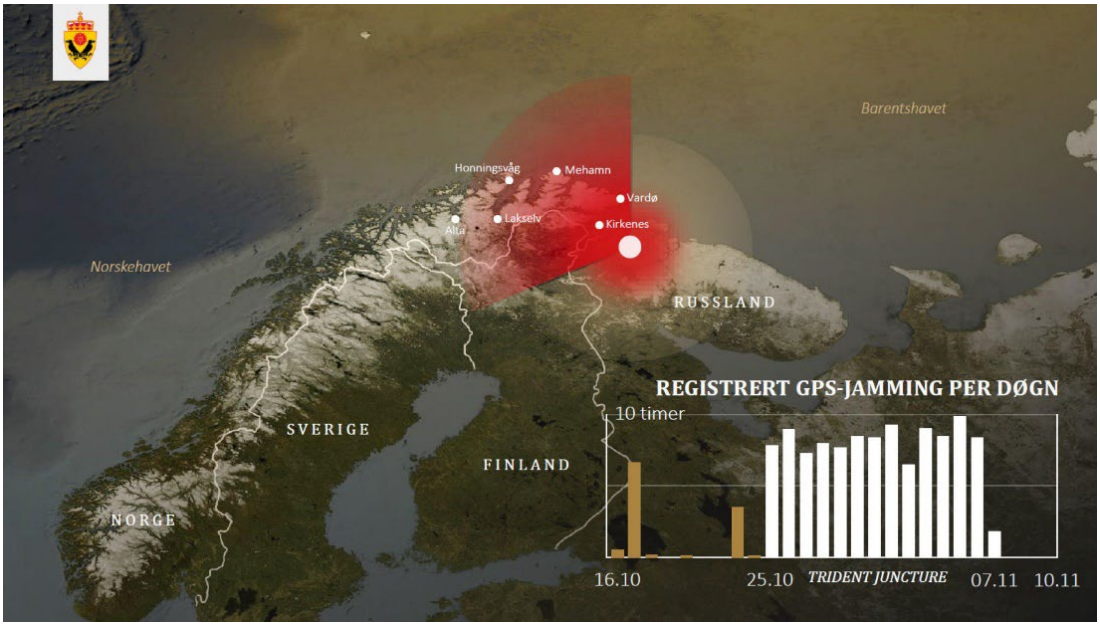
navigasjonssystemer da degradere eller falle helt bort. Utover dette blir i sin tur også en rekke tjenester som er avhengig av brukers posisjonsangivelse til enhver tid satt ut av spill. Dette vil igjen føre til degradering av nytteverdien til en rekke særlig kart- og telefonbaserte tjenester. I tillegg blir det meget nøyaktige tidssignalet i GPS-systemet mer og mer brukt til kontroll av forskjellige nettverk. Dette gjelder både for strømsystemer og finansielle tjenester.



Figur 2.4 Oversikt over områder og systemer hvor GPS-signaler utgjør en integrert del. Illustrasjon: U.S. Department of Homeland Security

Militært vil tap av tilgang til PNT-systemer medføre degradering av egen posisjonsinformasjon samt de tjenester som er avhengige av den. Dette kan være alt fra oppsett av nettverk, til «friendly-force-tracking» og styring av presisjonsvåpen.

I tillegg til romværeffekter er også kunstige trusler en utfordring. Et spesifikt eksempel på effekten av jamming utspilte seg under NATO-øvelsen Trident Juncture høsten 2018. Aktivitet med jamming fra russisk territorium var meget høy i en periode. Dette medførte forstyrrelser over et stort område i Finnmark som illustrert i Figur 2.5.



Figur 2.5 Statistikk over registrert GPS-jamming under øvelsen Trident Junction 2018. Illustrasjon: Etterretningstjenesten

Det er rimelig å anta at hensikten var å forstyrre norsk og alliert øvingsvirksomhet. Imidlertid vil jamming av GPS-signal også i høyeste grad forstyrre mye sivil aktivitet samtidig. Særlig går dette utover flytrafikk og sivil beredskap. I dette tilfellet måtte Avinor innføre alternative flyrutiner. Flere passasjerfly mistet GPS-signal i luftrommet mellom Kirkenes og Lyngen i Troms.[43] Dette er dog systemer som kan gjenopprettes relativt snart etter at signalet er gjenvunnet. Derfor vil også de økonomiske konsekvensene bli håndterbare. I tilfeller hvor kraftdistribusjonssystemer blir rammet, kan dette bli mer omfattende.

Strømnett

En potensielt mer økonomisk utfordrende konsekvens er en eventuell fysisk destruksjon av sentrale komponenter i strømnettet. Dette kan skje som følge av geomagnetisk induserte strømmer i bakken knyttet til variasjoner i jonosfæriske strømmer under romværhendelser. Det kan også være en følge av ukontrollerte styreprosesser ved f.eks. tap av tidssignal. På grunn av slike nettverks natur, kan ødeleggelse av en sentral komponent føre til en rekke følgefeil som forsterker den opprinnelige skaden betydelig. Spesielt kan transformatorer bli ødelagt ved at ukontrollerte strømvariasjoner omdanner elektrisk energi til varme slik at kjernen ødelegges. Slike transformatorer er dyre og fordrer lang bestillingstid. I en situasjon hvor erstatninger ikke nødvendigvis kan anskaffes hurtig kan det få langvarige effekter. Det kan følgelig lede til store stats- og samfunnssikkerhetsmessige konsekvenser og økonomiske tap.

[43] For mer om dette temaet se artikkel i Norsk militært tidsskrift om elektronisk krigføring (EK) i gråsoneoperasjoner, Hovland et al., 2021

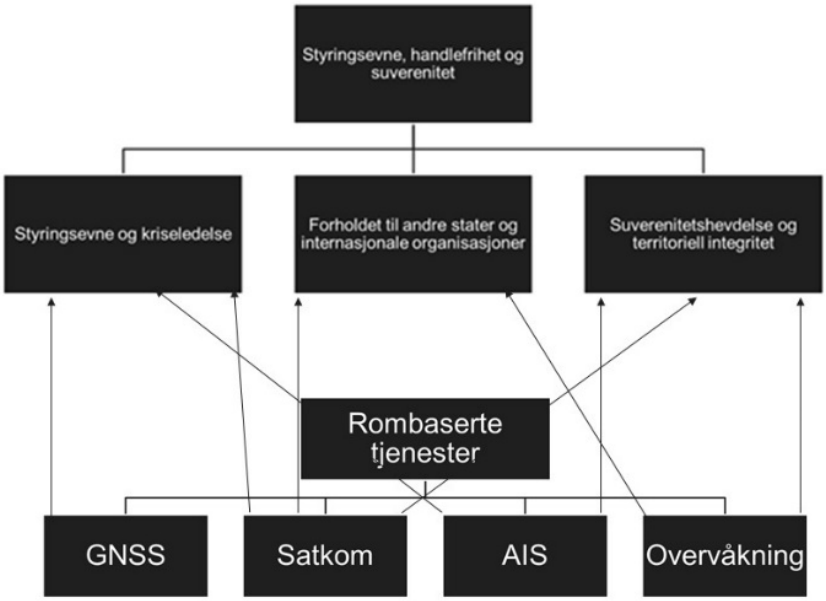
Et eksempel på dette er strømutfallet i Quebec på vinterstid i 1989. Her ble seks millioner innbyggere sittende uten strøm i ni timer 13. mars det året. Dette ga også opphav til en kaskade av følgefeil som påvirket strømnettet i store deler av østkysten i USA. Blant annet ble en transformator i New Jersey, til ti millioner dollar, fullstendig ødelagt.

Hvis en tar høyde for en slik hendelse, vil da signalutfall kunne gi opphav til mer vidtrekkende og langvarige konsekvenser enn bare de mer sannsynlige utfallene i seg selv. Dermed blir også de samfunnsmessige konsekvensene atskillig mer alvorlige. For eksempel vil strømutfall i større områder kunne forårsake ytterligere dominoeffekter ved at både vannrensing og kommunikasjon også kan falle bort dersom strømbruddet blir langvarig. I slike tilfeller kan backup-løsninger med strøm fra batterier og aggregater stanse før strømmen er tilbake.

Tjenesteintegrasjon

I totalforsvarssammenheng betrakter man gjerne noen få viktige nasjonale funksjoner for så å kunne systematisere behov innen hvert av disse. Hvert av disse deles igjen opp med tanke på funksjon og behov slik at man til slutt får et hierarkisk system. Tradisjonelt har det vært vanlig å plassere rombaserte tjenester som et element under samfunnets funksjonalitet på linje med for eksempel transport og finansielle tjenester. Imidlertid er rombaserte tjenester i dag en integrert del av både transport og finansielle tjenesteytelse i form av kommunikasjon- og PNT-tjenester. Dette er også tilfelle for de andre hovedområdene. Et eksempel hentet fra området «styringsevne, handlefrihet og suverenitet» er illustrert i Figur 2.6. Her inngår rombaserte tjenester i alle underelementene. Derfor vil bortfall av rombaserte tjenester fort få følger for en lang rekke områder i et moderne samfunn. Særlig gjelder dette for kommunikasjons- og PNT-systemer. Disse systemene kan relativt hurtig medføre problemer siden dette er teknologier som regnes som åpent og kontinuerlig tilgjengelige for en mengde tjenester. På litt lengre sikt vil også bortfall av informasjonsinnsamling fra rommet medføre vansker med situasjonsforståelse både militært og sivilt. Arbeid for å bedre robusthet i romsystemer bør derfor ha høy prioritet fremover. Følgelig er da også flere rombaserte tjenester meldt inn som grunnleggende nasjonale funksjoner etter sikkerhetsloven.[44]

[44] NSM; *Oversikt over innmeldte grunnleggende nasjonale funksjoner*, 2022



Figur 2.6 Skjematisk framstilling av den inngripende avhengighet av rombaserte systemer for styringsverktøy i et moderne samfunn. Illustrasjon: FFI

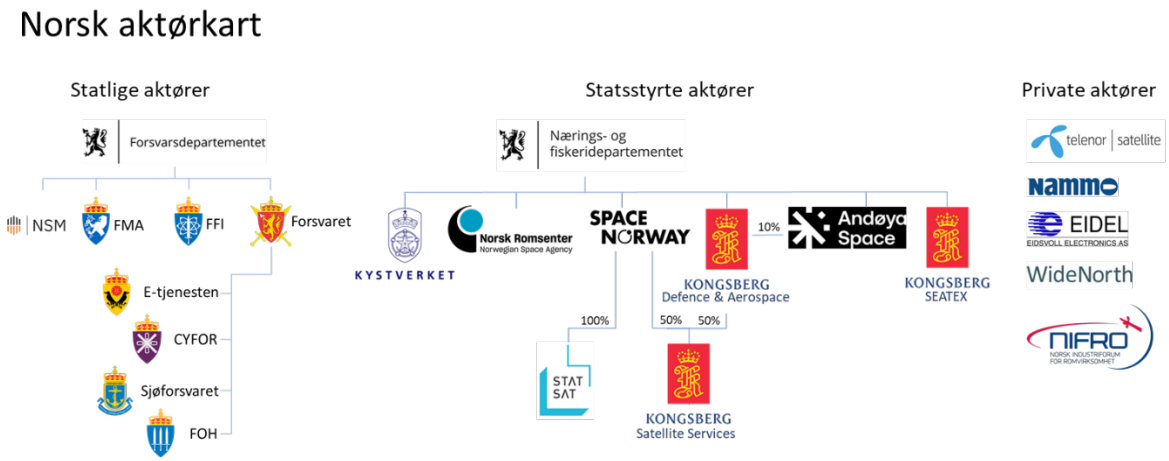
2.5.4 Trender

Bruken av rommet er for tiden under sterk utvikling både nasjonalt og internasjonalt. Fra 2020 har NATO betraktet rommet som et eget militært domene.[45] Noen andre hovedtrender er også allerede godt synlig og tas derfor med i det følgende.

Flere nasjonalstater

Fremveksten av stadig mer kapable småsatellitter har ført til at små nasjonalstater har sett muligheten av å benytte seg av romsystemer i flere sammenhenger. Norge har for eksempel tatt i bruk satellitter i maritim overvåkning og vil også i større grad gjøre det i forsvarssammenheng. Den store mengden av nasjonale aktører gjør i seg selv at romdomenet blir mer uoversiktlig og gjenstand for kryssende interesser. Dermed blir det for eksempel vanskeligere å oppnå en global konsensus for regulering av aktiviteten. Dette er problematisk fordi både baneplassering og særlig båndbredde i realiteten er endelige naturressurser. Også her i Norge er det en utvikling på dette området. De fleste aktørene tradisjonelt vært tilknyttet Forsvarsdepartementet og Nærings- og fiskeridepartementet (Figur 2.7). Ettersom rommet nå er blitt et eget militært domene, er det å vente at Forsvaret også vil ta en mer selvstendig rolle på dette området. Med et økende aktivitet i dette domenet vil dette også bli et mer interessant marked for industriaktører.

[45] NATO STO, 2023



Figur 2.7 Oversikt over nasjonale aktører innen romteknologi og rombaserte tjenester. Illustrasjon: FFI

Kommersialisering

Det har lenge vært et kommersielt element i utnyttelsen av rommet i form av tilbydere av kommunikasjonsressurser særlig fra geostasjonær bane. Imidlertid har det i løpet av det siste tiåret vært en formidabel eksplosjon av private aktører i alle deler av romsystemene. Dermed har man sett framvekst av egne investeringsfirma som hovedsakelig satser på å finansiere nye romsystemer. Dette har medført at det i dag er kommersielle aktører inn i alle tenkelig deler av romsystemer som oppskytning, plattformtilvirkning, instrumenttilvirkning, kommunikasjon, datainnsamling og tolkning samt etterretning. Riktignok er fremdeles en god del av denne forretningsvirksomheten avhengig av det offentlig som hovedkunde. Dette gjelder for eksempel innen innsamling av meteorologiske data, miljødata og vitenskapelige data. I tillegg er det nå to private firma (SpaceX og Blue Origin) som står for transporten av astronauter til og fra den internasjonale romstasjonen. NASA har ikke lenger kapasitet til å gjøre dette selv.

Også innen innsamling av etterretningsdata fra rommet gjør nå private aktører seg gjeldende på samme måte som andre aspekter av etterretning også privatiseres. Dette illustreres best ved å se på hvordan billedinformasjon i forbindelse med den pågående invasjonen av Ukraina har vært brukt i det offentlige rom. Veldig mye av bildene brukt i nyhetssammenheng har blitt innsamlet av Maxar Technology og frigitt i forståelse med amerikansk etterretning, som også er deres hovedkunde. Det mest kjente eksempelet er kanskje den enorme russiske militærkolonnen vist i Figur 2.8.

Figur 2.8 Deler av en stor russisk militærkolonne i nærheten av Kyiv fra april 2022. Foto: NTB/ AFP PHOTO / Satellite image ©2022 Maxar Technologies

Også signaletterretning blir nå kommersialisert. Den fremste eksponenten for dette er amerikanske Hawkeye 360. De har sin egen konstellasjon som samler inn og lokaliserer kilder i en svært vid del av radiofrekvensspektrumet. Hawkeye har påvist og offentliggjort omfattende russiske forsøk på jamming av GPS-signaler under Ukraina-invasjonen.

Blant Hawkeye 360s produkter finnes det, i tillegg til deteksjon av GPS-jammere, også deteksjon av skipsradarer, L-bånd satellitt-telefoner, nødpeilesendere, AIS-sendere og skipsradioer. Franske Unseenlabs har et lignende forretningsområde. I Norge har Kongsberg Defence & Aerospace AS (KDA) varslet at de vil satse på en egen konstellasjon av maritime overvåkningssatellitter (Figur 2.9). Disse vil detektere AIS-sendere og skipsradarer.

Figur 2.9 Illustrasjon av Kongsberg Defence & Aerospaces maritime overvåkningskonstellasjon. Illustrasjon: Norsk romsenter

Også høykvalitet syntetisk aperture radar (SAR) data er nå tilgjengelig kommersielt. Det opprinnelige finske selskapet Iceye kan levere slike data med bedre enn en meter oppløsning.

Selv PNT-konstellasjoner (som GPS og Galileo) kan få privat konkurranse fra for eksempel det amerikanske firmaet Xona Space Systems. De planlegger en egen konstellasjon av mikrosatellitter i lav jordbane. Også tjenester innen Space Situational Awareness (som vedlikehold av katalogtjenester for objekter i bane) er interessant for private firma. For eksempel leverer LeoLabs allerede utmerkete tracking-tjenester for lavbane satellitter og romsøppel. Dette var det tidligere bare offentlige institusjoner som det amerikanske forsvaret eller ESA som hadde tilstrekkelige ressurser til å gjennomføre.

Megakonstellasjoner

De nye megakonstellasjonene som Starlink, OneWeb og Kuiper utgjør et nytt element i lav jordbane. Dette vil kunne medføre en økning i kjente problemer som kollisjonsfare, signalinterferens og «tracking» (situasjonsforståelse i rommet). Dermed vil de kunne utgjøre en ny risiko (Figur 2.10). På den annen side vil dette også kunne øke fleksibiliteten av systemer ved at de inneholder mange innbyrdes utskiftbare elementer. Dette vil da gi en øket robusthet. Dette illustreres kanskje best ved å se på den sentrale verdien av Starlink for Ukrainas kommunikasjon med utenverden under den russiske invasjonen. Donasjonen av terminaler og fri tilgang til dette systemet har muliggjort en fortsatt internettdekning over hele landet. I realiteten

har Starlink på meget kort tid blitt et alternativt nasjonalt kommunikasjonssystem. I en krigssituasjon er dette selvfølgelig en stor fordel, men i andre situasjoner kan dette derimot bety tap av nasjonal kontroll av systemet.

Figur 2.10 Illustrasjon av internettdekning ved hjelp av lav-bane satellitter til megakonstellasjoner som Starlink, OneWeb og Kuiper. Illustrasjon: Adobe Stock

3 Klima og energisikkerhet

Menneskeskapte klimaendringer har ført til at gjennomsnittstemperaturen øker og ekstremvær vil ramme oss hyppigere, over større tidsintervall og mer ekstremt enn tidligere. Vi opplever allerede oftere og kraftigere hetebølger og tørke, kraftig nedbør og hyppighet, samt intensitet av tropiske sykloner og reduksjon i arktisk havis, snømengder og permafrost. I det følgende skal vi se nærmere på Norges utslippsforpliktelser, endringer i energisystemet og hvilken betydning dette kan få for energisikkerhet og nasjonale sikkerhetsinteresser.

3.1 Klimamål og forpliktelser

Paris-avtalen fra 2015 setter et globalt mål om maksimalt 1,5 °C temperaturøkning for å unngå de største klimamessige påvirkningene og katastrofene. Med dagens tempo i reduksjon av klimagasser og overgang til fornybare energikilder, vil det tilgjengelig karbonbudsjettet i beregningene for 1,5 °C-målet være brukt opp allerede i 2030, og det ligger an til en temperaturøkning på 2,3 °C innen 2100.[46,47]

Gjennom ECs GreenDeal har kravene til utslippskutt i EU og EØS blitt styrket. Gjennom «Fit for 55»-planen av juli 2021 er ambisjonen for medlemslandene i EUs klimalovgivning at klimagassutslippene skal kuttes med minst 55 % innen 2030 i henhold til 1990-nivået.[48] Dette er et delmål på veien til å oppnå karbonnøytralitet innen 2050. De styrkede kravene fra EU ble dermed lansert før Norge økte sine forpliktelser til kutt av klimagassutslipp til 55 % under COP26 i Glasgow i november 2021. Dette indikerer at Norge ikke lenger ligger i front med å ta initiativ til klimakutt.

Norge har forpliktet seg til å redusere utslippet av klimagasser med 55 % sammenliknet med 1990-nivå innen 2030 og å nå et karbonnøytralt lavutslippssamfunn innen 2050 ved å redusere utslippene med 90–95 %.[49] I april i 2022 konkluderte Organisasjonen for økonomisk samarbeid og utvikling (OECD) med at Norges innsats for å begrense klimagassutslipp frem til i fjor setter Norge på kurs mot 20 prosent kutt i klimagassutslipp innen 2030.[50] Det betyr at Norge har brukt 30 år på å redusere landets utslipp med i underkant av 5 prosentpoeng, og at vi nå har knappe 8 år på å kutte resten.[51] Den lave reduksjonen i klimagassutslipp per år fram til nå betyr at vi må få en betraktelig økning i reduksjonen per år i de gjenværende årene fram mot 2030. Det grønne skiftet er derfor en enorm utfordring der det fortsatt er usikkerheter i hvordan man skal

[46] IPCC; *AR6 Climate Change 2021: The Physical Science Basis, Technical summary*, 2021

[47] DNV; *Energy Transition Outlook 2021*, 2021

[48] EC, *Fit for 55*, 2023

[49] Meld. St. 13 (2020–2021), 2021

[50] NrK; *OECD kritiserer Norges klimainnsats: Ligger ikke an til å nå målene*, 2022

[51] SSB; *Forurensning og klima - Utslipp til luft*, 2022

balansere klimakutt og kost-effektivitet med hva som er politisk, sosialt og miljømessig akseptabelt.

I klimaplanen for 2021–2030 fastslås det at for å nå klimamålene så kreves det elektrifisering av samfunnet så som transportsektoren, industri og innen olje- og gassproduksjon.[52] Selv om Norge ligger langt framme med tanke på elektrifisering og andel fornybare energikilder og transport i energimiksen, så bruker vi mer energi (~50 %) og slipper ut mer klimagasser (~20 %) per innbygger enn gjennomsnittet i EU.[53] Gjennom Helsinki-deklarasjonen forplikter Norge seg til å samarbeide med de nordiske landene for å nå klimamålsetningene. For å oppnå full overgang til fornybare energikilder i Norden, må energisystemene samhandle og koordineres på tvers av landegrensene.[54] Dette krever et transnasjonalt samarbeid langt utover kun dagens felles el-marked Nord Pool.

Som følge av energikrisen i Europa og den negative effekten Russlands invasjon av Ukraina har hatt på det globale energimarkedet, har EU også lansert planen «REPowerEU».[55] Planen skal sørge for energieffektivisering, akselerert produksjon av og overgang til ren energi og diversifisering av energiforsyningen. Videre skal planen støttes opp av økonomiske og juridiske tiltak for å bygge den energiinfrastrukturen og -systemet som Europa trenger i et energisystem basert på fornybare energikilder.

Behovet for raskere utslippskutt og overgang til fornybare energikilder, forventede ytterligere styrking av kravene til utslippskutt fra EU og kompleksiteten i et energisystem med variable energikilder og gjensidig energiavhengighet på tvers av landegrenser danner et komplekst grunnlag for utviklingen av framtidens energisystem.

3.2 Utslippskutt i et nordisk energisystem

Det har blitt publisert en rekke rapporter om status for klimaendringer, framtidsutsikter og hvordan vi skal kunne kutte utslipp av klimagasser i tide for å kunne forhindre de største klimaendringene. *Nordic Clean Energy Scenarios* er en rapport som har utviklet tre scenarioer for hvordan Norden i fellesskap skal oppnå karbonnøytralitet innen 2050.[56] Scenarioene baserer seg på samhandling mellom de nasjonale energisystemene og på optimalisert bruk av hvert enkelt lands hovedressurser. Felles for disse scenarioene er at energiforbruket må ned gjennom direkte elektrifisering og økt energieffektivisering. Andelen fossilt drivstoff i Nordens primære energiforsynlig må reduseres fra ca. 40 % i 2020 til mindre enn 10 % i 2050. Samtidig øker Nordens strømbehov med 40–100 % fra 2020–2050, hvilket viser viktigheten av elektrisitet som energibærer. I luftfarten er utslippsnivåene antatt å forbli på 2019-nivå fram til 2030,

[52] Meld. St. 13 (2020–2021), 2021

[53] NER; *Nordic Clean Energy Scenarios – Solutions for carbon neutrality*, 2021

[54] NER; *Nordic Clean Energy Scenarios – Solutions for carbon neutrality*, 2021

[55] EC; *REPowerEU: A plan to rapidly reduce dependence on Russian fossil fuels and fast forward the green transition*, 2022

[56] NER; *Nordic Clean Energy Scenarios – Solutions for carbon neutrality*, 2021

deretter må den reduseres til 0 % i 2050. Utslippsnivåene i shipping reduseres lineært med 90 % innen 2050. Atferdsendring og energieffektivisering er viktige faktorer som kan lette overgangen i alle scenarioene.

3.3 Elektrifisering av samfunnet

Gjennomføringen av forpliktelsene i Helsinki-deklarasjonen er avgjørende for å få en full overgang til og fornuftig bruk av de fornybare energibærerne i Norden. Det siste årets utvikling i elektrisitetsforsyning og -marked har satt stort fokus på framtidige sårbarheter i energisystemet. Dette er sårbarheter som befolkningen antakelig ikke har hatt høy bevissthet om, men som nå er høyt på samfunnsagendaen.

Elektrifiseringen av samfunnet gir økt strømbehov. Kombinasjonen av økt strømbehov og variable energikilder gir utfordringer med tanke på optimalisering i sammensetningen av energimiksen av variable energikilder og responstid dersom feil skulle oppstå. Elektrifiseringen av ulike sektorer i samfunnet slik som transportsektoren, kraftkrevende industri og bygg og anlegg fører til en tett kopling med energisektoren. Behovet for økt fleksibilitet og optimalisering av systemet vil kreve full automatisering for å kunne møte utfordringene som oppstår i et svært komplekst, sektorkoblet system. Digitalisering vil dermed danne grunnlaget for et effektivt, karbonnøytralt energisystem som bevarer den energisikkerheten samfunnet er vant til å ha.

For å kunne nå klimamålene, må integreringen av fornybare energikilder i energisystemet og implementeringen av nye kontrollsystemer for å håndtere dette gå raskt. Det medfører en økt risiko for svakheter i disse systemene. Dette er en følge av at alle nye systemer vil inneha en viss grad av feil og i tillegg fordi disse systemene vil være svært komplekse. Ettersom kompleksiteten og digitaliseringen av energisystemet øker, vil frekvensen av uventede hendelser øke. Automatiserte systemer gjør samtidig at tregheten i systemet blir mindre. Dette gjør systemet mer følsomt for slike hendelser og gir oss kortere responstid for å håndtere feil og forhindre kaskadekonsekvenser. Energisystemet blir derfor mer sårbart for tilsiktede handlinger så som cyber- og fysiske angrep, men også for hendelser som følge av menneskelige feil, ekstremvær, uventede produksjonsstopp, endringer i forbruk og transmisjon, sosial manipulering av energiadferd med mer.

Økt sårbarhet, utfordringer med pålitelighet og motstandsdyktighet i systemet, økt kompleksitet i feilsøking og dermed reparasjonstid øker potensialet for hyppigere, langvarige strømbrudd over større områder, ikke bare i Norge, men i Norden. Disse utfordringene vil ha direkte, fysisk påvirkning på samfunnet siden de kan føre til bortfall av kritiske samfunnsfunksjoner så som vannforsyning, helsetjenester, elektronisk kommunikasjon, betalingstjenester mm. Dette har store innvirkninger på samfunnssikkerhet, energisikkerhet og cybersikkerhet på et transnasjonalt nivå, ikke kun nasjonalt nivå, og vil medføre gjensidig avhengighet mellom oss og våre nordiske naboer. Sikring av fysisk og digital energiinfrastruktur, fleksibilitet og motstandsdyktighet i systemet er avgjørende. Gitt kompleksiteten i nye systemer og de transnasjonale avhengighetene i framtidens energisystem, bør nye systemer koordineres på tvers

av landegrensene og sikringstiltak utvikles i samarbeid med våre nordiske naboer. Dette er viktig både for å forhindre sikringstiltak i systemet som potensielt kan motarbeide hverandre under en håndtering av en hendelse og sikre tilstrekkelig drift, men også for raskere og mer kostnadseffektivt finne gode løsninger som sikrer funksjonaliteten i våre fremtidige samfunn.

Videre kan den privatiserte kraftforsyningen og ren markedsøkonomisk styring gi oss en rekke utfordringer fremover utover forsyningssikkerhet av elektrisitet. I et bredere samfunnsmessig perspektiv kan for eksempel energifattigdom også bli et samfunnsproblem av betydning i Norge. Energisikkerhet og et resilient energisystem basert på fornybar energi som også er utviklet med tanke på sosial bærekraft, bevaring av naturmangfold og flere av FNs bærekraftsmål bør være sentralt.

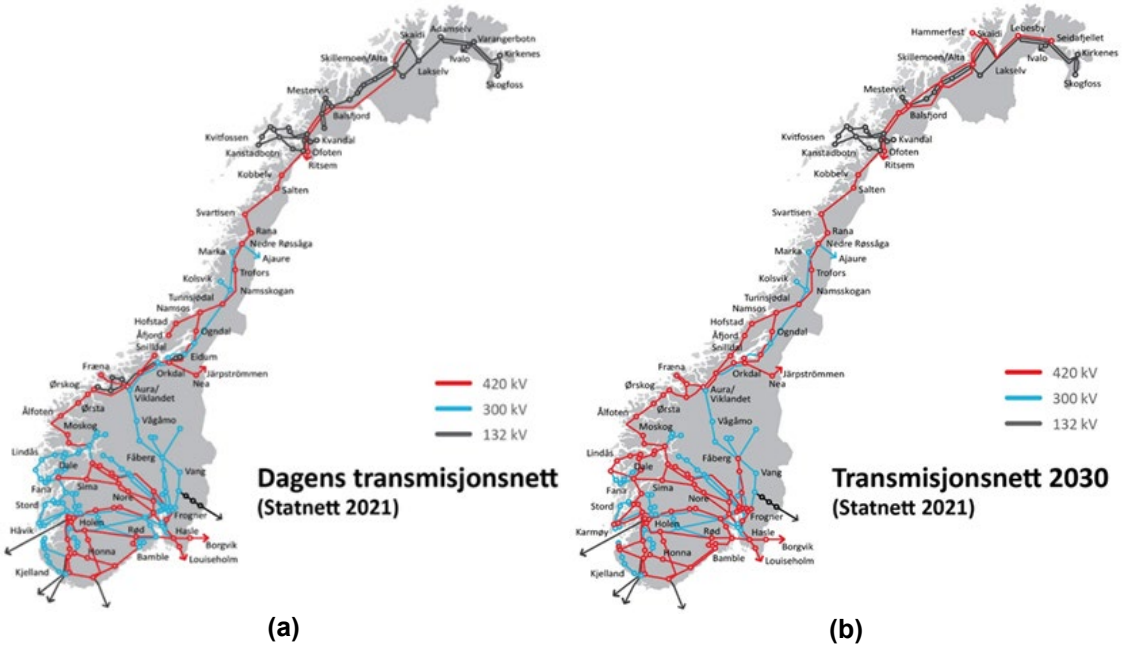
3.4 Drift av kritiske samfunnsfunksjoner

I dette delkapitlet vil vi se på planlagt utvikling av transmisjonsnettet og noen mulige tiltak for å sikre drift av kritiske funksjoner i samfunnet, hvilket også vil være av høy viktighet for totalforsvaret.

3.4.1 Planlagt utvikling av Norges transmisjonsnett

Kartet over dagens transmisjonsnett i Figur 3.1a viser tydelig at det kun er én 420 kV overføringslinje mellom Nord-Norge og Trøndelag. Denne ene hovedåren har en begrenset overføringskapasitet, som igjen begrenser overføringskapasiteten mellom nord og sør i Norge. Dette er en av årsakene til at det ikke har vært mulig å dekke strømbehovet sør i Norge i 2022, og dermed utjevne prisene, ved å overføre nok billig strøm fra et Nord-Norge med gode produksjonsforhold til et Sør-Norge med lav fyllingsgrad i vannmagasinene. Dagens transmisjonsnett viser dermed tydelig sårbarhetene i strømforsyning mellom Nord- og Sør-Norge.

