FFI Forsvarets forskningsinstitutt

21/01237

FFI-RAPPORT

Hvordan gjøre samfunnet mer robust mot uønsket påvirkning i sosiale medier

Eskil Grendahl Sivertsen
Nina Hellum
Arild Bergh
Anne Lise Bjørnstad

Hvordan gjøre samfunnet mer robust mot uønsket påvirkning i sosiale medier

Eskil Grendahl Sivertsen
Nina Hellum
Arild Bergh
Anne Lise Bjørnstad

Forsvarets forskningsinstitutt (FFI) 9. juni 2021

Emneord
Desinformasjon
Påvirkningsoperasjoner
Sosiale medier
Sammensatte trusler

FFI-rapport
21/01237

Prosjektnummer
1582

Elektronisk ISBN
978-82-464-3356-1

Engelsk tittel
How to increase resilience against unwanted influence on social media

Godkjennere
Janet Blatny, *forskningsdirektør*

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Sammendrag

Uønsket påvirkning ved bruk av blant annet desinformasjon i sosiale medier er blitt en synlig samfunnsutfordring. Under covid-19-pandemien har dette blitt spesielt tydelig, hvor spredning av desinformasjon har fått konsekvenser for liv og helse i flere land og undergraver tilliten mellom befolkningen og myndighetene. Derfor er det viktig og nødvendig at samfunnet blir mer robust i møtet med påvirkningsforsøk i sosiale medier.

Med denne rapporten ønsker FFI å gjøre norske myndigheter, Forsvaret og totalforsvarsaktørene, og dermed samfunnet, bedre rustet til å forstå og gjenkjenne desinformasjon og påvirkningsoperasjoner i sosiale medier, for slik å kunne identifisere og beskytte egne sårbarheter gjennom konkrete tiltak og prioriteringer. Påvirkningsoperasjoner foregår gjerne fordekt og opphavet tåkelegges. De er derfor krevende å oppdage uten kunnskap, gode metoder og digitale verktøy. Rapportens overordnede problemstilling er hvordan samfunnet kan gjøres mer robust mot uønsket påvirkning i sosiale medier og det er fire forskningsspørsmål som rapporten adresserer:

- Hvordan kan norske borgere påvirkes av desinformasjon og påvirkningsforsøk i sosiale medier?
- Hvilke konkrete metoder og plattformer benyttes i påvirkningsoperasjoner/forsøk?
- Hvilke typer aktører forsøker å påvirke Norge?
- Hvilke tiltak bør vurderes for å gjøre samfunnet mer robust mot uønsket påvirkning i sosiale medier?

Rapporten beskriver hva desinformasjon og påvirkningsoperasjoner er, og hvilke sentrale sårbarheter det norske samfunnet har i møte med trusselen fra desinformasjon og påvirkningsoperasjoner. Videre, tar rapporten for seg konkrete metoder og plattformer som benyttes i påvirkningsoperasjoner, i tillegg til noen bakenforliggende psykologiske prosesser. Det er både statlig- og ikke-statlige aktører som kan stå bak en påvirkningsoperasjon og rapporten beskriver ulike typer aktører fra fremmede stater, som Russland og Kina, til terrororganisasjoner, svindlere og ulike interessegrupper, som kan forsøke å påvirke Norge.

Rapporten fremmer en rekke anbefalinger på hvordan man kan styrke vår robusthet mot uønsket påvirkning i sosiale medier. Anbefalingene er blant annet tilknyttet risiko- og sårbarhetsanalyser, metoder for å avdekke og håndtere desinformasjon, utvikling av digitale verktøy, og øke motstandsdyktighet i samfunnet og på myndighetsnivå. Det er nødvendig med kontinuerlig kunnskapsbygging innen dette feltet pga. den rivende utviklingen innen teknologi og det cyber-sosiale informasjonsdomenet. Det er behov for økt innsikt i, og kunnskap om, deteksjon av trender, forebyggende sikkerhet og langtidseffektene som des- og feilinformasjon i sosiale medier kan ha på nasjonal sikkerhet og bruk og effekt av kommunikasjon som et strategisk virkemiddel i fred, krise og krig.

Påvirkningsoperasjoner utgjør en betydelig del av såkalte «sammensatte» eller «hybride» trusler. Den viktigste konklusjonen er at for å forstå og håndtere dem trengs det en tilnærming som går på tvers av tradisjonelle skillelinjer som stats- og samfunnssikkerhet, sivilt-militært, totalforsvaret, sektorene i norsk statsforvaltning og vår tradisjonelle forståelse av kategoriene fred, krise og krig.

Summary

Malign influence through disinformation in social media has become a visible societal challenge. This has been especially evident during the Covid-19 pandemic, during which the spread of disinformation has had a direct impact on life and health in several countries and threatened to undermine trust among populations and to government institutions. This shows how important and necessary it is to strengthen society's resilience against malign influence in social media.

The aim of this report is to increase knowledge and awareness among Norwegian authorities and public institutions, the Norwegian Armed Forces and the Total Defence actors on disinformation and influence operations in social media. Its purpose is to contribute to improved preparedness and resilience.

Influence operations are usually covert and their origins clouded. That makes them difficult to detect without knowledge, effective methods and digital tools. This report seeks to answer the question of how to increase resilience against unwanted influence on social media, by addressing four key sub-questions – the latter also being the conclusion.

- How are Norwegian citizens influenced by disinformation and influence attempts in social media?
- Which specific methods and platforms are used in influence operations/attempts?
- Which actors are performing influence operations against Norway?
- Which measures should be considered in order to increase resilience against unwanted influence on social media?

The report describes and explains disinformation and influence operations, and identifies key vulnerabilities of the Norwegian society in facing the threat from both. Furthermore, it presents specific methods and platforms for influence operations as well as the underlying psychological processes that make them effective. Both state and non-state actors can initiate influence operations against Norway. Actors range from foreign states like Russia and China to terrorist organizations, criminals and different interest groups.

The report presents a number of recommendations on how to strengthen our resilience against unwanted influence on social media. The recommendations include risk and vulnerability analyses, methods for detecting and dealing with disinformation, development of digital tools and ways to increase awareness across governmental sectors and in society as a whole. Continuous knowledge building in this field is necessary, due to the rapid development of technology and the cyber-social information domain.

Influence operations constitute a significant part of so-called "hybrid threats". As such, this report concludes that such operations should be met with a whole-of-society approach across government sectors and the established separations of responsibilities, namely state vs. societal security, civilian vs. military and the increasingly irrelevant threshold definitions between peace, crisis and war.

Innhold

Forord

Denne rapporten er skrevet av FFI på oppdrag fra Justis- og beredskapsdepartementet i første halvdel 2021. Dens hensikt er å gjøre norske myndigheter, Forsvaret og totalforsvarsaktørene bedre rustet til å forstå og gjenkjenne desinformasjon og påvirkningsoperasjoner i sosiale medier, for å dermed kunne identifisere og beskytte egne sårbarheter gjennom konkrete tiltak og prioriteringer.

Påvirkningsoperasjoner kan favne bredt og inkludere virkemidler både i og utenfor det digitale domenet. I denne rapporten fokuserer vi først og fremst på sosiale medier, men beskriver også andre virkemidler og hvordan de spiller sammen.

Dette er ikke en forskningsrapport i den forstand at den er et resultat av egen forskning. Mye av innholdet er basert på både internasjonal og nasjonal forskning, samt FFIs forskningsrapporter, men kildegrunnlaget er mye bredere enn det. Rapporten er i så måte en sammenstilling av kunnskap og innsikt fra en lang rekke kilder, støttet av både reelle og tenkte eksempler på desinformasjon og påvirkningsoperasjoner. Det går tydelig fram hva som er reelt og fiktivt.

Formålet er å skape et kunnskapsgrunnlag som i form og innhold skal være mest mulig egnet til at ansatte i både offentlig og privat sektor skal kunne ta kunnskapen i bruk i sitt daglige virke. Dette er i seg selv et viktig grep for å gjøre samfunnet mer robust mot uønsket påvirkning i sosiale medier.

Takk til Justis- og beredskapsdepartementet for godt samarbeid og dialog, og til Lars van Diepen ved FFI for støtte til ferdigstillelse av rapporten.

Oslo, 08.06.21

Eskil Grendahl Sivertsen, Nina Hellum, Arild Bergh, Anne Lise Bjørnstad

1 Innledning

I langtidsplanen for forsvarssektoren (Det Kongelige Forsvarsdepartement, 2020) og samfunnssikkerhetsmeldingen (Justis- og beredskapsdepartementet, 2020) beskrives «sammensatte trusler» som en sentral utfordring mot norsk sikkerhet. Begrepene «sammensatte trusler» og «hybride trusler» brukes ofte om hverandre og beskriver situasjoner der en aktør bruker ulike, og ofte fordekte, virkemidler i kombinasjon for å ramme eller utnytte sårbarheter i samfunnet. Påvirkningsoperasjoner er en del av dette virkemiddelapparatet, hvor desinformasjon på sosiale medier utgjør en betydelig bestanddel. Denne typen trusler mot demokratiet, norske interesser og nasjonal handlefrihet er løftet høyt på agendaen av både Etterretningstjenesten, Nasjonal Sikkerhetsmyndighet (NSM) og Politiets sikkerhetstjeneste (PST) i deres trusselvurderinger for 2021 (Etterretningstjenesten, 2020; Nasjonal sikkerhetsmyndighet, 2021; Politiets Sikkerhetstjeneste, 2021).

Sammensatte trusler, inkludert datainnbrudd og påvirkning gjennom sosiale medier, er blitt et fremtredende trekk ved væpnet konflikt, men også i fredstid (Weissmann et al., 2021). Dette er virkemidler som kan være vanskelige å oppdage og som kan skape betydelig effekt under terskelen for hva vi normalt vil gjenkjenne som en krise. For fremmede stater er påvirkningsoperasjoner egnet til å skape fordelaktige forutsetninger for å nå egne strategiske mål uten risikoene og kostnadene knyttet til å bruke eller true med konvensjonell militærmakt, sanksjoner eller aggressivt diplomati. Derfor brukes påvirkningsoperasjoner, i både fred, krise og krig, som en del av staters forsøk på å påvirke andre stater, institusjoner og befolkning. Men også andre, som terrororganisasjoner, interessegrupper og økonomisk motiverte, profesjonelle desinformasjonsaktører, benytter desinformasjon i sosiale medier for å oppnå sine mål.

Forebygging og forsvar mot sammensatte trusler krever god og lik situasjons- og sikkerhetspolitisk forståelse på tvers av sektorer, kunnskap om truslene, virkemidlene og aktørene, hvilken hensikt disse kan ha og hvilke effekter de sannsynligvis er ute etter å skape. Og ikke minst krever det, på nasjonalt strategisk nivå, en tverrsektoriell evne til å fange opp, analysere, vurdere og hurtig koordinere og utføre eventuelle mottiltak, om nødvendig. Forebygging i form av å redusere sannsynligheten for at en påvirkningsaktør lykkes med å nå sine mål, er likevel mest effektivt. Det krever kunnskap og den samme evnen som beskrevet over.

I forbindelse med statsbudsjettet 2021, tydeliggjorde regjeringen seks mål og prioriteringer for Justis- og beredskapssektoren: 1) effektiv kamp mot kriminalitet, 2) rettssikkerhet, 3) trygghet i samfunnet, 4) kontrollert og bærekraftig innvandring, 5) godt forvaltede polarområder og 6) et godt og moderne lovverk (Justis- og beredskapsdepartementet, 2021:12). Påvirkningsoperasjoner kan utgjøre en trussel mot samtlige. Det er viktig å understreke at det ikke nødvendigvis dreier seg om lineære angrep mot ett eller flere av målene. En betydelig svekkelse av befolkningens tillit til myndighetene for eksempel, vil kunne få effekt på samtlige departementers måloppnåelse uavhengig av tema eller sektor. Forebygging er derfor avgjørende for å redusere effekten av uønsket påvirkning mot Norge.

Rapporten søker å gi svar på følgende spørsmål:

- Hvordan kan norske borgere påvirkes av desinformasjon og påvirkningsforsøk i sosiale medier?
- Hvilke konkrete metoder og plattformer benyttes i slike påvirkningsoperasjoner/forsøk?
- Hvilke typer aktører forsøker å påvirke Norge?
- Hvilke tiltak bør vurderes for å gjøre samfunnet mer robust mot uønsket påvirkning i sosiale medier?

1.1 Grunnlagsmateriale for studien

Grunnet rivende utvikling innen feltet finnes det mye informasjon og kunnskap tilgjengelig om tematikken for denne rapporten. Samtidig gjør den samme utviklingen, som er drevet både av teknologi, sikkerhets- og samfunnspolitiske endringer og trusselaktørenes tilpasninger til disse, at både virkemidler, metoder, aktører og deres hensikter er i kontinuerlig utvikling. Utviklingen forsterkes av tiltakende stormaktsrivalisering og en stadig mer krevende og uforutsigbar sikkerhetssituasjon.

En rapport som dette må derfor sees i lys av den perioden den utarbeides i. Kildegrunnlaget er variert. Både akademiske, populærvitenskapelige og faglitterære bøker og artikler er med. Det samme er utvalgte artikler fra aviser og tidsskrifter, kronikker, blogginnlegg, og innlegg fra sosiale medier. Forskningsrapporter, utredninger og offentlige dokumenter som Stortingsproporsjoner og strategiplaner ligger også til grunn. Informasjonen kommer i tillegg fra relevante offentlige hjemmesider for statlige aktører, offentlige etater og organisasjoner, samt fra organisasjoner som arbeider med påvirkningsproblematikk, som blant annet EUs East Stratcom Task Force, Nato StratCom Center of Excellence, US State Department's Global Engagement Center, Bellingcat, akademiske miljøer og faktasjekkere som faktisk.no. Sammen danner disse kildene et helhetsbilde som presenteres i rapporten. En fullstendig referanseliste ligger som vedlegg.