I Statnetts planer for utbygging av transmisjonsnettet for 2030 (Figur 3.1b) er det fokusert på en del utbygging av 420 kV-overføringskapasitet i Sør-Norge og noe utvidelse med parallelle transmisjonslinjer i Nord-Norge, men det skjer lite eller ingen endringer i området fra nord i Trøndelag til området noe nord for Lofoten/Balsfjord.



Figur 3.1 Transmisjonsnett i Norge med hovedoverføringslinjer for strøm for (a) dagens situasjon og (b) i 2030. Illustrasjon: Statnett nettutviklingsplan 2021

3.4.2 Mikrodrift i øymodus

Gitt problemene med pålitelighet og resiliens i det kommende energisystemet, bør man se på hvilke muligheter som finnes for å opprettholde kritiske funksjoner i samfunnet og totalforsvaret. Mikrodrift i øymodus av kritiske områder kan være en løsning som kan bidra til å redusere sårbarheten for og effekten av langvarige strømbrudd. Microdrift i øymodus betyr her at lokale/regionale områder kan driftes separat fra nasjonalt strømnett basert på lokale energikilder og energilagring. Dette vil kunne være spesielt viktig i områdene nord for Trøndelag der utfordringene er aller størst dersom det skulle oppstå en hendelse i transmisjonsnettet. I dette området er det store avstander, utfordrende geografi/topografi, utfordrende klima og tiltagende ekstremvær som følge av klimaendringene. Det er også et område som er svært viktig med hensyn til alliert mottak og forsvar av landet mot et potensielt russisk angrep. Alle disse faktorene bidrar til økt sårbarhet i dette området. Klimaendringene med reduksjon i havis og endrede sikkerhetspolitiske forhold gir økt press i området og ytterligere behov for sikring og drift av energisystemet.

Hensikten med mikrodrift i øymodus er å kunne opprettholde forsyningssikkerhet av strøm, og dermed også drift av de funksjonene som er kritiske for samfunn og sikkerhet. Etter hvert vil man også forhåpentlig kunne sikre et minimum av drift for private husstander og andre offentlige tjenester. Det kan også bidra til styrket forsyningssikkerhet i en normaltilstand, og dermed bidra til å økt redundans som reduserer behovet for å overføre strøm mellom regioner i transmisjonsnettet på maksimal kapasitet.

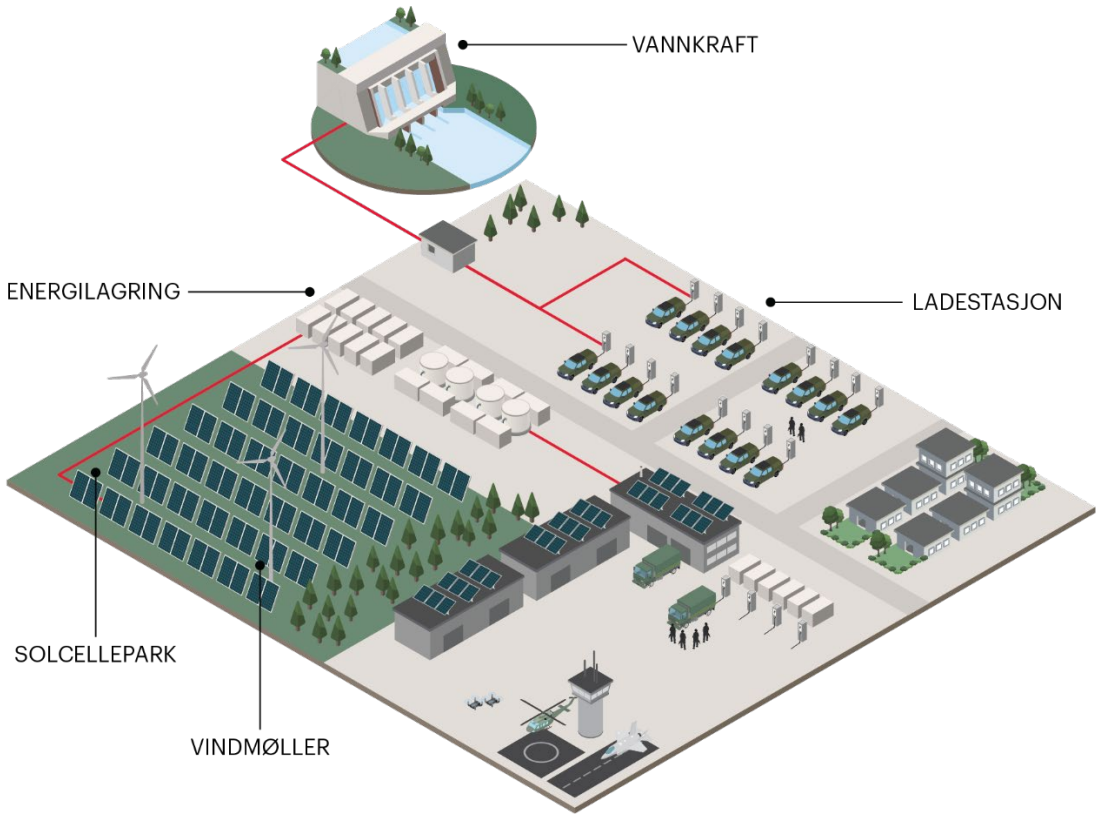
For å kunne sikre drift av kritiske samfunnsfunksjoner gjennom å introdusere et mikrogridsystem i et gitt område, så må den geografiske plasseringen av nåværende og potensielle energikilder, både lokalt og regionalt, samt lagringsmuligheter for energi sees i sammenheng med lokalisering av disse funksjonene. Videre må systemavhengigheter og energibehov kartlegges og både nasjonale og transnasjonale muligheter for energitilgang bør vurderes. I et totalforsvarsperspektiv bør både sivile og militære behov vurderes og sammenliknes. En helhetlig tilnærming i utviklingen av løsninger der aksept i befolkningen og påvirkning på miljø og natur har en sentral plass vil være avgjørende. Et tenkt kritisk område med muligheter for mikrodrift i øymodus er illustrert i Figur 3.2.

Figur 3.2 Illustrasjon av et tenkt område der kritiske funksjoner er lokalisert og med utnyttelse av lokale energimuligheter for å sikre mikrodrift av disse kritiske funksjonene i øymodus. Illustrasjon: AdobeStock

Som illustrert i Figur 3.2, kan flere små enheter gi nok effekt til å drifte det som er mest kritisk. Dette kan være mer akseptabelt for befolkningen og bidra til mindre påvirkning på miljø og natur. I tillegg vil dette fra et sikkerhetsperspektiv kunne bidra til å redusere risiko siden mange små enheter er vanskeligere å slå ut enn noen få store.

På samme måte som kritiske områder i det sivile kan driftes i øymodus, kan man også se for seg forsvarsbaser som små lokalsamfunn med kritiske funksjoner, med tillegg av spesielle behov innen drift av våpensystemer, operative systemer og støttesystemer (Figur 3.3). Man bør dermed gjøre de samme avhengighets- og behovsvurderinger som i det sivile tilfellet, og undersøke

hvilke kombinasjoner av energikilder og lagringsmuligheter som kan brukes på en forsvarsbase. Dette kan bidra til å redusere Forsvarets avhengighet av nasjonalt strømnett og til sivil understøttelse, muliggjøre selvforsyning av energi for forsvarsbaser og redusere muligheten for en potensiell kamp om energi mellom sivile og militære interesser i en krisesituasjon. Dette temaet og konsekvenser av klimaendringene og klimatilpasninger for Forsvaret behandles i rapport til Forsvarskommisjonen *Konsekvenser av klimaendringer og klimatilpasninger for Forsvaret fram mot 2040 – rapport til Forsvarskommisjonen*.[57]



Figur 3.3 Illustrasjon av muligheter for generering og lagring av energi ved en tenkt forsvarsbase. Illustrasjon: FFI

3.5 Energisikkerhet og transnasjonale avhengigheter

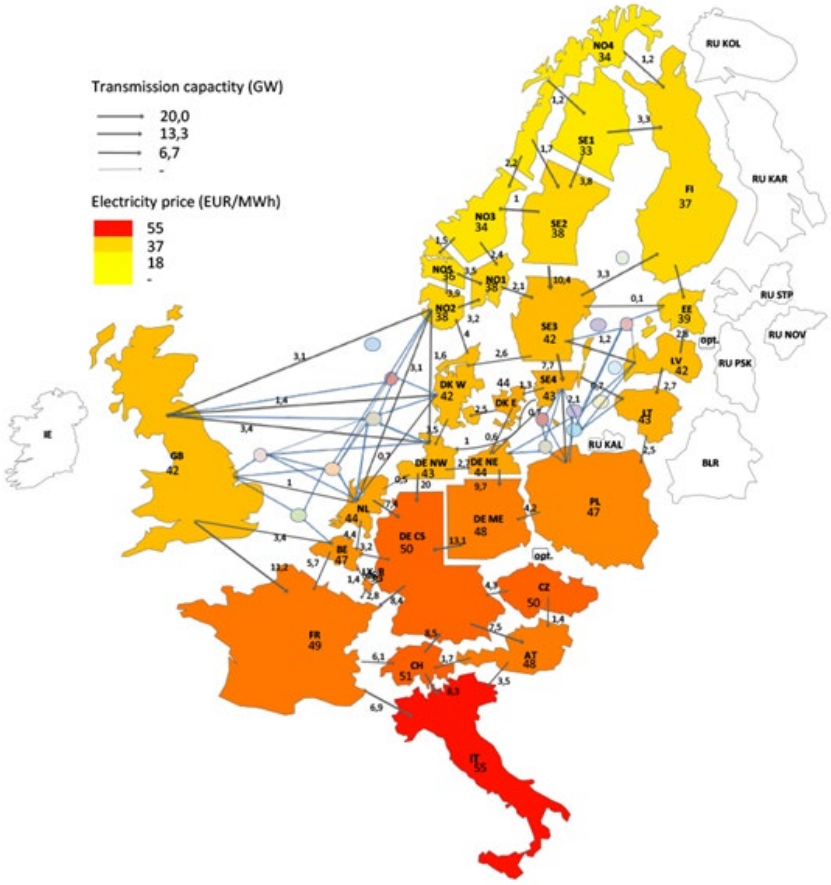
I en situasjon med stadig strengere klimatiltak og omlegging av alle energisystemets bestanddeler, med avtaler om økt nordisk forsvarssamarbeid og med Sverige og Finland som nye NATO-medlemmer, er det viktig å se på mulighetene som ligger i utviklingen av felles løsninger. Ikke bare fordi dette kan bidra til å finne nye løsninger raskere og potensielt mer kostnadseffektivt, men det kan også være avgjørende for å sikre og opprettholde operasjonskapabilitet på tvers av landegrensene. Figur 3.4 viser transmisjonsnettet i Norden i

[57] Granlund et al., 2022

2021. Kartet viser at både Sverige og Finland har mange av de samme utfordringene som Norge i form av utbygging av transmisjonsnett. Dette har blitt tydelig det siste året da også Sverige og Finland har hatt utfordringer med transmisjonskapasitet fra nord til sør og dermed kraftig økende strømpriser. Videre har begge land tilsvarende geografi og klimatiske utfordringer, særlig i nord hvor energisystemet er dårligst utbygd. Vi har energikilder som er både like, men også som komplementerer hverandre. Da de nordiske land har kommet langt i overgangen til fornybare energikilder, har vi gjennom samarbeid om utvikling av framtidens energisystemer en unik mulighet til å oppnå energisikkerhet på grunnlag av fornybare kilder i Norden. Videre har vi også mulighet til ikke bare å eksportere grønn energi til Europa, vi kan også eksportere de løsningene vi utvikler for framtidas energisystem.

Figur 3.4 Transmisjonsnett i Norden i 2020. Illustrasjon: [Svenska Kraftnät]

Videre er energiproduksjon og -sikkerhet i Norden av stor betydning også for et stabilt europeisk energisystem. Som illustrert Nordic Clean Energy Scenarios-rapporten for framtidig prisnivå og transmisjonskapasitet i Europa i 2050 i Figur 3.5, er det store avhengigheter mellom europeiske land og til eksport av strøm fra Norden, herunder spesielt fra Norge.[58] Det kan medføre at det norske og nordiske energisystemet vil bli mer attraktivt for både cyber- og fysiske angrep ettersom effektene av slike angrep vil kunne få følgeeffekter langt utover Norge og Nordens grenser. Dette understreker ytterligere viktigheten av felles utvikling av et resilient, framtidig energisystem der kompatible løsninger og transnasjonale avhengigheter er i fokus.



Figur 3.5 Framtidig handel og transmisjonskapasitet i Europa i 2050 som beregnet i Nordic Clean Energy Scenarios. Illustrasjon: Nordic Clean Energy Scenarios, 2021

[58] NER; *Nordic Clean Energy Scenarios – Solutions for carbon neutrality*, 2021

4 Sammensatte trusler

I dette kapittelet beskrives hvordan sammensatte trusler kan påvirke Norges nasjonale sikkerhetsinteresser. Sammensatte trusler er en betegnelse på:

> «….strategier for konkurranse og konfrontasjon under terskelen for direkte væpnet konflikt som kan kombinere diplomatiske, informasjonsmessige, militære, økonomiske og finansielle, etterretningsmessige og juridiske virkemidler for å nå strategiske målsettinger. Virkemiddelbruken er gjerne bredt distribuert, er langsiktig i sin tilnærming og kombinerer åpne, fordekte og skjulte metoder.»[59]

De utvalgte virkemidlene som behandles i denne rapporten er cyberoperasjoner, påvirkningsoperasjoner i informasjonsmiljøet og økonomisk virkemiddelbruk.

4.1 Cyberoperasjoner

Dette delkapittelet vil fokusere på ressurssterke avanserte aktører som kan true stats- eller samfunnssikkerheten i Norge. Spennet av trusler er bredt og inkluderer aktivister, kriminelle og statlige aktører. Trusselvurderinger fra Etterretningstjenesten og PST trekker spesielt frem Russland og Kina som de alvorligste truslene.[60,61] Etterretnings- og sikkerhetstjenester i disse landene står bak de mest avanserte operasjonene, men begge landene bruker også stedfortredere som for eksempel kriminelle eller hacktivistgrupper. Det finnes også en rekke kommersielle leverandører av komplette skadevareløsninger eller komponenter som kan brukes ved utvikling av skadevare. Enkelte stater bruker slike leverandører i sine offensive cyberoperasjoner.[62] Dette kan tilføre ekstra kompleksitet i en eventuell hendelseshåndtering.

4.1.1 Typer av offensive cyberoperasjoner

Statlig maktanvendelse i det digitale rom deles ofte inn i offensive og defensive cyberoperasjoner. Offensive cyberoperasjoner deles igjen inn i cyberoperasjoner for etterretning og cyberoperasjoner for effekt. Det er formålet med cyberoperasjonen som avgjør om vi klassifiserer den for å være for etterretning, effekt eller eventuelt begge.

Offensive cyberoperasjoner med **etterretningsformål** gjennomføres for å oppnå uautorisert tilgang til informasjon som befinner seg utenfor egne datasystemer. De bryter således med systemenes konfidensialitet. Primærformålet er å bidra med situasjonsforståelse og fungere som

[59] Meld. St. 10 (2021–2022) s. 15, 2022

[60] Etterretningstjenesten; *FOKUS 2022*, 2022

[61] PST; *Nasjonal trusselvurdering 2022*, 2022

[62] For eksempel Zerodium (https://zerodium.com/) eller NSO Group (https://www.nsogroup.com/)

beslutningsstøtte på, hovedsakelig, strategisk og operasjonelt nivå, men enkelte land benytter dem også for økonomisk vinning. Denne typen etterretningsoperasjoner, ofte omtalt som nettverksoperasjoner, utgjør således ikke noe nytt. Likevel gjør cyberdomenets egenskaper at denne etterretningsvirksomheten kan gjøres i en mye større skala nå enn hva som var mulig tidligere. Da hensikten til etterretningsoperasjoner er å få tilgang til sensitiv informasjon, er det ofte essensielt at motparten ikke forstår at informasjonen er på avveie. Cyberoperasjoner med etterretningsformål er derfor omgitt av hemmelighold. For å unngå å bli oppdaget, er det viktig at den tekniske gjennomføringen ikke medfører forstyrrelser på målet. For angriper betyr dette at han ønsker at egen aktivitet ikke blir kompromittert i noen faser av operasjonen. For virksomheten som angripes kan det være vel så viktig å skjule at en inntrenger er detektert, egne kapasiteter og kapabiliteter og hvilke mottiltak virksomheten planlegger å iverksette etter at inntrenger er detektert.

Offensive cyberoperasjoner med **effektformål** vil i motsetning til etterretningsoperasjoner, gjennomføres for å skape tilsiktede effekter i en motparts IKT-systemer eller enheter som kontrolleres eller brukes av motpartens IKT-systemer. Dette kan inkludere systemer som eies av en tredjepart, eksempelvis kommersielle eller privateide tjenester som servere, webhoteller, skytjenester og operasjonell teknologi (OT). Effektmålet for trusselaktøren er ikke IKT-systemet eller nettverket i seg selv, men å påvirke en virksomhets eller samfunnets evne og vilje, gjennom å ramme tjenester som IKT-systemet kontrollerer.

Offensive cyberoperasjoner (både for effekt og etterretning) kan benyttes i hele konfliktspekteret, inklusive fredstid. De kan i prinsippet understøtte målsettinger fra det stridstekniske og til det politiske kommandonivå. De kan benyttes mot militære mål, som kommandofunksjoner og våpensystemer, eller grunnleggende samfunnsfunksjoner som internettleverandører, vannforsyning og finansielle tjenester. Offensive cyberoperasjoner kan også understøtte påvirkningsoperasjoner for eksempel gjennom å skaffe tilveie informasjon som lekkes til offentligheten, undergraver tillit til datasystemer og statens evne til å ivareta dem eller bruke dem til å løse viktige oppgaver. Et kjent eksempel på dette var presidentvalgkampen i USA i 2016. I dette tilfellet ble eposter fra den demokratiske nasjonale komiteen (DNC) offentliggjort av det som antas å være russisk etterretning.[63]

Effektiviteten til en cyberoperasjon kan man se på som et trilemma av hurtighet, intensitet og kontroll.[64]

- Hastighet – tiden fra planlegging av en operasjon starter til effekt produseres på målet
- Intensitet – hvor stor effekt, eller påvirkning, man har på målet
- Kontroll – hvor stor kontroll trusselaktøren har over målet

[63] Crowdstrike; *CrowdStrike's work with the Democratic National Committee: Setting the record straight*, 2020

[64] Maschmeyer, *The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations*, 2021

Disse tre faktorene virker mot hverandre på den måten at en endelig mengde ressurser må fordeles på de tre variablene og man må avveie hvilke egenskaper som er viktigst for den aktuelle operasjonen.

Felles for de avanserte offensive cyberoperasjonene er at de krever mye ressurser, kompetanse, etterretningsstøtte og forberedelsestid. Planlegging, ledelse og utvikling av offensive cyberoperasjoner som skal være skjult i lang tid krever spisskompetanse innenfor mange ulike fagdisipliner. Derfor kan det ofte kreve flere årsverk fra planlegging til iverksettelse av en cyberoperasjon. Personellinnsats kombinert med etterretningsstøtte og eventuelle anskaffelser av infrastruktur eller spesialutstyr tilsier at dette er aktiviteter hovedsakelig forbeholdt stater. Samtidig finnes enkle og langt mindre ressurskrevende teknikker som også kan anvendes for effekt, som tjenestenekt eller nettsidevandalisme. De kan også ha vesentlige effekter på datasystemer og det som beror på dem, men rent teknisk vil de som regel være lite destruktive og med begrenset varighet. Til gjengjeld er de ofte veldig synlige og får gjerne uforholdsmessig stor oppmerksomhet i media og samfunnet forøvrig.

4.1.2 Trender innen offensive cyberoperasjoner

I det følgende belyses noen trender som vil være relevante for hvordan forfatterne mener at trusselaktører antas å utøve cyberoperasjoner mot Norge i nær fremtid.

Cyberoperasjoner for etterretningsformål

Vi må være forberedt på et stort trykk fra utenlandsk etterretning mot norske organisasjoner, sivile og offentlige og norsk infrastruktur.[65, 66] Etterretningsoperasjonene må forventes å dekke hele spennet fra de enkle, støyende som er lette å oppdage til klandestine operasjoner, som er svært ressursintensive for trusselaktørene, som vi muligens ikke oppdager. Norske myndigheter, virksomheter og organisasjoner må være forberedt på å håndtere hele spennet. Dette inkluderer hendelseshåndtering samt, for eksempel ved hjelp av elementer fra «zero trust» sikkerhetsmodeller,[67] å bygge IKT-infrastrukturen vår på en slik måte at vi kan beskytte våre verdier under antagelsen om at trusselaktører har kompromittert elementer av vår infrastruktur.

Et eksempel på en svært avansert operasjon er den som rammet SolarWinds.[68] SolarWinds er et høyteknologisk firma som leverer programvare til andre teknologibedrifter. Operasjonen mot SolarWinds var i så måte et leverandørkjedeangrep. Dette var en langvarig og svært avansert operasjon som både USA og Storbritannia har attribuert til Russlands utenriks etterretningstjeneste (Sluzhba Vneshney Razvedki, SVR).[69] Trusselaktøren viste her evne til å ramme mange organisasjoner og operere skjult over lengre tid. Denne typen avanserte leverandørkjedeangrep vil sannsynligvis få konsekvenser for vestlige mål i lang tid framover

[65] Etterretningstjenesten; *FOKUS 2022*, 2022

[66] PST; *Nasjonal trusselvurdering 2022*, 2022

[67] National Security Agency; *Embracing a Zero Trust Security Model*, 2022

[68] TechTarget, Oladimeji, Kerner; *SolarWinds hack explained: Everything you need to know*, 2022

[69] National Cyber Security Centre; *UK and US call out Russia for SolarWinds compromise*, 2021

blant annet på grunn av informasjonsomfanget som trusselaktøren tilegner seg i en vellykket operasjon.

I den andre enden av skalaen har enkelte aktører spesialisert seg på å utnytte sårbarheter som publiseres offentlig. Aktørene tilpasser sårbarhetene til egne operasjoner og bruker dem mot målsystemer før det foreligger sikkerhetsoppdateringer eller før målorganisasjonen har rukket å oppdatere sine systemer. Et eksempel på dette er kinesiske trusselaktørers bruk av Microsoft Exchange-sårbarheten som ble omtalt av Microsoft i 2021.[70] Da en alvorlig sårbarhet i Microsoft Exchange ble gjort offentlig tilgjengelig, var det indikasjoner på at flere ulike kinesiske grupperinger brukte den til innhenting fra Exchange-eposttjenere i et stort antall virksomheter, også norske. Et annet eksempel på tilsvarende operasjonsmåte er den såkalte Log4j-sårbarheten.[71]

Tjenestenektangrep og nettsidevandalisme

Selv om tjenestenektangrep og nettsidevandalisme er relativt lite sofistikerte angrep, ser vi fortsatt signifikant utbredelse av dette. De forekommer ofte med økt frekvens når det er konflikt mellom land, og frekvensen i tilknytning til krigen i Ukraina fremstår høy.[72] Det må forventes at trusselaktører vil utføre distribuerte tjenestenektangrep mot norske virksomheter. Med et voksende antall datamaskiner som kobles på nett, anser vi det som plausibelt at denne typen angrep vil fortsette tross bruk av beskyttelsesmekanismer mot tjenestenektangrep i infrastrukturen. Tjenestenektangrep kan også brukes til å skjule og avlede under forsøk på inntrenging i IKT-systemene.

En annen aktivitet vi ofte ser i forbindelse med konflikter og andre spente situasjoner er mer eller mindre opportunistisk nettsidevandalisme. Ved å lete etter webtjenere som for eksempel mangler sikkerhetsoppdateringer, kan aktører utnytte dette til å skifte ut budskapet på den tilhørende nettsiden. Det nye budskapet kan være ren propaganda eller mer sofistikerte forsøk på å påvirke den reelle målgruppen til nettsiden. Medieoppslag om slik aktivitet kan bidra til økt oppmerksomhet rundt trusselaktørens sak.

Cyberoperasjoner som en tjeneste

Hos enkelte aktører er det en tendens til at hele eller deler av verdikjeden til offensive cyberoperasjoner og cyberkriminalitet blir kommersialisert og man kjøper elementer eller tjenester som inngår i en kampanje. Eksempelvis har kriminelle tilgang til å kjøpe ferdige pakker for løsepengevirus (ofte omtalt som Crime-as-a-service – CAAS),[73] mens stater kan kjøpe ferdige upatchede sårbarheter på det mer eller mindre åpne markedet.[74] Dette senker

[70] Microsoft Threat Intelligence Center; *HAFNIUM targeting Exchange Servers with 0-day exploits*, 2021

[71] NSM; *Nasjonalt cybersikkerhetssenter – Samleside for Apache Log 4j*, 2023

[72] Se for eksempel: Microsoft Digital Security Unit, *Special Report: Ukraine – An overview of Russia's cyberattack activity in Ukraine*, 2022

[73] Europol; *Internet Organised Crime Threat Assessment (IOCTA) 2021*, 2021

[74] Wired, Perlroth; *The Untold History of America's Zero-Day Market*, 2021

kompetanseterskelen for de mindre sofistikerte aktørene, både kriminelle og stater, som har en viss risikovillighet. For operasjoner med høye krav til operasjonssikkerhet og krav til å operere skjult over tid, settes det derimot stadig høyere krav til kompetanse og ressurser. Dette gjelder typisk etterretningsoperasjoner fra ressurssterke stater.

Løsepengevirus

En av de store inntektskildene til cyberkriminelle de senere årene har vært løsepengevirus («ransomware»). Norske bedrifter har ikke vært forskånet fra dette.[75] I tillegg til å kryptere all data i bedriften, tar ofte trusselaktøren en kopi av sensitiv data og truer med å publisere denne offentlig med mindre løsepenger blir betalt. Dermed vil ikke gode sikkerhetskopierings- og gjenopprettelsesrutiner alene være beskyttelse nok mot slike trusler. I tillegg kan de kriminelle aktørene bruke uthentet informasjon som et middel for utpressing, ofte omtalt som «dobbel utpressing».[76] Det eksisterer et velutviklet marked innen CAAS hvor tilgang til kompromitterte nettverk selges på svarte markeder. Slik tilgang kan deretter for eksempel brukes til å spre løsepengevirus i en virksomhet.[77]

I Ukrania-krigen er det også eksempler på at det er spredt skadevare som utgir seg for å være løsepengevirus, men uten mulighet for å gjenopprette kryptert data. Disse er for alle praktiske formål en form for «wiper». Slike kampanjer er sabotasjekampanjer som gjør IKT-systemer utilgjengelige inntil de er gjenopprettet, med potensielt vesentlige kostnader både økonomisk og i form av tapt data.[78]

Det norske samfunnet må være forberedt på å håndtere kriminell aktivitet som løsepengevirus og «wipere» både i private og offentlige virksomheter.

Evne og vilje til å gå mot operasjonell teknologi (OT)

Basert på informasjon fra åpne kilder, har det vært svært få vellykkede alvorlige cyberoperasjoner rettet mot industrikontrollsystemer/operasjonell teknologi (OT). Likevel har trusselaktører vist evne og vilje til å gå mot OT. Fremtredende eksempler på slike operasjoner er Stuxnet[79], kampanjene mot energiforsyning i Ukraina i 2015[80] og 2016[81] og operasjonen mot

[75] Microsoft Source, Briggs; *Hackers hit Norsk Hydro with ransomware. The company responded with transparency*, 2019

[76] Trend Micro, Agcaoili et al.; *Ransomware Double Extortion and Beyond: REvil, Clop, and Conti*, 2021

[77] Europol; *Internet Organised Crime Threat Assessment (IOCTA) 2021*, 2021

[78] Microsoft Digital Security Unit; *Special Report: Ukraine – An overview of Russia's cyberattack activity in Ukraine*, 2022

[79] Langner, 2013

[80] Cherepanov, Lipovsky, 2016

[81] Cherepanov et al., *Industroyer/Crashoverride: Zero Things Cool About A Threat Group Targeting The Power Grid* (presentasjon), 2017

iranske stålverk[82]. Det ble også funnet skadevare i ukrainske systemer våren 2022 som virker å være en videreutvikling av skadevaren som ble brukt under kampanjen i 2016. Skadevaren inneholder funksjonalitet for å styre systemene som kontrollerer strømforsyning.[83]

Det foregår en digitalisering av samfunnet og innføring av «smart teknologi» i både private husholdninger og i offentlig infrastruktur og tjenester (for eksempel innen ekom eller energiproduksjon og -distribusjon som beskrevet i kapittel 3.3-3.4). Dette innfører en større digital angrepsflate. Ved innføring av ny teknologi, er det viktig å bruke nok ressurser på å sikre de kritiske tjenestene. Det må også finnes beredskapsplaner for hvordan samfunnet skal håndtere eventuelle angrep på tjenestene. FFI har tidligere vurdert hvordan utvikling innen Internet of Things (IoT) påvirker nasjonal sikkerhet.[84]

Bruk av kunstig intelligens i cyberoperasjoner

Maskinlæring og kunstig intelligens til hjelp under ulike faser av cyberoperasjoner har vært et aktivt forskningsfelt i flere år.[85] [86] Til å finne enklere programmeringsfeil er potensialet stort.[87] En annen bruk av maskinlæring og kunstig intelligens innen cyberoperasjoner er å benytte tekstgenereringstjenester, som ChatGPT, til å produsere tekst til phishing eposter.[88] Det er ingen konsensus rundt i hvor stod grad kunstig intelligens vil lette det betydelige arbeidet som kreves for å finne og utnytte avanserte sårbarheter, og dermed heller ikke om kunstig intelligens vil være en såkalt «game changer» eller ikke. Dette er et forskningsfelt det er nødvendig å følge frem mot 2030.

Cyberoperasjoner i påvirkningskampanjer

Cyberoperasjoner har lenge vært benyttet i påvirkningskampanjer.[89] Påvirkning kjennetegnes blant annet ved at en i årsakskjeden mellom maktmiddel og ønsket utfall beror på å endre menneskers adferd på bestemte måter. For eksempel kan en ved bruk av informasjon endre deres virkelighetsoppfatning og derigjennom adferd. En kan imidlertid også gå frem på andre måter som ved å påtvinge endringer i strukturer individer befinner seg i. Helt vesentlig er imidlertid at dette ikke gjøres for sportens skyld, men snarere for at effektene på mennesker i sum bidrar til ønskelige utfall i politikk (innenriks, utenriks, militære operasjoner med videre). Når de inntreffer, vil den sentrale utfordringen i håndteringen av påvirkningseffekten være å

[82] CYBERSCOOP, Vicens; *Iranian steel facilities suffer apparent cyberattacks*, 2022

[83] MANDIANT, Brubaker et al., INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems, 2022

[84] Farsund et al. (20/01745), 2020

[85] Fioraldi et al., 2020

[86] IEEE; *IEEE Security & Privacy*, 2018

[87] Grammatech; *Machine Learning for Finding Programming Defects and Anomalies*, 2023

[88] Abnormal Blog, Hassold; *The Double-Edged Sword of ChatGPT: How Threat Actors Could Use It for Evil*, 2022

[89] Rid, 2020

forstå betydningen for egne verdier. FFI har tidligere vist hvordan et land som Norge kan begynne å tilnærme seg denne typen arbeid.[90]

Mulighetene for påvirkning ved bruk av cyberoperasjoner er mange og økende på grunn av den rollen det digitale rom har og får i moderne samfunn. Det digitale rom er ikke bare sentralt i måten vi tar til oss informasjon på, men også i sosiale strukturer. Det vil si at beskrivelser av måten en liten virksomhet, et departement, en beslutningsløkke, militære operasjoner eller andre ansamlinger sosiale prosesser fungerer på, i de aller fleste tilfeller, inneholder beskrivelser av hvordan det digitale rom ser ut og benyttes.[91]

Cyberoperasjoner benyttes til å skaffe til veie, endre, ødelegge og/eller spre informasjon med mulige påvirkningseffekter. Dette kan være fra teknisk sett enkle til vanskelige operasjoner avhengig av formålet med påvirkningskampanjen. Et velkjent eksempel fra nyere tid er russisk militære etterretningscyberoperasjoner i opptaktene til det amerikanske presidentvalget i 2016. Informasjon skaffet tilveie gjennom disse operasjonene ble frigitt på Internett i håp om å øke støtten til Donald J. Trump og sverte Hillary Clintons kandidatur. Cyberoperasjoner benyttes også til å skape informasjon med mulige påvirkningseffekter. Teknisk sett enkle operasjoner omfatter for eksempel ulike former for tjenestenekt og nettsidevandaliseringer. De kan følgelig forestås av både ikke-statlige og statlige aktører – herunder også stedfortredere. Dette ser en gjerne med åpenlys politisk motivasjon i forbindelse med viktige hendelser i internasjonal politikk. Det være seg i fred, som tjenestenektene mot flere norske mål i forbindelse med Sverige og Finlands søknad om NATO-medlemskap i 2022,[92] eller i væpnet konflikt, som i Ukraina våren 2014.[93] Teknisk sett vanskeligere operasjoner med mulige påvirkningseffekter inkluderer for eksempel i Ukraina sabotasje av datasystemer benyttet i forbindelse med gjennomføringen av nasjonale valg.[94] Cyberoperasjoner kan benyttes til å gjøre endringer i datasystemer som i tur skal påvirke individers gjennomføring av sosiale prosesser, som for eksempel militære planprosesser. Denne kategorien nevnes for å illustrere at påvirkning ikke behøver omhandle informasjon på den måten man ofte hører om. Et eksempel på denne formen for påvirkning ved bruk av cyberoperasjoner kunne være bruken av løsepengevirus eller wiper for å sabotere datasystemer på måter som sakker beslutningsløkker i militære operasjoner

Offensive cyberoperasjoner kan ha både intenderte og uintenderte påvirkningseffekter og disse kan være viktige å oppnå en grad av kontroll over for både angriper og mål. Målet kan ikke regne med å vite om angriperens intensjon inkluderer påvirkningseffekter. Selv kjennskap til denne kan ikke bøte på behovet for å gjøre selvstendig vurdering av de faktiske påvirkningseffektene ved en gitt operasjon. Det betyr for eksempel at Russlands sabotasje av ukrainsk kraftforsyning i 2016 kan ha hatt påvirkningseffekter det var i Ukrainas interesse å håndtere, selv om påvirkning ikke behøver å ha vært Russlands mål. For å beskytte egne

[90] Kveberg, et al. (19/01766), 2019

[91] Larkin, 2013

[92] NrK, Norum et al.; *Russisk hackergruppe skal ha startet angrep mot Norge*, 2022

[93] REUTERS, Croft, Apps; *NATO websites hit in cyber attack over Crimea stance*, 2014

[94] Rid, 2020

interesser, er det avgjørende å søke forståelse ikke bare for hvordan cyberoperasjoner utføres, men mulige påvirkningseffekter de har og hvordan disse i tur kan påvirke nasjonale interesser.[95]

Fysisk tilgang

Enkelte cyberoperasjoner er av en slik natur at de ikke utelukkende kan utføres med operatører som geografisk sitter langt fra målet og utfører all aktivitet over internett. I noen situasjoner trengs personell i fysisk nærhet av målet. Dette kan være fordi målsystemet er «airgappet», altså fysisk frakoblet andre nett som internett, eller fordi inngangsvektoren til IT-systemet krever fysisk nærhet via for eksempel trådløst nettverk. Eget personell som befinner seg i fysisk nærhet av målsystemet er et virkemiddel som en trusselaktør kan bruke for å bøte på denne utfordringen. De kan enten fysisk koble seg til et nettverkspunkt eller å være innenfor rekkevidde av eventuelle trådløse nettverk. Forsøket på å utføre en cyberoperasjon mot Organisasjonen for forbud mot kjemiske våpen (OPCW)[96] er et eksempel på denne typen cyberoperasjoner. Det kan dermed argumenteres for at når IT-systemer blir stadig sikrere, vil verdien av å ha en innsider med lovlig tilgang til IT-systemene øke. Innsideren kan lures, presses eller overtales til å være en komponent i en cyberoperasjon mot en virksomhet.[97]

4.1.3 Trender som kan påvirke digital sikkerhet

Normer og regler

Over de siste ti årene har det vært flere viktige utviklinger som kan forstås som verdens innledende steg i etableringen av normer og regler for akseptabel, statlig adferd i det digitale rom. Generelt kan en se et vesentlig taktskifte fra vestlige land innen offentlig attribusjon som uttrykk for å holde noen til ansvar for handlinger,[98, 99, 100] og også uttalt aksept for at eksisterende internasjonal rett er dekkende. Akademiske arbeider om anvendelsen av eksisterende internasjonal rett i form av Tallinn-manualen[101] kan ses som ledd i dette..

FN har også prosesser rundt politikkutforming innen digital teknologi og normer og regler rundt maktbruk i det digitale rom. Dette inkluderer *World Summit on the Information Society* (WSIS),[102] *United Nations Group of Governmental Experts on Advancing responsible state behaviour in cyberspace in the context of international security* (GGE),[103] *Open-Ended Working group (OEWG) on security of and in the use of information and communications technologies*

[95] Kveberg et al., 2019

[96] The Guardian, Crerar et al.; *Russia accused of cyber-attack on chemical weapons watchdog*, 2018

[97] Slagnes (22/01309), 2022

[98] Egloff, 2020

[99] Egloff, Smeets, 2021

[100] Rid, Buchanan, 2015

[101] Schmitt, 2017

[102] ITU; World summit on the information society, 2006

[103] UN Digital Library, Group of Governmental Experts, 2018

2021-2025[104] og Sikkerhetsrådet. FN-prosessene har bidratt til delvis enighet rundt normer og regler i det digitale rom, men de har også synliggjort de store uenighetene mellom stater på området. FN-prosessene, blant annet omkring Sikkerhetsrådets håndtering av digitale trusler, er relevante arenaer for det globale arbeidet med digital sikkerhet.

Teknologiske endringer

Kompleksitet: Moderne IKT-systemer blir stadig mer komplekse og automatiserte. Som nevnt i kapittel 2, blir ressursbruk og optimalisering i systemer av en viss størrelse styrt av algoritmer uten at mennesker er del av beslutningstakingen. Dette kan føre til at det blir vanskeligere for sikkerhetspersonell å ha oversikt over IKT-systemene og risikoen i dem. Dette fører til at man i større grad må stole på at de automatiserte systemene, typisk basert på kunstig intelligens-modeller, tar de riktige avgjørelsene når det gjelder risiko.

Sikkerhetsbevissthet og kryptering: Brukere blir stadig mer sikkerhets- og personvernsfokuserte. Dette medfører blant annet at andelen legitim trafikk som er kryptert eller bruker andre sikkerhets- og personvernsmekanismer øker. Dette er en positiv utvikling både for enkeltpersoner og virksomheter, men en trusselaktør kan benytte tilsvarende teknikker for å skjule opprinnelsen til og tilstedeværelsen av sin egen cyberoperasjon. For forsvarersiden kan det, paradoksalt nok, dermed bli stadig mer utfordrende å skille en trusselaktørs teknikker fra teknikker en sikkerhets- og personvernsbevisst bruker benytter seg av.

Stordata: Mengden med dataelementer, både fra endepunkter og i nettverk som er relevant for operativt sikkerhetsarbeid, er økende og vil kreve at SIEM[105]-løsninger og liknende inkluderer metoder for å se etter angrepsmønstre ved hjelp av maskinlæringsteknikker. Her har myndighetene og tjenesteleverandørvirksomheter i alle sektorer et spesielt ansvar. De må legge til rette for opptrening og tilpassing av modeller i den enkelte virksomhet slik at den skal være mest mulig effektiv for å oppdage cyberoperasjoner rettet mot virksomheten. Det er også viktig å bistå universiteter, høyskoler og andre forskningsinstitusjoner, som i mindre grad besitter operasjonell data, med å utvikle og trene opp modeller for å oppdage cyberoperasjoner.

Moderne utviklingsmetodikk: Metodikk for utvikling og lansering av programvare har i stor grad endret seg fra å være milepælbasert, med lansering av flere «større» versjoner, til å være mer kontinuerlig lansering av mindre programvareoppdateringer. Dette omtales ofte som CI/CD (Continuous Integration/Continuous Delivery). CI/CD koples ofte sammen med «DevOps» hvor utviklere jobber tett og kontinuerlig sammen med brukere og operatører for å forbedre og videreutvikle produkter. Dette gir en mer smidig utviklingsmetodikk og bedre tilpasning mellom behov og utviklet funksjonalitet. Disse utviklingsmetodene krever at en også må være oppmerksom på at sikkerhetsmessige forhold blir ivaretatt. CI/CD medfører blant annet at kvalitetssikring av programvare skjer fortløpende istedenfor i en rigid testing i etterkant av

[104] UN, Open-ended Working Group on security of and in the use of information and communications technologies 2021-2025, 2023

[105] Security Information and Event Management.

utviklingsprosessen. Dette krever endrede prosesser og bevissthet rundt sikkerhet og kvalitet i produktutvikling. Et problem som er spesielt utfordrende er leverandørkjedeproblematikk i form av tredjepartsprogramvare og -biblioteker. Det har i de senere år vært mye fokus på sårbarheter, både bevisst innførte bakdører og tilsynelatende reelle utviklingsfeil i slik tredjepartsprogramvare. Telenor sine åpne trusselvurderinger fra 2020[106] og 2021[107] er eksempler på det. Selv om det er økende bevissthet rundt dette i industrien, er dette fremdeles ny utviklingsmetodikk som krever et ekstra sikkerhetsfokus.[108]

Digitale tvillinger: Digital tvillinger er digitale representasjoner av noe fysisk i den virkelige verden. Dette kan for eksempel være byplanlegging, personer, hus, gater, biler, industriprosesser, lagre, flyktningstrømmer, toaletter eller en graviditet. [109] [110] [111] Forenklet sagt er de digitale tvillingene en speiling av den virkelige informasjonen og kan kontinuerlig analyseres. Avhengig av koblingen, kan endringer som gjøres i den digitale tvillingen også få effekt både for den digitale tvillingen og i den fysiske verdenen. For eksempel kan en insulinpumpe startes ved behov eller et bygg kan lade batterier når strømprisen er lav. Når den digitale tvillingen representerer en fysisk prosess som kan styres digitalt, er det en åpenbar kobling mot IoT og OT.

Den store datamengden virksomheter, som blant annet Google, Facebook, Tik Tok, Snapchat og Schibsted, besitter om oss er eksempler på digitale tvillinger som eksisterer i forskjellige digitale samfunn. I kommersiell sammenheng kan disse digitale tvillingene være mye verdt. For eksempel kan mobilbevegelser legges ut for salg som beskrevet av NRKbeta.[112] Disse digitale tvillingene kan følges og forfølges av våre venner og motstandere. Det er de digitale tvillingene som blir blokkert og undergravet om noen velger å angripe noens representasjon på for eksempel et sosialt medium.

Etter hvert som ulike former for digitale tvillinger kobles sammen i forskjellige univers (her kalt metavers), så vil dette kunne generere nye former for verdiskaping med tilhørende sårbarheter. Cyberoperasjoner kan derfor fokusere på det komplekse nettverket av digitale tvillinger fremfor å rette seg mot de fysiske subjektene, objektene og prosessene. De digitale tvillingene vil også kunne være verdifulle mål for cyberoperasjoner for etterretning, i fred, krise og krig. Med andre ord vil fremtidens offensive cyberoperasjoner kunne få en enorm stor angrepsflate i et metavers og ramme verdiskaping som skjer fysisk, digitalt eller begge steder. Det er også tilfeller hvor verdiskapning utelukkende skjer digitalt i form av digitale tjenester i et virtuelt spill eller samfunn eller ved utvinning av digital valuta. Selv om flere viktige og store aktører har stort

[106] Telenor; *Når nettene blir lange. Digital Sikkerhet 2020*, 2020

[107] Telenor; *Digital sikkerhet 2021 – Leveransekjeder - en kjent risiko som krever bevisste valg*, 2021

[108] Cisco Blogs, Developer, Chenetz; *Who Needs to Shift Left in Security, and Why*, 2022

[109] Infrastructure Intelligence, Walker; *Principles to guide development of national digital twin released*, 2018

[110] Deloitte, Parrot, Warshaw; *Industry 4.0 and the digital twin – Manufacturing meets its match*, 2017

[111] Bruynseels et al., 2018

[112] NrKbeta, Gundersen; *Trykker du «godta» kan mobilbevegelsene dine legges ut for salg*, 2021

fokus på digitale tvillinger og metavers, gjenstår det å se hvor stor utbredelse de vil få, og i hvilken grad de vil være en viktig arena for verdiskapning.[113]

Kompetanse- og utdanningsbehov: Basert på en kartlegging gjort av Samfunnsøkonomisk Analyse i 2021,[114] vil det være behov for 40.000 flere sysselsatte med IKT-utdanning i 2030. Med dagens utdanningstakt vil ikke Norge ha mulighet til å løse dette. Dette tallet inkluderer ikke andre sikkerhetsrelevante behov som for eksempel personer med kompetanse innen risikostyring, trusselforståelse, sikkerhetsledelse osv. Dette er et globalt problem.

Mange stillinger og roller i virksomheter som forvalter kritisk norsk infrastruktur eller andre grunnleggende nasjonale funksjoner har krav om sikkerhetsklarering for å inneha slike stillinger. Dette reduserer ytterligere tilgangen på kompetent personell. Det kan derfor vurderes om en andel av plassene på studier som gir relevant kompetanse for slike stillinger skal forbeholdes personer som antas å kunne sikkerhetsklareres. Sammenliknet med mange av våre allierte, er Norge et lite land med lavt innbyggertall. Dersom Sverige og Finland blir medlem av NATO, kan det være lettere å danne utdannings- og kompetansemiljøer med en kritisk masse som sannsynliggjør at disse miljøene opprettholdes.

Det er viktig å få realkompetanse inn som en del av undervisningen. Ved Politihøgskolen underviser eksempelvis personell fra Telenor Norge politistudentene om trusselaktørers handlemåter og virkemidler i det digitale rom. Å trekke industrien og andre deler av norsk sikkerhetsmiljø inn i undervisningen har hatt gode resultater blant annet ved NTNU, UiO og Høgskolen i Innlandet.

Kommunikasjon rundt egne cyberkapasiteter

Over siste tiår har stater i økende grad omtalt egne cyberkapasiteter. I dette legger vi uttalelser som å offentliggjøre at man har slike kapasiteter, hvem som har ansvaret for dem, og i senere år rekrutteringskampanjer med høy synlighet. Vi inkluderer imidlertid også handlinger som å etablere mulighet for trening og øving både nasjonalt og i alliansekontekst, utvikling av doktriner eller attribusjon. I sum er en hel del mer kjent i dag enn for relativt få år siden. Et viktig spørsmål er imidlertid i hvilken grad bildet man får gjennom slik kommunikasjon er representativt for virkelige kapasiteter, om det er kapasiteter slik statene selv ønsker å fremstille dem eller en mer eller mindre kontrollert miks av de to. Denne problematikken kompliserer for eksempel begynnende forsøk på å rangere verdens land etter cybermakt. Det er etter vårt skjønn ingen godt etablert forskning på hvordan stater kommuniserer rundt egne cyberkapasiteter, herunder hvilke måter de gir slike uttrykk på eller hva driverne for dette er. Dermed blir det vanskelig å komme med tydelige forventninger til fremtiden. For eksempel kan det være at senere års åpenhet i form av villet kommunikasjon først og fremst er vestlig og reverseres i møte med økt rivalisering med Russland på kort sikt og Kina på lang sikt. Det kan også være at åpenheten må forstås som ledd i forsøket på å etablere normer og regler for det digitale rom og

[113] The New York Times, Mac; *Meta's Profit Slides by More Than 50 Percent as Challenges Mount*, 2022

[114] Eggen et al., 2021

at interessen på sikt avtar eller utfordres gjennom andre lands beskrivelser av vestlig cybermaktbruk.

4.1.4 Erfaringer fra Ukraina

Observasjoner av Russlands cyberoperasjoner i krigen i Ukraina kan, basert på rapportering i åpne kilder, omtaltes som å være i relativt stort omfang, men lite sofistikert.[115] Det store volumet av operasjoner har vært tjenestenektangrep, nettsidevandalisme (defacing) og løsepengevirus (wipere).

I tillegg til de mindre sofistikerte kampanjene, er det også offentlig kjent at Russland tidlig i krigen hadde en operasjon som satte store deler av satelittkommunikasjonstjenesten til Viasat ut av spill.[116] Dette rammet brukere både i Ukraina og i resten av verden. Sammen med andre avdekkede russiske cyberoperasjoner, viser dette at Russland har kapabilitet til å utføre avanserte operasjoner i det digitale rom. Samtidig har de evne til å utføre flere parallelle mindre sofistikerte operasjoner. Russlands utstrakte bruk av stedfortredere antas å bidra til denne evnen.

Som nevnt i avsnittet om løsepengevirus er det også observert at Russland i krigen i Ukraina har utført operasjoner som utgir seg for å være løsepengevirus-kampanjer utført av kriminelle, men som i realiteten er sabotasjekampanjer. Det finnes ingen metode for å gjenopprette de krypterte filene og IKT-systemene blir utilgjengelige inntil de er gjenopprettet fra backup eller reinstallert.

4.2 Påvirkningsoperasjoner i informasjonsmiljøet

Med påvirkningsoperasjoner (information influence operations) menes her «en aktørs koordinerte bruk av illegitime og fordekte metoder for å påvirke meninger og virkelighetsoppfatninger hos mennesker og grupper uten at disse er klar over det, i den hensikt å skape forutsetninger for å oppnå egne strategiske mål».[117] Påvirkningsoperasjoner kan dermed forstås som en form for maktbruk hvis hensikt er å manipulere andre lands befolkninger og politiske eller militære ledelse til å tenke eller handle i tråd med påvirkerens interesser. Eksempler inkluderer forsøk på å påvirke demokratiske valg og politiske beslutninger, svekke tilliten i og mellom stater og tåkelegge fakta.

Virkemidlene og metodene kan rettes mot hele samfunnet på tvers av sektorer. De kan være vanskelige å oppdage og kan skape betydelig effekt under terskelen for vår tradisjonelle oppfatning av en krise.

[115] Microsoft, Smith; *Defending Ukraine: Early Lessons from the Cyber War*, 2022.

[116] Forbes, Mathews; *Viasat Reveals How Russian Hackers Knocked Thousands Of Ukrainians Offline*, 2022

[117] Sivertsen et al., 2021

Noen eksempler på illegitime og fordekte metoder er:

- Spredning av desinformasjon og malinformasjon
- Manipulasjon av den offentlige samtalen på sosiale medier og på nett
- Falske profiler på sosiale medier
- Falske nyhetsnettsider og organisasjoner
- Falske dokumenter, bilder og filmer
- Kloning av nettsider eller profiler på sosiale medier
- Automatiserte kontoer for å forsterke innhold på sosiale medier (bots)
- Bruk av stedfortredere (som influensere, byråer eller tilsynelatende uavhengige aktører)
- Hack & release (deling av stjålet, kompromitterende informasjon)
- Tåkelegging av informasjonens opphav gjennom «information laundering»

Fordi påvirkningsoperasjoner i sin natur er fordekte og kan utnytte de fleste digitale plattformer og sosiale medier, finnes det ingen fasit på hvor omfattende utfordringen er. Ifølge Meta, som eier Facebook, Instagram og WhatsApp, har selskapet tatt ned mer enn 200 nettverk for påvirkningsoperasjoner i perioden 2017 til og med 2022. Operasjonene foregikk i 68 land og på 42 språk. I 2/3 av disse kunne nettverkene lokaliseres til det samme landet som befolkningen den forsøkte på påvirke.[118] Det er rimelig å anta at omfanget kan være vesentlig større, da uavhengige undersøkelser tyder på at plattformene i begrenset grad evner å fange opp og stenge ned inautentiske profiler som brukes til koordinert manipulasjon.[119]

Både stater og ikke-statlige grupper og organisasjoner utfører påvirkningsoperasjoner for å oppnå fordeler. For Norges del, peker både Etterretningstjenesten[120] og PST[121] på Russland og Kina som de største statlige trusselaktørene. Attribusjon kompliseres ved at aktivitetene ofte utføres av kommersielle selskaper, organisasjoner eller grupper som opererer på oppdrag fra aktøren[122] eller stedfortredere med skjult eller ingen direkte tilknytning.

4.2.1 Effekter og konsekvenser

Russiske påvirkningsoperasjoner forsøker typisk å skape falsk legitimitet for Russlands handlinger, svekke Vestens maktposisjon og den rettsbaserte verdensordenen og undergrave tilliten eller påvirke politiske prosesser i demokratiske samfunn. Det gjøres blant annet gjennom å forsterke konflikter, spre desinformasjon og konspirasjonsteorier og skape usikkerhet eller likegyldighet til sannhet og fakta.

[118] Meta, Nimmo, B., *Recapping Our 2022 Coordinated Inauthentic Behavious Enforcements*, 2022

[119] NATO Strategic Communications Centre of Excellence, Fredheim; *How Social Media Companies are Failing to Combat Inauthentic Behaviour Online*, 2019

[120] Etterretningstjenesten, 2022

[121] PST, 2022

[122] Bradshaw et al., 2020

Kinesiske operasjoner har lenge handlet om å promotere Kina og kinesiske interesser, men har de siste årene i større grad også tatt i bruk «russiske» metoder for å villede, spre desinformasjon eller undergrave stater, organisasjoner og personer som handler mot kommunistpartiets interesser. Begge stater har etablert omfattende nettverk for påvirkning med både åpne og skjulte, autentiske og inautentiske metoder og virkemidler.

Etterretningstjenesten skriver i sin ugraderte vurdering, *Fokus 2022*[123] *(s. 21)*:

> «Russland og Kina har over tid vist vilje og evne til innblanding i politiske prosesser i vestlige land. Russiske medier har forsterket eksisterende konspirasjonsteorier om biologisk krigføring og Covid-19-vaksiner. De siste månedene har Russland søkt å påvirke meningsdannelsen i Vesten ved å framstille NATO og Ukraina som aggressorer i Ukraina-spørsmålet. Kinesiske myndigheter har søkt å så tvil om Covid-19-virusets opprinnelse og samtidig høste anerkjennelse for håndteringen på hjemmebane. Kina legger store ressurser i å hindre kritikk av sin politikk på Taiwan, Hong Kong og Xinjiang. Statstilknyttede aktører har opprettet titusenvis av falske kontoer på sosiale medier for å fremme propaganda.»

I det enkelte land fremstår ikke slike påvirkningsoperasjoner nødvendigvis som forsøk på påvirkning utenfra, men som legitim debatt og interaksjon mellom landets innbyggere. De kan pågå i lang tid uten at de blir oppdaget og få konsekvenser både for statssikkerhet, samfunnssikkerhet, politikk og samfunnet for øvrig. Ifølge PSTs nasjonale trusselvurdering 2021 kan slike aktiviteter – dersom de ikke avdekkes og motvirkes:[124]

- Svekke demokratiet vårt
- Svekke vår sivile og militære krisehåndteringsevne
- Redusere norske myndigheters legitimitet i befolkningen
- Påvirke politiske beslutningsprosesser i strid med norske interesser
- Svekke norske standpunkt i internasjonale forhandlinger
- Begrense enkeltpersoners ytringsfrihet

4.2.2 Russiske påvirkningsoperasjoner

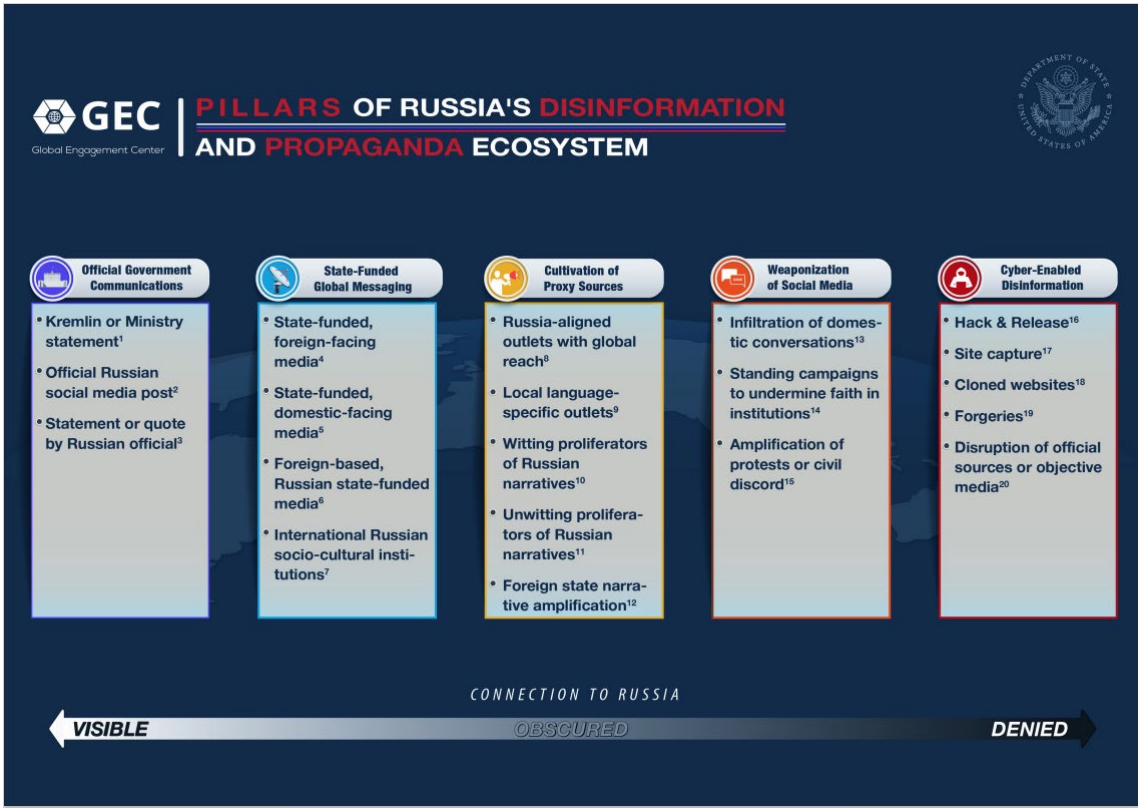
Russiske påvirkningsoperasjoner er i seg selv ikke noe nytt. «Aktivnye meropriyatiya», eller «active measures» er et begrep for politisk krigføring fra russisk doktrine fra Sovjettiden og rommer blant annet påvirkning gjennom desinformasjon, propaganda, villedning, sabotasje og

[123] Etterretningstjenesten, 2022

[124] PST, 2021

spionasje.[125] Digitalisering, internett og sosiale medier har imidlertid åpnet for nye muligheter og større effekt med liten eller ingen risiko.

Russland har over mange år bygget opp et globalt påvirkningsnettverk, som kan beskrives som et økosystem for russisk desinformasjon og propaganda, styrt fra Kreml. Det amerikanske utenriksdepartementet beskriver økosystemet gjennom fem «pilarer» i spennet fra åpent til fordekt: (1) official government communications, (2) state-funded global messaging, (3) cultivation of proxy sources, (4) weaponization of social media og (5) cyber-enabled disinformation.[126] «Proxy sources», eller «stedfortredere», fremstår gjerne som uavhengige og troverdige kilder, organisasjoner eller personer, men som støtter – eller kontrolleres av – russiske myndigheter eller etterretningstjenester. Aktørene i hver pilar forsterker og bygger på hverandres propaganda og manipulasjon for å oppnå maksimal effekt.



Figur 4.1 *«Pillars of Russia's Disinformation and Propaganda Ecosystem" av Global Engagement Center (GEC) i det amerikanske utenriksdepartementet. Illustrasjon: U.S. Department of State, Global Engagement Center, 2020, s. 8*

[125] Darczewska, Żochowski, 2017

[126] U.S. Department of State, Global Engagement Center, 2020

Det kanskje mest kjente eksempelet på en russisk påvirkningsoperasjon i nyere tid er forsøket på å påvirke det amerikanske presidentvalget i 2016. Her forsøkte Russland å framprovosere og forsterke politisk og sosial uenighet i USA, manipulere valgsystemet, skade Hillary Clintons kandidatur og forsterke Donald Trumps.[127] I ettertid er lista blitt lang.

De senere årene er det kartlagt en rekke russiske, statsstyrte påvirkningsoperasjoner ikke bare i forbindelse med valg i demokratiske land, men blant annet for å forsterke konflikter i samfunnet (f.eks. De Gule Vestene i Frankrike i 2017[128]), tåkelegge statskriminalitet og krigsforbrytelser (f.eks. forgiftningen av Sergej Skripal i 2018[129] og tortur og drap på sivile i Ukraina siden 2014[130]) og skape falsk legitimitet for Russlands krig mot Ukraina.[131]

En av de siste avslørte russiske påvirkningsoperasjonene høsten 2022 ble av Meta beskrevet som «den største og mest komplekse» operasjonen selskapet hadde avdekket siden Russlands fullskala invasjon av Ukraina 24. februar 2022.[132] Den hadde til hensikt å undergrave europeisk støtte til Ukraina. Operasjonen bestod av 60 klonede, falske europeiske nettaviser, 1633 falske Facebook-profiler, 703 falske Facebooksider (pages), 29 falske Instagram-profiler og et hundretalls falske Twitterprofiler. Den foregikk gjennom misbruk av Metas plattformer YouTube, Telegram, Twitter og nettsider som tilbyr spørreundersøkelser.[133]

Det er ikke bare Vesten som er mål for russiske påvirkningsoperasjoner. Russland bruker betydelige ressurser på å påvirke målgrupper i Afrika,[134] Latin-Amerika og Karibien[135] for å undergrave tilliten til USA og Europa og styrke sin egen posisjon.

4.2.3 Kinesiske påvirkningsoperasjoner

Selv om Russland har fått mye oppmerksomhet for større, grundig forberedte påvirkningsoperasjoner, er det liten tvil om hvor viktig Kina anser informasjonsmiljøet for å være i fremtidige konkurranse- og konfliktsituasjoner. Siden den første Gulf-krigen i 1990, gjennom flere vestlige intervensjoner i konflikter som tidligere Jugoslavia og Afghanistan, en rekke revolusjoner og folkeopprør i autokratiske land og til Ukrainakrigen i 2022, ser det ut til at det kinesiske militæret har inntrykk av at det globale informasjonsmiljøet beherskes av USA.