2 Hvordan kan norske borgere påvirkes av desinformasjon og påvirkningsforsøk i sosiale medier?

2.1 Hva er desinformasjon?

Med «desinformasjon» menes her utvikling og spredning av bevisst feilaktig eller villedende informasjon i den hensikt å påvirke menneskers virkelighetsoppfatning, holdninger og handlinger. Dette er ikke et nytt fenomen, men internett og sosiale medier (SoMe) har skapt helt nye muligheter for effektiv spredning av desinformasjon og dermed også økt kraft og betydning. Dette utnyttes bevisst og systematisk til forskjellige formål av ulike aktører, fra fremmede stater til terrororganisasjoner, svindlere og ulike interessegrupper.

Motivene varierer tilsvarende. Statsdrevet desinformasjon på sosiale medier søker gjerne å påvirke virkelighetsoppfatningen til, og/eller å forsterke konflikt mellom, befolkningsgrupper i et samfunn i den hensikt å skape best mulige forutsetninger for å nå egne strategiske mål. Målet trenger ikke nødvendigvis alltid å være å få folk til å tro på noe som ikke er sant. Det kan like gjerne være å skape tvil, usikkerhet, økt oppmerksomhet eller avledning. Terrororganisasjoner bruker gjerne desinformasjon for radikalisering og rekruttering, mens andre aktører kan ha utelukkende økonomiske motiver som økt salg eller annonseinntekter basert på datatrafikk. Selv om aktørene og hensiktene er ulike, har bruken av desinformasjon det til felles at den søker å påvirke menneskers holdninger og handlinger.

Desinformasjon trenger ikke nødvendigvis å være uriktig informasjon. Informasjonen kan være helt eller delvis korrekt, men tatt ut av sammenheng, tillagt en annen avsender eller på andre måter bevisst framsatt på en feilaktig eller villedende måte med intensjon om å oppnå en eller annen effekt på bestemte målgrupper.

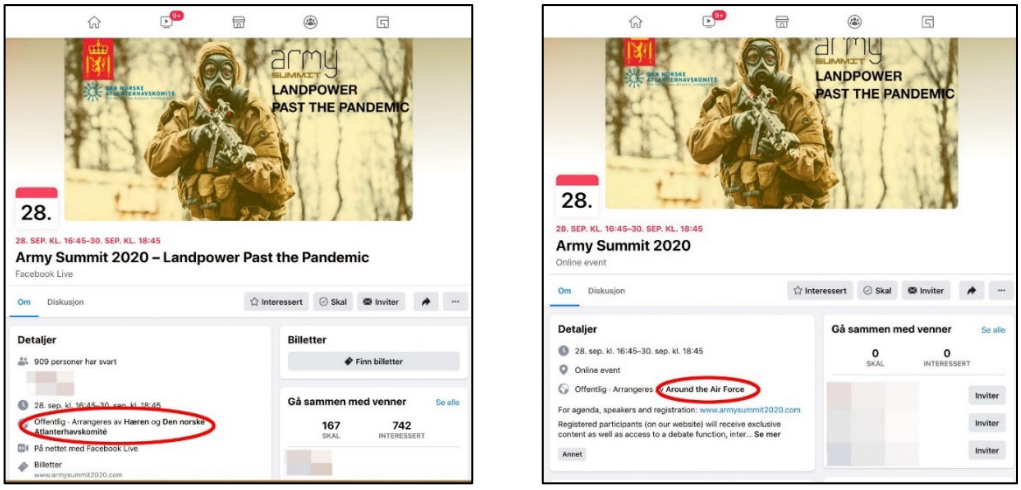
Begrepene «desinformasjon» og «feilinformasjon» brukes av og til om hverandre, men det er en forskjell. Feilinformasjon er falsk eller misvisende informasjon som man deler fordi man faktisk tror den er sann. Et enkeltstående eksempel på spredning av desinformasjon og spredning av feilinformasjon kan altså se helt likt ut. Forskjellen er hvorvidt det ligger en bevisst, manipulativ hensikt bak eller om det gjøres i god tro. Effekten kan være den samme. Dette har først og fremst betydning for forebygging og håndtering; en aktør som bevisst sprer desinformasjon vil neppe slutte med det fordi noen påpeker at informasjonen er feil, mens en aktør som sprer feilinformasjon kan med større sannsynlighet påvirkes til å korrigere sin atferd så lenge vedkommende ikke aktivt ønsker å dele informasjon som ikke er riktig eller har en overbevisning tuftet på desinformasjon eller konspirasjonsteorier.

Koronapandemien har for alvor vist at problemet med desinformasjon på sosiale medier har blitt betydelig, med til dels alvorlige følger. I Storbritannia har folk satt fyr på 5G-master i den tro at 5G svekker immunforsvaret og gjør befolkningen mer mottakelige for å bli smittet og syk av covid-19 (BBC News, 2020a). I USA og Iran har mennesker mistet livet fordi de trodde på at man dreper

viruset ved å drikke klor eller alkohol (Spring, 2020). Og i mange land, Norge inkludert, kan håndteringen av pandemien forpurres hvis nok mennesker tror på at covid-19 bare er som en influensa, at vaksinen er helseskadelig eller at myndighetene har en hemmelig agenda. Eksemplene er mange, og ikke begrenset til koronapandemien. Stormingen av den amerikanske kongressen 6. januar 2021 skjedde som konsekvens bl.a. av omfattende desinformasjon om valgfusk og konspirasjonsteorien Qanon gjennom sosiale medier (Holt et al., 2021; Yurieff, 2021), og viser hvordan desinformasjon kan utgjøre en trussel mot demokratiet, ikke bare gjennom å undergrave demokratiske verdier, men også gjennom å føre til demokratifiendtlige handlinger i den fysiske verden (Etter, 2017; Paul, 2020).

Det kan være lett å avfeie slike eksempler som lite relevante for en norsk befolkning som tross alt kjennetegnes av et generelt høyt utdanningsnivå og høy tillit til myndighetene. Dette kan gi grunn til å anta at den norske befolkningen er ganske motstandsdyktig mot desinformasjon. Men desinformasjon sniker seg inn i alles liv gjennom sosiale medier hele tiden, på subtile og ofte fiffige måter. Selv om majoriteten av Norges befolkning kanskje ikke vil la seg forlede av de mest utrerte enkelteksemplene på desinformasjon, viser erfaring at de fleste kan la seg påvirke. Profesjonelt utført desinformasjon er laget på måter som gjør den vanskelig å avsløre, og overdreven tro på egne evner kan øke risikoen for å bli lurt (Lyons et al., 2021).

For eksempel ble Facebook-arrangementene til både Army Summit 2020 og Etterretningstjenestens og PSTs framleggelse av trusselvurderingene for 2021 klonet av fremmede aktører. En rekke personer, mange i sentrale stillinger innen forsvar, sikkerhet og beredskap, meldte seg på de falske arrangementene. Hensikten er ikke kjent, men kan ha vært å få oversikt over personell og nettverk, sabotere de faktiske arrangementene eller lure folk for penger. Flere rapporterte om at de, av de falske arrangørene, hadde blitt bedt om å oppgi kredittkortinformasjon for å få tilgang til arrangementene (som var gratis). Det er uvisst om svindelforsøket indikerer et økonomisk motiv eller i seg selv var et forsøk på å tåkelegge den egentlige hensikten.



Figur 2.1 *Til venstre er det ekte arrangementet som ble arrangert av Hæren og Den norske Atlanterhavskomité. Til høyre er det falske arrangementet som ble opprettet av en ukjent aktør «Around the Air Force».*

Selv om hver og en av oss kanskje kan gjennomskue enkelteksempler på desinformasjon, kan summen av målrettet desinformasjon på flere kanaler og plattformer over tid likevel gradvis påvirke holdninger og/eller oppfatninger om bestemte tema uten at man nødvendigvis er bevisst det. Dette gjelder spesielt på tema som er egnet til å vekke sterke følelser og skape konflikt, som f.eks. covid-19 smittevernstiltak, klimapolitikk og innvandring.

Figur 2.2 Eksempel på desinformasjon tilbakevist av faktisk.no

Eksempelet over er fra 2019 og ble tilbakevist av faktisk.no (Karlsen & Skiphamn, 2019). Det viser tre viktige ting: For det første hvor stor spredning desinformasjon kan få selv fra en privatperson (300 delinger). For det andre hvordan desinformasjon gjerne blander fakta, løgn og påstander, og for det tredje hvor krevende det kan være å utøve faktasjekk av slike poster som inneholder mange forhold som krever tid og kunnskap å undersøke.

Figur 2.3 Eksempel på desinformasjon egnet til å forsterke danskenes motstand mot regjeringens håndtering av pandemien.

Til høyre er et annet og nyere eksempel fra Danmark, hvor misnøye over regjeringens håndtering av koronapandemien er et aktuelt og konfliktskapende tema i den offentlige debatten. Sammenligningen mellom Danmark og Norge er laget av det politiske partiet Liberal Alliance, og er hyppig delt i sosiale medier. I skrivende stund

har det opprinnelige innlegget 3.400 reaksjoner/likes og er delt 1300 ganger.[1] Hver deling kan igjen få videre forgreininger, som vist her hvor den danske folketingspolitikeren fra Det Konservative Folkeparti, Rasmus Jarlov, sitt innlegg er delt ytterligere 618 ganger. Ett enkelt innlegg kan slik oppnå ekstrem spredning gjennom eksponentiell vekst.

I tillegg til å vise effekten av spredning, viser dette eksempelet også hvordan desinformasjon lages for å trigge en emosjonell respons. Dersom man har en oppfatning av, eller interesse av å hevde, at den danske regjeringens håndtering er håpløs, vil man her få bekreftet sitt syn. Hos mange kan behovet for å bevise at man har rett, eller få bekreftet sine følelser eller oppfatninger, være større enn behovet for å finne ut hva som er sant (Schulz et al., 2020).

Eksempelet viser også hvordan desinformasjon gjerne overforenkler, konstruerer falske motsetninger eller kontraster og består av både sann og usann informasjon; noe informasjon om Norge er korrekt, noe er feil, noe har vært rett på et tidspunkt, men er det ikke lenger. Dette er således også et godt eksempel på «cherry picking», hvor man håndplukker informasjon som støtter ens påstand og utelater informasjon eller kontekst som svekker den.

Desinformasjon kan altså komme i mange ulike varianter og former, og være vanskelige å avsløre. Den kan komme fra ulike aktører med ulike hensikter. Faktisk.no gir følgende, illustrerende (men på ingen måte uttømmende) eksempler (Faktisk.no, 2020):

- Når noen sprer usannheter i forkant av et valg for å forsøke å endre valgresultatet.
- Når en stat sprer usannheter for å påvirke holdningene eller handlingene til innbyggerne.
- Når en løgnfabrikk eller et viralnettsted lager saker som ikke nødvendigvis er sanne for å få mange klikk på nettsidene sine, og igjen tjener penger på det.
- Når reklame fremstår som informasjon uten at man får vite at det er reklame.
- Når folk lures via e-post til å gi fra seg personlig informasjon eller logge inn på en falsk nettside, slik at de kan svindles.

Desinformasjon på sosiale medier er i seg selv en stor utfordring, men blir spesielt utfordrende når den settes i system og kombineres med andre virkemidler. Hensikten er fortsatt å påvirke, men da inngår desinformasjon som ett av flere virkemidler i en større påvirkningsoperasjon. Et eksempel på dette er Russlands respons til avsløringer rundt nedskytingen av Malaysian Airlines Flight 17 over Donetsk i 2014 (Hammond-Errey, 2019).

[1] https://www.facebook.com/LiberalAlliance/posts/3767467526625407

2.2 Hva er en påvirkningsoperasjon?

Påvirkning er i seg selv verken ulovlig eller problematisk, og kan skje gjennom alt fra reklame til TV-debatter. «Alle» gjør det, fra politiske partier og interesseorganisasjoner, til kommersielle bedrifter og kommunikasjonsbyråer. Dette er en del av et åpent, demokratisk samfunn. Slik påvirkning er ikke en del av denne rapporten. Med «påvirkningsoperasjon» 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.

Russlands forsøk på å påvirke det amerikanske presidentvalget i 2016 er et godt eksempel på en påvirkningsoperasjon. I ettertid er det identifisert over 10 millioner tweets og bilder fra 3841 falske profiler (Gadde & Roth, 2018) og 3517 Facebook-annonser som til sammen ble sett ca. 146 millioner ganger (Lapowsky, 2018). Analyser viser at operasjonen startet før 2014 (Howard et al., 2018) og er fremdeles pågående. Amerikansk etterretning offentliggjorde 15. mars 2021 en rapport som fastslår at bl.a. Russland forsøkte å påvirke det amerikanske presidentvalget også i 2020 (National Intelligence Council, 2021). Ifølge Oxford Internet Institute, ble 81 land utsatt for politisk propaganda og desinformasjon i 2020 (Norge var ikke med i studien) dette inkluderer intern påvirkning av egen befolkning (Bradshaw et al., 2021). I det enkelte land, fremstår ikke dette nødvendigvis som forsøk på påvirkning utenfra, men som legitim debatt mellom landets innbyggere.

I slike statsstyrte påvirkningsoperasjoner inngår desinformasjon og sosiale medier som sentrale virkemidler, men da som en del av et omfattende økosystem laget for å oppnå maksimal effekt.

Statsstyrte operasjoner forsøker hovedsakelig å undergrave tilliten eller påvirke politiske prosesser i demokratiske samfunn gjennom å forsterke konflikter, spre desinformasjon og konspirasjonsteorier og skape usikkerhet eller likegyldighet til sannhet og fakta. Under covid-19-pandemien i 2020 ble slike desinformasjonstaktikker benyttet av både russiske og kinesiske aktører mot europeiske land, ifølge rapporter fra EU (*EEAS SPECIAL REPORT UPDATE*, 2021). Formålet ser ut til å ha vært å spre uro i befolkningen om hvorvidt demokratiske land kunne håndtere pandemien, og fremheve Russland og Kinas egen håndtering som overlegen.

Statsstyrte, etterretningsdrevne påvirkningsoperasjoner kan 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 (Politiets Sikkerhetstjeneste, 2021):

- 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

For å forstå og håndtere påvirkningsoperasjoner som en del av sammensatte trusler, trengs derfor en tilnærming som går på tvers av tradisjonelle skillelinjer som stats- og samfunnssikkerhet, sivilt-militært, sektorene i norsk statsforvaltning og vår tradisjonelle forståelse av kategoriene fred, krise og krig.

Påvirkningsoperasjoner kan være både åpne og skjulte. Noen har en klar avsender og åpenbar hensikt, mens det med andre er uklart hvem som står bak (om forsøket oppdages) og hva som er intensjonen. De kan også være «falsk flagg»-operasjoner, hvor aktøren utgir seg for å være noen andre. Avanserte påvirkningsoperasjoner benytter gjerne flere metoder i kombinasjon. Spesielt Russland har lang erfaring med det. «Aktivnye meropriyatiya», eller «active measures» er et begrep for politisk krigføring fra russisk doktrine tilbake til 1920-tallets Sovjetunionen og rommer nettopp det vi i dag kaller «sammensatte virkemidler»; påvirkning gjennom desinformasjon, propaganda, villedning, sabotasje og spionasje m.m. (Abrams, 2016; Rid, 2020). Selve fenomenet er med andre ord ikke nytt. Men internett og sosiale medier har åpnet for nye muligheter og større effekt. En ting som ikke har endret seg, er at slike aktiviteter kan pågå i lang tid uten at de blir oppdaget og at skaden de gjør kan være vanskelig å rette opp når den først har skjedd.

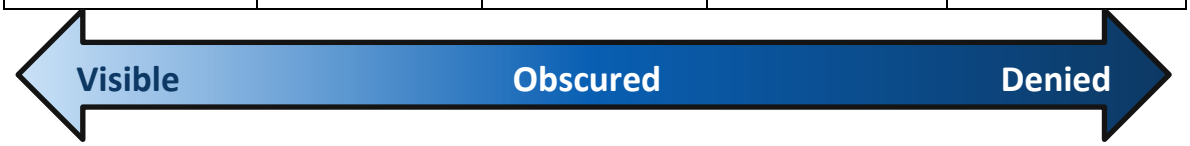
2.3 Hvordan fungerer en påvirkningsoperasjon?

Påvirkningsoperasjoner utføres på ulike måter avhengig av aktør, målgrupper og hensikt. De endrer seg også over tid gjennom teknologisk og politisk utvikling og tilpasning. I tillegg er de opportunistiske av natur ved å raskt utnytte muligheter som oppstår, og benytter flere ulike plattformer, kanaler, teknikker og avsendere med koordinerte tiltak og utspill.

Selv om påvirkningsoperasjoner med utstrakt bruk av desinformasjon via sosiale medier ikke er forbeholdt russiske myndigheter, er Russland, ifølge Etterretningstjenesten og PST, den statlige aktøren som utgjør den største trusselen mot norske interesser på dette området. Måten russiske myndigheter gjør dette på er også etter hvert godt kartlagt og kopieres av andre, og gir verdifull innsikt i sammensatt metodebruk med desinformasjon på sosiale medier som en viktig driver. Det vies derfor ekstra oppmerksomhet til russisk metodikk i denne rapporten, da den gir en god, allmennyttig forståelse for hvordan ulike metoder og virkemidler kan spille sammen for å oppnå størst mulig effekt.

Påvirkningsoperasjoner har blitt stadig mer sofistikerte, og fungerer i dag gjennom et stort økosystem som kan beskrives gjennom fem «pilarer» (Global Engagement Center, 2020) i spekteret fra åpent/offisielt til lukket/fordekt.

Official Government Communications	State-funded Global Messaging	Cultivation of Proxy Sources	Weaponization of Social Media	Cyber-Enabled Disinformation
• Kremlin or Ministry Statement • Official Russian social media post • Statement or quote by Russian official	• State-funded, foreign-facing media • State-funded, domestic-facing media • Foreign-based, Russian state-funded media • International Russian socio-cultural institutions	• Russia-aligned outlets with global reach • Local language specific outlets • Witting proliferators of Russian narratives • Unwitting proliferators of Russian narratives • Foreign state narrative amplification	• Infiltration of domestic conversations • Standing campaigns to undermine faith in institutions • Amplification of protests or civil discord	• Hack & Release • Site capture • Cloned websites • Forgeries • Disruption of official sources or objective media



Kobling til Russland

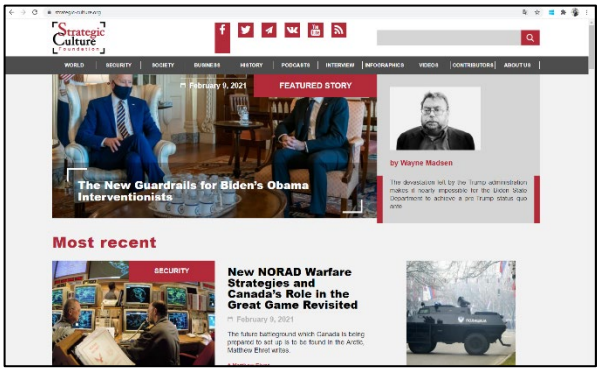
Figur 2.4 De fem pilarene for Russlands desinformasjons- og propaganda økosystem (Global Engagement Center, 2020).

Et eksempel for å illustrere hvordan dette kan fungere i Norge er datainnbruddet på Stortinget i 2020 som PST har attribuert til russisk etterretning (Staff, 2020). Vi vet ennå ikke hva hensikten var, men én av flere mulige hensikter kan ha vært å tilegne seg informasjon eller kompromitterende opplysninger som er egnet til å påvirke den offentlige debatten i Norge i forkant av Stortingsvalget 2021, såkalt «hack & release». Dette er oppskriften russisk etterretning benyttet seg av i forkant av det amerikanske valget i 2016, hvor de brøt seg inn på serverne til det demokratiske partiet og hentet ut informasjon som ble taktisk lekket gjennom bl.a. Wikileaks, ifølge amerikanske myndigheter for å skade Hillary Clintons kandidatur og fremme Donald Trumps (Mueller, 2019).

Dersom noe tilsvarende skulle skje i Norge, kan vi forvente at en taktisk lekkasje av faktisk og/eller forfalsket materiale frigis via en tredjepart og/eller proxy-sider, blir til nyhetssaker i russisk-kontrollerte medier og på andre proxy-sider, spres via sosiale medier og forsterkes gjennom russiske offisielle kanaler som dekkes av andre typer medier, som igjen genererer flere nyhetssaker som igjen spres via sosiale medier og proxy-sider osv. Informasjonen som lekkes, om den er ekte eller forfalsket, vil gjerne struktureres i forkant og slippes gradvis slik at sakene utvikler seg over tid og holdes gjennom flere nyhetssykluser hvor den enes input blir den andres output i en selvforsterkende runddans. Hele økosystemet som vist i figur 2.4 kan dermed benyttes for maksimal effekt. Den

kanskje største effekten i dette tenkte tilfellet kan imidlertid skapes av norsk presse. Flere norske mediehus har uttalt at de ikke utelukker at de vil kunne bruke slik stjålet informasjon dersom den er av stor offentlig interesse, selv om de da samtidig bidrar til å skape nettopp den effekten russiske myndigheter er ute etter (Johansen, 2021). Det finnes gode grunner både for og imot, noe som stiller pressen overfor et krevende dilemma.

Det er verdt å merke seg at pilaren «Cultivation of Proxy Sources» har blitt stadig viktigere for russisk påvirkning, brukt i kombinasjon med sosiale medier. Men også Kina og andre aktører benytter dette i økende grad for å tåkelegge egen rolle og skape et inntrykk av legitimitet gjennom tilsynelatende uavhengige og troverdige kilder. Det finnes en mengde slike tenketanker, organisasjoner og nyhetssider som er enten etablert, finansiert eller på andre måter knyttet til en stats myndigheter/etterretning. Her er to eksempler (Global Engagement Center, 2020):



Figur 2.5 www.strategic-culture.org.

Eies av russisk etterretning, koblet til russisk UD. Faglig journal for vestlige «fringe thinkers», rettet mot vestlig publikum.

Figur 2.6 www.globalresearch.ca

«Canadisk», basert i Montreal. Kvasivitenskapelig plattform for russisk og kinesisk desinfo rettet mot vestlig publikum.

Det finnes også en rekke slike nettsteder som ikke er knyttet til en stat, men som lager og sprer desinformasjon for å skape annonseinntekter. Felles for mange, uavhengig av statlig tilknytning, er at de er på engelsk og er rettet mot et vestlig publikum. De både produserer og videreformidler en blanding av falske og ekte nyheter, falske forskningsrapporter og annet innhold som igjen blir formidlet og delt via sosiale medier, samt ikke minst «alternative medier». Tidvis finner falske nyheter også veien til redaktørstyrte, troverdige medier (Grut, 2020). NRK Betas gjennomgang i 2020 fant flere eksempler i norske medier, men av lav alvorlighetsgrad. For pressen er dette imidlertid en betydelig utfordring; når seriøse medier uforvarende deler desinformasjon (feilinformasjon), bidrar de til at desinformasjonens troverdighet styrkes og effekten av den øker, i tillegg til at pressens legitimitet kan svekkes. Dette kan være et mål i seg selv for aktørene som står bak.

2.4 Sårbarheter

I FFI-rapporten *Tilsiktede handlinger som kan true Norges sikkerhet – scenarioer for politiet, PST og påtalemyndigheten* (2021) beskrives ni scenarioer utviklet på oppdrag fra Justis- og beredskapsdepartementet for å vise hvor og hvordan justis- og beredskapssektoren kan være sårbare for ulike typer operasjoner, hendelser og angrep. Rapporten er gradert og gjengis derfor ikke her. Det er imidlertid verdt å merke seg at påvirkningsoperasjoner er et relevant og sannsynlig virkemiddel i forbindelse i samtlige scenarioer, enten det dreier seg om lavintensitets subversjon, data-angrep, terror eller strategisk overfall.

Påvirkningsoperasjoner rettes gjerne mot samfunnets sårbarheter, uavhengig av sektor. Det trenger ikke være en direkte sammenheng mellom målet og hensikten; påvirkning innenfor én sektor kan gjøres for å oppnå effekt i en annen sektor, på helt andre områder eller på samfunnet som helhet. Dette kompliserer vår evne til å fange opp og forstå at det er et påvirkningsforsøk på gang og hvilken effekt som forsøkes oppnådd.

Scenario-eksempel

Regjeringen foreslår å legge ned flere lokale helsetilbud på mindre steder i Nord-Norge for å heller bygge større kompetansemiljøer ved de større, regionale sykehusene. Forslaget møter stor lokal motstand og skaper mye sinne og engasjement i sosiale medier og regional og nasjonal presse.

Russisk etterretning går inn i denne debatten med falske SoMe-kontoer av tilsynelatende vanlige nordmenn («sokkedukker») som de bruker til å piske opp stemningen på begge sider ved utstrakt bruk av desinformasjon og følelsesmessig engasjerende innhold. Bl.a. «lekkes» et lydopptak (deep fake) av en samtale mellom statsministeren og helseministeren, hvor de fleiper om nordlendinger i nedsettende ordelag.

En av de falske, russiskkontrollerte profilene oppretter Facebook-gruppa «Nordlendinger mot Oslo-eliten», og gir en håndfull av de mest engasjerte medlemmene moderator-rettigheter. Disse kultiveres og motiveres til innsats gjennom smiger over hvor viktige de er for saken («love bombing»). Gruppa får raskt flere titalls tusen medlemmer, hvorav mange nå intetanende vil kunne være «nyttige idioter» som påvirkes direkte og indirekte av russiske påvirkningsagenter til å mobilisere massiv kritikk av myndighetene i Oslo. De trykker t-skjorter, arrangerer demonstrasjoner både i Nord-Norge og foran Stortinget og retter over 2000 koordinerte innsynsforespørsler til Helse- og omsorgsdepartementet på samme dag for å ramme embetsverket.

På grunn av det høye engasjementet i sosiale medier, kaster kommersielt motiverte desinformasjonsaktører seg på for tjene annonsepenger på deling av emosjonelt engasjerende innhold. Dette forsterker effekten av den pågående operasjonen.

I dette eksempelet blir det som startet som et genuint, folkelig engasjement en potent bevegelse som har skapt et høyt konfliktnivå og en betent politisk debatt preget av konspirasjonsteorier og desinformasjon, kuppet av russisk etterretning og forsterket av tredjeparts kommersielle aktører. Deltakerne i Facebook-gruppa og befolkningen for øvrig er uvitende om denne innblandingen. Og vel så viktig: deres engasjement er like fullt genuint og legitimt, og beskyttet av grunnleggende demokratiske verdier som ytringsfrihet, (mer)offentlighetsprinsippet og retten til å samles. Hvordan skal norske myndigheter håndtere dette? En debatt om helsetilbud som i dette tenkte eksempelet faller under Helse- og omsorgsdepartementets (HOD) ansvarsområde, og håndteres der.

Russlands mål med påvirkningen er imidlertid ikke å styrke lokale helsetilbud i Nord-Norge, men å øke den allerede eksisterende misnøyen mot myndighetene i Oslo. Her utnytter russisk etterretning tre kjente konfliktlinjer i det norske samfunnet (sentrum - periferi, nord - sør og folket - «eliten») og forsøker å forsterke disse for å oppnå effekt på en kjent sårbarhet i demokratiske samfunn: tilliten mellom befolkning og myndigheter. Dette må forstås for at myndighetene skal kunne reagere riktig. Evner HOD å identifisere at det er en påvirkningsoperasjon på gang? Selv om dette mistenkes eller bevises, er det ikke sikkert at det er HOD som sitter på de mest effektive tiltakene for å forebygge eller redusere effekten av påvirkningen.

Eksemplet viser at det er likevel nødvendig, om enn ikke tilstrekkelig, for det enkelte departement å identifisere sårbarheter og risikoer innenfor egen sektor, da det gjerne er førstelinjeaktørene i de ulike sektorene som først vil kunne fange opp påvirkningsforsøk.