[127] Mueller, 2019

[128] DW, *POLITICS – France's "yellow vests" and Russian trolls*, 2018

[129] EUvsDiSiNFO; *FIGURE OF THE WEEK: 138*, 2019

[130] archive.today, Higgins; *Russia's Bucha "Facts" Versus the Evidence*, 2022

[131] EUvsDiSiNFO, *DISINFORMATION CASES ABOUT UKRAINE*, 2023

[132] Nimmo, Torrey, 2022

[133] Institute for Strategic Dialogue, digital dispatches; *Pro-Kremlin Network Impersonates Legitimate Websites and Floods Social Media with Lies*, 2022

[134] U.S. DEPARTMENT of STATE, Patel, V., *Yevgeniy Prigozhin's Africa-Wide Disinformation Campaign*, 2022

[135] CSIS, *Russia in the Western Hemisphere: Assessing Putin's Malign Influence in Latin America and the Caribbean*, 2022

De ønsker derfor at Kina skal bygge opp tilsvarende kapasiteter for hva de kaller informasjonskrigføring.[136, 137, 138, 139]

Samtidig er Kina, på den sivile siden, svært opptatt av å markedsføre landet som en fredelig stormakt og en god samarbeidspartner gjennom myk propaganda.[140] I tillegg angriper eller forsøker de å avspore negativ omtale mot styresmaktene, for eksempel i forbindelse med omfattende menneskerettighetsbrudd i Xinjiang-provinsen.[141]

Resultatet av dette er en stor, 360-graders investering i alt fra utdannelse av journalister fra afrikanske land og inngåelse av avtaler om nyhetsutveksling med lokale aviser til skjulte og svært aggressive påvirkningsoperasjoner rettet mot kritikere i sosiale medier. Dette arbeidet er ofte rettet mot Taiwan som kan sees på som et laboratorium for påvirkningsforsøk for Kina,[142] spesielt i forbindelse med valg og sensitive episoder som Nancy Pelosis besøk til øya i 2022.

Kina jobber også målrettet over tid for å forbedre rekkevidde og effekten av propagandaen. Under Hong Kongs studentdemonstrasjoner i 2019 ble mange dårlig skjulte forsøk på påvirkning, gjennom spamkontoer og stjålne kontoer, avslørt av Twitter.[143] Tre år senere har de bygget opp et nettverk av utenlandske påvirkere. Påvirkerne bruker blogger og sosiale medier for diskusjoner om kinesisk mat og turisme blandet med et stadig drypp av propaganda-snakkepunkter om sensitive temaer som Xinjiang.[144, 145] Den brede tilnærmingen resulterer i at i søk på temaer hvor Kina er kritisert internasjonalt, vil nettsider med Kinas synspunkter være overrepresentert i på toppen av søkeresultatene.[146, 147]

Mye av propagandavirksomheten er satt ut til private, kinesiske mediefirmaer. Dette favner fra intern overvåkning på kommunenivå til internasjonale kampanjer.[148, 149] Dette benyttes også

[136] Anand, 2006

[137] War on the Rocks, Mattis; *China's "Three Warfares" in Perspective*, 2018

[138] MERICS, Brussee; *China's Defense against the War of Words*, 2022

[139] The Japan Times, Torode et al.; *Russia's Ukrainian Quagmire Providing Tough Lessons for China*, 2022

[140] DiResta, 2020

[141] PROPUBLICA/The New York Times, Kao et al.; *How China Spreads Its Propaganda Version of Life for Uyghurs*, 2021

[142] Sinopsis, Cole; *Taiwan and CCP Political Warfare: A Blueprint*, 2019

[143] Nimmo et al., 2019

[144] Digital Threat Analysis Center, Eide; *"The One Like One Share Initiative" - How China Deploys Social Media Influencers to Spread Its Message*, 2021

[145] PROPUBLICA/The New York Times, Kao et al.; H*ow China Spreads Its Propaganda Version of Life for Uyghurs*, 2021

[146] Brandt et al., 2022

[147] ProPublica, Kao, Shuang; *How China Built a Twitter Propaganda Machine Then Let It Loose on Coronavirus*, 2020

[148] The New York Times, Xiao et al.; *Buying Influence: How China Manipulates Facebook and Twitter*, 2021

[149] ChinaTalk. Baughman; *Selling China's Story: How the Chinese Gov't Privatized Facebook Propaganda*, 2021

sammen med en rekke andre verktøy som for eksempel finansielle virkemidler, aggressivt diplomatisk press, elite capture og akademisk samarbeid.[150, 151] I motsetning til de fleste andre land, benytter Kina ofte sin egen befolkning som angripere ved å spille på nasjonalistiske følelser mot internasjonale selskaper eller andre land. De anser også den kinesiske diasporaen[152] i alle land som et hovedmål for kontroll gjennom Kina-vennlig propaganda, ofte gjennom kinesiske sosiale medier som brukes lite i verden ellers.[153]

Utad er det overordnede målet å stoppe kritikk av Kina og å vise Kina som en ansvarlig stormakt og et alternativ til USA. Det interne, og ultimate, målet er å sikre kommunistpartiets makt over Kina gjennom påvirkning og utstrakt sensur av hva innbyggerne kan si og lese på sosiale medier. Dette gjøres delvis gjennom kritikk av demokratiske land og idealer generelt og i forbindelse med spesielle hendelser så som Covid-19-pandemien.[154, 155] Problemet for land som Norge er derfor todelt. Desinformasjon om demokratiske land, myndigheter og beslutninger bidrar til å øke splittelser i samfunnet, mens en konstant «skjønnmaling» av Kina kan begrense mulighetsrommet for mottiltak. Det er klart at å håndtere Kinas voksende «diskursmakt»[156] vil trenge sektorovergripende tiltak fra demokratiske land.

4.2.4 Sosiale medieplattformer

Sosiale medieplattformer liker å sammenligne seg selv med tidlige tiders postvesen og telefonselskaper. De tilrettelegger kun for overføring av informasjon, men er nøytrale og kan ikke klandres for innholdet. I virkeligheten spiller disse plattformene en aktiv rolle i online påvirkning. Ikke fordi de bevisst ønsker å støtte påvirkning, men fordi de tar aktive valg med hensyn til:

a) teknologier de utvikler hvis karakteristikker bidrar til spredning av informasjon
b) hvilket innhold som sjekkes og muligens fjernes, eller ikke

Det som ligger til grunn for punkt a) er ikke samfunnets behov, men forretningsmodellen som all sosiale medier deler og som manifester seg selv i teknologiene som benyttes. Denne forretningsmodellen består i å få mest mulig oppmerksomhet fra brukere gjennom gratis

[150] Se for eksempel: Martin, P., 2021

[151] Se for eksempel: Fulda, A., 2021

[152] Diaspora er opprinnelig en betegnelse på jødenes spredning blant andre nasjoner, men brukes i dag også om andre folkegrupper som bor fjernt fra sine opprinnelige hjemland, holder sammen og pleier sin opprinnelige kultur. Kilde: Store norske leksikon

[153] Chiu, J., 2021

[154] Bērziņa-Čerenkova et al., 2022

[155] Lucas et al., 2021

[156] The Diplomat, Jones, *China's Quest for Greater "Discourse Power"*, 2021

tjenester og selge denne oppmerksomheten til annonsører. Sentralt i denne forretningsmodellen er bruk av automatiserte beslutninger i programvare, ofte referert til som algoritmer.[157]

Algoritmer søker å øke brukeres engasjement (som gir mer oppmerksomhet) gjennom klassifisering av innhold. Plattformene viser så brukere det innholdet den tror brukerne vil være interessert i. Eksempelvis har TikTok på få år vokst seg til det tredje mest brukte sosiale mediet gjennom å skape større brukerengasjement ved å fokusere på algoritmisk innholdsmatching, i motsetning til venner/følger-paradigmet som Facebook, Twitter og andre benytter.[158, 159] Det er denne dynamiske og automatiske koblingen av innhold og bruker som påvirkningsoperasjoner i sosiale medier søker å manipulere for å få oppmerksomhet for sitt innhold. Provoserende meninger får ofte mer oppmerksomhet og oppnår bedre spredning grunnet behovet for oppmerksomhet. Et slikt fokus øker splittelser i et samfunn. Fremvoksende teknologier som deepfakes eller metaverset kan skape uro, men det er nåværende teknologier som legger grunnlaget for spredning av desinformasjon og misinformasjon.

Når det gjelder punkt b), er dette både et teknisk og et policy-problem. For eksempel blokkerte Facebook i noen timer alle innlegg med ordet «vote» i forbindelse med valget i Storbritannia i 2019 grunnet en endring i algoritmene som skulle oppdage manipulering.[160] Lekkede dokumenter har vist at Facebook prioriterte fjerning av desinformasjon i vestlige land fremfor land i Afrika og Asia, selv om problemet kunne være større der, grunnet kapasitetsproblemer.[161] Blokkering av individuelle brukere eller emner (innholdsmoderering) skjer ofte som resultat av eksternt press i en opphetet situasjon. Kvaliteten på beslutningene kan derfor være av varierende kvalitet. Samlet sett betyr dette at sosiale medieplattformer er en aktiv, men uforutsigbar, aktør i påvirkningsøyemed.

De sosiale medieplattformene er under press for blant annet å stoppe spredning av desinformasjon og bruk av falske kontoer. EUs Digital Markets Act og Digital Services Act[162] trer i kraft i løpet av 2023 og 2024 og er et skritt i riktig retning av bedre regulering av det digitale landskapet for misbruk, men det gjenstår å se hva effekten faktisk blir.

4.2.5 Avskrekking, avdekking og håndtering av påvirkningsoperasjoner

Avskrekking i tradisjonell forstand forstås som å forhindre et angrep gjennom å påvirke en motparts kost-nytte-kalkyle.[163] For Norge utgjør NATO-medlemskapet den viktigste avskrekkende faktoren. Kostnaden ved å angripe Norge militært vil være så høy at risikoen for

[157] Bergh, 2020
[158] The Verge, Heath; *How Facebook Plans to Become More like TikTok*, 2022
[159] CNBC, Sherman; *TikTok Reveals Detailed User Numbers for the First Time*, 2020
[160] Sky News, Manthorpe; *Facebook Posts with the Word "vote" Blocked after Leaders' TV Election Debate*, 2019
[161] BuzzFeed News, Silverman et al.; *"I Have Blood On My Hands": A Whistleblower Says Facebook Ignored Global Political Manipulation*, 2020
[162] EC, *Shaping Europe's digital future – The Digital Services Act package*, 2023
[163] RAND, Mazarr; *Understanding Deterrence*, 2018

at det skal skje er liten. Bruk av sammensatte virkemidler, som påvirkningsoperasjoner, mot hele samfunnet under terskelen for krise og krig utfordrer dette konseptet. Selv om NATO har besluttet at artikkel fem skal gjelde også ved både cyberangrep og «hybride angrep»,[164] er terskelen høy, uklar og har aldri vært prøvd.

Forskning på avskrekking av påvirkningsoperasjoner identifiserer noen tiltak for nektelse (denial) gjennom motstandsdyktighet (resilience), avskrekkere (deterrents) og mottiltak (countermeasures).[165] Avskrekking bør altså forstås som bredere enn å skape høy risiko for gjengjeldelse (punishment), og bør inkludere nektelsestiltak for å begrense påvirkningsaktørers tekniske og kognitive handlingssrom og mulighet for å skape ønskede effekter.

Det er de siste årene utviklet en rekke råd og anbefalinger for hvordan man kan øke motstandsdyktigheten mot påvirkningsoperasjoner. Kildekritikk, digital kompetanse, økt kunnskap, tekniske evner til deteksjon og strategisk kommunikasjon for forebygging (prebunking[166]) og håndtering er gjennomgående. En kortfattet oversikt over ulike former for operasjoner, virkemidler og anbefalinger kan leses i FFI-rapporten *Hvordan gjøre samfunnet mer robust mot uønsket påvirkning i sosiale medier*.[167] Den har til hensikt å bidra til å gjøre norske myndigheter, Forsvaret og totalforsvarsaktørene, og dermed samfunnet, bedre rustet til å forstå og gjenkjenne påvirkningsoperasjoner i sosiale medier. Dette er imidlertid et område under kontinuerlig endring.

Mens metodene, teknikkene og virkemidlene vil fortsette å utvikle seg og ny teknologi åpne for nye sårbarheter, er det vi ønsker å beskytte mer konstant. Sikkerhetsloven[168] skal definere hva som skal beskyttes, men det er usikkert om den er dekkende. Påvirkningsoperasjoner vil kunne true Norges interesser, handlefrihet og omdømme på områder som ikke omfattes av den.

FFI-rapporten *Defence against foreign influence – a value-based approach to define and assess harm, and to direct defence measures* argumenterer for et verdibasert forsvar mot fremmedstatlig påvirkning.[169] Forsvarsoppgaven handler da om å identifisere verdiene Norge ønsker å beskytte (for eksempel styreform og politisk handlefrihet) og å tufte forståelsen for forsvarsoppgaven på dem. Rapporten foreslår at skade inntreffer når fremmedstatlige påvirkningsaktiviteter har uønskede effekter på essensielle stats- og samfunnssikkerhetsinteresser. Meningsfulle mottiltak må da ha som formål å styrke evnen til å beskytte disse interessene. Forskning tilsier at en effektiv strategi for å gjøre det er gjennom

[164] NATO, 2022

[165] Pamment, Agardh-Twetman, 2019

[166] First Draft, Garcia, Shane; *A guide to prebunking: a promising way to inoculate against misinformation*, 2021

[167] Sivertsen et al., 2021

[168] Lov om nasjonal sikkerhet, 2018

[169] Kveberg et al., 2019

«psykologisk inokulasjon». Akkurat som vaksine reduserer effekten av et virus, kan «prebunking» redusere effekten av skadelige, falske narrativer.[170]

4.2.6 Utfordringer for Norge per i dag

Situasjonsforståelse og kapabiliteter

Forebygging og forsvar mot påvirkningsoperasjoner krever god og lik situasjons- og sikkerhetspolitisk forståelse på nasjonalt og lokalt nivå i alle sektorer, kunnskap om truslene, virkemidlene og aktørene, hvilken hensikt disse kan ha og hvilke effekter de sannsynligvis er ute etter å skape.[171]

På tross av økt oppmerksomhet og trusselvurderinger fra Etterretningstjenesten og PST, er det i Norge fortsatt uavklart hvem som har det overordnede ansvaret for å avdekke, analysere og håndtere påvirkningsoperasjoner som rettes mot samfunnet i sin helhet, uavhengig av aktør og under terskelen for det som er kriminelle handlinger. Både sivile og militære myndigheter i flere land, EU og NATO har etablert ulike former for samarbeid og funksjoner for å gjøre det. Her er noen eksempler:

- **EU:** East Stratcom Task Force,[172] inkludert EUvsDisInfo[173]
- **NATO:** NATO Stratcom Center of Excellence[174] og Public Diplomacy Division
- **USA:** Global Engagement Center[175]
- **Storbritannia:** Rapid Response Unit knyttet til Cabinet Office og Statsministerens kontor, koordinerer med Counter Disinformation Cell i Department for Digital, Culture, Media and Sport[176]
- **Sverige:** Myndigheten för psykologiskt försvar[177]
- **Litauen:** Egen analyseenhet i forsvarsdepartementet
- **Tyskland:** En rekke tiltak og arbeidsgrupper spesielt knyttet til valg[178]
- **Frankrike:** Viginum, enhet underlagt Secrétariat général de la défense nationale[179]

[170] Roozenbeek et al., 2022

[171] Bergaust et al., 2022

[172] EU, EEAS, *Questions and Answers about the East StratCom Task Force*, 2021

[173] EUvsDiSiNFO, 2023

[174] NATO Strategic communication centre of excellence, 2023

[175] U.S. DEPARTMENT of STATE, Global Engagement Center, 2023

[176] GOV.UK, Cyber security, *Government cracks down on spread of false coronavirus information online*, 2020

[177] Myndigheten for psykologiskt försvar, 2023

[178] EU Disinfo Lab, Miguel, *The battle against disinformation in the upcoming federal election in Germany: actors, initiatives and tools*, 2021

[179] SGDSN, *Service de vigilance et protection contre les ingérences numériques étrangères*, 2022

Juridiske forhold

I Norge foreligger det et lovforslag[180] om å gjøre det straffbart å samarbeide med fremmed etterretningstjeneste om å utøve påvirkningsvirksomhet. Forslaget har høstet kritikk fra flere hold blant annet fra Advokatforeningen.[181] Om vedtatt, vil forslaget muliggjøre mer informasjonsdeling mellom EOS-tjenestene, men likevel kun omfatte personer som aktivt samarbeider med fremmed etterretning. Siden fremmedstatlige påvirkningsoperasjoner først og fremst gjennomføres fra utlandet og av utenlandske borgere, er det usikkert hvor stor effekt en slik hjemmel vil ha.

Fra 1. januar 2023 åpner politiregisterloven for at PST kan lagre, systematisere og analysere stordata fra åpne kilder til utarbeidelse av analyser og trusselvurderinger i opptil fem år.[182] I høringsutkastet var det foreslått 15 år. Advokatforeningen og EOS-utvalget mente forslaget ikke var godt nok utredet,[183] og det ble kritisert for å være for bredt på bekostning av personvernet. Selv om slik innsamling og analyse er nødvendig for å oppdage og forstå påvirkningsoperasjoner, betyr ikke det at PST nå vil kunne gjennomføre dette med mindre det foreligger mistanke om strafferettslig kriminell aktivitet, noe mye av påvirkning ikke er.

4.2.7 Utvikling framover

Påvirkningsoperasjoner utvikler seg kontinuerlig og er ofte opportunistiske av natur. De søker å skape og utnytte mulighetsrom. Virkemidlene som benyttes begrenses kun av teknologiske og samfunnsmessige muligheter og aktørens fantasi, ressurser og prioriteringer. Når aktørers metoder avsløres og noen ganger begrenses, som f.eks. ved fjerning av falske profiler på sosiale medier, finner de nye og mer sofistikerte måter å operere på. Teknikkene vi kjenner fra russiske operasjoner brukes også av andre aktører, både med og uten statlig tilknytning. De største sosiale medieplattformene er fortsatt relativt enkle å utnytte tross teknologiselskapenes arbeid for å begrense det.[184] Påvirkningsoperasjoner forventes å utgjøre en betydelig og økende utfordring spesielt på grunn av tre forhold:

Økt geopolitisk rivalisering

Dagens sikkerhetspolitiske situasjon preges av stormaktsrivalisering og at fremmedstatlige aktører i økende grad tar i bruk metoder som kombinerer åpne, skjulte og fordekte militære og ikke-militære virkemidler for å nå sine strategiske målsettinger. Stormaktrivaliseringen har med andre ord bidratt til å skape et mer sammensatt trusselbilde, hvorav påvirkningsoperasjoner utgjør en viktig komponent. I den statsvitenskapelige litteraturen plasseres denne typen virkemidler under det relativt nye begrepet «sharp power». Denne typen maktbruk kjennetegnes

[180] Justis- og beredskapsdepartementet, *Høringsnotat om endringer i straffeloven mv. – påvirkningsvirksomhet*, 2021

[181] Advokatforeningen, *Høringsuttalelser - Endringer i straffeloven mv. – påvirkningsvirksomhet*, 2021

[182] Prop. 31 L (2022-2023), 2022

[183] Rett 24, Kolsrud, *Forslaget om å la PST overvåke åpne kilder får hard medfart i høringen*, 2022

[184] Bay et al., 2022

av at den aktuelle aktøren forsøker å manipulere en målgruppe med sikte på å oppnå sine strategiske målsettinger,[185] ofte gjennom påvirkning og/eller destabilisering.[186] Et særtrekk ved denne typen maktbruk generelt, og påvirkningsoperasjoner spesielt, er at målgruppen ofte er sivilbefolkningen i et land og at handlingene foregår under terskelen for væpnet konflikt. Et annet viktig poeng er at informasjonspåvirkning, til sammenlikning med tradisjonelle militære virkemidler, har relativt lave kostnader og liten risiko for å bli oppdaget. Dette medfører en lavere sannsynlighet for negative konsekvenser for aktøren som står bak. Dette igjen resulterer i at en aktør vil ha lite å tape på å benytte seg av påvirkningsoperasjoner. Dagens utvikling med økt stormaktsrivalisering, kombinert med påvirkningsoperasjoners lave politiske og økonomiske kostnad, gir grunn til å tro at informasjonspåvirkning vil utgjøre en økende utfordring i tiden fremover.

Økt misnøye og usikkerhet

Russlands krig mot Ukraina faller sammen med klimakrisen og flere andre utviklingstrekk som har utløst kjedereaksjoner vi ennå ikke kjenner omfanget av. Dette skaper en ny og forverret situasjon for hele verdens befolkning, også i Norge. Høyere renter, økte priser og kutt i offentlige tjenester skaper økt misnøye som kan bidra til økt polarisering og svekket tillit til politikere og demokratiske institusjoner i alle stater som opplever dette – også i Norge. Russiske påvirkningsoperasjoner rettet mot Europa det siste året har også forsøkt å forsterke denne misnøyen og usikkerheten og bruke den til å undergrave tilliten til europeiske lands myndigheter og svekke europeisk støtte til Ukraina.

Teknologisk utvikling

Utbredelsen av 5G, tingenes internett, kunstig intelligens, quantum computing og nye plattformer og digitale virkeligheter som metaverset,[187] hvis visjonene en dag realiseres, skaper nye sårbarheter i samfunnet og nye teknologiske muligheter for påvirkningsaktører. Nyhetsartikler og annet innhold med ønsket vinkling kan produseres automatisk og i store mengder med stadig bedre kvalitet. Deepfake-teknologi begynner å bli allment tilgjengelig og kan ha blitt tatt i bruk av ondsinnede aktører for å utgi seg for å være noen andre enn de er. Et mulig eksempel er fra i juni år, da ordførerne i Wien, Madrid og Berlin skal ha blitt lurt til å tro at de hadde videosamtaler på Webex med Kyivs ordfører Vitali Klitschko.[188] Metaverset er foreløpig heftet med usikkerhet med hensyn til om visjonene kan realiseres, men kan i så fall gi muligheter for psykologisk manipulasjon på et nivå som i dag er utenkelig.[189]

[185] Cristóbal, 2021

[186] Bernal et al., 2020

[187] WIRED, Ravenscraft; *What is Metaverse, Exactly?*, 2022

[188] The Guardian, Oltermann; *European politicians duped into deepfake video calls with mayer of Kyiv*, 2022

[189] RAND, Waltzman; *Facebook Misinformation Is Bad Enough. The Metaverse Will Be Worse*, 2022

4.2.8 Kognitiv krigføring

Fremmedstatlige aktørers påvirkningsoperasjoner i informasjonsmiljøet har blitt et utbredt og effektivt maktpolitisk virkemiddel mot vestlige demokratier. Uønsket påvirkning er ikke et nytt fenomen, men den senere utviklingen innenfor teknologi og sosiale medier har skapt nye muligheter for en aktør til å oppnå betydelig større effekt i forhold til innsats og risiko. Påvirkningsforsøk rettet mot demokratiske prosesser i en rekke vestlige land de siste årene har bidratt til å synliggjøre de potensielle alvorlige konsekvensene påvirkningsoperasjoner kan ha for vestlige demokratiske verdier og levesett.

NATOs nye strategiske konsept (2022) legger vekt på å beskytte alliansens demokratiske verdier.[190] Alliansen sender et tydelig signal om at trusselen påvirkningsoperasjoner kan utgjøre mot demokratiet vil være en viktig prioritering i årene fremover gjennom sitt nye arbeid med såkalt «kognitiv krigføring». Det finnes ikke en etablert enighet om én definisjon av «kognitiv krigføring», men kjernen i den nåværende forståelsen av begrepet er at dette er handlinger som har til hensikt å endre en målgruppes oppfatninger og videre hvordan målgruppen handler basert på disse oppfatningene. Målet for aktøren som utfører disse handlingene er å oppnå er fordel for seg selv, for eksempel gjennom å påvirke en annen stats politikk (for eksempel på utenriks- eller forsvarsfeltet) eller gjennom destabilisering.[191, 192] Det er viktig å presisere at dette arbeidet befinner seg i startfasen. Likevel er det en tydelig indikasjon på at problemstillinger knyttet til kognitiv krigføring og påvirkningsoperasjoner vil være svært viktige for NATO i tiden fremover. Sentrale problemstillinger alliansen står ovenfor er blant andre hvordan medlemslandene på best mulig måte skal forsvare seg mot kognitive angrep, inkludert påvirkningsoperasjoner, samt ansvars- og rollefordelingen knyttet til dette.

4.3 Økonomisk virkemiddelbruk

Dette delkapitlet beskriver utviklingstrekk innen staters bruk av økonomiske virkemidler for å oppnå utenrikspolitiske, strategiske mål (økonomisk statshåndverk) som kan ha særlig betydning for nasjonal sikkerhet i et 2030-perspektiv. Fokus er lagt på hvordan andre stater kan bruke økonomiske virkemidler mot Norge, enten for å utøve makt eller for å akkumulere makt. Diskusjonen knyttes opp mot nasjonale sikkerhetsinteresser i henhold til definisjonen gitt i sikkerhetsloven. Delkapitlet bygger på innsikt fra øvrig arbeid om økonomiske virkemidler ved FFI.

En kort bakgrunn om hva økonomiske virkemidler er og hvordan stater kan bruke økonomiske virkemidler på måter som potensielt er sikkerhetstruende gis i kapittel 4.3.1. Deretter drøftes potensielle implikasjoner for norsk sikkerhet med hensyn på utvalgte stater – Kina og Russland – sin bruk av økonomiske virkemidler. Dette er basert på litteraturgjennomganger og analyser av historiske hendelser over disse statenes økonomiske statshåndverk (kapittel 4.3.2). Kapittel

[190] NATO, 2022

[191] Backes, Swab, 2019

[192] Bernal et al., 2020

4.3.3 fokuserer spesifikt på potensielle implikasjoner av den teknologiske utviklingen på staters muligheter til å bruke økonomiske virkemidler og mulige konsekvenser for norsk sikkerhet. I kapittel 4.3.4 følger en diskusjon.

4.3.1 Hva er økonomisk statshåndverk?

Økonomi og sikkerhet har tradisjonelt blitt forstått som separate domener. Globalisering, internasjonalisering av finansmarkedene, digitalisering og fremvoksende økonomiers, herunder spesielt Kinas, økte tyngde i verdensøkonomien har bidratt til at staters evne til å utnytte økonomisk aktivitet for strategiske formål har økt. Med det har også viktigheten av å se domenene i sammenheng blitt viet større oppmerksomhet.[193]

Begrepet økonomisk statshåndverk (*economic statecraft*) benyttes her som betegnelse på en stats bruk av økonomiske virkemidler for å oppnå utenrikspolitiske, strategiske mål.[194] Dette innebærer at staten (intensjonelt) manipulerer eller på andre måter utnytter økonomisk aktivitet for strategiske formål.[195, 196] Eksempler på økonomiske virkemidler er sanksjoner, investeringer, handel, lån, bistand og valuta. Staten og landet som utfører økonomisk statshåndverk omtales her som avsenderstat og -land og mottakerstat og -land for enhetene som statshåndverket rettes mot.

Alle stater kan ta i bruk slike virkemidler for å utøve press eller forme interessene i andre land. USA er storbruker av handelssanksjoner[197] og har også begynt å ta i bruk finanssanksjoner, for eksempel mot Iran[198] og mot Russland i 2014[199] og 2022,[200] sammen med andre vestlige land. Kina blir beskrevet som «verdens ledende utøver av geoøkonomi».[201] Eksisterende litteratur og empiri tilsier at Kina har brukt økonomiske virkemidler aktivt og variert de siste tiårene.[202] Russland har også benyttet økonomisk statshåndverk mot «det nære utland», mot andre europeiske land og globalt.[203] Ved flere tilfeller etter invasjonen av Ukraina 24. februar 2022, har Russland tilsynelatende utnyttet europeisk avhengighet av russisk olje og gass til å forsøke å

[193] Se for eksempel: Blackwill, Harris, 2016; Cohen, 2009; Drezner, 2008; Mastanduno, 1998; Retter et al., 2020

[194] Baldwin, 1985

[195] Norris, 2016

[196] Siden økonomiske transaksjoner utføres av økonomiske aktører med i hovedsak kommersielle formål, handler økonomisk statshåndverk om å skape insentiver for økonomiske aktører til å agere i tråd med statsledelsens politiske og strategiske formål (Norris 2016).

[197] Morgan et al., 2014

[198] Farrell, Newman, 2019

[199] NATO Review, Christie; *Sanctions after Crimea: Have They Worked?*, 2015

[200] BBC News, *What Sanctions Are Being Imposed on Russia over Ukraine Invasion?*, 2022

[201] Blackwill, Harris, 2016

[202] Waage et al., 2022

[203] Udal et al., 2022

svekke EU-landenes støtte til Ukraina og innføring av sanksjoner mot Russland.[204] I seg selv impliserer ikke begrepet økonomisk statshåndverk at det foregår sikkerhetstruende aktivitet. For eksempel inkluderer økonomisk statshåndverk virkemidler som at land forsøker å promotere egen valuta til bruk i internasjonale transaksjoner,[205] så vel som økninger i handel, investeringer og lån for å forsøke å fremme vestlige verdier som demokrati og menneskerettigheter.

Tidligere arbeid ved FFI har derfor utarbeidet en typologi som kan bidra til å styrke forståelsen av når økonomisk statshåndverk potensielt kan være sikkerhetstruende. Tabell 4.1 presenterer denne typologien. Den består av to maktdimensjoner – maktatferd og maktkanal – med to utfall per dimensjon. For maktatferd skiller vi mellom *utøvelse* og *akkumulasjon* av makt. Makt kan utøves ved å ta i bruk økonomiske virkemidler for å oppnå politiske og strategiske mål, som i å straffe og belønne mottakerstaten eller begrense handlingsrommet til mottakerstaten. Men makt kan også akkumuleres ved å utnytte økonomiske transaksjoner på tvers av landegrenser for å legge til rette for økonomisk – eller annen – maktbruk i fremtiden. For maktkanal skiller vi mellom *bilateral kanal* og *nettverkskanal*. Økonomisk statshåndverk og maktbruk i internasjonal politikk har tradisjonelt blitt forstått i bilaterale relasjoner. Men makt kan også akkumuleres eller utøves i nettverk. Globaliseringen har bidratt til utviklingen av store nettverk med en topografi av asymmetrisk karakter, der noen av nodene (*nodes*) er knutepunkt (*hub*) med forbindelser til hele eller store deler av nettverket. Slike nettverk tilbyr strukturell makt, hvor noen land – et knippe stormakter som USA og Kina – har evne til å utnytte deres uforholdsmessige gunstige posisjonering i regionale og globale nettverk for å oppnå strategiske mål.[206] Eksempler på slike nettverk inkluderer globale finansnettverk (for eksempel SWIFT), internettplattformer, kommunikasjonsteknologi, nettverk for deling av sensitiv teknologi eller utvikling av militære våpensystemer, samt energi- og transportnettverk.[207] Til sammen danner dimensjonene fire kategorier. I hver kategori er det identifisert mulige handlingsmåter av økonomisk statshåndverk som potensielt kan utgjøre en trussel mot norske sikkerhetsinteresser. Med handlingsmåter menes her de typene av handlinger stater kan utføre ved bruk av økonomiske virkemidler.[208] Handlingsmåtene utdypes ikke her av plasshensyn, men det henvises i stedet til øvrige publikasjoner[209] for en grundigere beskrivelse av dem.

[204] Se for eksempel: The Economist, *Russia is using energy as a weapon*, 2022

[205] Se for eksempel: Cohen, 2008

[206] Farrell, Newman, 2019

[207] Drezner et al., 2021

[208] Det betyr at etterretningsvirksomhet for eksempel i form av rekruttering av innsidere ikke er økonomisk statshåndverk, mens innhenting av informasjon gjennom utføring av økonomisk aktivitet er det.

[209] Se for eksempel: Waage et al., 2022; Udal et al., 2022; Waage, Lindgren, 2022

Tabell 4.1 Typologi over handlingsmåter av økonomisk statshåndverk som potensielt kan utgjøre en trussel mot norsk sikkerhet.