Påvirkningsoperasjoner kan true alle departementenes måloppnåelse. En påvirkningsaktør kan bidra til at målene blir vanskeligere å nå, men enda enklere og billigere er det å forsøke å påvirke befolkningens inntrykk av det. Fakta taper ofte kampen mot emosjonelt engasjerende historier og troverdige vitner som «beviser» at den er feil. I tillegg kan opplevd gap mellom politikernes virkelighetsbeskrivelse og den virkeligheten man selv opplever bl.a. gjennom sosiale medier, bidra til å svekke tilliten til både politikerne, myndighetene og pressen som rapporterer om det. Hvis man tror at regjeringen lyver eller har en skjult agenda, vil man heller ikke tro på tall og fakta den presenterer. Tvert imot ser man ofte eksempler på at dette blir tatt som bekreftelse på at man har rett.

Her er fire sentrale sårbarheter for det norske samfunnet i møte med trusselen fra desinformasjon og påvirkningsoperasjoner:

2.4.1 Sårbarhet: Den viktige tilliten

Norge er et åpent og velfungerende demokrati som i stor grad er basert på tillit. Per i dag har befolkningen høy tillit både til hverandre, til myndighetene, mediene og demokratiske institusjoner

(Kolsrud, 2021). Denne tilliten gjør oss, som nasjon, sannsynligvis mer robuste mot fremmed påvirkning enn tilfellet vil være i f.eks. USA, hvor tilliten til myndighetene og til hverandre er lavere og forskjeller og motsetninger mellom folk er større. Et generelt høyt utdanningsnivå bidrar også sannsynligvis til økt robusthet mot påvirkning (Seo et al., 2020).

Likevel, det finnes flere grupper i det norske samfunnet som har lav tillit til myndighetene og mediene, og som er spesielt sårbare for påvirkning som kan skape utfordringer for samfunnet - selv om antallet er lite. For eksempel kan en relativt liten gruppe som nekter å følge smittevernråd under koronapandemien forårsake uforholdsmessig store konsekvenser for liv, helse og samfunnet for øvrig.

Tillit er en viktig forutsetning for demokratiet, og nettopp derfor også en sårbarhet. Vi bør derfor være spesielt oppmerksomme på saker, narrativer, hendelser og utviklingstrekk som er egnet til å svekke tilliten befolkningen har til myndighetene, politikere, media og hverandre. Disse oppdages gjerne i sosiale medier først. Hvis tilliten i samfunnet går ned vil det kunne få negativ innvirkning på alt fra politiske prosesser til sikkerhets- og forsvarspolitisk handlingsrom i fred, krise og krig. Russland og Kina benytter påvirkningsoperasjoner blant annet til å forsøke å redusere tilliten andre lands befolkning har til egne myndigheter, andre land (spesielt USA) og institusjoner som Nato, og utnytte den reduserte tilliten til å oppnå egne strategiske mål (Rosenberg et al., 2020).

2.4.2 Sårbarhet: Demokratiske samfunnsverdier

Ytringsfriheten er en av demokratiets bærebjelker, og viktigheten av en åpen, fri og kritisk meningsbrytning er udiskutabel for et demokratis legitimitet. Samtidig er en åpen, offentlig debatt sårbar for å bli manipulert av en påvirkningsaktør. I en situasjon med et hardt debattklima og et sterkt polarisert offentlig ordskifte, kan befolkningen være spesielt sårbar for påvirkningsforsøk i form av desinformasjon, falske nyheter og konspirasjonsteorier.

Større økonomisk eller sosial ulikhet mellom befolkningsgrupper vil sannsynligvis gjøre oss mer sårbare for påvirkning som kan slå en kile i skillelinjer i det norske samfunnet, som fattig - rik, sør - nord, by – land og folket – «eliten». Overordnede temaer fra internasjonale konspirasjonsteorier om en «elite» som kynisk søker makt, innflytelse eller rikdom på bekostning av «folket» er også tilstede i den norske debatten (Anonym, 2021; Dahlback, 2020), og kan forsterkes når man opplever økt ulikhet.

2.4.3 Sårbarhet: Varierende sikkerhetsbevissthet

Økt sikkerhetsbevissthet og –kunnskap trengs både blant organisasjoner og individer i samfunnet generelt, ikke minst i statsforvaltningen, akademia, næringsliv og blant aktørene i totalforsvaret. I 2020 gikk PSTs avdeling for kontra-etterretning ut med hard kritikk av universiteter og høyskoler, som de mener er naive i deres manglende forståelse av hvilken sikkerhetsrisiko det innebærer å tillate studenter fra land som Kina og Iran på studier hvor de får tilgang til sensitiv kunnskap og infrastruktur (Kibar & Engen, 2021). Naive eller ikke, står utdanningsinstitusjonene i et krysspress mellom ulike departementer med ulike prioriteringer. Åpenhet og akademisk frihet må balanseres opp mot økende etterretnings- og spionasjevirksomhet fra fremmede makter, men bevisstheten og

kunnskapen om det siste er varierende i så vel departementer som institusjoner. Et annet ferskt eksempel er forsøket på å selge Bergen Engines til et russisk-eid selskap (NTB, 2021), som synliggjorde utfordringer både mht. anvendelse av sikkerhetsloven og de ulike departementenes forståelse av sikkerhetspolitisk risiko og sårbarhet. Problemstillingen er høyst relevant også for næringsliv, organisasjoner og befolkningen for øvrig.

Sammensatte trusler rettes mot sårbarheter i hele samfunnet, og utfordrer det norske sektorprinsippet. Å foreta sikkerhetspolitiske risiko- og sårbarhetsanalyser knyttet til beslutninger blir derfor relevant for alle departementer og på områder man normalt ikke har tenkt på som relevante i den sammenheng. For eksempel, ble Søreide bedehus utenfor Bergen solgt til den russiskortodokse kirke i 2016 (Rønningen, 2016). Bedehuset har siktlinje rett inn til Sjøforsvarets base på Haakonsvern. Dette trenger ikke bety noe, og er ingen insinuasjon om at det lå andre hensikter bak enn å dekke behovet for et nytt kirkelokale. Men når man vet at den russiskortodokse kirke er tett koblet til den russiske staten og at oppkjøp av strategisk plassert eiendom er en kjent metode for skjult etterretningsvirksomhet, er det en åpenbar sårbarhet dersom slike forhold ikke vurderes. Både offentlige og private aktører bør derfor gjennomføre analyser som en del av sine beslutningsprosesser ved å i hvert fall spørre seg selv; kan denne beslutningen få konsekvenser for norsk sikkerhet eller kunne utnyttes av en påvirkningsaktør? Og hvis ja, hvordan kan dette unngås, reduseres eller håndteres?

Å øke den sikkerhetspolitiske forståelsen og bevisstheten både i statsforvaltningen, i akademia, i næringslivet og i befolkningen kan redusere sårbarheter både mot spionasje, sabotasje, subversjon og påvirkningsoperasjoner.

Til sist er personlig sikkerhetsbevissthet og god sikkerhetskultur viktig. Mange har forhåpentligvis fått med seg at man bør utvise kildekritikk og unngå å trykke på lenker fra ukjente avsendere (Medietilsynet, 2021), men å redusere digital og kognitiv sårbarhet på dette området krever økt kunnskap og bevissthet på individnivå om hvordan påvirkningsaktører opererer og hva de gjerne forsøker å oppnå.

2.4.4 Sårbarhet: Begrenset felles situasjonsforståelse

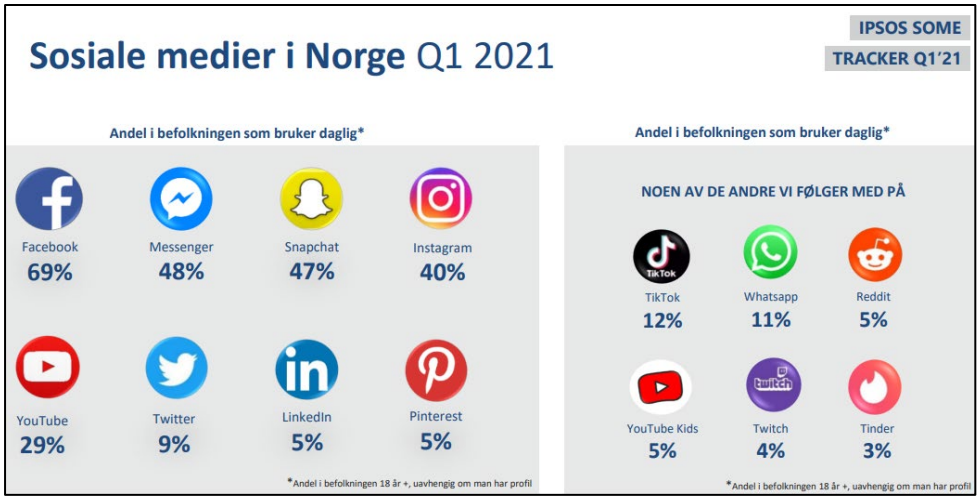
I departementene og etatene er det kommunikasjonsenhetenes ansvar å følge med på hva som skjer i mediene og på sosiale medier innenfor sin sektor. I så måte utgjør de også en naturlig førstelinje for å kunne fange opp forsøk på påvirkning i sosiale medier. Det krever kunnskap om både metoder, sårbarheter og effekter, og til en viss grad også aktører. Det er nødvendig med økt kunnskap i kommunikasjonsenhetene, så vel som i departementene for øvrig, om hvordan man skal fange opp og forebygge uønsket påvirkning. En god situasjonsforståelse i den enkelte sektor er imidlertid ikke tilstrekkelig, som illustrert i eksempelet innledningsvis i dette kapittelet.

Fordi påvirkningsoperasjoner kan være komplekse og vanskelige å oppdage, er Norge som nasjon sårbar hvis vi ikke er i stand til å ha et helhetsbilde på tvers av sektorer. NSM skriver at mangelfull oversikt over verdikjeder og avhengigheter mellom virksomheter og tjenester på tvers av sektorene utgjør en nasjonal sårbarhet i denne sammenhengen (Nasjonal sikkerhetsmyndighet, 2021). Fordi påvirkning innenfor én sektor kan få effekter på helt andre områder, er det avgjørende at

observasjoner og kunnskap aggregeres til en felles situasjonsforståelse på strategisk nivå, og at det her finnes kompetanse, ressurser og verktøy til å kunne gjøre analyser og gi råd om håndtering.

3 Hvilke konkrete plattformer og metoder benyttes i påvirkningsoperasjoner?

3.1 Plattformer



Figur 3.1 Oversikt over sosial medie-bruk i Norge (Ipsos, 2021).

For å forstå hvordan sosiale medier brukes til påvirkning, bør man se det som en del av det overordnede økosystemet for påvirkning som beskrives i figur 2.4. Det som er viktig å forstå er at ulike plattformers karakteristikker gir forskjellige muligheter for å drive påvirkning. Samtidig kan påvirkningsaktører også flytte kampanjer mellom plattformer for å unngå deteksjon.

Norske brukertall er fra Ipsos sosiale medier-tracker (1. kvartal 2021) som vises i figur 3.1 (Ipsos, 2021).

Facebook står i en særklasse blant sosiale medier. Dette er verdens største plattform, med 2.85 milliarder månedlige aktive brukere (Facebook Inc., 2021) og 3,5 millioner norske brukere (83% av befolkningen over 18). Facebook er også unik fordi den tilbyr en rekke funksjoner man ikke nødvendigvis forbinder med sosiale medier, fra kalendere til pengeinnsamling. Dette gjør at den blir benyttet i mange forskjellige sammenhenger og desinformasjon kan nå flere brukere i situasjoner når ens årvåkenhet er lavere. Facebook er også velegnet til påvirkning pga. antall brukere, temabaserte grupper (åpne og lukkede) og massive datasett på brukeres aktiviteter som gjør at man kan treffe svært spesifikke målgrupper. Facebook er godt egnet for å nå eldre målgrupper, og de

over 60 år har ofte ukritisk medieforståelse og kan være mer sårbare for påvirkning (Medietilsynet, 2021).

Twitter er en mikrobloggtjeneste og et nettsamfunn for debatt. Det har 1,1 millioner norske brukere (27% av befolkningen over 18). Twitter er en betydelig plattform bl.a. for politisk debatt og som ressurs for journalister. Plattformen er mye brukt og velegnet til påvirkning pga. stort spredningspotensial forsterket av automatiserte kontoer (bots), direkte tilgang på innflytelsesrike enkeltpersoner og målgrupper, og muligheten til å samle og nå mennesker rundt temaspesifikke emneknagger. Twitter er hyppig brukt til påvirkning (se for eksempel Romano, 2018; Jones, 2019; Kao & Li, 2020).

LinkedIn er et sosialt nettverk for rekruttering, nettverksbygging og diskusjoner om fag og jobb. Det har 1,2 millioner norske brukere (30% av befolkningen over 18), med en høy andel høytlønnede og beslutningstakere i sentrale posisjoner. LinkedIn benyttes blant annet av utenlandske etterretningstjenester til å kartlegge personell og nettverk og til å rekruttere kilder (Parello-Plesner, 2018; Ponniah, 2020; E. Wong, 2019).

Instagram, YouTube, TikTok og andre multimedia-plattformer er sosiale nettverk for deling av bilder og videoer. De har henholdsvis 2,6; 1,8 og 1,2 millioner norske brukere (63, 45 og ukjent prosent over 18). Bruk av bilder og video er svært godt egnet til påvirkning fordi de er effektive emosjonelle triggere (gjelder uavhengig av plattform). En spesifikk variant er *memes*, små humoristiske, visuelle informasjons-snutter som ofte deles mer fordi de er morsomme og aktuelle. Både Instagram og YouTube har blitt benyttet aktivt til påvirkning, spesielt desinformasjon (se for eksempel Kuo, 2020; Faddoul et al., 2020; Frenkel, 2017). TikTok har mye desinformasjon rundt for eksempel covid-19, men viser ingen tegn til å ha blitt brukt for organisert påvirkning. YouTube er spesielt populær blant ungdom og innvandrere, hvorav 53% av sistnevnte bruker plattformen daglig. YouTube er velegnet til påvirkning pga. sin popularitet og algoritmer som serverer brukerne mer av samme type innhold som de ser på. YouTubes algoritmer har ofte ikke klart å stoppe desinformasjon i forbindelse med nyhetssaker (Warzel, 2017).