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

4.3.2 Implikasjoner av Kinas og Russlands økonomiske statshåndverk i et 2030-perspektiv

I dette delkapitlet sees det nærmere på Kina og Russland. Alle land kan i prinsippet ta i bruk virkemidler fra det økonomiske domenet for å forsøke å oppnå sine strategiske, utenrikspolitiske mål. I lys av Kinas fremvekst som en sentral politisk, økonomisk og militær aktør – utenfor det atlantiske sikkerhetsfellesskapet – er det imidlertid behov for å forstå bedre implikasjoner av Kinas økonomiske statshåndverk for norsk sikkerhet. Russland er, i likhet med Kina, ikke en del av det vestlige sikkerhetssamarbeidet. I den forbindelse – samt etter Russlands invasjon av Ukraina 24. februar 2022 – er det også behov for å forstå implikasjoner av Russlands økonomiske statshåndverk for norsk sikkerhet. I både Kina og Russland er dessuten koblingene mellom stat og økonomiske aktører tettere enn i demokratiske økonomier. Det er blant annet relativt høye andeler statseide selskaper og gjennom lovgivning kan staten kreve at økonomiske aktører samarbeider med staten av hensyn til nasjonal sikkerhet. Siden økonomisk statshåndverk fordrer statlig kontroll/manipulasjon av økonomiske aktører og deres økonomiske transaksjoner, skaper disse trekkene ved den kinesiske og russiske økonomien bedre forutsetninger for å utføre økonomisk statshåndverk.

Kina

Den norske økonomien er mindre avhengig av handel, investeringer og lån med Kina enn flere andre avanserte økonomier, særlig i Asia og Oseania. Samtidig er Kina en av Norges viktigste handelspartnere, og videre vekst i den kinesiske økonomien kan bidra til å øke Norges

avhengighet av den kinesiske økonomien i årene fremover.[210] Norge er ikke på samme vis en viktig økonomi for Kina. Kina har dessuten relativt små eierinteresser i Norge. Det gir en asymmetri i det bilaterale handels- og investeringsforholdet som potensielt kan utnyttes.[211] Kina er dessuten en viktig økonomi også for mange andre land, som eksportør, importør og/eller kilde til kapital. Det betyr at Kina kan forsøke å utnytte sin økonomiske samhandling med tredjeland til å utøve press. Ifølge litauiske myndighetspersoner, opplevde Litauen i 2021 at Kina presset multinasjonale selskaper, som har deler av verdikjeden sin i Litauen, til å trekke ut denne produksjonen for å kunne fortsette å handle med Kina.[212] Så selv om Litauen har lite direkte handel med Kina, utnyttet Kina Litauens økonomiske interaksjon med tredjeland som pressmiddel.

Samlet vurderes Kina til å ha potensial til å utøve makt mot Norge ved å bruke økonomisk statshåndverk, og at dette potensialet vil vedvare frem mot 2030. Det kan særlig være aktuelt for Kina å manipulere norske bedrifters tilgang til å selge varer og tjenester til det kinesiske markedet, enten i form av importrestriksjoner, utgående turismerestriksjoner, forbrukerboikotter og/eller restriksjoner i mulighetene for bedriftsetablering i Kina. Dette er handlinger Kina tilsynelatende har benyttet mest for å utøve makt mot andre land i perioden 2000 – 2021, inkludert mot Norge etter Nobelprisutdelingen til Liu Xiaobo i 2010.[213] Det er relativt lave kostnader for Kina å innføre slike reguleringer som rammer mottakerlandets eksportsektor, mens effekten i mottakerlandet – på grunn av størrelsen til det kinesiske markedet – kan være betydelig. Reguleringene kan dessuten begrunnes og legitimeres med henvisninger til sikkerhet, produktkvalitet og lignende hensyn.

Det er imidlertid uklart om denne typen handlinger truer norsk sikkerhet. I tidligere tilfeller hvor Kina tilsynelatende har innført strategisk motiverte import- og turismerestriksjoner, har motivasjonen vært å fremtvinge endring i politikk hos mottakerstaten. Waage et al. identifiserer mange hendelser hvor det fremstår som at Kina har brukt slike virkemidler for å fremme og forsvare sine kjerneinteresser, blant annet knyttet til Taiwan, Xinjiang og Øst- og Sør-Kina-havet.[214] Dersom Norges nasjonale sikkerhetsinteresser knyttet til «de øverste statsorganers virksomhet, sikkerhet og handlefrihet» inkluderer at øverste statsorganer skal kunne trosse andre staters kjerneinteresser, kan den politiske handlefriheten potensielt bli truet av kinesisk bruk av økonomisk statshåndverk for å påvirke og legge press på norske myndigheter. Dersom øverste statsorganer primært skal kunne bestemme interne forhold i Norge, er det mer usikkert i hvilken grad Kinas bruk av økonomisk statshåndverk kan true den

[210] Den kinesiske økonomien opplever for tiden problemer, blant annet på grunn av ”null-covid”-regimet, nedstengninger og problemer i eiendomsmarkedet, se for eksempel: The Economist; *China's rulers seem resigned to a slowing economy*, 2022

[211] For ytterligere detaljer om Kinas økonomi, se Lindgren, 2022

[212] South China Morning Post, Ng, Lo; *China-Lithuania tension: German firms may have to shut factories in Baltic state amid Beijing retaliation*, 2021

[213] Waage et al., 2022

[214] Waage et al., 2022

politiske handlefriheten. Mellom disse ytterpunktene eksisterer det et rom der det fremstår mer usikkert hvorvidt handlefriheten potensielt kan trues av kinesisk bruk av økonomisk statshåndverk. Spørsmål knyttet til Norges valg av forsvarspolitiske allianser, Norges internasjonale posisjoner, handlingsrommet til å utestenge kinesisk teknologi av hensyn til nasjonal sikkerhet og kinesiske forsøk på å forme den norske debatten om kinesiske interesser havner i denne kategorien.

Forstyrrelser i Norges utenriksøkonomi kan potensielt utgjøre en trussel mot nasjonale sikkerhetsinteresser knyttet til økonomisk stabilitet.[215] Generelt er det uklart hvor omfattende eventuelle forstyrrelser må være før det vurderes at norsk sikkerhet blir truet. For eksempel kan reduksjoner i handel eller utenlandsinvesteringer ha en negativ påvirkning på norsk sysselsetting. Det virker likevel rimelig å anta at omfanget må være betydelig før det kan sies at norsk sikkerhet er truet. Derfor virker det ikke sannsynlig at Kina, per i dag, kan være i stand til å true nasjonale sikkerhetsinteresser knyttet til den norske økonomiens stabilitet ved for eksempel å innføre importrestriksjoner rettet mot enkeltnæringer i Norge. Den kinesiske økonomiens størrelse gjør imidlertid at (trusler om) redusert tilgang til det kinesiske markedet, også for bedrifter i tredjeland som handler med norske bedrifter, kan lede til større økonomiske konsekvenser for den norske økonomien. Men det forutsetter at Norges handelspartnere lar seg presse. I tillegg til Kina, er Norges viktigste handelspartnere vest-europeiske land og USA. Dermed framstår Kinas muligheter til å utnytte tredjeland til å legge press på Norge som begrenset. Dersom den kinesisk-norske økonomiske interaksjonen vokser absolutt og relativt i årene fremover, som følge av fortsatt økonomisk vekst i Kina, vil det imidlertid kunne bidra til at kinesisk økonomisk statshåndverk mot Norge kan utgjøre en større trussel mot Norges økonomiske stabilitet i fremtiden.

I et 2030-perspektiv vil det også være relevant å vurdere hvorvidt Kina kan være i stand til å forme (sær)interesser og oppfatninger blant næringslivet, beslutningstagere og befolkningen i Norge og hvorvidt slike forsøk vil være sikkerhetstruende. Eksempler kan for eksempel være forsøk på å lokke utvalgte næringer eller geografiske regioner i Norge med særlig lukrative kontrakter og avtaler. Dette for å stimulere til at disse igjen søker å påvirke norske beslutningstagere i en strategisk viktig sak for Norge. Men nok en gang kan man stille spørsmålstegn ved om slik påvirkningsaktivitet er tilstrekkelig til å utgjøre en trussel mot nasjonale sikkerhetsinteresser knyttet til «de øverste statsorganers virksomhet, sikkerhet og handlefrihet». Dersom påvirkningsaktivitet ved bruk av positive økonomiske insentiver (som investeringer, lån, og lignende) til enkeltgrupper i det norske samfunn involverer forsøk på å skape polarisering mellom nord og sør, kan aktiviteten potensielt true Norges nasjonale sikkerhetsinteresser knyttet til forsvar, sikkerhet og beredskap. Imidlertid er det nok nødvendig

[215] Økonomisk stabilitet dreier seg om utviklingen i makroøkonomiske hovedstørrelser (for eksempel inflasjon, valutakurs, vekst og sysselsetting), systemer for å håndtere offentlige ytelser og inntekter, kapitalforhold ovenfor utlandet, den finansielle infrastrukturen og finansmarkedene. NSM, 2020

at omfanget og varigheten av den økonomiske aktiviteten er av en viss størrelse for at den eventuelt skal kunne utgjøre en trussel mot Norges nasjonale sikkerhetsinteresser.

Kinesiske oppkjøp av norske bedrifter kan føre til kunnskapsoverføring og potensielt styrke Kinas militære kapabiliteter. Norge har og er ledende på teknologi som også kan ha et militært brukspotensial, inkludert undervannsteknologi.[216] Norge har også en konkurransedyktig forsvarsindustri med høyteknologi for militær anvendelse. Det kan være av interesse for andre stater, inkludert Kina, å få tilgang til disse teknologiene. Waage et al. diskuterer flere tilfeller av at Kina tilsynelatende har klart å tilegne seg militær- og flerbruksteknologi, særlig fra USA.[217] I disse tilfellene har Kina tilsynelatende oppnådd dette blant annet gjennom å manipulere handelsinformasjon, investere i selskaper, stjele bedriftshemmeligheter og rekruttere forskere. I et 2030-perspektiv kan Kina forsøke å utføre slik aktivitet rettet mot selskaper og kunnskapsmiljøer i Norge. Frem mot 2030 er det også viktig å være klar over at Kina kan forsøke å sikre seg tilgang til strategisk infrastruktur, eiendeler og lokasjoner i Norge og nordområdene. Dette kan bidra til å gi landet en militær fordel vis-à-vis Norge/NATO. Investeringer i selskaper og eiendom[218] og posisjonering i verdikjeder kan dessuten åpne muligheter for Kina til å bedrive etterretningsvirksomhet og datainnsamling rettet mot norsk næringsliv, offentlig sektor, politikere, befolkningen og Forsvaret. Bruken av økonomiske virkemidler, som beskrevet i dette avsnittet, kan potensielt true Norges nasjonale sikkerhetsinteresser knyttet til forsvar, sikkerhet og beredskap. Det kan være at én eller et relativt lavt antall transaksjoner er tilstrekkelig for å utgjøre en sikkerhetstrussel. Forsøk på teknologioverføring og etterretningsvirksomhet gjennom økonomisk aktivitet kan også utgjøre en trussel mot nasjonale sikkerhetsinteresser knyttet til forholdet til andre stater og internasjonale organisasjoner. Dette kan være en trussel siden disse sikkerhetsinteressene inkluderer at Norge bidrar til å ivareta allierte staters sikkerhet.[219]

Myndigheter og næringslivet i Norge bør også være bevisste på at økonomiske virkemidler som investeringer, salg av produkter og komponenter eller posisjonering i verdikjeder kan åpne muligheter for å utføre sabotasje på et senere tidspunkt. I et slik tilfelle kan også ikke-økonomiske virkemidler fra for eksempel cyberdomenet være involvert.[220] Posisjonering for fremtidig sabotasje kan spesielt utgjøre en trussel mot nasjonale sikkerhetsinteresser knyttet til forsvar, sikkerhet og beredskap samt samfunnets grunnleggende funksjoner og befolkningens sikkerhet. Det kan for eksempel være tilfellet dersom slik økonomisk aktivitet gjør det mulig å ramme funksjonsevnen til kritiske tjenester så som telekommunikasjon, vann og avløp eller kraftforsyning. Disse tjenestene kan rammes ved å sabotere forsyning, IT-systemer og

[216] PST, 2021

[217] Waage et al., 2022

[218] Eiendommer som er geografisk lokalisert i nærheten av strategisk viktig infrastruktur eller aktiviteter potensielt kan brukes til overvåking og spionasje.

[219] NSM, 2020

[220] Se ulike former for cyberoperasjoner i tidligere kapittel. For ytterligere detaljer om dette, se også kapittel 5 i Waage et al., 2021

lignende.[221] Økonomiske virkemidler kan også åpne muligheter for å sabotere eller på andre måter svekke systemer for å håndtere offentlige ytelser og inntekter eller den finansielle infrastrukturen. Nasjonale sikkerhetsinteresser knyttet til økonomisk stabilitet kan dermed potensielt bli truet. Det kan være rimelig å forvente at Kina stadig blir en viktigere eksportør til Norge, også innenfor høyteknologiske bransjer, da kinesiske bedrifter produserer og eksporterer stadig mer komplekse produkter. Som Tabell 4.2 viser, kan mulighetene for å bruke økonomiske virkemidler som inngangsportal for annen virkemiddelbruk dessuten øke i takt med den teknologiske utviklingen. Det bidrar til å aktualisere problemstillingen om hvordan økonomisk aktivitet (spesielt med Kina) kan fungere som en inngangsportal for sabotasjevirksomhet.

Som typologien i Tabell 4.1 viser, kan man skille på økonomisk statshåndverk som utnytter bilateral økonomisk interaksjon mellom avsender- og mottakerlandet, og økonomisk statshåndverk hvor det er avsenderstatens muligheter til å kontrollere knutepunkt i globale eller regionale økonomiske nettverk som gir opphav til statshåndverket. Det er i økende grad oppmerksomhet rundt hvordan Kina søker å posisjonere seg som et knutepunkt i globale økonomiske nettverk. De utfordrer dermed den dominerende posisjonen USA har hatt i slike nettverk siden slutten av andre verdenskrig. Gjennom opprettelsen av den asiatiske infrastrukturinvesteringsbanken (AIIB), promotering av renminbi til bruk i internasjonale transaksjoner og etablering av CIPS (et alternativ til SWIFT for internasjonale transaksjoner, men ennå ikke særlig i bruk utenfor Kina), styrkes Kinas plass i internasjonale finansnettverk.[222] Silkeveiinitiativet (*Belt and Road Initiative* – BRI), inkludert utbygging av transportinfrastruktur på land (for eksempel jernbaner), maritim transportinfrastruktur (for eksempel havner) og digital kommunikasjonsinfrastruktur (gjennom «den digitale silkeveien»), bidrar til å styrke Kinas sentralitet i globale verdikjede-, kommunikasjons- og transportnettverk.[223] Frem mot 2030 forventes det derfor at Kinas innflytelse over globale og regionale nettverk øker på bekostning av betydningen USA tradisjonelt har hatt i disse nettverkene. Dette er en sentral utviklingstrend innen kinesisk, økonomisk statshåndverk som norske myndigheter og beslutningstakere bør være klar over og forstå kinesisk økonomisk aktivitet i lys av.[224]

[221] Eksempler på tilrettelegging kan være salg av systemer med bakdører, programvareoppdateringer fra leverandør som åpner sårbarheter eller å få på plass for eksempel vedlikeholdspersonell som får tilgang til sensitive systemer. I tillegg til å tilrettelegge for sabotasjeaktiviteter, kan sabotasje gjennom økonomisk statshåndverk i prinsippet forekomme ved å utnytte eierskapskontroll over infrastruktur, underleverandører, til å skape forstyrrelser, endringer i driften av selskaper som infrastrukturer avhenger av samt forsøk på å svekke viktige/kritiske selskaper ved å trekke ut eventuelle investeringer. Manipulering av ressurstilgang, for eksempel gjennom eksportrestriksjoner for innsatsfaktorer, kan også være en måte å forsøke å sabotere viktige eller kritiske systemer og infrastruktur.

[222] Se for eksempel: Cohen, 2019; Goddard, 2021; Oatley, 2021

[223] Se for eksempel: Hillman, 2021; Cavanna, 2021; Clarke et al., 2020

[224] Noen studier peker på at USA fortsatt dominerer internasjonale nettverk, som for eksempel Winecoff, 2020

Russland

Russlands økonomi er betydelig mindre enn Kinas økonomi,[225] og Russlands betydning i det internasjonale økonomiske system er også mindre. Den økonomiske aktiviteten på tvers av Norge og Russland er heller ikke spesielt stor verken fra russisk eller norsk side.[226] Aktiviteten er også redusert som følge av sanksjonene fra begge sider etter annekteringen av Krim i 2014 og ytterligere i 2022 som følge av vestlige sanksjoner mot Russland etter invasjonen av Ukraina. Videre er ikke Norge avhengig av verken olje- eller gassimport fra Russland. Dette begrenser Russlands muligheter til å bruke sin markedsmakt direkte mot Norge. Det betyr at selv om Russland tilsynelatende har utnyttet økonomiske virkemidler for å utøve makt mot andre land, spesielt i form av importrestriksjoner og reduksjoner i gassleveranser, virker Russlands muligheter for å kunne utøve tilsvarende makt mot Norge begrenset. Norge blir imidlertid påvirket av redusert tilbud av naturgass i Europa, siden Norge er tett integrert i et (nord)europeisk strømmarked. Dagens utsikter for Russlands økonomiske utvikling, kombinert med sikkerhetspolitiske forhold, tilsier ikke at Norges økonomiske interaksjon med Russland kommer til å øke frem mot 2030. Dette vil dermed ikke styrke Russlands potensial til å utnytte interaksjonen strategisk til å utøve makt. Derimot kan det være aktuelt for Russland å utnytte økonomiske virkemidler mot Norge i et 2030-perspektiv for å akkumulere makt (se tabell 4.1), på måter som potensielt kan true flere av Norges nasjonale sikkerhetsinteresser.

Russland søker å bedrive påvirkningsaktivitet mot Norge gjennom økonomisk statshåndverk slik som Kina. Udal et al. identifiserer flere hendelser hvor Russland kan ha forsøkt å skape særinteresser for å påvirke politikk i ulike mottakerland, men da først og fremst i tidligere sovjetstater og andre østblokkland.[227] For Norge kunne slik aktivitet for eksempel ta form som russiske investeringer i næringsvirksomhet i Nord-Norge og Svalbard. Slik aktivitet kan være motivert av rene kommersielle hensyn, men investeringer kan potensielt også utføres som forsøk på å gjøre næringsliv og befolkning i nordområdene mer russlandsvennlig eller utføres av både kommersielle og strategiske hensyn. Forsøk på å forme interesser og oppfatninger kan potensielt også true nasjonale sikkerhetsinteresser knyttet til forsvar, sikkerhet og beredskap samt Norges forhold til andre stater og internasjonale organisasjoner. Eksempler på dette kan være forsøk på å skape polarisering mellom nord og sør eller motstand mot NATO-samarbeid gjennom ulike økonomiske insentiver. Likevel er det nok nødvendig med et relativt stort omfang av økonomiske transaksjoner over tid for at Russland eventuelt skulle kunne oppnå disse effektene. Gitt den begrensede økonomiske interaksjonen mellom Norge og Russland per dags dato, er det trolig at slike handlingsmåter i liten grad utgjør en trussel mot norsk sikkerhet på kort til mellomlang sikt.

Russland kan potensielt også bruke økonomiske virkemidler på andre måter som vil kunne true nasjonale sikkerhetsinteresser knyttet til forsvar, sikkerhet og beredskap og Norges forhold til

[225] Kinas BNP er til sammenligning nesten ti ganger så stort som Russlands BNP.

[226] Se Udal et al. (2022) for detaljer.

[227] Udal et al., 2022

andre stater og internasjonale organisasjoner. I rapporten *Russisk økonomisk statshåndverk – implikasjoner for norsk sikkerhet* nevner Udal et al. flere tilfeller der Russland kan ha klart å tilegne seg militær- og flerbruksteknologi, særlig fra USA og Tyskland.[228] I hendelsene har Russland tilsynelatende oppnådd dette gjennom å manipulere handelsinformasjon, gjennom investeringer i selskaper og ved å opprette selskaper i tredjeland. Gjennom økonomisk statshåndverk kan Russland potensielt også utføre etterretningsvirksomhet i Norge. Lazarev-saken[229] er et eksempel på hvordan lovlig økonomisk aktivitet potensielt kan åpne muligheter for russisk etterretningsvirksomhet. Norsk næringsliv og offentlig sektor bør derfor være forberedt både på russiske forsøk på å få tak i sensitiv militær- og flerbruksteknologi og på å utføre etterretningsvirksomhet gjennom økonomisk statshåndverk i et 2030-perspektiv.

Siden et relativt lavt antall økonomiske transaksjoner i prinsippet kan fungere som inngangsportaler for fremtidig sabotasje, kan Russland, som Kina, være i stand til å benytte handlingsmåtene «sabotere infrastruktur (gjennom eierskapskontroll)» og «tilrettelegge for skjult sabotasje» mot Norge i et 2030-perspektiv. Dessuten kan Russland forsøke å øke enkelte viktige/kritiske selskapers eller sektorers avhengighet til russiske aktører ved at de etablerer seg som leverandører av komponenter, ressurser og/eller kompetanse. Dette på tross av at den norske økonomiens totale avhengighet til Russland er lav. Manipulering av ressursavhengighetene kan i neste omgang inngå som del av press- og sabotasjeforsøk. Som redegjort for under delen om Kina, kan disse handlingsmåtene potensielt true nasjonale sikkerhetsinteresser knyttet til forsvar, sikkerhet og beredskap, økonomisk stabilitet og samfunnets grunnleggende funksjoner og befolkningens sikkerhet. Russlands betydning som leverandør av (høy)teknologiske produkter og systemer globalt og til Norge er imidlertid lav sammenlignet med Kina. Det betyr at selv om Russland i prinsippet også kan benytte handlingsmåter som beskrevet i dette kapitlet, vil det nok være mer krevende å få effekt av bruken for Russland enn det vil være for Kina.

4.3.3 Implikasjoner av den teknologiske utviklingen

Den teknologiske utviklingen under den fjerde industrielle revolusjonen (4IR) kan endre hvordan stater utfører økonomiske statshåndverk. Mye av den eksisterende litteraturen innen økonomisk statshåndverk fokuserer på tradisjonelle sanksjoner som importrestriksjoner.[230] Det er også i økende grad fokus på hvordan positive virkemidler som investeringer og lån kan utnyttes av stater

[228] Udal et al., 2022

[229] I 2021 ble det avslørt for offentligheten at et russisk forskningsfartøy (Lazarev) er ett av flere sivile fartøy som mistenkes for å systematisk kartlegge norsk sokkel for å få tak i viktig informasjon om kritisk norsk infrastruktur på havbunnen. Dette kan være kommunikasjons- og elektrisitetsnett og olje- og gassrørledninger. Det eksisterer også bekymringer rundt rekruttering av russiske sjøfolk til norske fartøy på grunn av deres mulighet for å tilegne seg kunnskap om norskekysten i arbeidshverdagen. Se for eksempel: Dagens Næringsliv, Kibar, *OPERASJON LAZAREV: Slår alarm om kartlegging av Norges kritiske infrastruktur*, 2021

[230] Se for eksempel: Drezner, 1998; Pape, 1997; Peksen, 2009; Early, Cilizoglu, 2020

for å fremme deres interesser.[231] Med enkelte unntak, er det imidlertid svært få studier som analyserer hvilke implikasjoner ny teknologi og økt digital sammenkobling har for bruken av økonomiske virkemidler.[232] Dette er til tross for at moderne økonomier og internasjonal økonomisk aktivitet blir stadig mer digitalisert og automatisert.

I et forsøk på å adressere dette gapet i eksisterende litteratur, har Waage og Lindgren (2022) gjennomført en forstudie av hvordan den teknologiske utviklingen kan påvirke staters evne til å ta i bruk økonomiske virkemidler som er relevante i et 2030-perspektiv. Rapporten har fokus på fire nye teknologier: kunstig intelligens, 5G, skytjenester og tingenes internett (IoT). Tabell 4.2, hentet fra Waage og Lindgren,[233] oppsummerer noen sentrale observasjoner per handlingsmåte i typologien over potensielt sikkerhetstruende økonomisk statshåndverk. I det følgende vil noen av funnene og potensielle implikasjoner for norsk sikkerhet drøftes nærmere.

Tabell 4.2 Oppsummerende vurderinger per handlingsmåte av hvordan den teknologiske utviklingen kan endre mulighetsrommet for økonomisk statshåndverk. Kilde: Waage og Lindgren (2022).

Handlingsmåte	Vurdering av implikasjoner av teknologiutviklingen
Utøve makt	
Manipulere tilgang til salg til innenlandsk marked	Økt potensial gjennom bruk av kunstig intelligens og stordata til å utforme virkemidler. Aktuelle økonomiske virkemidler er fremdeles importrestriksjoner, turismerestriksjoner og lignende. For enkelte stater også økt potensial pga. store innenlandske forbrukergrupper som blir viktigere med den teknologiske utviklingen.
Manipulere tilførselen av ressurser	Økt potensial gjennom nye avhengigheter til ressurser som kompetanse, varer, tjenester og råvarer. Disse får større betydning med den teknologiske utviklingen. Kunstig intelligens kan bidra til mer effektiv utforming av virkemidler. Manipulering av kompetanse kan spesielt bli et mer potent økonomisk virkemiddel for enkelte stater.
Sabotere infrastruktur (gjennom eierskapskontroll)	Økt potensial for sabotasje ved at samfunnet avhenger av tjenester og systemer blir sammenkoblet i større grad. Det oppstår flere angrepspunkter, inkludert større muligheter for sabotasje, utført gjennom eierskap i utlandet. Aktuelle økonomiske virkemidler er fremdeles investeringer og oppkjøp.

[231] Se for eksempel: Norris, 2016; Norris, 2021; Pape, 1997; Reilly, 2013; Xiaotong, Keith, 2017

[232] Se også: Waage et al., 2021

[233] Waage, Lindgren, 2022

Manipulere tilgang til nettverksstrømmer	Digitale og andre fysiske valutaer kan svekke USDs dominans i det internasjonale finanssystemet. Digitale valutaer kan på sikt svekke mulighetene til å utnytte internasjonale finansnettverk til å utøve makt. På den annen side også økt potensial ved at internettplattformer kan bli benyttet som virkemiddel til å presse og lokke med hhv. utestengelse fra, eller tilgang til, plattformene. Potensial for å utnytte muligheter til å utestenge stater fra «nettverk» av høyteknologiske produkter, tjenester og kritiske innsatsfaktorer.
Akkumulere makt	
Forme (sær)interesser og oppfatninger i mottakerlandet	Økonomiske virkemidler er fremdeles lån, oppkjøp, investeringer osv., men de kan bli mer potente. Økt potensial pga. at antallet mulige inngangsportaler for å bedrive for eksempel påvirkningsoperasjoner øker betraktelig med nye teknologier som skytjenester, 5G og IoT. Det blir også lettere å bedrive denne handlingsmåten fra utlandet og lettere å spre positiv (des)informasjon om avsenderstaten.
Øke avhengighet til ressurser og innenlandsk marked	Potensialet kan øke for enkelte land som besitter knappe ressurser, teknologisk kompetanse, viktig produksjon og/eller attraktive innenlandske markeder. Næringspolitikk, med geopolitisk motivasjon, kan utnyttes som økonomisk virkemiddel for å styrke egen økonomi og ressurskontroll.
Etterretningsvirksomhet (gjennom økonomisk aktivitet)	De økonomiske virkemidlene er de samme, men mulighetene for innhenting av informasjon og data øker betydelig med bl.a. IoT og 5G. Også økt potensial siden (digitale) verdikjeder blir lengre, mer geografisk spredt og mer uoversiktlige, samt pga. muligheter til å legge inn bakdører via kontinuerlige programvareoppdateringer (se også cyberkapittel). Samtidig kan den økte kompleksiteten også vanskeliggjøre utnyttelsen av økonomisk aktivitet til etterretningsformål.
Styrke materielle/ militære kapabiliteter	Den teknologiske utviklingen har bidratt til å aktualisere næringspolitikk med geopolitisk motivasjon som et økonomisk virkemiddel. Forståelsen av økonomisk statshåndverk som «utadrettet» bør revideres i lys av den teknologiske utviklingen. Flere inngangsportaler som følge av økt (digital) sammenkobling kan dessuten øke muligheten til å tilegne seg sensitiv/beskyttet teknologi, programvare, patenter og andre immaterielle rettigheter, for eksempel gjennom teknologityveri og omgåelse av eksportkontroll.

Tilrettelegge for (skjult) sabotasje	Økt potensial spesielt for å utnytte økonomisk aktivitet til å legge til rette for operasjoner i cyberdomenet blant annet pga. mer kompliserte og sammenkoblede systemer, økt automatisering av arbeidsoppgaver og økt behov for tjenesteutsetting. Samtidig fremstår terskelen for å utføre sabotasje ved bruk av cybervirkemidler som høy med potensielt store, negative konsekvenser for avsenderstaten og involverte kommersielle aktører.
Etterretningsvirksomhet gjennom økonomisk aktivitet og datainnhenting (Panoptikon)	Virkemidlene er de samme, men mulighetene for overvåking og innhenting av informasjon og data øker betydelig. Det økte potensialet kommer både av mer sammenkoblede nettverk og økt generering av data.
Øke avhengighet til knutepunkt	Økt potensial, i hovedsak for store økonomier, til å utnytte sentralitet i nettverk for global produksjon, distribusjon og salg av varer og tjenester. Årsaker til dette er blant annet økt markedskonsentrasjon, muligheter til å oppnå en monopolistposisjon innen global forsyning av teknologisk viktige ressurser, innsatsfaktorer og kompetanse (som sjeldne jordarter eller kompetanse på hvordan 6G-nettet fungerer). Den teknologiske utviklingen påvirker hvilke økonomiske virkemidler en har tilgjengelig. Noter særlig at standardsetting og næringspolitikk med geopolitisk motivasjon er relevante, men tidligere lite vektlagte virkemidler.

Nye eller økte avhengigheter

De fleste økonomier er avhengige av flere typer ressurser utenfra som råvarer, halvfabrikata, komponenter, ferdigvarer, kapital, teknologi, immaterielle rettigheter, arbeidskraft og kompetanse. Muligheten til å (gi løfter om å) øke tilførselen av ressurser eller (true med å) redusere tilførselen av ressurser åpner opp for maktbruk. Den teknologiske utviklingen kan bidra til å styrke enkelte staters muligheter til å utnytte mottakerlandets avhengighet til ressurser for å utøve makt. Årsaker til dette kan både være kompetansemangel, økt konkurranse om knappe ressurser, innsatsfaktorer som halvleder-teknologi og sjeldne metaller, økt markedskonsentrasjon med færre alternative leverandører samt økt (digital) sammenkobling. Slike avhengigheter kan utnyttes av enkelte stater til (fordekt) å sabotere og undergrave systemer. For eksempel kan selskaper i avsenderlandet potensielt gi beskjed om at vedlikeholdstjenester, av ulike årsaker, ikke kan bli utført før om seks måneder. Denne formen for maktutøvelse kan foregå fordekt og være vanskelig å attribuere til en avsenderstat, siden det tilsynelatende er organisatoriske forhold hos en leverandør som forårsaker forstyrrelsene.

Den teknologiske utviklingen kan også øke mulighetene for, og effekten av, å utnytte eierskap eller underleverandører til å utøve makt gjennom sabotasje av infrastruktur. Dette fordi stadig

større deler av samfunnet avhenger av tjenester og fordi systemer i stadig større grad blir sammenkoblet. Videre øker mulighetene for å utføre sabotasje fra utlandet, hvor eierskap er utenfor mottakerstatens kontroll, mens det tidligere i større grad var nødvendig med tilgang i mottakerlandet for å kunne ramme dette landets infrastruktur. Den teknologiske utviklingen kan derfor også gi styrkede muligheter til å utnytte eierskapskontroll til å sabotere og undergrave systemer og infrastruktur. Det kan også gi mulighet til å komme i posisjon til å utføre sabotasje med ikke-økonomiske virkemidler som cybervirkemidler. Fordekt sabotasje gjennom forstyrrelser i tilførselen av ressurser, som forsinkelse i vedlikeholdstjenester, fremstår imidlertid som en mer aktuell handlingsmåte dersom den er tilgjengelig. Dette fordi slike handlinger er krevende å attribuere og dermed kan redusere de negative konsekvensene for avsenderstaten.