Telegram, WhatsApp og Signal og andre krypterte meldings-apper. Telegram er russisk-utviklet, WhatsApp eies av Facebook og Signal er en såkalt åpen kildekode-app, utviklet av en non-profit-organisasjon. Alle brukes i Norge. Pga. kryptering gir de beskyttelse mot overvåking og brukes derfor av alt fra politikere og sikkerhetspersonell til terrornettverk og kriminelle i tillegg til vanlige brukere. Det er også mulig å opprette grupper på disse plattformene, noe som kan benyttes til å spre informasjon til større grupperinger uten at det kan oppdages av utenforstående (Walther & McCoy, 2021). Det finnes flere eksempler på spredning av desinformasjon via WhatsApp, som bl.a. førte til voldelige opptøyer i India i 2017 (BBC News, 2018).

Gab, Parler og 4-chan er eksempler på mindre, spesialiserte sosiale medieplattformer, ofte med et fokus på (amerikanske) høyrekonservative eller ekstremister og konspirasjonstilhengere. Antall brukere er svært små i forhold til de største sosiale medie-plattformene, men de tillater ofte åpne og mer ekstreme hatytringer. Selv om de er små kan de bidra til økt polarisering (Crenshaw, 2021), for eksempel økte brukermassen til Parler etter at Twitter og Facebook utestengte president Trump og slo hardere ned på desinformasjon i forbindelse med det amerikanske presidentvalget i 2020 og

stormingen av den amerikanske kongressen 6. januar 2021 (Dzhanova, 2021). Disse plattformene har ukjent utbredelse i Norge. I en påvirkningssammenheng er det usikkert om brukerne av slike plattformer er en direkte målgruppe, men de kan muligens benyttes til å få informasjon inn i andre medier slik som Sintef observerte i sin rapport om kommunevalget i 2019 (Grøtan et al., 2019).

De fleste sosiale medier nevnt her er amerikanskeide, ingen er norske. Dette gir problemer med hensyn til jurisdiksjon og kultur når det gjelder å håndheve norske lover og normer for hva som er akseptable ytringer. Det vil også være praktiske problemer når man melder fra om ulovlige eller falske innlegg, det at man ser verden fra et annet perspektiv betyr at norske bekymringer vil sees på som relativt små, og andre problemer vil prioriteres (J. C. Wong, 2021).

3.2 Metoder

Påvirkningsaktører bruker mange ulike metoder og teknikker, ofte i kombinasjon, for å nå sine mål. Overordnet kan man si at formålet er å få mest mulig oppmerksomhet for et budskap, og at budskapet ikke avfeies. Her er en oversikt over noen vanlige metoder. Engelsk metodenavn benyttes der etablerte norske oversettelser ikke finnes.

METODE	EKSEMPEL
Pseudonymitet Dette dreier seg om å skjule hvem som egentlig står bak innlegg, narrativ og budskap. Anonymitet er en variant av pseudonymitet, men det er mer formålstjenlig for påvirkning om personen/ gruppen som en profil referer fremstår som a) ekte og b) med innsikt som er troverdig, gjerne med spesiell innsikt.	**Astroturfing** Å skjule den egentlige aktøren bak et budskap eller organisasjon slik at engasjementet ser ut til å komme fra, eller være støttet av, grasrotbevegelser. **Sokkedukker** Utgi seg for å være noen andre. Kan gjøres for å skape flere profiler i samme debatt (man kontroller retningen på debatten) eller for å unngå å bli sperret ute fra en gruppe e.l. **Catfishing** Å opprette profiler med falsk identitet på sosiale medier i den hensikt å forlede andre, som regel utvalgte enkeltpersoner. Det er med andre ord mer spisset enn sokkedukker.
Falske responser Manipulasjon av responsen (reaksjoner) på innlegg i sosiale medier vha. bots, massemobilisering av brukere eller kjøpte reaksjoner fra en nettjeneste. Overordnet kan man si at falske responser enten promoterer	**Love bombing** Overøse en eller flere personer med positiv støtte og oppmerksomhet, for å manipulere vedkommendes adferd gjennom økt følelse av tilhørighet og lojalitet. **Trolling** Å kommentere i nettfora, kommentarfelt og sosiale medier med hensikt å provosere fram reaksjoner eller debatter.

informasjon og synspunkter som gagner påvirker eller sverter informasjon og synspunkter som strider mot påvirkers mål.	Benytter ofte ondsinnet retorikk for å undergrave en debatt og undertrykke meningsmotstandere. **Satire og parodi** Latterliggjøring av individer, argumenter eller saker for å undergrave disses legitimitet.
Falsk informasjon Kjernen i påvirkning er informasjon som på forskjellige måter fordreier eller ignorerer fakta, for å promotere noe som gagner den som står bak påvirkningen. Et viktig element er at den falske informasjonen «pakkes inn» i formater som fremstår som troverdig.	**Falske nyheter** Nyheter som fremstilles som ekte, men som er helt eller delvis usanne eller misvisende. Ofte basert på en kjerne av sannhet, og vinklet for å trigge følelser og engasjement. **Manipulerte dokumenter** Innhold som er helt eller delvis fabrikkert eller endret fra sin originale form og fremstilt som autentisk. Flere ganger brukt i forbindelse med eposter som har blitt lekket etter innbrudd i epost-kontoer. **Falsk forskning** Dette kan vær ren forfalskning, men er ofte forskning som tas til inntekt for noe den egentlig ikke diskuterer, eller mindre biter informasjon som tas ut av sammenheng. **Konspirasjonsteorier** Narrativer som hevder at noe skjules fra allmenheten, ofte knyttet til store nyhetssaker, fra månelandingen til hvordan covid-19 startet.
Informasjonsmanipulasjon På samme måte som falske responser søker å støtte egen informasjon er formålet med manipulasjon av informasjon å øke troverdigheten ytterligere.	**Hvitvasking av informasjon** Falsk eller villedende informasjon legitimeres gjennom et nettverk av mellomledd som skjuler opprinnelsen. NRK lager en sak basert på en sak fra CNN. CNN har basert den på uttalelser fra en anerkjent forsker, som referer til en forskningsrapport fra et institutt som er en kamuflert proxy site for kinesiske myndigheter. **Kildeforvrenging** Uriktig kobling av et argument eller synspunkt til en annen person. For eksempel når en offentlig person er bevisst feilsitert eller feilaktig oppgitt som kilde.

3.3 Psykologien bak fenomener på sosiale medier

Metoder og teknikker brukt i sosiale medier virker i påvirkningsøyemed gjennom hvordan vi mennesker fungerer. Dette kapittelet er ment å gi noen eksempler på psykologien bak noen fenomener på sosiale medier (for en mer grundig gjennomgang, se f.eks. Bjørnstad, 2019). Dette dreier seg om hvordan vi tenker og oppfatter (kognitive prosesser og persepsjon), adferd, hvordan følelsene påvirker oss (emosjoner), og den sosiale sammenhengen (sosialpsykologiske faktorer inkludert gruppeprosesser og tilhørighet) – for å nevne noe. Tabellen nedenfor presenterer eksempler og fenomener og noen av de viktigste bakenforliggende psykologiske prosessene (eksemplene/fenomenene er gruppert når de er nært relatert og kan forklares gjennom flere av de samme psykologiske faktorene). Det er ofte mange ulike psykologiske prosesser bak et gitt fenomen på sosiale medier.

PSYKOLOGISKE PROSESSER / FAKTORER	FENOMENER I SOSIALE MEDIER
Bandwagon effect Sosialpsykologiske faktorer som troen på at det mange mener er riktig og ønsket om å være med på/gjøre det samme som det som oppfattes som majoriteten reflekteres blant annet i denne effekten (f. eks. Barnfield, 2020).	Sannsynligheten for at en person **deler innhold** øker når vedkommende ser at den deles av mange. Automatisk genererte profiler (bots), falske profiler og retoriske teknikker kan brukes for å skape inntrykk av at det er mange som deler noe.
Gruppepolarisering Grupper blir mer ekstreme i meninger og adferd basert på manglende motargumenter og ønske om anerkjennelse og tilhørighet i gruppen (se f.eks., Sabini, 1995 for en oversikt). «**Groupthink»** (Janis, 1972) er beslektet og oppstår når ønsket om intern enighet og harmoni går på bekostning av kritisk og konstruktiv meningsbrytning. Gir **falsk konsensus** og beslutningene risikerer å bli dårlige.	Dette ser man for eksempel i **ekkokammer-effekten**, hvor forsterking og/eller radikalisering av meninger og holdninger blant likesinnede i en lukket gruppe, blant annet fordi budskapet deles av andre kombinert med fravær av motforestillinger. Meningene flyttes i mer ekstrem retning. En lokal folkebevegelse mot vindkraftutbygging forener sinte meningsfeller mot utbygging og mot kommunen. Diskusjonen blir unyansert og ensidig.
Bekreftelsestendens Menneskelig tendens til å søke informasjon som bekrefter egne oppfattelser og tolke slik informasjon mer positivt («Confirmation bias», f.eks. Nickerson, 1998).	**Algoritmene** som velger innhold for brukerne på sosiale medie-plattformene er designet nettopp for å utnytte menneskers behov for bekreftelse gjennom å servere innhold som er i tråd med brukerens politiske meninger, interesser og aktiviteter på nett. Algoritmene fanger dermed brukeren i en «boble» (**filterboble**).

Sosiale kontrollmekanismer Mennesker bryr seg om hva andre mener – spesielt de med samme tilhørighet og som man identifiserer seg med gruppen (se f.eks. Sabini, 1995). Generelt promoterer sosiale kontrollmekanismer prososial adferd, men kan også gi usosial adferd hvis dette er frontet av gruppen individet er en del av og identifiserer seg med. Ved **anonymitet** blir de vanlige sosiale kontrollmekanismene borte (f.eks. i kommentarfelt senkes derfor terskelen for å innta ellers ikke sosialt akseptable holdninger og adferd).	**Trolling/nettaggresjon** Aggressiv adferd på nett (anonymisert eller i lukket gruppe). Hets og trusler mot for eksempel politikere i kommentarfelt og sosiale nettverk fører ofte til at disse trekker seg eller slutter å uttale seg om kontroversielle saker.
Sosial kategorisering og gruppetilhørighet Tendens til å oppfatte gruppemedlemmer (inngruppe) mer positivt og som mer heterogene enn de utenfor (utgruppe) (Tajfel et al., 1979). Dekker psykologiske basisbehov som anerkjennelse, tilhørighet og positiv selvoppfattelse.	Det finnes **grupper** for «alt» på sosiale medier. Kan gi enkeltpersoner med hatske meninger og usosial oppførsel en gruppe de kan finne meningsfeller i. Gir dem troen på at det de mener og gjør er «normalt», også når det ligger langt utenfor. Man ser ofte negativ stereotypering av folk som ikke er innenfor samme gruppe på sosial medier. Gruppen kan være definert på basis av hva som helst (meninger, politisk tilhørighet, hat, etc.).
«Persuasion» Persuasjon dreier seg om hvordan man kan påvirke andre gjennom et sett med prinsipper som har vist seg å gi økt sannsynlighet for påvirkning eller overtalelse: like (ofte basert på likhet), resiprositet, sosial bekreftelse/ konsensus, konsistens, autoritet, og knapphet (f.eks. Cialdini, 2001).	Mange av persuasjonsprinsippene ligger bak muligheten for å påvirke gjennom **grupper på sosiale media**. I en gruppe med likesinnede har man mennesker man liker, respekterer, er enig med, som man får positive tilbakemeldinger fra og som man dermed lett lar seg påvirke av. Dette forsterkes av felles gruppetilhørighet.
Attribusjon Hvordan vi forklarer hendelser eller adferd, dvs. attribuerer kausalitet til observert adferd (for en oversikt se f.eks. Fiske & Taylor, 2017). Vi attribuerer både på individ og gruppenivå.	

Fundamental attribusjonsfeil Tendensen til å legge for stor vekt på person istedenfor situasjon når man skal forklare en hendelse (f. eks. Ross, 1977). **«Self-serving», selvsentrerte og defensive attribusjoner** Tendensen til å selv ta æren for suksess, nedtone betydningen av andres innsats/arbeid og til å gi andre skylden hvis noe mislykkes (for en oversikt se f.eks. Fiske & Taylor, 2017). **Falsk konsensus-bias** Antakelsen om at ens egne meninger, tro, verdier og vaner er vanligere i befolkningen enn de egentlig er (f. eks. Ross et al., 1977).	Hvis noen gjør noe vi reagerer på, er vi raske til å knytte handlingen til person/gruppe fremfor å spørre oss selv hva i situasjonen som gjorde at vedkommende valgte å handle på akkurat den måten. Attribusjonsfeilene gjør at mennesker lett kan forledes til å forklare negative hendelser med negative fortolkninger av andre personer eller grupper. Forsterkes av gruppetilhørighet på sosiale medier.
Naiv realisme Troen på at egne fortolkninger er korrekte (f. eks. Pronin et al., 2004).	Frontene i **kommentarfeltene** blir harde (alle mener de har rett).
Heuristikker Kognitive snarveier mennesker er avhengig av for å kunne prosessere store mengder informasjon (f. eks. Chaiken, 1980). Hjernen tilstreber minst mulig innsats (se også «cognitive misers»; Schumann et al., 2012). Bruk av heuristikker betyr mindre grundig tenkning, og oppfattelser basert på heuristikker kan være mer sårbare for påvirkning (f.eks. Chaiken, 1980; Petty & Cacioppo, 1986). Emosjoner (følelser), troverdighet og attraktivitet kan eksempelvis trigge bruk av heuristikker (f. eks. Fiske & Taylor, 2017; Petty et al., 2003).	**Bilder/videoklipp** brukes ofte i alle slags medier for å vekke **følelsene** hos folk. **Karismatiske ledere** har ofte følgere som ikke tenker så nøye igjennom det egentlige budskapet og kan bli mindre kritiske. Effekten av emosjonsvekkende bilder/videoer og karismatiske ledere forsterkes gjennom sosiale medier som for eksempel Facebook og Twitter, hvor følgerne kan få stadig nye oppdateringer/ «holdes varme».
«Framing» Sammenhengen en sak blir presentert i påvirker hvordan den oppfattes (f. eks. Tversky & Kahneman, 1981).	En hendelse kan settes i **positiv eller negativ kontekst** for å påvirke tolkningen. **Falske nyheter** blir ofte forsøkt presentert på samme måte som reelle nyheter for å øke sannsynligheten for at de oppfattes som reelle.