Norske avhengigheter til kompetanse, råvarer, komponenter og høyteknologiske produkter kan i prinsippet utnyttes av en avsenderstat på måter som er sikkerhetstruende. Dette kan gjøres gjennom å forstyrre eller strupe forsyningen for å legge press på og/eller sabotere viktige eller kritiske samfunnsfunksjoner, eventuelt også forsvarsfunksjoner. Det kan potensielt true «de øverste statsorganers virksomhet, sikkerhet og handlefrihet». Det kan potensielt også utgjøre en trussel mot «økonomisk stabilitet og handlefrihet» og «samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet» dersom vedlikehold eller oppdateringer av systemer og infrastruktur, som understøtter finansielle transaksjoner og andre samfunnsfunksjoner, bortfaller over en periode. Sikkerhetsinteressen «forsvar, sikkerhet og beredskap» kan potensielt også bli truet av avhengighet av utenlandsk kompetanse på nye teknologier dersom Norge blir sårbart overfor eventuelle brudd i forsyningslinjene av tjenester som er kritiske for Forsvaret.

Data som strategisk ressurs

Innen akkumulering av makt – det vil si tilrettelegging for fremtidig økonomisk eller annen maktbruk – vil den teknologiske utviklingen særlig styrke mulighetene til å utnytte økonomisk aktivitet til å hente inn informasjon og data. Som følge av at data blir viktigere, blir også tilgang og eierskap til data viktigere. Det kan blant annet resultere i at investeringer og oppkjøp av selskaper med god tilgang til data blir en stadig mer aktuell måte å sikre seg kontroll over dataene selskapene besitter. I tillegg kan det være aktuelt å promotere produkter og tjenester til selskaper og forbrukere fordi det bidrar til datainnsamling.

Dersom fremmede stater får tilgang til data gjennom økonomisk aktivitet, kan det utgjøre en trussel mot flere av Norges nasjonale sikkerhetsinteresser. For det første kan norsk suverenitet og «de øverste statsorganers virksomhet, sikkerhet og handlefrihet» potensielt bli truet dersom data om det norske samfunnet, norsk økonomi og/eller norske innbyggere utnyttes til å forsøke å påvirke (sær)interesser og oppfatninger i Norge. Det er viktig at både norske myndigheter, det norske næringslivet og den norske befolkningen er bevisst på hvordan økonomiske transaksjoner kan være en måte å komme i posisjon til å utføre påvirkningsoperasjoner i fremtiden. Dette kan være seg enten ved at de økonomiske transaksjonene i realiteten er motivert av slike strategiske hensyn eller ved at transaksjonene er kommersielt motivert, men likevel åpner muligheter som kan utnyttes på et senere tidspunkt.

For det andre kan mulighetene til å utføre etterretningsvirksomhet gjennom økonomisk aktivitet i Norge og å trekke ut data fra nettverk norske aktører er en del av[234] øke med den teknologiske utviklingen. Slike handlinger kan både utgjøre en trussel mot Norges nasjonale sikkerhetsinteresser knyttet til «de øverste statsorganers virksomhet, sikkerhet og handlefrihet», «forsvar, sikkerhet og beredskap» og «forholdet til andre stater og internasjonale organisasjoner». Sikkerhetsloven skal i utgangspunktet beskytte sensitive og skjermingsverdige data. Økte muligheter for datainnsamling kombinert med avanserte analyseverktøy som kunstig intelligens, som styrker evnen til å trekke ut innsikt fra dataene, kan imidlertid medføre at data som ikke dekkes av sikkerhetsloven likevel kan ha strategisk verdi for utenlandske etterretningsorganisasjoner.[235]

For det tredje kan data fra offentlig og private virksomheter i Norge dessuten være viktig for å styrke bedrifter i avsenderlandets evner til å bedrive produktutvikling og -forbedring og derigjennom hevde seg i global konkurranse. Hvis slike data blir benyttet av fremmede stater utenfor NATO-alliansen til å utvikle militær- eller flerbruksteknologi, som kunstig intelligens, vil det kunne utgjøre en trussel mot sikkerhetsinteressene «forsvar, sikkerhet og beredskap» og «forholdet til andre stater og internasjonale organisasjoner».

For det fjerde kan både økonomiske og ikke-økonomiske data spille en viktig rolle for avsenderstaten i forbindelse med å utforme mer effektiv bruk av økonomiske virkemidler mot Norge. Dette inkluderer å identifisere sårbarheter dens økonomiske statshåndverk kan rettes inn mot. Slik bruk av data kan i prinsippet utgjøre en trussel mot alle de fem nasjonale sikkerhetsinteressene i sikkerhetsloven ved at det kan styrke avsenderstatens muligheter til å utføre målrettet påvirkning og sabotasje.

Rivaliseringen mellom USA og Kina

I den tradisjonelle litteraturen om økonomisk statshåndverk er det kun fokus på hvordan stater bruker økonomiske virkemidler for å oppnå utenrikspolitiske, strategiske mål slik som Baldwin.[236] Her faller altså all politikk og handlingsmåter som har fokus på å styrke økonomiens stilling og konkurransekraft utenfor. Slik politikk og handlingsmåter kan selvsagt også bli omtalt som statshåndverk, men i studiet av internasjonal politikk avgrenses som regel begrepet om økonomisk statshåndverk til staters atferd som er rettet mot å oppnå politisk innflytelse eller autonomi internasjonalt.

Noen bidrag i litteraturen har dog begynt å anerkjenne at det kan være vanskelig å skille politikk som er rettet mot styrking av egen økonomisk verdiskaping, konkurransekraft, sysselsetting og lignende fra politikk som er rettet mot strategiske mål i internasjonal politikk. En sterk økonomi

[234] Denne handlingsmåten er kalt «panoptikon» av Farrell og Newman, 2019.

[235] I den forbindelse fremheves det at det kan være krevende å vite hvilke data som har verdi, og hvordan de kan bli brukt i dag og i fremtiden. For eksempel nevner Matz et al. hvordan lokasjonsdata potensielt kan være tett knyttet til helsedata. Lokasjonsdata burde dermed beskyttes selv om slike data i utgangspunktet ikke fremstår som like sensitive som helsedata. Matz et al., 2020

[236] Baldwin, 1985

vil igjen kunne benyttes til å oppnå mer makt og innflytelse internasjonalt. Rivaliseringen mellom USA og Kina og konkurransen innenfor forskning, utvikling og innovasjon vestlige land (inklusive USAs allierte i Øst-Asia) opplever fra fremvoksende økonomier fører til en mer multipolar verden. Dette bidrar til at næringspolitiske virkemidler for å styrke materielle og militære kapabiliteter blir viktigere fremover. Slik bruk av økonomiske virkemidler gir stater muligheter til å beskytte egen teknologi gjennom bruk av eksklusive teknologinettverk mellom allierte. I tillegg kan ressurstilgangen til geopolitiske konkurrenter forstyrres.

Rivaliseringen mellom USA og Kina vil høyst sannsynlig ha konsekvenser for Norge. Norge er medlem av NATO-alliansen og USA er Norges fremste sikkerhetsgarantist. Hvis Beckley har rett i sin analyse, vil USA legge press på sine allierte til å «velge side, overtale dem til å omdirigere forsyningskjeder og omfavne [det amerikanske] økosystemet av teknologier og standarder».[237] Det er mulig rivaliseringen mellom Kina og USA blir mindre dramatisk enn dette, men Norge må uansett forvente å bli trukket mer med i politiske og økonomiske forsøk på å demme opp for den kinesiske økonomiske og teknologiske fremgangen. NATOs nye strategiske konsept nevner Kina som en utfordrer for første gang:

> «Folkerepublikken Kinas (PRC) uttalte ambisjoner og tvangspolitikk utfordrer våre interesser, sikkerhet og verdier».[238]

NATOs strategiske konsept peker på at Kinas politiske, økonomiske og militære virkemidler har globalt nedslag gjennom ødeleggende cyber- og påvirkningsoperasjoner, mål om å kontrollere teknologiske og industrielle sektorer, å skape avhengigheter, forsøk på å underminere den regelbaserte orden og utdyping av det strategiske partnerskapet med Russland. Dette danner grunnlag for hvordan Kina utfordrer alliansens interesser, sikkerhet og verdier. NATO argumenterer for at fremvoksende og disruptive teknologier «endrer konflikters karakter, får større strategisk betydning og blir nøkkelarenaer for global konkurranse».[239] Derfor vil NATO promotere innovasjon og beskytte «våre innovasjonsøkosystemer».

For å ivareta norske nasjonale sikkerhetsinteresser særlig knyttet til «forholdet til andre stater og internasjonale organisasjoner», kan det derfor bli viktigere fremover at Norge beskytter norsk (og alliert) teknologi og data samt bidrar i satsningen på norsk (og alliert) næringsvirksomhet innen viktige høyteknologiske industrier. I den forbindelse virker det også sannsynlig at det vil bli økt press på norske virksomheter til å bli mindre avhengige av kinesiske leverandører og verdikjeder. Videre er det ønskelig å redusere Kinas tilgang til ressurser, komponenter og kompetanse som styrker og fremmer kinesisk teknologiutvikling.

[237] Beckley, 2022

[238] NATO, 2022

[239] NATO, 2022

Forhold som kan gjøre bruken av økonomiske virkemidler mer utfordrende

Mange forhold tilsier at staters – særlig stormakters – muligheter til å utføre økonomisk statshåndverk øker i takt med den teknologiske utviklingen (Tabell 4.2). Likevel er det noen forhold som også kan utfordre bruken av økonomiske virkemidler:

For det første fordrer økonomisk statshåndverk en (sterk) grad av statlig kontroll over kommersielle aktører. For eksempel vil både informasjons- og datainnsamling, tilrettelegging for påvirkningsoperasjoner og forsøk på forstyrrelser og sabotasje gjennom økonomisk statshåndverk kreve at kommersielle aktører samarbeider med staten. Dette kan potensielt medføre (store) kostnader både økonomisk og omdømmemessig. I hvilken grad ulike stater vil lykkes med å påvirke og kontrollere økonomiske aktører til å tjene statens formål, er et tema innen økonomisk statshåndverk hvor det er behov for mer forskning.[240] Temaet bør også studeres nærmere i lys av den teknologiske utviklingen. For eksempel kan det være relevant å undersøke nærmere hvordan endringer i så som organisasjonsformer, markedskonsentrasjon og graden av internasjonalisering kan påvirke staters muligheter til å utøve kontroll over kommersielle aktører.

For det andre kjennetegnes den teknologiske utviklingen av at produkter, tjenester og systemer blir mer komplekse. Dette er blant annet som følge av at kunstig intelligens i økende grad blir anvendt til drift, vedlikehold og oppgaveløsning. Verdikjedene blir også mer uoversiktlige og det knyttes høyere usikkerhet til verdien av tjenester for ulike brukere. Den økte kompleksiteten kan ikke bare bidra til å gjøre mottakerland mer sårbare, men også gjøre det mer utfordrende for avsenderstater å innrette sitt økonomiske statshåndverk.

For det tredje kan ny teknologi og økt grad av tjenesteutsetting også bidra til å redusere sårbarheter. Arbeidsdeling, spesialisering og fokus på kjernevirksomheten bidrar med en mer effektiv utnyttelse av kompetanse og kapital. Å overlate oppgaver til underleverandører, i inn- og utland, kan derfor gjøre at bedrifter og offentlige virksomheter utfører egne hovedarbeidsoppgaver bedre. Samtidig kan tjenester og varer de mottar være av høyere kvalitet og/eller til en lavere kostnad enn de ville fått til selv. Det er nemlig skalautbytte i spesialisering og arbeidsdeling. Slike underleverandører kan spesialisere seg på å levere sikre systemer, varer og tjenester. De har også insentiver til å unngå å bli leddet som skaper sikkerhetsutfordringer for næringslivet og det offentlige i mottakerlandene. Det er derfor ikke sikkert at forsøk på å bygge kompetanse internt i egen virksomhet vil redusere sårbarhetene i en økonomi der teknologien blir mer og mer kompleks.

Waage og Lindgren vurderer samlet sett at mulighetene for å utføre økonomisk statshåndverk blir styrket av den teknologiske utviklingen og vil ha potensielle negative konsekvenser for norsk sikkerhet.[241] Likevel gjenstår det et (stort) behov for videre forskning på temaet for å få et bedre grep om nettoeffekten både totalt, innenfor hver handlingsmåte av økonomisk

[240] Se også: Norris, 2016; Norris, 2021

[241] Waage, Lindgren, 2022

statshåndverk og i kombinasjon med ikke-økonomiske virkemidler som del av staters sammensatte virkemiddelbruk.

4.3.4 Vurdering

Dette kapitlet vil drøfte utviklingstrekk innen staters (særlig Kinas og Russlands) bruk av økonomiske virkemidler for å oppnå utenrikspolitiske, strategiske mål – økonomisk statshåndverk – som kan ha særlig betydning for nasjonal sikkerhet i et 2030-perspektiv. De viktigste punktene sammenfattes, og det redegjøres for områder hvor det er behov for ytterligere innsats for å sette norske myndigheter og norsk næringsliv bedre i stand til å forebygge og håndtere potensielt sikkerhetstruende økonomisk aktivitet.

Kina er verdens nest største økonomi etter USA og verdens største økonomi målt i kjøpekraftsparitet.[242] Landets tosifrede økonomiske vekst gjennom flere tiår og den kinesiske statsledelsens aktive bruk av økonomiske virkemidler for å oppnå utenrikspolitiske, strategiske mål har spesielt bidratt til å sette søkelys på hvordan (lønnsom) økonomisk aktivitet kan ha negative konsekvenser for mottakerlands sikkerhet. Kina er også en av Norges viktigste handelspartnere. Likevel er Norge per dags dato mindre avhengig av økonomisk interaksjon med Kina enn flere andre land, særlig i Asia og Oseania. Kina har likevel potensial til å utøve makt mot Norge ved å ta i bruk økonomiske virkemidler i et 2030-perspektiv, slik Norge allerede opplevde etter Nobelprisutdelingen i 2010. Russlands kapabiliteter til å gjøre det samme er imidlertid begrenset, siden den økonomiske interaksjonen mellom Russland og Norge er relativt liten. Russland er heller ikke i nærheten av å være en like viktig økonomi globalt som Kina. Både Russland og Kina har imidlertid potensial til å akkumulere makt gjennom bruken av økonomiske virkemidler mot Norge. Dette kan skje gjennom forsøk på å skaffe seg innflytelse ved å forme særinteresser og oppfatninger og forsøk på å få tilgang til teknologi, ressurser, ekspertise, informasjon og data av strategisk og militær verdi. Dessuten kan økonomiske virkemidler potensielt tas i bruk for å etablere inngangsportaler for å utføre sabotasjeaktiviteter, enten gjennom eierskapskontroll eller gjennom bruk av andre typer virkemidler (som cyberoperasjoner, kapittel 4.1).

Den teknologiske utviklingen vil høyst sannsynlig endre mulighetsrommet for økonomisk statshåndverk, men dette er i liten grad studert i eksisterende litteratur. Det vil derfor kreve samarbeid på tvers av tradisjonelle fagfelt som (internasjonal) økonomi, sikkerhetsstudier og teknologiske disipliner for å forstå mulige implikasjoner for Norge. Fra forstudien til Waage og Lindgren (2022) fremheves det at den teknologiske utviklingen særlig har potensial til å skape nye eller økte avhengigheter i det norske næringslivet til utenlandsk kompetanse, råvarer, produkter, komponenter og tjenester som systemdrifts- og vedlikeholdsstøtte.[243] Den kan også

[242] Kjøpekraftsparitet (kkp eller purchasing power parity, ppp) er den verdien av en valutakurs som svarer til forholdet mellom to pengeenheters innenlandske kjøpekraft. To valutaer er i paritet hvis man fr det samme beløpet kan kjøpe de samme mengden varer og tjenester i de to landene. Kilde: Store norske leksikon

[243] Waage, Lindgren, 2022

øke den strategiske betydningen av data produsert av det norske næringslivet, norsk offentlig sektor og norske forbrukere. I tillegg driver spesielt teknologirivaliseringen mellom USA og Kina frem en ny form for økonomisk statshåndverk hvor beskyttelse og promotering av egen teknologi – potensielt på bekostning av globale, kostnadseffektive verdikjeder – får økt oppmerksomhet sammenliknet med tidligere. For Norges del kan det bety økte forventninger til beskyttelse av norsk (og alliert) teknologi og data samt bidrag i satsningen på norsk (og alliert) næringsvirksomhet innen viktige høyteknologiske industrier.

Ikke alle former for økonomisk statshåndverk er sikkerhetstruende. Handlingsmåter av økonomisk statshåndverk som i prinsippet kan utgjøre sikkerhetstruende virksomhet er ikke nødvendigvis det i praksis, med mindre omfanget av den økonomiske aktiviteten er omfattende nok. Hvilke former for økonomisk statshåndverk kan skape størst utfordringer for nasjonal sikkerhet? Økonomisk statshåndverk i form av manipulering av markedstilgang og forsøk på å forme særinteresser og oppfatninger blant næringsliv, eliter og befolkninger får mest oppmerksomhet i akademisk litteratur. Dette er nok likevel de handlingsmåtene som relativt sett har minst potensial til å true norsk sikkerhet frem mot 2030. Manipulering av ressurstilgang kan potensielt utgjøre en større trussel, men mottakerland kan tilpasse seg og redusere negative virkninger over tid.[244] I en pågående konflikt kan imidlertid konsekvensene av å strupe tilgang til viktige/kritiske ressurser være alvorlige.[245] Sett i lys av den teknologiske utviklingen frem mot 2030, fremstår det likevel som at det særlig er muligheter for å utnytte økonomiske virkemidler for å posisjonere seg for fremtidig etterretningsaktivitet, og eventuelt sabotasjevirksomhet, som har størst potensial til å true norsk sikkerhet på mellomlang til lang sikt. Mens investeringer og oppkjøp er sentrale virkemidler for å oppnå posisjonering, er det også viktig å være klar over at andre virkemidler kan tjene samme formål så som salg av systemer, produkter, komponenter, reservedeler og drifts- og vedlikeholdstjenester.

En av de aller største utfordringene, knyttet til å forebygge og håndtere potensielt sikkerhetstruende økonomisk aktivitet, er avveiingen mellom behovet for åpne og forutsigbare rammer for internasjonal økonomisk aktivitet og behovet for å hindre trusselaktører fra å kunne utnytte lønnsomme økonomiske transaksjoner og økonomisk (gjensidig) avhengighet. Norsk næringsliv og norsk offentlig sektor er, og forblir, både avhengig av ressurser, varer, tjenester, teknologi, kompetanse, ekspertise og kapital fra utlandet og muligheter for selv å kunne handle

[244] Studier viser for eksempel til at Kinas eksportstopp av REE til Japan i 2010 ledet til at Japan og andre vestlige land investerte i REE-produksjon andre steder og slik reduserte avhengigheten til import fra Kina. Se for eksempel: Wilson, 2018; Vekasi, 2019

[245] Det diskuteres også i litteraturen hvor omsettbar økonomisk makt er. Ross mener for eksempel at Kina i liten grad klarer å omsette sin økonomiske størrelse til å endre de militære alliansene i Øst-Asia i sin favør (Ross, 2019). Det fremstår for oss som en uhensiktsmessig test for å forstå hvorvidt økonomiske virkemidler er nyttige for avsenderstaten. Hvilke virkemidler fra andre domener ville kunne endret de militære alliansene i Øst-Asia når Kinas fremvekst blir sett på som en av de større sikkerhetsmessige truslene for landene som befinner seg i Kinas nærområder? Økonomiske virkemidler må i stedet sees i lys av de potensielle kostnadene og gevinstene av slike virkemidler opp mot hvilke andre virkemidler landene har til rådighet (Baldwin, 1985).

og investere i utlandet. Med stadig mer teknologisk avanserte systemer og komplekse, moderne verdikjeder både internt i Norge og transnasjonalt, fremstår det imidlertid krevende å utforme lovverk som avgrenser seg til kun å regulere økonomisk aktivitet som potensielt kan være sikkerhetstruende og samtidig være dekkende nok. Det er likevel aktuelt å styrke forståelsen av om det er særskilte sektorer, teknologier eller virksomheter i Norge som spesielt er utsatt. Dette inkluderer virksomheter som i utgangspunktet ikke er dekket av sikkerhetsloven.

Frem mot 2030 vil det bli viktig for Norge, som for andre vestlige økonomier, å arbeide videre med å forstå, forebygge og håndtere potensielt sikkerhetstruende økonomisk aktivitet. Sikkerhetsloven skal forebygge økonomisk aktivitet som kan utgjøre en trussel mot norsk sikkerhet. Den teknologiske utviklingen, med økt kompleksitet og sammenkobling av systemer og infrastrukturer, bidrar imidlertid til å gjøre det mer krevende å regulere og forebygge potensielt sikkerhetstruende økonomisk aktivitet. Det blir for eksempel vanskeligere å identifisere og ha kontroll over hvilke selskaper, leverandører, data, m.m. som kan utnyttes av en avsenderstat til formål som truer en eller flere av Norges nasjonale sikkerhetsinteresser. Virkemidlene som stater potensielt kan søke å utnytte i sitt økonomiske statshåndverk utvides også fra «tradisjonelle» investeringer og oppkjøp til drifts- og vedlikeholdstjenester, reservedeler, programvareoppdateringer og lignende. Det er i tillegg noen former for potensielt sikkerhetstruende bruk av økonomiske virkemidler som ikke lar seg forebygge med hjemmel i Sikkerhetsloven slik som påvirkningsforsøk ved å skape og forme særinteresser og oppfatninger. Sikkerhetsloven egner seg heller ikke til å forebygge potensielle forsøk på å presse eller straffe norsk politikk og beslutningstaking som følge av importrestriksjoner eller andre former for manipulering av bilaterale handelsstrømmer. Det imidlertid uklart når disse formene for økonomisk statshåndverk er omfattende eller alvorlig nok til å true nasjonale sikkerhetsinteresser (og bør søkes regulert). Det er et behov for å definere bedre med hvilket omfang og på hvilke områder disse formene for økonomisk statshåndverk potensielt kan true norsk sikkerhet frem mot 2030.

5 Betydning for nasjonale sikkerhetsinteresser

Denne rapporten har beskrevet en del utviklingstrekk mot 2030 som kan påvirke nasjonale sikkerhetsinteresser innenfor temaene teknologi, klima og sammensatte virkemidler. Rapporten danner et bredt kunnskapsgrunnlag for NSMs arbeid med Sikkerhetsfaglig råd. Dette kapitlet vil dermed ikke gi konkrete anbefalinger, men vil sammenstille viktige perspektiver av betydning for Norges nasjonale sikkerhetsinteresser.

5.1 Teknologibruk, verdiskapning og 5G

Kommersielle behov og utsikter i samfunnet styrer mye av teknologiutviklingen. Dette betyr at det i enda større grad enn tidligere vil være kommersielle muligheter som styrer hvilke teknologier som vil bli videreutviklet. *Hvis norske myndigheter ikke signaliserer tydelig nok hva behovene er og legger til rette for et stort nok «kommersielt marked», så kan det være at viktige teknologimuligheter ikke blir implementert av de kommersielle aktørene*. I et slikt tilfelle kan det bli mye dyrere og ta lengre tid for myndigheter og offentlige etater å få implementert nødvendig funksjonalitet som er viktig for beskyttelse av nasjonale sikkerhetsinteresser.

Fremtidens kommunikasjonsnettverk (5G), med tilstøtende infrastrukturer, vil ikke kun utnyttes for mobiltelefoni. Det vil også danne basis for alle eller de aller fleste kommunikasjonstjenester som blir levert av de store aktørene. 5G har dermed stor betydning for våre nasjonale sikkerhetsinteresser frem mot 2030, og spesielt signalering av kommersielle behov innen 5G til ekomtilbyderne vurderes som viktig. 5G vil bestå av mye programvare som kjøres som virtuelle prosesser i datasentre. Dette er til dels samme teknologiutvikling som står bak veksten innen skytjenester og datasentra. Det vil si at *5G vil få andre og nye sårbarheter sammenliknet med tidligere generasjoner mobiltelefoni. Disse to forholdene til sammen betyr at sikkerhetsmyndighetene må ha spesielt stort fokus på 5G-infrastrukturer fremover*.

Den økende avhengighet av private skyleverandører for norsk verdiskaping og sikkerhet vil handle om mer enn teknologi. Det vil også handle om statshåndverk og nasjonale sikkerhetsinteresser der forskjellige hensyn må balanseres opp mot hverandre. Nasjonalt bør vi blant annet ha et forhold til den makten store amerikanske skyleverandører vil kunne få som (ene)leverandører til mange av våre grunnleggende nasjonale funksjoner.

En egenskap med moderne verdiskapning er at virksomheter i mindre grad kan oppnå suksess alene, og det er derfor ofte behov for utstrakt og dynamisk samarbeid. Sikkerhetsarbeidet må ta hensyn til dette samarbeidsbehovet og dette øker den organisatoriske kompleksiteten. Data og kompetanse kan sees på som sjeldne ressurser der forskjellige nasjoner har forskjellig tilnærminger rundt tilgang og bruk av data. Dette kan skape store forskjeller i utnyttelse av teknologi og utvikling av kompetanse. *Over tid vil potensielt andre nasjoners overlegne utnyttelse av og tilgang på data negativt kunne påvirke norske nasjonale sikkerhetsinteresser gjennom blant annet bedre situasjonsforståelse og bedre datadrevne beslutninger*.

5.2 Kvanteteknologi

De siste årene har det vært en betydelig framgang i evnen til å kunne utnytte kvanteteknologi, og NATO forventer at anvendbare produkter vil kunne gi operativ nytte om 5-15 år. Dette er innenfor levetiden til de militære systemene vi har i dag eller de vi er i ferd med å anskaffe. Til tross for store usikkerheter, antas det at utviklingen vil kunne medføre store endringer i ytelse for militære og sivile systemer innen autonomi (posisjonering, navigasjon og timing (PNT)), sensorer for etterretning, overvåkning og målfatning, kommunikasjon/krypto og dataprosessering (kvantedatamaskiner). For enkelte kapabiliteter og kapasiteter vil endringen kunne bli disruptiv både for oss og våre motstandere. Dette vil således kunne ha stor betydning for norske nasjonale sikkerhetsinteresser.

Det brukes internasjonalt store ressurser innen utviklingen av kvanteteknologi, mens satsingen i Norge er liten. *Norge bør bygge kompetanse slik at nasjonen som et minimum kan bidra til at både Forsvarets og sivilsamfunnets sentrale kapabiliteter og kapasiteter utvikles basert på tilstrekkelig informasjon om utviklingen innen kvanteteknologi, både hos allierte og våre motstandere.*

5.3 Romvirksomhet

Det foregår en rivende utvikling innen romvirksomhet. Stadig bedre tjenester utvikles innen blant annet kommunikasjon, posisjonering, navigasjon, tidsangivelse, jordobservasjon og etterretning. Den delen av romsystemene som er lettest tilgjengelig, og følgelig mest utsatt for trusler, er bakkesegmentet. Likevel, hvis for eksempel en satellitt blir utsatt for en cyberoperasjon som får effekt vil det kunne være krevende eller umulig å gjenvinne kontrollen over satellitten. Ved en fiendtlig overtagelse av satellitten, vil denne i tillegg kunne tapes fullstendig ved at det for eksempel gis kommandoer som tømmer batteriene helt.

Militært tap av satellittkommunikasjon vil først og fremst føre til degradering av kommando og kontroll. I tillegg hindres distribusjon av etterretningsinformasjon, samt annen kommunikasjon utover direkte siktlinje. Sivilt vil tap av satellittkommunikasjon medføre at et vidt spekter av tjenester i blant annet samfunnskritiske funksjoner, forretningsdrift, underholdning og andre segmenter, som er en integrert del av forventede samfunnsfunksjoner, faller bort. Dette vil følgelig kunne få store, og til dels uoversiktlige, økonomiske og sikkerhetsmessige ringvirkninger. I tillegg blir det meget nøyaktige tidssignalet i GNSS mer og mer brukt til kontroll av forskjellige nettverk. Dette gjelder både for strømsystemer og finansielle tjenester. *Tap av rombaserte tjenester vil således kunne ha stor påvirkning på norske nasjonale sikkerhetsinteresser og utviklingen bør følges tett av sikkerhetsmyndighetene.*

5.4 Klima og energisikkerhet

Norge har gjennom Helsinki-deklarasjonen forpliktet seg til å samarbeide med de andre nordiske landene for å nå klimamålsetningene. Det er avgjørende at man får til en full overgang til og fornuftig bruk av de fornybare energibærerne i Norden for at klimamålene skal nås.

Framtidens energisystem med variable, fornybare energikilder vil kreve et digitalisert og automatisert energisystem.

Variable energikilder, økt ekstremvær, automatisering, transnasjonale avhengigheter og økt potensiale for cyberhendelser og kaskadefeil medfører at kompleksiteten i energisystemet og frekvensen av uønskede hendelser vil kunne øke betydelig. Det gir økt sårbarhet, utfordringer med pålitelighet og motstandsdyktighet i systemet og mulighet for hyppigere, langvarige strømbrudd over større områder i Norden. Disse utfordringene vil ha direkte, fysisk påvirkning på samfunnet, siden de kan føre til bortfall av funksjoner som er kritiske for drift av samfunnet slik som vannforsyning, helsetjenester, elektronisk kommunikasjon, betalingstjenester med mer. *Dette har store innvirkninger på samfunnssikkerhet, energisikkerhet og cybersikkerhet på et transnasjonalt nivå, ikke kun nasjonalt nivå, og vil medføre gjensidig avhengighet mellom oss og våre nordiske naboer. Energisystemene må derfor samhandle og koordineres på tvers av landegrensene, noe som krever et transnasjonalt samarbeid langt utover et fellesnordisk kraftmarked.*

5.5 Sammensatte trusler

I lengre tid har man sett at fremmede stater benytter sammensatte trusler for å oppnå sine strategiske målsetninger under terskelen for direkte væpnet konflikt.[246] Følgende drivere har vært viktige for fremveksten av sammensatte trusler:[247]

- økende økonomiske og politiske kostander ved anvendelse av konvensjonell maktbruk
- risiko for eskalering til kjernefysisk nivå
- en stadig tiltakende teknologisk utvikling

Bruk av sammensatte trusler er derfor både en strategisk mulighet og en strategisk nødvendighet. Muligheten oppstår som følge av økte gjensidige avhengigheter mellom ulike samfunnssektorer, mens nødvendigheten oppstår som følge av en innstramming av statlig handlefrihet og en vegring mot å ta høy økonomisk, diplomatisk eller militær risiko.[248] Fremtidig utvikling knyttet til sammensatte trusler må derfor sees i lys av disse forholdene. Samtidig kan bruk av militærmakt øke handlingsrommet for annen, ikke-militær virkemiddelbruk.

Generelt kan man si at *sammensatt virkemiddelbruk kan skape sårbarheter, forsterke effekten av virkemiddelbruken eller legitimere bruk av andre virkemidler*.[249] I denne rapporten har vi sett nærmere på cyberoperasjoner, påvirkning i informasjonsmiljøet og økonomisk virkemiddelbruk

[246] Beadle et al., 2019

[247] Diesen, 2018

[248] Palmer, 2015

[249] Waage et al., 2021

fordi Norge, som en nasjon med åpen økonomi og høy grad av digitalisering, kan være sårbar overfor fremmede staters bruk av slike virkemidler.