«Priming» Priming handler om å aktivere minner, slik at de blir mer **tilgjengelige** (f.eks. Fiske & Taylor, 2017). Aktiverte minner kan farge oppfattelsen av saker som kommer opp, vurderingen av hvor sannsynlig noe er, osv.	Negative rykter på sosiale medier kan brukes for å påvirke befolkningen til å oppfatte en sak eller person på en negativ måte. Kan for eksempel brukes under en valgkamp. Etter bomben i regjeringskvartalet 22. juli 2011, antok mange at det var ekstreme islamister som stod bak fordi dette er gruppen som oftest har blitt knyttet til terror i mediene de seneste år. Hatprat i kommentarfelt kan lede leserne til å tro det er mer hat i samfunnet enn det reelt sett er. (Den moderate majoritets fravær i mange kommentarfelt forsterker effekten).
«Base-rate Fallacy» Menneskers tendens til å vektlegge kasushistorier fremfor statistisk eller generell informasjon (f. eks. Fiske & Taylor, 2017).	**Kasushistorier** brukes i alle slags medier for å skape engasjement for en sak. Kan få ekstra personlig tilsnitt og effekt når de blir delt av venner eller noen som tilhører samme sosiale nettgruppe.

4 Hvem kan forsøke å påvirke Norge og hvorfor?

4.1 Aktører

Etterretningstjenesten og PST har spesielt pekt på at fremmede stater, først og fremst Russland og Kina, men også Iran og Pakistan, forsøker å påvirke Norge. Men også utenlandske og nasjonale politiske bevegelser, terrororganisasjoner og interessegrupper kan forsøke å påvirke norsk opinion gjennom bruk av desinformasjon og illegitime metoder vi kjenner fra påvirkningsoperasjoner.

Det er imidlertid viktig å understreke at uønsket påvirkning, spesielt gjennom spredning av desinformasjon, ikke behøver å ha som mål å påvirke Norge eller norske interesser selv om det kan være en (bi)effekt. En rekke aktører produserer og distribuerer desinformasjon av økonomiske grunner, da det genererer mye datatrafikk og derfor også inntekter (Soares & Davey-Attlee, 2017).

4.1.1 Fremmede stater: Russland

Russland trekkes frem av norske sikkerhetstjenester som den aktøren som har størst påvirkningsaktivitet rettet mot Norge. Det kan i særlig grad være interessant for Russland å påvirke holdninger i den norske befolkningen og Norges posisjon i internasjonal politikk, grunnet den geostrategiske plasseringen Norge har som naboland og Natomedlem, og for tiden også som medlem av FNs sikkerhetsråd. Russisk påvirkningsaktivitet er godt dokumentert, og har sannsynligvis som mål å svekke vestlige demokratier gjennom økt polarisering, svekkelse av tilliten i befolkningen og til myndighetene og undergraving og manipulasjon av virkelighetsoppfatningen til både egen og andre lands befolkning. I tillegg benytter Russland desinformajon til å tåkelegge egne aktiviteter og folkerettsbrudd, som vist ved den ulovlige annekteringen av Krim og nedskytingen av Malaysian Airlines Flight 17 over Donetsk i 2014, den vedvarende destabiliseringen av Øst-Ukraina, forgiftningen av Sergej Skripal og hans datter i 2018 og en rekke andre eksempler.

I 2020 gikk den norske regjering til det skritt å peke på Russland som den aktøren som stod bak datainnbruddet på Stortinget samme år (Staff, 2020). PST konkluderte senere med at en undergruppe tilhørende GRU (den militære etterretningsorganisasjonen i Russland), kalt Fancy Bear eller APT-28, sannsynligvis sto bak angrepet. Videre er russiske myndigheter og personell ved den russiske ambassaden i Oslo aktive, både gjennom diplomati, etterretning, lobbyvirksomhet og aktivitet i redaksjonelle og sosiale medier. Russiske etterretningstjenester, som GRU og SVR (utenlandstjenesten) har høy etterretnings- og påvirkningsaktivitet i det digitale rom.

4.1.2 Fremmede stater: Kina

Etterretningstjenesten peker på at også Kina gjør framstøt for å påvirke politiske prosesser i vestlige land. Kina har lenge benyttet seg av en lang rekke virkemidler for påvirkning, spesielt bruk av økonomiske maktmidler, og har de siste 2-3 årene i økende grad tatt i bruk desinformasjon på internasjonale sosiale medier (Hamilton & Ohlberg, 2020).

I august 2019 stengte Facebook og Twitter henholdsvis 1000 og 200.000 kinesiske kontoer som blant annet ble brukt til å sverte demokratiforkjempere i Hong Kong (Facebook Inc., 2019). Kinas bruk av desinformasjon på sosiale medier har hatt et oppsving som følge av koronapandemien. I juni 2020 stengte Twitter ytterligere 170.000 kontoer knyttet til kinesiske påvirkningsnettverk som ble brukt blant annet til å fremme Kinas håndtering av covid-19-pandemien og skape tvil om dets opprinnelse (BBC News, 2020b).

Kinesiske myndigheter går ofte hardt ut mot kritikk av Kina, og benytter sosiale medier til å utøve målrettet press mot både andre stater, organisasjoner og enkeltpersoner. For eksempel har Sverige fått merke dette de siste årene etter at svenske myndigheter kritiserte Kina for pågripelsen av en svensk statsborger (Jerdén & Bohman, 2019). I 2020 uttalte en samlet svensk presse at Kina fortsetter å angripe uavhengig journalistikk, svenske medieforetak og svenske forlag, og ba den svenske regjeringen gå sammen med EU for å reagere mot Kinas forsøk på å påvirke pressefriheten (Utgivarna, 2020).

Kina har i flere tilfeller påvirket egen befolkning til å angripe konkrete mål på sosiale medier, noe som både tåkelegger hvem som står bak og skaper inntrykk av et folkelig engasjement (Bergh, 2020).

Der hvor russisk påvirkning ofte forsøker å skape splid, har Kina først og fremst forsøkt å bruke påvirkning til å posisjonere seg selv som en ideologisk og økonomisk stormakt. Dette henger sammen med landets øvrige innsats for å øke egen makt og innflytelse. De siste par årene har kinesiske operasjoner imidlertid i større grad også kopiert russiske metoder som å spre motstridende desinformasjon for å så splid internt i andre land og svekke særlig USAs posisjon i land i Asia (et eksempel er Tang, 2021).

4.1.3 Politiske partier, grupper og enkeltpersoner

I et åpent og velfungerende demokrati som Norge, hvor befolkningen generelt har tillit til myndighetene og politiske prosesser, er det i dag mindre sannsynlig at de etablerte partiene eller politikerne bevisst benytter desinformasjon på sosiale medier, spesielt i et omfang hvor det kan true samfunnets sårbarheter. Et eksempel på hvordan dette kan utspille seg, er tidligere president Trumps stadige løgner og angrep på pressen og demokratiske institusjoner i sitt eget land.

Det kan imidlertid være ulike oppfatninger om hvor grensen skal gå for hva som er et politisk spisset budskap og når det kan kategoriseres som desinformasjon. I 2018 spurte Sylvi Listhaug (Frp) retorisk på Facebook om Arbeiderpartiet og byrådet i Oslo ikke eide skam, fordi de kastet ut gråtende eldre beboere fra St. Hallvardshjemmet for å tilby overnatting til romfolk. Påstanden ble tilbakevist av faktisk.no. Sannheten var at St. Hallvardshjemmet uansett skulle legges ned og beboerne hadde flyttet ut et halvt år tidligere. Beslutningen ble forøvrig tatt av Kirkens bymisjon, ikke byrådet.

Meldingen er et godt eksempel på hvordan mis- og desinformasjon kan konstrueres ved å sette sammen sanne, halvsanne og/eller usanne forhold på en måte som i sum forteller en følelsesladet, villedende historie egnet til å skape konflikt eller påvirke folks virkelighetsforståelse.

Det kan imidlertid ikke utelukkes at andre grupper med politiske eller ideologiske mål kan benytte desinformasjon i sosiale medier for å påvirke befolkningen eller beslutningstakere. Med sosiale medier har det også blitt enkelt å danne en gruppe av politiske eller ideologiske meningsfeller og mobilisere disse til handling, som å spre desinformasjon.

4.1.4 Særinteressegrupper og kommersielle organisasjoner

Desinformasjon om enkeltsaker kan lages og spres av en rekke ulike aktører, fra kjendiser og aktivister til grupper og organisasjoner for eller imot enkeltsaker. Man kan se for seg at enkelte aktivistgrupper knyttet til kontroversielle temaer som klima, innvandring, vindkraft, bompenger, vaksiner m.m. kan benytte desinformasjon som en del av sin strategi for å nå sine mål, uten at dette har vært undersøkt konkret til denne rapporten. Slike grupper kan også leie eksterne byråer for å hjelpe seg. For eksempel, avslørte en etterforskning i 2020 at den amerikanske tenketanken *Heartland Institute* støttet klimafornektere i Tyskland med å undergrave den tyske regjeringens

klimatiltak, og man fant en forbindelse mellom de tyske klimafornekterne og det tyske ytre-høyre-partiet AfD (Alternative für Deutschland) (CORRECTIV & Frontal21, 2020). Slik kan ulike aktørers interesser spille på lag og tåkelegge hvem som står bak hva.

4.1.5 Terrororganisasjoner

Terrororganisasjoner benytter aktivt desinformasjon og manipulasjon gjennom sosiale medier for å påvirke virkelighetsoppfatningen til ulike befolkningsgrupper, rekruttere medlemmer, oppmuntre til terrorhandlinger og/eller bygge sin egen «organisasjonskultur» blant sine tilhengere. Terrororganisasjonen ISIL var på sitt sterkeste kjent for sin profesjonelle propaganda og effektive bruk av sosiale medier (Gates & Podder, 2015). Høyreekstreme og andre radikale organisasjoner benytter sosiale medier og desinformasjon som sentrale virkemidler for å nå sine mål. Både Anders Behring Breivik og Philip Manshaus ble til dels radikalisert gjennom internett. Lukkede fora i sosiale medier og på diskusjonsplattformer, og ekkokammereffektene de medfører, er spesielt potente når det gjelder radikalisering.

4.2 Motiver

Motivene til en påvirkningsaktør vil variere. Mens fremmede stater gjerne bruker desinformasjon og påvirkning til å styrke sin innflytelse og skape bedre forutsetninger for å oppnå egne strategiske mål, kan andre aktører ha som mål å få gjennomslag for enkeltsaker, rekruttere personell, tjene penger eller skape kaos.

4.2.1 Økt makt og innflytelse

De praktiske aspektene av statsorganiserte operasjoner kan utføres både av statlige og ikke-statlige aktører, og kan bruke en mengde ulike verktøy i kombinasjon i hele spennet fra åpen og offentlig til skjult og fordekt. Desinformasjon brukes aktivt til å øke splittelser og undergrave befolkningens tillit til myndighetene og mellom grupper i samfunnet, tåkelegge egne handlinger, skape forvirring og villedning og/eller forsøke å svekke andre staters innflytelse på tema eller i regioner. En svekkelse av vestlige demokratier kan i neste omgang føre til en svekkelse også av multinasjonale, demokratiske institusjoner som EU og Nato. Også politiske/ideologiske organisasjoner kan ha økt makt og innflytelse som motiv.

4.2.2 Gjennomslag for enkeltsaker

Spesielt for særinteressegrupper som har én kampsak, kan motivet være å få gjennomslag for denne, hvor desinformasjon benyttes til påvirke befolkningsgrupper eller beslutningstakere. Gjennomslag for enkeltsaker som motiv henger gjerne sammen med et motiv om økt makt og innflytelse.

4.2.3 Økonomisk gevinst

Det finnes et helt økosystem av aktører på sosiale medier som benytter falske nyhetssider og profiler og samme type verktøy og virkemidler for å tjene penger. Falske nyheter og desinformasjon er designet for å trigge en emosjonell respons, og sprer seg seks ganger raskere enn vanlige nyheter

(Vosoughi et al., 2018). Derfor er spredningen både effektiv og inntektsbringende. Sensitiv informasjon skaffet til veie gjennom datainnbrudd kan selges eller brukes til utpressing. Selv om motivasjonen til disse aktørene er økonomisk, kan desinformasjonen de sprer også bidra til den splittende effekten i samfunn som statlige aktører er ute etter, da konfliktlinjene og temaene som utnyttes gjerne er de samme. I så måte kan økonomiske motiverte aktører bidra til å forsterke fremmedstatlig påvirkning, selv om de ikke trenger å ha noe med hverandre å gjøre.

Fremmede stater og andre aktører kan også kjøpe kampanjer for å utøve påvirkning fra uavhengige byråer som har spesialisert seg på dette (Mittermaier et al., 2020). Da tåkelegges opprinnelsen ytterligere, og motivene bak en operasjon kan f.eks. både være økt makt og innflytelse (oppdragsgiverens mål) og økonomisk gevinst (byråets mål).

4.2.4 For å diskreditere

Desinformasjon, spesielt gjennom direkte, målrettede operasjoner, er egnet til å undergrave andres troverdighet. Politikere og fageksperter er spesielt sårbare her, da undergraving av deres troverdighet også kan undergrave tilliten til myndighetene eller institusjonen de jobber for. Målet i seg selv trenger imidlertid ikke være å diskreditere den aktuelle aktøren, men å påvirke en målgruppes holdninger eller handlinger for å oppnå noe annet som er til egen fordel. For eksempel, undergraving av NRK gjennom hacking, kloning og desinformasjon kan være egnet ikke bare til å svekke NRKs troverdighet, men til å samtidig lokke målgruppa over på andre, alternative nyhetsplattformer. Statlige, ideologiske og saksspesifikke påvirkningsaktører kan gjøre dette for å øke og samle målgruppa for sin egen strategiske påvirkning, mens en økonomisk motivert aktør kan gjøre det for å generere mer trafikk og annonseinntekter.

4.2.5 Fordi jeg kan

Først og fremst et fenomen innen hacking, men også relevant for påvirkning. Å oppnå effekt gjennom påvirkning og desinformasjon krever et bredt sett kunnskap og ferdigheter både innen teknologi, politikk, historie, samfunnsforhold og psykologi. Nettopp fordi det er krevende, kan dette være en interessant utfordring for enkelte personer og grupper, spesielt i kombinasjon med økonomisk gevinst. Selv om motivet til en «fordi jeg kan»-aktør kan være helt eller delvis å se om man får til noe vanskelig, kan aktivitetene denne gjennomfører bidra til å direkte eller indirekte støtte opp om fremmedstatlige påvirkningsoperasjoner, uten at dette er hensikten.

5 Hvilke tiltak bør vurderes for å gjøre samfunnet mer robust mot uønsket påvirkning i sosiale medier?

Å begrense eller stoppe uønsket påvirkning i sosiale medier er svært krevende. Selv om de store teknologiplattformene nå er under økende politisk press både fra EU og USA og selv har begynt å

forsøke å bekjempe desinformasjon på ulike måter, er det usikkert hvor effektivt dette vil være. Covid-19-infodemien har vist at plattformene gjør mye for å fjerne desinformasjon, men den har også vist begrensingene for deres tilnærminger (Colliver & King, 2020). I tillegg vil påvirkningsaktørene tilpasse metoder og virkemidler etter de til enhver tids rådende muligheter. FFI-rapporten *Påvirkningsoperasjoner i sosiale medier – oversikt og utfordringer* (Bergh, 2020) konkluderte med at det per i dag er vanskelig å stoppe påvirkningsoperasjoner direkte. En mer egnet tilnærming er å heller forsøke å begrense effektene av dem. Det krever kunnskap, verktøy, ressurser og en målrettet, statlig satsning.

FFI anbefaler at Norge utvikler en kunnskapsbasert strategi for håndtering av påvirkning i rammen av totalforsvaret, med konkrete, finansierte planer for å forebygge og håndtere problemer som kan oppstå som et resultat av cyber-sosiale påvirkningsforsøk. Som et utgangspunkt for en slik strategi bør man først identifisere egne sårbarheter og hvordan en aktør kan utnytte dem. Når det gjelder nasjonal sårbarhet mht. nasjonal sikkerhet, har FFI skrevet en egen rapport om dette, *Defence against foreign influence – a value-based approach to define and assess harm, and to direct defence measures* (Kveberg et al., 2019). FFI viser også til den tidligere nevnte graderte rapporten FFI skrev på oppdrag fra Justis- og beredskapsdepartementet, *Tilsiktede handlinger som kan true Norges sikkerhet – scenarioer for politiet, PST og påtalemyndigheten* (2021).

Anbefalte tiltak:

1. **Risiko- og sårbarhetsanalyse (ROS eller Center of Gravity).** Hva er Norges sårbarheter som samfunn? Nevnte eksempler er tillit i befolkningen og til myndighetene, demokratiske verdier og lav/ulik sikkerhetspolitisk forståelse blant aktørene i totalforsvaret. Sårbarheter kan også være knyttet til samfunnskritiske funksjoner og grunnleggende nasjonale funksjoner (GNF). I tillegg til en overordnet, nasjonal analyse bør hvert departement gjennomføre risiko- og sårbarhetsanalyser for sin sektor. Når sårbarheter er kartlagt, vil de danne grunnlaget for å identifisere ytterligere tiltak for å redusere dem. De følgende tiltak anbefales likevel uavhengig av dette.

2. **Identifisere tema og saker som er egnet til påvirkning.** Dette er gjerne temaer som skaper mye engasjement og hvor det allerede eksisterer konflikt. Innvandring og klimatiltak er to eksempler. Nå under koronapandemien er også myndighetenes smitteverntiltak godt egnet. Noen tema kan være av nasjonal relevans, andre mer lokale. Noen kan også være veldig konkrete og med direkte sikkerhetspolitisk betydning, f.eks. knyttet til Svalbard eller Norges medlemskap i Nato eller EØS. En risiko- og sårbarhetsanalyse vil sannsynligvis avdekke flere og vekte dem ut ifra sannsynlighet og skadepotensial.

3. **Avklaring av roller, ansvar og myndighet.** Hvem har det overordnede ansvaret for å beskytte Norge mot uønsket påvirkning, på tvers av sektorer? Hvilket ansvar ligger på nasjonale, regionale og lokale myndigheter, på de ulike sikkerhetstjenestene og på aktørene i totalforsvaret? Er ansvaret kjent og er det gitt tilstrekkelige forutsetninger, mandat og ressurser til å lykkes? Er dagens funksjoner, prosesser og rutiner i myndighetsapparatet tilstrekkelig?

4. **Etablering av en egnet funksjon.** Det bør etableres en permanent funksjon på strategisk nivå som kan sikre felles situasjonsforståelse og bedre kunnskap på tvers av sektorer og – ved behov - samordning av forebygging og mottiltak i alle ledd, offentlig og privat, sivilt og militært. Land det er naturlig å sammenligne oss med, inkl. nære allierte som USA og Storbritannia, men også Danmark, Finland og Sverige, har gode erfaringer med ulike løsninger for det.

   Sverige oppretter i disse dager en egen myndighet for psykologisk forsvar som skal være på plass i januar 2022, og skal ha følgende oppgaver (Psykförsvarsutredningen, 2020):

   - Identifisere, analysere og gi støtte i møtet med uønsket informasjonspåvirkning og annen villedende informasjon som rettes mot Sverige eller svenske interesser.

   - Bedrive utdanning og øvingsvirksomhet innen myndighetenes ansvarsområde.

   - Sørge for samvirke mellom myndigheter og øvrige aktører i det forebyggende arbeidet, samt skape forutsetninger for – og bidra til – å sikre samordnet operativ håndtering.

5. **Utvikle og implementere metoder for å avdekke og håndtere desinformasjon.** Det finnes flere ulike tilnærminger, da dette er et felt i stadig utvikling. Det vil være forskjellige behov hos ulike aktører. Kommunikasjonsutøvere, for eksempel, vil ha mindre nytte av attribusjon, noe som kan være svært viktig innen etterretningsarbeid. Storbritannia har utviklet en egen modell for de som jobber med strategisk kommunikasjon, *RESIST – counter-disinformation toolkit,* som er ment å benyttes på tvers av britiske departementer (Pamment et al., 2020). Dette har blitt vurdert og oversatt til norsk av den Forsvarsdepartementsledede Depstrat-gruppa høsten 2020 og er delt med departementenes kommunikasjonsenheter. Men det finnes andre modeller enn RESIST som bør vurderes om er egnet. Andre relevante eksempler som går utover ren desinformasjon inkluderer FFIs *Situasjonsforståelse ved sammensatte trusler* (2021) (Malerud et al., 2021) og *The EU Cyber Diplomacy Toolbox*.

6. **Utvikle og implementere egnede digitale verktøy.** Grunnet enorme mengder data og påvirkningsoperasjoners skjulte natur, trengs det digitale verktøy for å fange opp og analysere påvirkningsforsøk – innenfor rammene av personvernforordningen (GDPR) og norsk lov. Det finnes flere kommersielle verktøy, men en foreløpig gjennomgang FFI gjorde høsten 2020 (Bergh, 2021), viser at de fleste ser ut til å ha begrensninger som kan gjøre dem mindre egnede, enten pga. begrenset funksjonalitet, rettigheter eller sikkerhet. For å sikre norske myndigheters evne til å fange opp og håndtere påvirkningsoperasjoner både i fred, krise og krig, er det viktig at både selve verktøyet og serverne det kjøres på er under nasjonal kontroll og eierskap. FFI har utviklet en demonstrator for et slikt verktøy (Bergh, 2019).

7. **Øke motstandsdyktighet i befolkningen.** Norske elever har lavere kompetanse på kildekritikk enn svenske, danske og finske elever. En undersøkelse fra 2021 viser at kun 2 av 10 unge mener de kan skille ut falske nyheter, og et fåtall gjør noe for å sjekke om det de

mistenker er en falsk nyhet faktisk er det (Medietilsynet, 2020). Finland har siden 2014 hatt et «anti fake news»-prosjekt der opplæring av den allmenne befolkningen, samt studenter, journalister og politikere skal gjøre dem robuste i møte med desinformasjon (Mackintosh, 2019). Finland rangeres på topp av 35 europeiske land målt på robusthet mot desinformasjon, på grunn av kvaliteten på utdanning, pressefrihet og høy tillit i befolkningen (Lessenski, 2021). Det tyder på at bred kompetanseheving fra tidlig alder og til hele befolkningen og konkrete yrkesgrupper har effekt. Utdanning i skolen er viktig, men samtidig er det i Norge gruppa over 60 år som peker seg ut som dem med mest ukritisk bruk av sosiale medier og lavest kompetanse på desinformasjon, og som burde få en kompetanseheving (Medietilsynet, 2021). Både Faktisk.no og Medietilsynet har egne opplegg for undervisning og opplæring.

8. **Øke motstandsdyktighet i departementer, etater og aktørene i totalforsvaret.** Personell som arbeider i virksomheter som er en del av totalforsvaret (både sivilt og militært personell) bør forstå hvilke særskilte sikkerhetstrusler- og utfordringer som er relevante for dem, inkludert påvirkning og desinformasjon. Hensikten er både å sette dem i stand til å fange opp påvirkning, men også å skape forutsetninger for at det gjøres gode vurderinger av risiko knyttet til beslutninger. Opplæring og bevisstgjøring av dette personellet bør være spesielt tilpasset deres roller. Trening og øving på håndtering av påvirkning bør prioriteres både som egne øvelser (skrivebordsøvelser) og som en del av mediespillet under felles øvelser. FFI jobber sammen med NTNUs «Norwegian Cyber Range» for å utvikle en simuleringsløsning for Facebook, Twitter, Instagram, YouTube og nettaviser, hvor både sivilt og militært personell kan øve mest mulig realistisk.

9. **Aktivt påvirke teknologiselskapene som eier SoMe-plattformer**. Forretningsmodellen til de fleste store sosiale mediene er basert på å innhente mest mulig data om brukerne og få disse til å bruke plattformene så ofte og så mye som mulig. Algoritmene som styrer brukeropplevelsen er derfor designet for å presentere den enkelte bruker med innhold som er egnet til å oppnå dette, og dette innholdet er gjerne det som bekrefter og forsterker eksisterende syn og/eller er egnet til å vekke engasjement og sterke følelser. Dette utnyttes bevisst av påvirkningsaktører, som dermed får stor drahjelp av plattformene i å oppnå sine mål. De siste par årene har store selskaper som bl.a. Facebook, Twitter og Instagram gjort flere grep for å begrense spredningen av desinformasjon og slette falske kontoer etter påtrykk fra blant annet amerikanske myndigheter og EU. Dette har hatt begrenset effekt. Jo flere myndigheter og organisasjoner som står sammen, desto større er sannsynligvis sjansen for å skape nødvendige endringer. EUs «Digital Services Act» kan bli et viktig virkemiddel i fremtiden (Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC, 2020).

10. **Forskning og løpende kunnskapsproduksjon.** Desinformasjon og påvirkningsoperasjoner blir stadig mer avanserte. Det utvikles hele tiden nye metoder og virkemidler, muliggjort av den teknologiske og politiske utviklingen. Denne typen operasjoner går på tvers av både de tradisjonelle skillene mellom statssikkerhet og samfunnssikkerhet og ansvarsområdene i sektorprinsippet, og utfordrer vår tradisjonelle forståelse av grensene mellom fred, krise og

krig. Dette er en utfordring som stiller nye og høyere krav til samhandling, kunnskapsutveksling og håndtering på tvers av tradisjonelle roller og ansvarslinjer for å sikre norske myndigheters evne til å ta riktige beslutninger til rett tid og unngå å komme i en situasjon som begrenser politisk, militært eller faglig handlingsrom. Som en del av en kunnskapsbasert strategi for håndtering, anbefales følgende:

- Kontinuerlig forskning og kunnskapsbygging, siden regelverk for, og bruk av, sosiale plattformer er i en rivende utvikling og nye påvirkningsmetoder utvikles kontinuerlig.

- Styrke forståelse og forskning på teknologiske trender og muligheter som vil påvirke sosiale medier og bruken av disse, inkludert utfordringer og sårbarheter, prediksjon og sikkerhetspolitisk utvikling innen teknologi, menneske og informasjonsmiljøet.

- Videreutvikle og vedlikeholde kunnskapen om bruk og effekt av kommunikasjon som et strategisk virkemiddel i fred, krise og krig, både defensivt og offensivt.

- Styrke kunnskap om langtidseffektene som des- og feilinformasjon i sosiale medier kan ha på nasjonal sikkerhet. Spesielt med tanke på at ulike aktørers anstrengelser for å skade Norge samles og forsterkes gjennom sosiale medier på en historisk unik måte.

- Deteksjon av trender, deriblant spesifikke narrativer i desinformasjon, i sosiale medier bør være en prioritet. Egnede digitale verktøy bør utvikles og deles på tvers av sektorer og nivåer i statsforvaltningen.

- Styrke kunnskap og forskning på sikkerhetskultur og –kompetanse blant relevante og utsatte målgrupper for å avdekke årsaker til (potensielle) brudd på sikkerhetsreglement og for å minske sårbarhet.

Robusthet bør bygges opp ikke bare på regjeringsnivå, og ikke bare i enkelte sektorer. Myndighetene bør være i stand til å forebygge, fange opp, forstå og håndtere påvirkning mot samfunnet på lokalt nivå på tvers av sektorer. Den enkelte sektor bør være i stand til å forebygge, fange opp og forstå påvirkning innenfor sine ansvarsområder og sørge for at kunnskapen aggregeres til strategisk nivå i myndighetsapparatet. Og den enkelte innbygger bør ha kunnskap nok til å være i stand til å utøve kritisk tenkning og kildekritikk.