5.5.1 **Cyberoperasjoner**

Offensive cyberoperasjoner med etterretningsformål gjennomføres for å oppnå uautorisert tilgang til informasjon. Offensive cyberoperasjoner med effektformål vil gjennomføres for å skape tilsiktede effekter i en motparts IKT-systemer eller enheter som kontrolleres eller brukes av motpartens IKT-systemer. Felles for de avanserte offensive cyberoperasjonene er at de krever mye ressurser, kompetanse, etterretningsstøtte og forberedelsestid. Planlegging, ledelse og utvikling av offensive cyberoperasjoner, som skal være skjulte i lang tid, krever spisskompetanse innenfor mange ulike fagdisipliner. Det vil ikke være unormalt at det kreves flere årsverk fra planlegging til iverksettelse av en cyberoperasjon. Ressursbruken, med personellinnsats i kombinasjon med etterretningsstøtte og eventuelle anskaffelser av infrastruktur eller spesialutstyr, tilsier at dette er aktiviteter hovedsakelig forbeholdt stater. Samtidig finnes enkle og langt mindre ressurskrevende teknikker ikke-statlige aktører kan anvende også for effekt, som tjenestenekt eller nettsidevandalisme. De kan også ha vesentlige effekter på datasystemer og det som beror på dem, men rent teknisk vil de som regel være lite destruktive og med begrenset varighet. Til gjengjeld er de ofte veldig synlige og får gjerne uforholdsmessig stor oppmerksomhet i media og samfunnet forøvrig. Disse egenskapene antar man vil holde seg frem mot 2030, og *aspekter fra offensive cyberoperasjoner må inkluderes i arbeidet med digital sikkerhet. Dette inkluderer blant annet norm- og sanksjonsarbeid, økt fokus på personellsikkerhet (en innsiders verdi økes for en trusselaktør), kontinuerlig utvikling av maskinlæringsteknikker for å detektere uønskede IKT-hendelser og kommunikasjons rundt egne cyberkapasiteter.*

Mulighetene for påvirkning ved bruk av cyberoperasjoner er mange og økende på grunn av den rollen det digitale rom har og får i moderne samfunn. Cyberoperasjoner vil benyttes til støtte for påvirkningskampanjer på tvers av konfliktspekteret. Når de inntreffer, vil den sentrale utfordringen i håndteringen av påvirkningseffekten være å forstå betydningen for egne verdier (et verdibasert forsvar).

5.5.2 Påvirkningsoperasjoner i informasjonsmiljøet

Påvirkningsoperasjoner kan være både åpne og skjulte og benytte en rekke ulike virkemidler og teknikker som har til hensikt å forlede, villede, øke konflikter, svekke tillit og skape tvil eller resignasjon. *Påvirkningsoperasjoner forventes å utgjøre en betydelig og økende utfordring spesielt på grunn av tre forhold:*

- *Økt geopolitisk rivalisering*
- *Økt misnøye og usikkerhet*
- *Teknologisk utvikling*

Påvirkningsoperasjoner er ikke noe nytt, men digitalisering, internett og sosiale medier har åpnet for nye muligheter og større effekt med liten eller ingen risiko. Påvirkningsoperasjoner kan pågå i lang tid uten at de blir oppdaget, og de kan potensielt skape betydelig skade det kan være vanskelig å rette opp når den først har skjedd (for eksempel på tilliten i samfunnet eller politisk handlingsrom).

Forskning på avskrekking av påvirkningsoperasjoner identifiserer noen tiltak for nektelse (denial) gjennom motstandsdyktighet (resilience), avskrekkere (deterrents) og mottiltak (countermeasures)[250]. Avskrekking bør altså forstås som bredere enn å skape høy risiko for gjengjeldelse (punishment). Det bør også inkludere nektelsestiltak for å begrense påvirkningsaktørers tekniske og kognitive handlingsrom og mulighet for å skape ønskede effekter.

Forebygging og forsvar mot påvirkningsoperasjoner krever god og omforent situasjons- og sikkerhetspolitisk forståelse i alle sektorer, kunnskap om truslene, virkemidlene og aktørene, hvilken hensikt disse kan ha og hvilke effekter de sannsynligvis er ute etter å skape. Ikke minst krever det en nasjonal, tverrsektoriell evne til å kartlegge og analysere skjulte, illegitime metoder og hurtig koordinere og utføre eventuelle responstiltak, om nødvendig. Forskning tilsier «psykologisk inokulasjon» kan være en effektiv strategi for å redusere effekten av påvirkningsoperasjoner. Akkurat som vaksine reduserer effekten av et virus, kan «prebunking» redusere effekten av skadelige, falske narrativer.

Det kan argumenteres for et verdibasert forsvar mot fremmedstatlig påvirkning. Forsvarsoppgaven handler da om å identifisere verdiene Norge ønsker å beskytte (f.eks. styreform og politisk handlefrihet) og å tufte forståelsen for forsvarsoppgaven på den. Skade vil kunne inntreffe når fremmedstatlige påvirkningsaktiviteter har uønskede effekter på essensielle statssikkerhetsinteresser, og meningsfulle mottiltak må ha som formål å styrke evnen til å ivareta disse interessene.

På tross av økt oppmerksomhet, er det i Norge fortsatt uavklart hvem som har det overordnede ansvaret for å forebygge, oppdage, kartlegge, analysere og håndtere påvirkningsoperasjoner som rettes mot samfunnet i sin helhet, uavhengig av aktør, og under terskelen for det som er kriminelle handlinger.

5.5.3 Økonomisk virkemiddelbruk

I denne rapporten benyttes begrepet økonomisk statshåndverk som betegnelse på en stats bruk av økonomiske virkemidler for å oppnå utenrikspolitiske, strategiske mål. Globalisering av verdens økonomier, økt betydning av internasjonale finansmarkeder, digitalisering og fremvoksende økonomier – herunder spesielt Kinas økende sentralitet i verdensøkonomien – har transformert staters evne til å benytte økonomiske virkemidler for å fremme sine interesser i internasjonal politikk.

[250] Pamment, Agardh-Twetman, 2019

Frem mot 2030 har Kina potensiale til å utøve makt mot Norge ved å ta i bruk økonomiske virkemidler. Både Kina og Russland har potensiale til å akkumulere makt gjennom økonomisk statshåndverk mot Norge. Dette inkluderer forsøk på å få tilgang til teknologi, ressurser, ekspertise, informasjon og data av strategisk og militær verdi og/eller forsøk på å etablere inngangsportaler for å komme i posisjon til å utføre sabotasjeaktiviteter i fremtiden. *Sett i lys av den teknologiske utviklingen frem mot 2030, fremstår det som at særlig utnyttelse av økonomiske virkemidler for å posisjonere seg for fremtidig etterretningsaktivitet, og potensielt sabotasjevirksomhet, har størst potensiale for å true norsk sikkerhet på mellomlang til lang sikt.*

Fremover vil det bli viktig for Norge, som for andre likesinnede land, å arbeide videre med å forstå, forebygge og håndtere potensielt sikkerhetstruende økonomisk aktivitet. Den teknologiske utviklingen bidrar til å gjøre det vanskeligere å identifisere og ha kontroll over hvilke selskaper, leverandører, data, med mer som kan utnyttes av andre stater til formål som truer en eller flere av Norges nasjonale sikkerhetsinteresser. Virkemidlene som stater potensielt kan søke å utnytte i sitt økonomiske statshåndverk utvides også fra «tradisjonelle» investeringer og oppkjøp til drifts- og vedlikeholdstjenester, programvareoppdateringer og lignende. Norge bør dessuten forvente å bli trukket mer med i politiske og økonomiske forsøk på å demme opp for den kinesiske økonomiske og teknologiske fremgangen. Disse utfordringene må balanseres med behovet for å ivareta åpne og forutsigbare rammer for internasjonal økonomisk aktivitet. Dette er nødvendig for å gi norsk næringsliv og norsk offentlig sektor tilgang til ressurser, varer, tjenester, teknologi, kompetanse, ekspertise og kapital fra utlandet og muligheter for selv å kunne handle og investere i utlandet.

Referanser

- Abnormalt Blog, Hassold, C., *The Double-Edged Sword of ChatGPT: How Threat Actors Could Use It for Evil*, tilgjengelig fra: https://abnormalsecurity.com/blog/double-edged-sword-of-chatgpt (nettside sist oppdatert: 12.12.2022, besøkt: 18.04.2023)

- Advokatforeningen, Høringsuttalelser; *Endringer i straffeloven mv. – påvirkningsvirksomhet* (2021), https://www.advokatforeningen.no/aktuelt/horingsuttalelser/2021/august/endringer-i-straffeloven-mv.---pavirkningsvirksomhet/ (nettside sist oppdatert: 11.08.2021, besøkt: 19.04.2023)

- Anand, V., Chinese Concepts and Capabilities of Information Warfare, *Strategic Analysis*, 2006, 30 (4).

- archive.today, Higgins, E., *Russia's Bucha "Facts" Versus the Evidence*, tilgjengelig fra: https://archive.ph/W0D6M (nettside sist oppdatert: 04.04.2022, besøkt: 19.04.2023)

- Backes, O., Swab, A. (2019), *Cognitive Warfare - The Russian Threat to Election Integrity in the Baltic States*. Tilgjengelig fra: https://www.belfercenter.org/sites/default/files/2019-11/CognitiveWarfare.pdf

- Baldwin, D. A., *Economic Statecraft* (1985), Princeton, NJ: Princeton University Press.

- Bay, S., Fredheim, R., Haiduchyk, T., Dek, A. ((2022), *Social media manipulation 2021/2022 – assessing the ability of social media companies to combat platform manipulation*. Tilgjengelig fra: https://stratcomcoe.org/publications/social-media-manipulation-20212022-assessing-the-ability-of-social-media-companies-to-combat-platform-manipulation/242/

- BBC News, *What sanctions are being imposed on Russia over Ukraine invasion?*, tilgjengelig fra: https://www.bbc.com/news/world-europe-60125659 (nettside sist oppdatert: 30.09.2022, besøkt: 20.04.2023)

- Beadle, A. W., Diesen S., Nyhamar T., Bostad E. K. (2019), *Globale trender mot 2040 – et oppdatert fremtidsbilde* (19/00045). Tilgjengelig fra: https://www.ffi.no/publikasjoner/arkiv/globale-trender-mot-2040-et-oppdatert-fremtidsbilde

- Beckley, M., Enemies of My Enemy: How Fear of China Is Forging a New World Order, *Foreign Affairs*, 2022, 101 (2), s. 68-85

- Bentstuen O. I. (2022), *Trender innen IKT – relatert til militærmakt* (22/00544), Tilgjengelig fra: https://www.ffi.no/publikasjoner/arkiv/trender-innen-ikt-relatert-til-

militaermakt

- Bergaust, J. C., Skjei, F., Sellevåg, S. R. (2022), *Hva kan Norge lære av andre lands tilnærming til sammensatte trusler? – rapport til Forsvarskommisjonen*. Tilgjengelig fra: https://www.ffi.no/publikasjoner/arkiv/hva-kan-norge-laere-av-andre-lands-tilnaerming-til-sammensatte-trusler-rapport-til-forsvarskommisjonen

- Bergh, A. (2020), *Påvirkningsoperasjoner i sosiale medier - oversikt og utfordringer* (20/01694). Tilgjengelig fra: https://www.ffi.no/publikasjoner/arkiv/pavirkningsoperasjoner-i-sosiale-medier-oversikt-og-utfordringer

- Bergsjø, L. O., *Digitalt kappløp - en verdikamp*, Bergsjø, H., Friis, K. (red.), Digitalisering og internasjonal politikk (2022), Oslo: Universitetesforlaget (s. 103-116)

- Bernal, A., Carter, C., Singh, I., Cao, K., Madreperla, O. (2020), *Cognitive Warfare: An Attack on Truth and Thought*. Tilgjengelig fra: https://www.innovationhub-act.org/sites/default/files/2021-03/Cognitive%20Warfare.pdf

- Bērziņa-Čerenkova, U. A., Svetoka, S., Lucas, E., Klekere, E., Jerdén. B., Bohman, V. (2022), *China's Influence in the Nordic-Baltic Information Environment: Latvia and Sweden (executive summary)*. Tilgjengelig fra: https://stratcomcoe.org/publications/chinas-influence-in-the-nordic-baltic-information-environment-latvia-and-sweden-executive-summary/218

- Blackwill, R. D., Harris, J. M., *War by Other Means: Geoeconomics and Statecraft* (2016), Cambridge, MA: Harvard University Press

- Bradshaw, S., Bailey, H., Howard, P. N. (2020), *Industrialized Disinformation – 2020 Global Inventory of Organized Social Media Manipulation*. Tilgjengelig fra: https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/02/CyberTroop-Report20-Draft9.pdf

- Brandt, J., Schafer, B., Aghekyan, E., Wirtschafter, V., Danaditya, A. (2022), *WINNING THE WEB: How Beijing exploits search results to shape views of Xinjiang and COVID-19*. Tilgjengelig fra: https://www.brookings.edu/wp-content/uploads/2022/05/FP_20220525_china_seo_v2.pdf

- Bruynseels, K., Santoni de Sio, F., van den Hoven, J., Digital Twins in Health Care: Ethical Implications of an Emerging Engineering Paradigm, *Frontiers in Genetics*, 2018, **9** (31). Tilgjengelig fra: https://doi.org/10.3389%2Ffgene.2018.00031

- BUSINESS INSIDER, *Zelenskyy awards Amazon the Ukraine peace prize after AWS helped save its 'digital infrastructure'*, tilgjengelig fra: https://www.businessinsider.com/zelenskyy-amazon-ukraine-peace-prize-digital-war-support-aws-2022-7?r=US&IR=T (nettside sist oppdatert: 06.07.2022, besøkt: 18.04.2023)

- BuzzFeed News, Silverman, C., Mac, R., Dixit, P., *"I Have Blood On My Hands": A Whistleblower Says Facebook Ignored Global Political Manipulation*, tilgjengelig fra: https://www.buzzfeednews.com/article/craigsilverman/facebook-ignore-political-manipulation-whistleblower-memo (nettside sist oppdatert: 14.09.2020, besøkt: 19.09.2020)

- Cavanna, T. P., Coercion Unbound? China's Belt and Road Initiative i *The Uses and Abuses of Weaponized Interdependence*, Drezner, D. W., Farrell, H., Newman, A. L. (red.), 2021, Brookings Institution Press, Washington, s. 221-36

- Cherepanov, A., Lipovsky, R., *Blackenergy – What We Really Know About The Notorious Cyber Attacks*, Virus Bulletin Conference, 2016, Denver, CO, USA. Tilgjengelig fra: https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Cherepanov-Lipovsky.pdf

- Cherepanov, A., Miller, B., Slowik, J. Lee, R. M., Lipovsky, R., *Industroyer/Crashoverride: Zero Things Cool About A Threat Group Targeting The Power Grid* (presentation), Black Hat USA, 2017, Las Vegas, NV, USA. Tilgjengelig fra: https://www.blackhat.com/docs/us-17/wednesday/us-17-Lee-Industroyer-Crashoverride-Zero-Things-Cool-About-A-Threat-Group-Targeting-The-Power-Grid.pdf

- ChinaTalk, Baughman, M., Selling China's Story: How the Chinese Gov't Privatized Facebook Propaganda, tilgjengelig fra: https://chinatalk.substack.com/p/selling-chinas-story-how-the-chinese (nettside sist oppdatert: 08.11.2021, besøkt: 12.07.2022)

- Chiu, J., *China Unbound: A New World Disorder* (2021), Toronto, Ontario: House of Anansi Press Inc.

- Cisco Blogs, Developer, Chenetz, M. (2022), *Who Needs to Shift Left in Security, and Why*, tilgjengelig fra: https://blogs.cisco.com/developer/whoneedsshiftleftsecurity01 (nettside sist oppdatert: 10.06.2022, besøkt: 18.04.2023)

- Clarke, M., Sussex, M., Bisley. N. (red.), *The Belt and Road Initiative and the Future of Regional Order in the Indo-Pacific*, 2020, New York: Lexington Books

- CNBC, Sherman, A., *TikTok reveals detailed user numbers for the first time*, tilgjengelig fra: https://www.cnbc.com/2020/08/24/tiktok-reveals-us-global-user-growth-numbers-for-first-time.html (nettside sist oppdatert: 24.08.2020, besøkt: 07.02.2022)

- Cohen, B. J., *Currency Statecraft: Monetary Rivalry and Geopolitical Ambition* (2019), Chicago: University of Chicago Press

- Cohen, B. J., Sovereign Wealth Funds and National Security: The Great Tradeoff, *International Affairs*, 2009, 85(4), s. 713-31

- Cohen, B. J., The International Monetary System: Diffusion and Ambiguity, *International Affairs*, 2008, 84 (3), s. 455–70.

- Cristóbal, D. M., The current perspective on sharp power: China and Russia in the era of (dis)information, *Revista Electronica de Estudios Internacionales (REEI)*, 2021, 42, s. 6. Tilgjengelig fra: https://dialnet.unirioja.es/servlet/articulo?codigo=8202335

- Crowdstrike, CrowdStrike's work with the Democratic National Committee: Setting the record straight, tilgjengelig fra: https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/ (nettside sist oppdatert: 05.06.2020, besøkt: 18.04.2022)

- CSIS, *Russia in the Western Hemisphere: Assessing Putin's Malign Influence in Latin America and the Caribbean*, tilgjengelig fra: https://www.csis.org/analysis/russia-western-hemisphere-assessing-putins-malign-influence-latin-america-and-caribbean (nettside sist oppdatert: 20.07.2022, besøkt: 22.04.2023)

- CYBERSCOOP, Vicens, A. J., *Iranian steel facilities suffer apparent cyberattacks*, tilgjengelig fra: https://www.cyberscoop.com/iran-cyberattack-israel-hacktivist-steel-ics/ (nettside sist oppdatert: 28.06.2022, besøkt: 18.04.2023)

- Dagens Næringsliv, Kibar, O., *OPERASJON LAZAREV: Slår alarm om kartlegging av Norges kritiske infrastruktur*, tilgjengelig fra: https://www.dn.no/magasinet/dokumentar/spionasje/russland/etterretningstjenesten/operasjon-lazarev-slar-alarm-om-kartlegging-av-norges-kritiske-infrastruktur/2-1-1085420 (nettside sist oppdatert: 22.10.2021, besøkt: 20.04.2023)

- Darczewska, J., Żochowski, P. (2017), *Active Measures – Russia's key export*. Tilgjengelig fra: http://aei.pitt.edu/88535/1/pw_64_ang_active-measures_net_0.pdf

- Deloitte (2021), 5G Empowers the future of Electricity. Tilgjengelig fra: https://www2.deloitte.com/cn/en/pages/energy-and-resources/articles/5g-empowers-smart-power-and-promotes-innovation.html

- Deloitte (2021), *Tech Trends 2021*. Tilgjengelig fra: https://www2.deloitte.com/content/dam/insights/articles/6730_TT-Landing-page/DI_2021-Tech-Trends.pdf

- Deloitte, Parrot, A., Warshaw, L., *Industry 4.0 and the digital twin – Manufacturing meets its match*, tilgjengelig fra: https://www2.deloitte.com/us/en/insights/focus/industry-4-0/digital-twin-technology-smart-factory.html (nettside sist oppdatert: 12.05.2017, besøkt: 18.04.2023)

- Diesen S. (2022), *Fra teknologi til strategi og operasjoner – teknologiutviklingens påvirkning på militære styrker og bruker av militærmakt* (22/01682), s. 7-8. Tilgjengelig fra: https://www.ffi.no/publikasjoner/arkiv/fra-teknologi-til-strategi-og-operasjoner-teknologiutviklingens-pavirkning-pa-militaere-styrker-og-bruken-av-militaermakt

- Diesen, S. (2018), *Lavintensivt hybridangrep på Norge i en fremtidig konflikt* (18/00080). Tilgjengelig fra: https://www.ffi.no/publikasjoner/arkiv/lavintensivt-hybridangrep-pa-norge-i-en-fremtidig-konflikt

- Digital Threat Analysis Center, Eide, C., Turner, L., Hinkis, N., Watts, C., *"The One Like One Share Initiative" - How China deploys social media influencers to spread its message*, tilgjengelig fra: https://miburo.substack.com/p/the-one-like-one-share-initiative (nettside sist oppdatert: 21.09.2021, besøkt: 02.06.2022)

- DiResta, R., Miller, C., Molter, V., Pomfret, J., Tiffert. G. (2020), *Telling China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives*. Tilgjengelig fra: https://stacks.stanford.edu/file/druid:pf306sw8941/sio-china_story_white_paper-final.pdf

- DNV, Energy Transition Outlook 2021 (2021). Tilgjengelig fra: https://eto.dnv.com/2021#ETO2021-top.

- Drezner, D. W., Conflict Expectations and the Paradox of Economic Coercion, *International Studies Quarterly*, 1998, 42 (4), s. 709–31

- Drezner, D. W., Farrell, H., Newman, A. L. (red.), *The Uses and Abuses of Weaponized Interdependence* (2021), Washington, D.C.: Brookings Institution Press.

- Drezner, D. W., Sovereign Wealth Funds and the (In)Security of Global Finance, *Journal of International Affairs*, 2008, 62 (1), s. 115–30

- DW, POLITICS – *France's "yellow vests" and Russian trolls*, Tilgjengelig fra: https://www.dw.com/en/frances-yellow-vests-and-the-russian-trolls-that-encourage-them/a-46753388 (nettside sist oppdatert: 15.12.2018, besøkt: 19.04.2023)

- Early, B. R., Cilizoglu, M., Economic Sanctions in Flux: Enduring Challenges, New Policies, and Defining the Future Research Agenda, *International Studies Perspectives*, 2020, 21 (4), s. 438–77

- EC, Fit for 55, tilgjengelig fra: https://www.consilium.europa.eu/en/policies/green-deal/fit-for-55-the-eu-plan-for-a-green-transition/ (nettside sist oppdatert: 29.03.2023, besøkt: 18.04.2023).

- EC, REPowerEU: A plan to rapidly reduce dependence on Russian fossil fuels and fast forward the green transition, tilgjengelig fra: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_3131 (nettside sist oppdatert: 18.05.2022, besøkt: 18.04.2023)

- EC, *Shaping Europe's digital future – The Digital Services Act package*, tilgjengelig fra: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package (nettside sist oppdatert: 09.02.2023, besøkt: 19.04.2023)

- EC, Shaping Europe's digital future | High-level expert group on artificial intelligence, tilgjengelig fra: https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai (nettside sist oppdatert: 22.06.2022, besøkt 18.04.2023)

- Eggen, F. W., Måøy, J., Røtnes, R., Norberg-Schultz M., Steen J. I. (2021), *Norges behov for IKT-kompetanse i dag og framover*. Tilgjengelig fra: https://static1.squarespace.com/static/576280dd6b8f5b9b197512ef/t/60100605a2339c4557ac1008/1611662856986/R1-2021+Behov+for+og+tilbud+av+IKT-kompetanse.pdf

- Egloff, F. J., Public attribution of cyber intrusions, *Journal of Cybersecurity,* 2020, **6** (1). Tilgjengelig fra: https://doi.org/10.1093/cybsec/tyaa012

- Egloff, F. J., Smeets, M., Publicly attributing cyber attacks: a framework, *Journal of Strategic Studies*, 2021. Tilgjengelig fra: https://doi.org/10.1080/01402390.2021.1895117

- Ericsson (2020)), *Bringing 5G to power*. Tilgjengelig fra: https://www.ericsson.com/4ac680/assets/local/reports-papers/industrylab/doc/bringing-5g-to-power---industrylab-report.pdf

- Etterretningstjenesten (2022), *FOKUS 2022*. Tilgjengelig fra: https://www.etterretningstjenesten.no/publikasjoner/fokus/fokus-norsk/Fokus-2022-til-web.pdf

- EU Disinfo Lab, Miguel, R., *The battle against disinformation in the upcoming federal election in Germany: actors, initiatives and tools*, tilgjengelig fra: https://www.disinfo.eu/publications/the-battle-against-disinformation-in-the-upcoming-federal-election-in-germany-actors-initiatives-and-tools/ (nettside sist oppdatert: 24.09.2021, besøkt: 19.04.2023)

- EU, EEAS, Questions and Answers about the East StratCom Task Force, tilgjengelig fra: https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en (nettside sist oppdatert: 27.10.2021, besøkt: 19.04.2023)

- Europol (2021), *Internet Organised Crime Threat Assessment (IOCTA) 2021*. Tilgjengelig fra: https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

- EUvsDiSiNFO, *DISINFORMATION CASES ABOUT UKRAINE*, tilgjengelig fra: https://euvsdisinfo.eu/ukraine/ (Nettside besøkt: 19.04.2023)

- EUvsDiSiNFO, *FIGURE OF THE WEEK: 138*, tilgjengelig fra: https://euvsdisinfo.eu/figure-of-the-week-138/ (nettside sist oppdatert: 05.03.2019, besøkt: 19.04.2023)

- EUvsDiSiNFO, tilgjengelig fra: https://euvsdisinfo.eu/ (Nettside besøkt: 19.04.2023)

- Farrell, H., Newman, A. L., How Global Economic Networks Shape State Coercion, *International Security*, 2019, 44 (1), s. 42-79

- Farsund, B. H., Søndrol, T., Nystuen, K. O., Hornfelt, L., Sellevåg, S. R., Pham, V. (2022), *Utviklingen av nye IoT-baserte infrastrukturer i samfunnet – utfordringer for nasjonal sikkerhet (revidert rapport)* (22/00631). Tilgjengelig fra: https://www.ffi.no/publikasjoner/arkiv/utviklingen-av-nye-iot-baserte-infrastrukturer-i-samfunnet-utfordringer-for-nasjonal-sikkerhet-revidert-rapport

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

- FFI, Kongsberg-gruppen og FFI samarbeider om maritime overvåkningssatellitter, tilgjengelig fra: https://www.ffi.no/aktuelt/nyheter/kongsberg-gruppen-og-ffi-samarbeider-om-maritime-overvakingssatellitter (Nettside oppdatert: 03.05.2022, besøkt: 03.05.2023)

- Fioraldi, A., Maier, D., Eißfeldt, H., Heuse, M., AFL++: Combining Incremental Steps of Fuzzing Research, WOOT '20: *14th USENIX Workshop on Offensive Technologies,* (2020), Boston, MA, USA. Tilgjengelig fra: https://aflplus.plus//papers/aflpp-woot2020.pdf

- First Draft, Garcia, L., Shane, T., *A guide to prebunking: a promising way to inoculate against misinformation*, tilgjengelig fra: https://firstdraftnews.org/articles/a-guide-to-prebunking-a-promising-way-to-inoculate-against-misinformation/ (nettside sist oppdatert: 29.06.2021, besøkt: 19.04.2023)

- Forbes, Mathews, L., *Viasat Reveals How Russian Hackers Knocked Thousands Of Ukrainians Offline*, tilgjengelig fra: https://www.forbes.com/sites/leemathews/2022/03/31/viasat-reveals-how-russian-hackers-knocked-thousands-of-ukrainians-offline/ (nettside sist oppdatert: 31.03.2022, besøkt: 22.04.2023)

- Forsvarsmateriell, *MAST*, tilgjengelig fra: https://www.fma.no/anskaffelser/virksomhetsprogrammet-mast, (nettside sist oppdatert: 20.02.2023, besøkt 16.04.2023)

- Fulda, A., Chinese Communist Party's Hybrid Interference and Germany's Increasingly Contentious China Debate (2018-21), *The Journal of the European Association for Chinese Studies*, 2021, 2, s. 205-234. Tilgjengelig fra: https://journals.univie.ac.at/index.php/jeacs/article/view/6564

- Future Today Institute (2021), *2021 Tech Trends report*, begrenset tilgjengelighet

- Gartner, Gartner Says Worldwide IaaS Public Cloud Services Market Grew 41.4% in 2021, tigjengelig fra: https://www.gartner.com/en/newsroom/press-releases/2022-06-02-gartner-says-worldwide-iaas-public-cloud-services-market-grew-41-percent-in-2021 (nettside sist oppdatert: 02.06.2022, besøkt: 18.04.2022)

- Gartner, Panetta, K., *Top 10 Strategic Technology Trends for 2019*, tilgjengelig fra: https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019 (Nettside oppdatert: 15.10.2018, besøkt: 20.04.2023)

- Gartner, Top Strategic Technology Trends for 2022, tilgjengelig fra: https://www.gartner.com/en/information-technology/insights/top-tech-trends (Nettside besøkt: 20.04.2023)

- Goddard, S. E., The Road to Revisionism - How Interdependence Gives Revisionists Weapons for Change i *The Uses and Abuses of Weaponized Interdependence*, Drezner, D. W., Farrell, H., Newman, A. L. (red.), 2021, Brookings Institution Press, Washington, s. 84-98

- GOV.UK, Cyber security, *Government cracks down on spread of false coronavirus information online*, tilgjengelig fra: https://www.gov.uk/government/news/government-cracks-down-on-spread-of-false-coronavirus-information-online (nettside sist oppdatert: 30.03.2020, besøkt: 19.04.2023)

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

- Grammatech, Machine Learning for Finding Programming Defects and Anomalies, tilgjengelig fra: https://codesonar.grammatech.com/wp-form-machine-learning-for-finding-programming-defects-and-anomalies (Nettside besøkt: 18.04.2023)

- Granlund, C., Lausund, K. B., Lausund, R., Klepper, K. B., Pedersen, M. N., Voie, Ø. A. (2022), Konsekvenser av klimaendringer og klimatilpasninger for Forsvaret fram mot 2040 – rapport til Forsvarskommisjonen (22/02438). Tilgjengelig fra: https://www.ffi.no/publikasjoner/arkiv/konsekvenser-av-klimaendringer-og-klimatilpasninger-for-forsvaret-fram-mot-2040-rapport-til-forsvarskommisjonen

- Gupta, S., Driving Digital Strategy: A Guide to Reimagining Your Business (2018), Boston: Havard Business Review Press

- Hillman, J. E., *The Digital Silk Road: China's Quest to Wire the World and Win the Future*, 2021, London: Profile Books Ltd

- Himswoth, M. Dr., *Quantum Sensing* and *Quantum Sensing in Defense and Security*, Topical Briefing given at the NATO STO SET PBM Oct. 2020.

- Hovland, H., Siedler, R. E., Bukkvoll, T., Bamford, E. A (2022). *Elektronisk krigføring (EK) i gråsoneoperasjoner*, Norsk militært tidsskrift, 2022, 191 (4).

- Iansiti, M., Lakhani, K. R. (2014), Digital Ubiquity: How Connections, Sensors, and Data Are Revolutionizing Business, *Harvard Business Rev.*, 2014, **92** (11).

- IEEE, *IEEE Security & Privacy*, 2018, **16** (02), pp. c4-c4. Tilgjengelig fra: https://doi.ieeecomputersociety.org/10.1109/MSP.2018.1870865

- Infrastructure Intelligence, Walker, A., *Principles to guide development of national digital twin released*, tilgjengelig fra: http://www.infrastructure-intelligence.com/article/dec-2018/principles-guide-development-national-digital-twin-released (nettside sist oppdatert: 07.12.2018, besøkt: 18.04.2023)

- Institute for Strategic Dialogue, digital dispatches, Pro-Kremlin Network Impersonates Legitimate Websites and Floods Social Media with Lies, tilgjengelig fra: (nettside sist oppdatert: 29.09.2022, besøkt: 19.04.2023) https://www.isdglobal.org/digital_dispatches/pro-kremlin-network-impersonates-legitimate-websites-and-floods-social-media-with-lies/

- IPCC, Working Group I IPCC Sixth Assessment Report (2021), Climate Change 2021: The Physical Science Basis, Technical summary. Tilgjengelig fra: https://www.ipcc.ch/report/ar6/wg1/downloads/report/IPCC_AR6_WGI_TS.pdf.

- ITU, World summit on the information society, tilgjengelig fra: World Summit on the Information Society : About WSIS (itu.int), (nettside sist oppdatert: 17.01.2006, besøkt 21.04.2023)

- Justis- og beredskapsdepartementet, *Høringsnotat om endringer i straffeloven mv. – påvirkningsvirksomhet* (2021), tilgjengelig fra: https://www.regjeringen.no/contentassets/4bc018494c444e3994569d15a9927276/horingsnotat-om-endringer-i-straffeloven-mv.-pavirkningsvirksomhet.pdf

- Knut Abrahamsen (DSB), *Nødnett - veien videre* (presentasjon) 2021, tilgjengelig fra: https://www.statsforvalteren.no/contentassets/469e4eccdc7742759258bb9208e10c44/knut-abrahamsen-dsb---nodnett.pdf

- Kveberg, T., Alme, V., Diesen, S. (2019), *Defence against foreign influence – A value-based approach to define and assess harm, and to direct defence measures* (19/01766). Tilgjengelig fra: https://www.ffi.no/en/publications-archive/defence-against-foreign-influence-a-value-based-approach-to-define-and-assess-harm-and-to-direct-defence-measures

- Lange, B.K. & Gausdal A.H., *Hvordan påvirker tillit og psykologisk trygghet implementasjon av radikale endringer*, Bastesen, I. J., Lange, B. K., Næss, H. E., Thon, A. N. (red.), Ledelse av mennesker i det nye arbeidslivet (2020), Oslo: Cappelen Damm Akademisk (s. 257-277)

- Langner, R. (2013), *To Kill a Centrifuge*. Tilgjengelig fra: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

- Larkin, B., The Politics and Poetics of Infrastructure, *Annual Review of Anthropology,* 2013, *42(1), s.327-343*. Tilgjengelig fra: https://doi.org/10.1146/annurev-anthro-092412-155522

- Lindgren, P. Y., Hemnes, P. F., Waage, K. (2022), *Kinas potensial for økonomisk statshåndverk – kinesisk økonomi og interaksjon med omverden* (22/00421).
- Lov om nasjonal sikkerhet (sikkerhetsloven), tilgjengelig fra: https://lovdata.no/dokument/NL/lov/2018-06-01-24

- Lucas, E., Morris, J., Rebegea, C., (2021), *INFORMATION BEDLAM: Russian and Chinese Information Operations during COVID-19*. Tilgjengelig fra: https://cepa.org/wp-content/uploads/2021/03/CEPA-Russia-China-3.9.21.pdf

- MANDIANT, Brubaker, N., Lunden, K., Proska, K., Umair, M., Zafra, K. P., Hildebrandt, C., Caldwell R., *INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems*, tilgjengelig fra: https://www.mandiant.com/resources/blog/incontroller-state-sponsored-ics-tool (nettside sist oppdatert: 02.12.2022, besøkt: 18.04.2023)

- Martin, P., *China's Civilian Army: The Making of Wolf Warrior Diplomacy* (2021), 1st edition, New York, NY: Oxford University Press.

- Maschmeyer, L., The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations, *International Security*, 2021, 46 (2). Tilgjengelig fra: https://doi.org/10.1162/isec_a_00418

- Mastanduno, M., Economics and Security in Statecraft and Scholarship, *International Organization*, 1998, 52 (4), s. 825–54

- Matz, S. C., Appel, R. E., Kosinski, M., Privacy in the Age of Psychological Targeting, *Current Opinion in Psychology*, 2020, 31, s. 116-21.

- Meld. St. 10 (2021–2022), *Prioriterte endringer, status og tiltak i forsvarssektoren* (2022), Forsvarsdepartementet. Tilgjengelig fra: https://www.regjeringen.no/contentassets/6dc9df35fdbb4a208794ba336efa1d45/no/pdfs/stm202120220010000dddpdfs.pdf

- Meld. St. 13 (2020–2021) *Klimaplan for 2021–2030* (2021), Klima- og miljødepartementet. Tilgjengelig fra: https://www.regjeringen.no/contentassets/a78ecf5ad2344fa5ae4a394412ef8975/nn-no/pdfs/stm202020210013000dddpdfs.pdf

- Meld. St. 22 (2020-2021), *Data som ressurs — Datadrevet økonomi og innovasjon* (2021), Kommunal- og moderniseringsdepartementet. Tilgjengelig fra: https://www.regjeringen.no/contentassets/4f357e18bd314dc08c8e1b447b71b700/no/pdfs/stm202020210022000dddpdfs.pdf

- MERICS, Brussee, V., *China's Defense against the War of Words*, tilgjengelig fra: https://merics.org/en/short-analysis/chinas-defense-against-war-words (nettside sist oppdatert: 05.01.2022, besøkt: 06.07.2022)

- Meta, Nimmo, B., *Recapping Our 2022 Coordinated Inauthentic Behavious Enforcements*, tilgjengelig fra: https://about.fb.com/news/2022/12/metas-2022-coordinated-inauthentic-behavior-enforcements/ (nettside sist oppdatert: 15.12.2022, besøkt: 18.04.2023)

- Microsoft Digital Security Unit (2022), *Special Report: Ukraine – An overview of Russia's cyberattack activity in Ukraine.* Tilgjengelig fra: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

- Microsoft Source, Briggs, B., *Hackers hit Norsk Hydro with ransomware. The company responded with transparency*, tilgjengelig fra: https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/ (nettside sist oppdatert: 16.12.2019, besøkt: 18.04.2023)

- Microsoft Threat Intelligence Center*, HAFNIUM targeting Exchange Servers with 0-day exploits*, tilgjengelig fra: https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/ (nettside sist oppdatert: 16.03.2021, besøkt: 18.04.2023)

- Microsoft, Smith, B., *Defending Ukraine: Early Lessons from the Cyber War*, tilgjengelig fra: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/ (nettside sist oppdatert: 22.06.2022, besøkt: 22.04.2023)

- Morgan, T. C., Bapat, N., Kobayashi, Y., Threat and Imposition of Economic Sanctions 1945–2005: Updating the TIES Dataset, *Conflict Management and Peace Science,* 2014 31 (5), s. 541–58. Tilgjengelig fra: https://eprints.whiterose.ac.uk/126201/3/TIESupdateRR11.25.2013.pdf

- Mueller, R. (2019), *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*. Tilgjengelig fra: https://www.justice.gov/archives/sco/file/1373816/download

- Myndigheten for psykologiskt försvar, tilgjengelig fra: https://www.mpf.se/ (Nettside besøkt: 19.04.2023)

- Nasjonal sikkerhetsmyndighet (NSM) (2020), *Veileder i departementenes identifisering av grunnleggende nasjonale funksjoner*. Tilgjengelig fra: https://nsm.no/getfile.php/132858-1591177514/NSM/Filer/Dokumenter/Veiledere/veileder-i-departementenes-identifisering-av-gnf.pdf

- Nasjonal sikkerhetsmyndighet (NSM), *Nasjonalt cybersikkerhetssenter – Samleside for Apache Log 4j*, tilgjengelig fra: https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/nyheter-fra-ncsc/samleside-for-log4j/ (Nettside besøkt: 18.04.2023)

- Nasjonal sikkerhetsmyndighet (NSM), *Oversikt over innmeldte grunnleggende nasjonale funksjoner*, tilgjengelig fra: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnleggende-nasjonale-funksjoner-gnf/grunnleggende-nasjonale-funksjoner/oversikt-over-innmeldte-grunnleggende-nasjonale-funksjoner/. (Nettside oppdatert 30.09.2022, besøkt 22.12.2022)

- *Nasjonal strategi for kunstig intelligens* (2020), Kommunal- og moderniseringsdepartementet. Tilgjengelig fra: https://www.regjeringen.no/contentassets/1febbbb2c4fd4b7d92c67ddd353b6ae8/no/pdfs/ki-strategi.pdf

- National Cyber Security Centre, *UK and US call out Russia for SolarWinds compromise*, tilgjengelig fra: https://www.ncsc.gov.uk/news/uk-and-us-call-out-russia-for-solarwinds-compromise (nettside sist oppdatert: 15.04.2021, besøkt: 18.04.2023)

- National Security Agency (2022), *Embracing a Zero Trust Security Model*. Tilgjengelig fra: https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

- NATO (2022), *NATO 2022 Strategic Concept*. Tilgjengelig fra: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

- NATO Review, Christie, E. H., *Sanctions after Crimea: Have They Worked?*, tilgjengelig fra: https://www.nato.int/docu/review/articles/2015/07/13/sanctions-after-crimea-have-they-worked/index.html (nettside sist oppdatert: 13.07.2015, besøkt: 26.05.2022)

- NATO Science & Technology Organization (2021), *Disruptive Technologies Table-Top Exercise (D3TX) - Summary Report*. Tilgjengelig fra: https://www.sto.nato.int/Lists/STONewsArchive/displaynewsitem.aspx?ID=609 (Nettside besøkt: 20.04.2023)

- NATO Science & Technology Organization, *Science & Technology Trends 2020-2040* (2020), vol 1 og 2. Tilgjengelig fra: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

- NATO Science &Technology Organization (2023), *Science & Technology Trends 2023-2043*. Tilgjengelig fra: stt23-vol1.pdf (nato.int)

- NATO Strategic communication centre of excellence, tilgjengelig fra: https://stratcomcoe.org/ (Nettside besøkt: 23.04.2023)

- NATO Strategic Communications Centre of Excellence, Fredheim, R., Bay, S., *How Social Media Companies are Failing to Combat Inauthentic Behaviour Online*, tilgjengelig fra: https://stratcomcoe.org/publications/how-social-media-companies-are-failing-to-combat-inauthentic-behaviour-online/33 (nettside sist oppdatert: 05.12.2019, besøkt: 18.04.2023)

- NATO, *NATO Topic - Emerging and disruptive technologies*, tilgjengelig fra: https://www.nato.int/cps/en/natohq/topics_184303.htm (nettside sist oppdatert: 08.12.2022, besøkt 16.04.2023)

- Nimmo, B., Shawn Eib, C., Tamora, L. (2019), *Cross-Platform Spam Network Targeted Hong Kong Protests*. Tilgjengelig fra: https://public-assets.graphika.com/reports/graphika_report_spamouflage.pdf

- Nimmo, B., Torrey, M. (2022), Detailed report – Taking down coordinated inauthentic behavior from Russia and China. Tilgjengelig fra: https://about.fb.com/wp-content/uploads/2022/09/CIB-Report_-China-Russia_Sept-2022-1.pdf

- Nordic Energy Research (2021), Nordic Clean Energy Scenarios – Solutions for carbon neutrality. Tilgjengelig fra: https://pub.norden.org/nordicenergyresearch2021-01/.

- Norris, W. J., China's Post-Cold War Economic Statecraft: A Periodization, *Journal of Current Chinese Affairs*, 2021, 50 (3), s. 294-316

- Norris, W. J., *Chinese Economic Statecraft: Commercial Actors, Grand Strategy, and State Control* (2016), Ithaca, NY: Cornell University Press

- NrK, Norum, H, Ulvin, P. B., Hestenes, S. G., Skei, L., Henriksen, T. K., Årtun, A. B., Kruse, J. E., Ekern, S., *Russisk hackergruppe skal ha startet angrep mot Norge*, Tilgjengelig fra: https://www.nrk.no/norge/russisk-hackergruppe-skal-ha-startet-angrep-mot-norge-1.16020947 (nettside sist oppdatert: 29.06.2022, besøkt 06.01.2023)

- NrK, OECD kritiserer Norges klimainnsats: Ligger ikke an til å nå målene, tilgjengelig fra: https://www.nrk.no/norge/oecd-kritiserer-norges-klimainnsats_-ligger-ikke-an-til-a-na-malene-1.15939841. (Nettside sist oppdatert: 22.04.2022, besøkt: 18.04.2023)

- NRKbeta, Gundersen, M., *Trykker du «godta» kan mobilbevegelsene dine legges ut for salg*, tilgjengelig fra: https://nrkbeta.no/2021/10/07/trykker-du-godta-kan-mobilbevegelsene-dine-legges-ut-for-salg/ (nettside sist oppdatert: 16.11.2021, besøkt: 18.04.2023)

- Oatley, T., Weaponizing International Financial Interdependence i *The Uses and Abuses of Weaponized Interdependence*, Drezner, D. W., Farrell, H., Newman, A. L. (red.), 2021, Brookings Institution Press, Washington, s. 115-132.

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

- Pamment, J., Agardh-Twetman, H., Can There Be a Deterrence Strategy for Influence Operations?, *Journal of Information Warfare*, 2019, 18 (3), s. 123-135. Tilgjengelig fra: https://www.jstor.org/stable/26894685

- Pape, R. A., Why Economic Sanctions Do Not Work, *International Security*, 1997, 22 (2), s. 90-136

- Peksen, D., Better or Worse? The Effect of Economic Sanctions on Human Rights, *Journal of Peace Research*, 2009, 46 (1), s. 59–77

- Politiets sikkerhetstjeneste (PST) (2021), Nasjonal trusselvurdering 2021, tilgjengelig fra: https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/

- Politiets sikkerhetstjeneste (PST) (2022), *Nasjonal trusselvurdering 2022*. Tilgjengelig fra: https://www.pst.no/globalassets/ntv/2022/nasjonal-trusselvurdering-2022-pa-norsk.pdf

- Prop. 31 L (2022-2023), *Endringer i politiloven og politiregisterloven (PSTs etterretningsoppdrag og bruk av åpent tilgjengelig informasjon)* (2022), tilgjengelig fra: https://www.regjeringen.no/no/dokumenter/prop.-31-l-20222023/id2949174/

- ProPublica, Kao, J., Shuang Li, M., *How China Built a Twitter Propaganda Machine Then Let It Loose on Coronavirus*, tilgjengelig fra: https://www.propublica.org/article/how-china-built-a-twitter-propaganda-machine-then-let-it-loose-on-coronavirus (nettside sist oppdatert: 26.03.2020, besøkt: 02.04.2022)

- ProPublica/The New York Times, Kao, J., Zhong, R, Mozur, P., Krolik, A., *How China Spreads Its Propaganda Version of Life for Uyghurs*, tilgjengelig fra: https://www.propublica.org/article/how-china-uses-youtube-and-twitter-to-spread-its-propaganda-version-of-life-for-uyghurs-in-xinjiang?token=WjNhZpgg60OVkrdfYYm_zkvbreJmdi1q, (nettside sist oppdatert: 23.06.2021, besøkt: 12.06.2022)RAND, Mazarr, M. J., Understanding Deterrence, tilgjengelig fra: https://www.rand.org/pubs/perspectives/PE295.html (nettside sist oppdatert: 2018, besøkt: 19.04.2023)

- RAND, Waltzman, R., *Facebook Misinformation Is Bad Enough. The Metaverse Will Be Worse*, tilgjengelig fra: https://www.rand.org/blog/2022/08/facebook-misinformation-is-bad-enough-the-metaverse.html (nettside sist oppdatert: 22.08.2022, besøkt: 19.04.2023)

- Reilly, J. (2013), *China's Economic Statecraft: Turning Wealth into Power*. Tilgjengelig fra: https://www.files.ethz.ch/isn/175042/reilly_chinas_economic_statecraft_web.pdf

- Rett 24, Kolsrud, K., *Forslaget om å la PST overvåke åpne kilder får hard medfart i høringen*, tilgjengelig fra: https://rett24.no/articles/forslaget-om-a-la-pst-overvake-apne-kilder-far-hard-medfart-i-horingen (nettside sist oppdatert: 05.01.2022, besøkt: 19.04.2023)

- Retter, L., Frinking, E. J., Hoorens, S., Lynch, A., Nederveen, F., Phillips, W. D. (2020), *Relationships between the Economy and National Security: Analysis and considerations for economic security policy in the Netherlands*, tilgjengelig fra: https://www.rand.org/pubs/research_reports/RR4287.html

- REUTERS, Croft, A., Apps, P., *NATO websites hit in cyber attack over Crimea stance*, tilgjengelig fra: https://www.reuters.com/article/us-ukraine-crisis-nato-idUKBREA2F01R20140316 (nettside sist oppdatert: 16.03.2014, besøkt 06.01.2023)

- Rid, T., *Active Measures* (2020), New York: Farrar, Straus and Giroux (kapittel 5 og 6)

- Rid, T., Buchanan, B., Attributing Cyber Attacks, *Journal of Strategic Studies*, 2015. Tilgjengelig fra: https://doi.org/10.1080/01402390.2014.977382

- Roozenbeek, J., van der Linden, S., Goldberg, B., Rathje, S., Lewandowsky, S., Psychological inoculation improves resilience against misinformation on social media, *Sci. Adv.*, 2022, 8 (34). Tilgjengelig fra: https://www.science.org/doi/10.1126/sciadv.abo6254

- Ross, R. S., On the Fungibility of Economic Power: China's Economic Rise and the East Asian Security Order, *European Journal of International Relations*, 2019, 25 (1), s. 302–27.

- Schmitt, M. (red.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2017), Cambridge: Cambridge University Press. Tilgjengelig fra: https://doi.org/10.1017/9781316822524

- Sellevåg, S. R., Bergh, A., Bruvoll, J. A., Høibråten, S., Jacobsen, H. L., Strand, M., Barland, B. (2021), *Samfunnsutvikling mot 2030 - utfordringer for politiet, PST og påtalemyndigheten* (21/01132). Tilgjengelig fra: https://www.ffi.no/publikasjoner/arkiv/samfunnsutvikling-frem-mot-2030-utfordringer-for-politiet-pst-og-patalemyndigheten

- Sellevåg, S. R., Brattekås, K., Bruvoll, J. A., Buvarp, P. M. H., Fardal, H., Farsund, B., Fykse, E. M., Gisnås, H., Hellesø-Knutsen, K., Kirkhorn, S., Nystuen, K. O., Olsen, R., Seehuus, R. A. (2020), *Samfunnssikkerhet mot 2030 – utviklingstrekk* (20/00530). Tilgjengelig fra: https://www.ffi.no/publikasjoner/arkiv/samfunnssikkerhet-mot-2030-utviklingstrekk

- SGDSN, *Service de vigilance et protection contre les ingérences numériques étrangères*, tilgjengelig fra: http://www.sgdsn.gouv.fr/le-sgdsn/fonctionnement/le-service-de-vigilance-et-de-protection-contre-les-ingerences-numeriques-etrangeres-viginum/ (nettside sist oppdatert: 17.11.2022, besøkt: 19.04.2023)

- Sinopsis, Cole, J. M., *Taiwan and CCP political warfare: A blueprint*, tilgjengelig fra: https://sinopsis.cz/en/taiwan-and-ccp-political-warfare-a-blueprint/ (nettside sist oppdatert: 27.12.2019, besøkt: 25.06.2022)

- Sivertsen, E. G., Hellum, N., Bergh, A., Bjørnstad, A. L. (2021), *Hvordan gjøre samfunnet mer robust mot uønsket påvirkning i sosiale medier* (21/01237). Tilgjengelig fra: https://www.ffi.no/publikasjoner/arkiv/hvordan-gjore-samfunnet-mer-robust-mot-uonsket-pavirkning-i-sosiale-medier

- Skauen, A. N. (2019), Ship tracking results from state-of-the-art space-based AIS receiver systems for maritime surveillance, *CEAS Space Journal*, 2019, 11, s. 301

- Skjelland, E., Berg-Knutsen, E., Arnfinnsson, B., Diesen, S., Glærum, S., Guttelvik, M.S., Kvalvik, S., Mørkved, T., Olsen, K.E., Sellevåg, S.R., Sendstad, C., Strand, K.R., Voldhaug, J.E. (2022), *Forsvarsanalysen 2022* (22/00659). Tilgjengelig fra: https://www.ffi.no/publikasjoner/arkiv/forsvarsanalysen-2022

- Sky News, Manthorpe, R., *Facebook posts with the word "vote" blocked after leaders' TV election debate*, tilgjengelig fra: https://news.sky.com/story/facebook-posts-with-the-word-vote-blocked-after-leaders-tv-election-debate-11865934 (nettside sist oppdatert: 21.11.2019, besøkt: 30.09.2022)

- Slagnes, B. (2022), *Forskning på innsiderisiko – hvor er kunnskapshullene?* (22/01309). *BEGRENSET*

- Smart Energy International, *Smart5Grid – the 5G smart grid use cases*, tilgjengelig fra: https://www.smart-energy.com/industry-sectors/smart-grid/smart5grid-the-5g-smart-grid-use-cases/ (nettside sist oppdatert: 03.01.2022, besøkt: 18.04.2022)

- Snow, C.C., Fjeldstad, Ø.D., Langer, A.M., Designing the digital organization, *J. Org. Design,* 2017, **6** (7).

- South China Morning Post, Ng, T., Lo, K., *China-Lithuania tension: German firms may have to shut factories in Baltic state amid Beijing retaliation*, tilgjengelig fra: https://www.scmp.com/news/china/diplomacy/article/3160982/china-lithuania-tension-german-firms-may-have-shut-factories (nettside sist oppdatert: 25.12.2021, besøkt: 26.05.2022)

- SSB, Forurensning og klima - Utslipp til luft, tilgjengelig fra: https://www.ssb.no/natur-og-miljo/forurensning-og-klima/statistikk/utslipp-til-luft (nettside sist oppdatert: 03.11.2022, besøkt: 18.04.2023)

- TechTarget, Oladimeji, S., Kerner, S. M., *SolarWinds hack explained: Everything you need to know*, tilgjengelig fra: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know (nettside sist oppdatert: 29.06.2022, besøkt: 18.04.2023)

- Telenor (2020), *Digital Sikkerhet 2020 – Når nettene blir lange*. Tilgjengelig fra: https://www.telenor.no/om/digital-sikkerhet/2020/artikler/nettene-blir-lange.jsp.

- Telenor (2021), *Digital sikkerhet 2021 – Leveransekjeder - en kjent risiko som krever bevisste valg*. Tilgjengelig fra: https://www.telenor.no/om/digital-sikkerhet/2021/naar-nettene-blir-lange2.jsp

- The Diplomat, Jones, H., *China's Quest for Greater "Discourse Power"*, tilgjengelig fra: https://thediplomat.com/2021/11/chinas-quest-for-greater-discourse-power/ (nettside sist oppdatert: 24.11.2021, besøkt: 06.07.2022)

- The Economist, *China's rulers seem resigned to a slowing economy*, tilgjengelig fra: China's rulers seem resigned to a slowing economy | The Economist, (nettside sist oppdatert: 20.09.2022, besøkt: 20.04.2023)

- The Economist, *Russia is using energy as a weapon*, tilgjengelig fra: https://www.economist.com/interactive/graphic-detail/2022/11/26/high-fuel-prices-could-kill-more-europeans-than-fighting-in-ukraine-has (nettside sist oppdatert: 26.11.2022, besøkt: 20.04.2023)

- The Guardian, Crerar, P., Henley, J., Wintour, P., *Russia accused of cyber-attack on chemical weapons watchdog*, tilgjengelig fra: https://www.theguardian.com/world/2018/oct/04/netherlands-halted-russian-cyber-attack-on-chemical-weapons-body (nettside sist oppdatert: 04.10.2018, besøkt 18.04.2023).

- The Guardian, Oltermann, P., European politicians duped into deepfake video calls with mayer of Kyiv, tilgjengelig fra: https://www.theguardian.com/world/2022/jun/25/european-leaders-deepfake-video-calls-mayor-of-kyiv-vitali-klitschko (nettside sist oppdatert: 25.06.2022, besøkt: 19.04.2023)

- The Japan Times, Torode, G., Pollard, M. Q., Tian, Y. L., Russia's Ukrainian quagmire providing tough lessons for China, tilgjengelig fra: https://www.japantimes.co.jp/news/2022/04/30/asia-pacific/china-lessons-ukraine-war-russia/ (nettside sist oppdatert: 30.04.2022, besøkt: 12.05.2022)

- The New York Times, Mac, R., *Meta's Profit Slides by More Than 50 Percent as Challenges Mount*, tilgjengelig fra: https://www.nytimes.com/2022/10/26/technology/meta-facebook-q3-earnings.html (nettside sist oppdatert: 26.10.2022, besøkt: 18.04.2023)

- *The New York Times,* Xiao, M., Mozur, P., Beltran, G., *Buying Influence: How China Manipulates Facebook and Twitter*, tilgjengelig fra: https://www.nytimes.com/interactive/2021/12/20/technology/china-facebook-twitter-influence-manipulation.html (nettside sist oppdatert: 20.12.2021, besøkt: 19.04.2023)

- The UK National Quantum Technologies, The UK National Quantum Technology Programme, tilgjengelig fra: https://uknqt.ukri.org/ (Nettside besøkt: 18.04.2023)

- The Verge, Heath, A., *Facebook is changing its algorithm to take on TikTok, leaked memo reveales*, tilgjengelig fra: https://www.theverge.com/2022/6/15/23168887/facebook-discovery-engine-redesign-tiktok (nettside sist oppdatert: 15.06.2022, besøkt: 09.08.2022)

- Trend Micro – Cybercrime & Digital Threats, Ransomware, Agcaoili, J., Ang, M., Earnshaw, E., Gelera, B., Tamaña, N., *Ransomware Double Extortion and Beyond: REvil, Clop, and Conti*. Tilgjengelig fra: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti (nettside sist oppdatert: 15.06.2021, besøkt: 18.04.2023)
- U.S. Department of State, Global Engagement Center, *GEC Special Report: Russia's Pillars of Disinformation and Propaganda* (2020). Tilgjengelig fra: https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf

- U.S. Department of State, Global Engagement Center, tilgjengelig fra: https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/

- U.S. Department of State, Patel, V., Yevgeniy Prigozhin's Africa-Wide Disinformation Campaign https://www.state.gov/disarming-disinformation/yevgeniy-prigozhins-africa-wide-disinformation-campaign/

- Udal, J. H., Waage, K., Engebretsen, P., Lindgren, P. Y. (2022), *Russisk økonomisk statshåndverk – implikasjoner for norsk sikkerhet* (22/00426)

- UN Digital Library, Group of Governmental Experts (2018), *Advancing responsible State behavior in cyberspace in the context of international security: draft resolution*. Tilgjengelig fra: Advancing responsible State behaviour in cyberspace in the context of international security : (un.org)

- UN, Office for Disarmament Affairs, Open-ended Working Group on security of and in the use of information and communications technologies, tilgjengelig fra: Open-ended working group on information and communication technologies (2021) | United Nations (unoda.org) (Nettside besøkt: 26.04.2023)

- Vekasi, K., Politics, Markets, and Rare Commodities: Responses to Chinese Rare Earth Policy, *Japanese Journal of Political Science*, 2019, 20 (1), s.2–20.

- Voldhaug, J. E., Hansen B. J., Lund, K., Mykkeltveit, A., Rytir, M., Bentstuen, O. I. (2021), *Hvordan kan ny IKT gjøre Forsvaret bedre*, (21/01819). Tilgjengelig fra: https://www.ffi.no/publikasjoner/arkiv/hvordan-kan-ny-ikt-gjore-forsvaret-bedre

- Waage, K., Kvalvik, S. N., Lindgren, P. Y. (2021), *Utenlandske investeringer og andre økonomiske virkemidler - når truer de nasjonal sikkerhet?* (20/03149). Tilgjengelig fra: https://www.ffi.no/publikasjoner/arkiv/utenlandske-investeringer-og-andre-okonomiske-virkemidler-nar-truer-de-nasjonal-sikkerhet

- Waage, K., Lindgren, P. (2022), *Økonomisk statshåndverk, teknologisk utvikling og implikasjoner for norsk sikkerhet – en forstudie* (22/01758)

- Waage, K., Lindgren, P. Y., Boye, E., Haug, I. D. (2022), *Kinesisk økonomisk statshåndverk og implikasjoner for norsk sikkerhet* (22/00422).

- War on the Rocks, Mattis, P., *China's "Three Warfares" in Perspective*, tilgjengelig fra: https://warontherocks.com/2018/01/chinas-three-warfares-perspective/ (nettside sist oppdatert: 30.01.2018, besøkt: 30.05.2022)

- Wilson, J. D., Whatever happened to the rare earths weapon? Critical materials and international security in Asia, *Asian Security*, 2018, 14 (3), s.358–73

- Winecoff, W. K., "The persistent myth of lost hegemony," revisited: structural power as a complex network phenomenon, *European Journal of International Relations*, 2020, 26 (1_suppl), s. 209-52.

- Wired, Perlroth, N., *The Untold History of America's Zero-Day Market*, tilgjengelig fra: https://www.wired.com/story/untold-history-americas-zero-day-market/ (nettside sist oppdatert: 14.02.2021, besøkt: 18.04.2023)

- WIRED, Ravenscraft, E., *What Is the Metaverse, Exactly?*, tilgjengelig fra: https://www.wired.com/story/what-is-the-metaverse/ (nettside sist oppdatert: 25.04.2022, besøkt: 19.04.2023)

- Xiaotong, Z., Keith, J., From Wealth to Power: China's New Economic Statecraft, *The Washington Quarterly*, 2017, 40 (1), s. 185–203.

Om FFI

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

FFIs formål

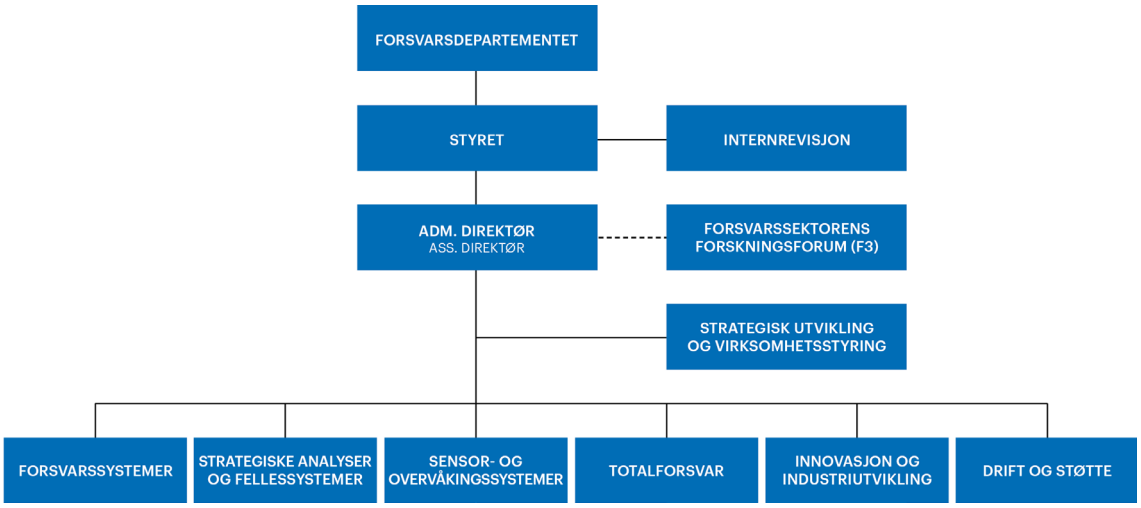
Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som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



Forsvarets forskningsinstitutt (FFI)
Postboks 25
2027 Kjeller

Besøksadresse:
Kjeller: Instituttveien 20, Kjeller
Horten: Nedre vei 16, Karljohansvern, Horten

Telefon: 91 50 30 03
E-post: post@ffi.no
ffi.no

Norwegian Defence Research Establishment (FFI)
PO box 25
NO-2027 Kjeller
NORWAY

Visitor address:
Kjeller: Instituttveien 20, Kjeller
Horten: Nedre vei 16, Karljohansvern, Horten

Telephone: +47 91 50 30 03
E-mail: post@ffi.no
ffi.no/en