Referanser

Abrams, S. (2016). Beyond Propaganda: Soviet Active Measures in Putin's Russia. *Connections*, *15*(1), 5–31.

Anonym. (2021, February 5). *Ingenting tilsa at kjæresten min skulle ende opp med å tro på konspirasjonsteorier*. Nettavisen. https://www.nettavisen.no/5-95-175929

Barnfield, M. (2020). Think twice before jumping on the bandwagon: Clarifying concepts in research on the bandwagon effect. *Political Studies Review*, *18*(4), 553–574.

BBC News. (2018, June 11). India WhatsApp 'child kidnap' rumours claim two more victims. *BBC News*. https://www.bbc.com/news/world-asia-india-44435127

BBC News. (2020a, May 24). Coronavirus: Derby 5G phone mast set on fire. *BBC News*. https://www.bbc.com/news/uk-england-derbyshire-52790399

BBC News. (2020b, June 12). Coronavirus: Twitter removes more than 170,000 pro-China accounts. *BBC News*. https://www.bbc.com/news/business-53018455

Bergh, A. (2019). Massage the message: Modularising software for influence operation detection in social media. *24th ICCRTS*. 24th International Command and Control Research and Technology Symposium 2015, Maryland, USA. http://www.dodccrp-test.org/s/071.pdf

Bergh, A. (2020). *Påvirkningsoperasjoner i sosiale medier—Oversikt og utfordringer* (FFI-rapport No. 20/01694; p. 58). Norwegian Defence Research Establishment (FFI). http://hdl.handle.net/20.500.12242/2724

Bergh, A. (2021). Are you seeing what I am seeing? Ensuring data relevance for online information environment assessments. In R. Gill & R. Goolsby (Eds.), *Covid-19 and disinformation*.

Bjørnstad, A. L. (2019). *Understanding influence in a defense context: A review of relevant research from the field of psychology* (FFI-Rapport No. 19/01224). FFI.

Bradshaw, S., Bailey, H., & Howard, P. (2021). *Industrialized Disinformation: 2020 Global Inventory of Organised Social Media Manipulation. Working Paper 2021.1. Oxford, UK: Project on Computational Propaganda.* (Working Paper 2021.1). Project on Computational Propaganda, Oxford University. https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/127/2021/02/CyberTroop-Report20-Draft9.pdf

Buggeland, S. A. (2020, September 22). *Forsvarsmøte forsøkt kapret på Facebook*. VG. https://www.vg.no/i/kRaXGX

Chaiken, S. (1980). Heuristic versus systematic information processing and the use of source versus message cues in persuasion. *Journal of Personality and Social Psychology*, *39*(5), 752.

Cialdini, R. B. (2001). Harnessing the Science of Persuasion A Conversation with Mark Morris. *Harv. Bus. Rev*, *R0109D*, 72–79.

Colliver, C., & King, J. (2020). *Coronavirus and Crisis Management on Social Media Platforms* (p. 38). Institute for Strategic Dialogue.

CORRECTIV, & Frontal21. (2020, February 11). The Heartland Lobby. *Correctiv.Org*. https://correctiv.org/en/top-stories-en/2020/02/11/the-heartland-lobby/

Crenshaw, M. (2021, February 10). I've Studied Terrorism for Over 40 Years. Let's Talk About What Comes Next. *The New York Times*. https://www.nytimes.com/2021/02/10/opinion/capitol-terrorism-right-wing-proud-boys.html

Dahlback, M. L. (2020). *Dette er QAnon i Norge*. Faktisk.no. https://www.faktisk.no/artikler/RZR/dette-er-qanon-i-norge

Det Kongelige Forsvarsdepartement. (2020). *Vilje til beredskap – evne til forsvar. Langtidsplan for forsvarssektoren*. Regjeringen Solberg. https://www.regjeringen.no/contentassets/b43ae5a187034670adc96a83fbf79651/no/pdfs/prp201920200062000dddpdfs.pdf

Dzhanova, Y. (2021). *Top conservative figures are tweeting to advertise their Parler accounts after Trump was permanently banned from Twitter*. Business Insider. https://www.businessinsider.com/top-conservatives-moving-to-parler-after-trumps-ban-from-twitter-2021-1

EEAS SPECIAL REPORT UPDATE: Short Assessment of Narratives and Disinformation Around the COVID-19 Pandemic (UPDATE DECEMBER 2020 - APRIL 2021). (2021, April 28). EU vs DISINFORMATION. https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid-19-pandemic-update-december-2020-april-2021/

Etter, L. (2017, December 7). Rodrigo Duterte Turned Facebook Into a Weapon, With a Little Help From Facebook. *Bloomberg.Com*. https://www.bloomberg.com/news/features/2017-12-07/how-rodrigo-duterte-turned-facebook-into-a-weapon-with-a-little-help-from-facebook

Etterretningstjenesten. (2020). *Fokus 2020—Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer*. Forsvaret. https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus/rapporter/Fokus2021-web.pdf/_/attachment/inline/b9d52b53-0abe-4d1c-9c51-bf95796560bf:8dd66029b7efb38aab37d13e8b387d2e6ed0bd05/Fokus2021-web.pdf

Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, (2020). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en

Facebook Inc. (2019, August 19). Removing Coordinated Inauthentic Behavior From China. *About Facebook*. https://about.fb.com/news/2019/08/removing-cib-china/

Facebook Inc. (2021). *Facebook Reports First Quarter 2021 Results*. https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-First-Quarter-2021-Results/default.aspx

Faddoul, M., Chaslot, G., & Farid, H. (2020). A Longitudinal Analysis of YouTube's Promotion of Conspiracy Videos. *ArXiv:2003.03318 [Cs]*. http://arxiv.org/abs/2003.03318

Faktisk.no. (2020). *Falske nyheter*. Faktisk.No. https://tenk.faktisk.no/tema/falske-nyheter

Fiske, S. T., & Taylor, S. E. (2017). *Social cognition: From brains to culture* (2nd ed.). Sage.

Frenkel, S. (2017, December 17). For Russian 'Trolls,' Instagram's Pictures Can Spread Wider Than Words. *The New York Times*. https://www.nytimes.com/2017/12/17/technology/instagram-russian-trolls.html

Gadde, V., & Roth, Y. (2018, October 17). *Enabling further research of information operations on Twitter*. Twitter. https://blog.twitter.com/en_us/topics/company/2018/enabling-further-research-of-information-operations-on-twitter.html

Gates, S., & Podder, S. (2015). *Social Media, Recruitment, Allegiance and the Islamic State*. *9*(4), 10.

Global Engagement Center. (2020). *Pillars of Russia's Disinformation and Propaganda Ecosystem* (p. 77). Global Engagement Center. https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf

Grøtan, T. O., Fiskvik, J., Haro, P. H., Auran, P. G., Mathisen, B. M., Karlsen, G. H., Magin, M., & Brandtzæg, P. B. (2019). *På leting etter utenlandsk informasjonspåvirkning*. SINTEF Digital. https://www.regjeringen.no/contentassets/4d850821991746ecbcd9477a475baf73/sintef-rapport_2019-01292_gradering_apen.pdf

Grut, S. (2020). *NRKbeta avslører: Alle store norske medier har blitt lurt av russiske troll-kontoer*. NRKbeta. https://nrkbeta.no/2020/03/03/nrkbeta-avslorer-alle-store-norske-medier-har-blitt-lurt-av-russiske-troll-kontoer/

Hamilton, C., & Ohlberg, M. (2020). *Hidden hand: Exposing how the Chinese Communist Party is reshaping the world*. Simon and Schuster.

Hammond-Errey, M. (2019). Understanding and Assessing Information Influence and Foreign Interference. *Journal of Information Warfare*, *18*(1), 1–22.

Holt, J., Brookie, G., & Brooking, E. (2021, January 7). FAST THINKING: How the Capitol riot was coordinated online. *Atlantic Council*. https://www.atlanticcouncil.org/content-series/fastthinking/fast-thinking-how-the-capitol-riot-was-coordinated-online/

Howard, P. N., Ganesh, B., Liotsiou, D., Kelly, J., & François, C. (2018). *The IRA, Social Media and Political Polarization in the United States, 2012-2018* (Working Paper, number 2018.2; p. 47). Oxford Internet Institute.

Ipsos. (2021). *Ipsos SOME Tracker Q1 2021* (Q4'21). Ipsos. https://www.ipsos.com/nb-no/ipsos-some-tracker-q121

Janis, I. L. (1972). *Victims of Groupthink: A psychological study of foreign-policy decisions and fiascoes.*

Jerdén, B., & Bohman, V. (2019). *China's propaganda campaign in Sweden, 2018–2019* (No. 4; UI Brief, p. 14). Swedish Institute of International Affairs (UI).

Johansen, A. E. B. (2021). *Presse-Norge åpner for å bruke stjålet hacker-informasjon*. Vårt Land. https://www.vl.no/kultur/2021/05/12/presse-norge-apner-for-a-bruke-stjalet-hacker-informasjon/

Jones, M. O. (2019, December 16). Twitter have quietly suspended a network of between 1000-2000 troll [...] [Tweet]. *@marcowenjones*. https://twitter.com/marcowenjones/status/1206672083889147904

Justis- og beredskapsdepartementet. (2020). *Samfunnssikkerhet i en usikker verden* (Stortingsmelding Meld. St. 5 (2020–2021)). regjeringen.no. https://www.regjeringen.no/no/dokumenter/meld.-st.-5-20202021/id2770928/

Justis- og beredskapsdepartementet. (2021. Statsbudsjettet 2021 (Prop. 1 S (2020 –2021)). Hentet fra https://www.regjeringen.no/contentassets/5b609e31442040a198daf3a9a97c927f/nn-no/pdfs/prp202020210001_jddddpdfs.pdf

Kao, J., & Li, M. S. (2020, March 26). *How China Built a Twitter Propaganda Machine Then Let It Loose on Coronavirus* (https://www.propublica.org/) [Text/html]. ProPublica; ProPublica. https://www.propublica.org/article/how-china-built-a-twitter-propaganda-machine-then-let-it-loose-on-coronavirus

Karlsen, M. L., & Skiphamn, S. S. (2019). *Nei, innvandrere får ikke 231 000 kroner mer i uføretrygd i statsbudsjettet*. Faktisk.no. https://www.faktisk.no/faktasjekker/X5G/nei-innvandrere-far-ikke-231-000-kroner-mer-i-uforetrygd-i-statsbudsjettet

Kibar, O., & Engen, S. (2021, January 5). *PST hudfletter universitetene: «Fullstendig blåøyde og veldig, veldig naive»*. www.dn.no. https://www.dn.no/magasinet/dokumentar/politiets-sikkerhetstjeneste/ntnu/tekna/pst-hudfletter-universitetene-fullstendig-blaoyde-og-veldig-veldig-naive/2-1-919171

Kolsrud, K. (2021, January 5). *Tiltroen til myndighetene rett til værs i korona-Norge*. Rett24. https://rett24.no/articles/tiltroen-til-myndighetene-rett-til-vaers-i-korona-norge

Kuo, L. (2020, August 6). *Google deletes 2,500 China-linked YouTube channels over disinformation*. The Guardian. http://www.theguardian.com/technology/2020/aug/06/google-deletes-2500-china-linked-youtube-channels-over-disinformation

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*.

Lapowsky, I. (2018, October 5). *House Democrats Release 3,500 Russia-Linked Facebook Ads*. Wired. https://www.wired.com/story/house-democrats-release-3500-russia-linked-facebook-ads/

Lessenski, M. (2021, March 14). Media Literacy Index 2021. *Osis.Bg*. https://osis.bg/?p=3750&lang=en

Lyons, B. A., Montgomery, J. M., Guess, A. M., Nyhan, B., & Reifler, J. (2021). Overconfidence in news judgments is associated with false news susceptibility. *Proceedings of the National Academy of Sciences*, *118*(23). https://doi.org/10.1073/pnas.2019527118

Mackintosh, E. (2019, May). *Finland is winning the war on fake news. Other nations want the blueprint*. https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/

Malerud, S., Hennum, A. C., & Toverød, N. (2021). *Situasjonsforståelse ved sammensatte trusler-et konseptgrunnlag* (No. 21/00246). FFI.

Medietilsynet. (2020). *Barn og Medier 2020—Om falske nyheter* (p. 13). Medietilsynet. https://www.medietilsynet.no/globalassets/publikasjoner/barn-og-medier-undersokelser/2020/200226-barn-og-medier-2020-delrapport-2.pdf

Medietilsynet. (2021). *Undersøkelse om kritisk medieforståelse i den norske befolkningen—Delrapport 1: Falske nyheter og desinformasjon* (ISBN: 978-82-8428-009-7). Medietilsynet. https://www.medietilsynet.no/globalassets/dokumenter/rapporter/kritisk-medieforstaelse-2021/210218-kmf-delrapport-1-falske-nyheter.pdf

Mittermaier, E., Granholm, N., & Veibäck, E. (2020). *Perspektiv på pandemin—Inledande analys och diskussion av beredskapsfrågor i ljuset av coronakrisen 2020* (p. 99). FOI.

Mueller, R. S. (2019). *Report on the Investigation into Russian Interference in the 2016 Presidential Election* (p. 448). Department of Justice. https://www.justice.gov/storage/report.pdf 1

Nasjonal sikkerhetsmyndighet. (2021). *Risiko 2021* (NSM RISISKO 2021; p. 44). Nasjonal sikkerhetsmyndighet. https://nsm.no/getfile.php/136165-1612871437/Demo/Dokumenter/Rapporter/Risiko%202021%20hand-out.pdf

National Intelligence Council. (2021). *Foreign Threats to the 2020 US Federal Elections* (ICA 2020-00078D). National Intelligence Council. https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf

Nickerson, R. S. (1998). Confirmation bias: A ubiquitous phenomenon in many guises. *Review of General Psychology*, *2*(2), 175–220.

NTB. (2021, March 23). *Stanser salget av Bergen Engines til russisk selskap*. Tu.no. https://www.tu.no/artikler/stanser-salget-av-bergen-engines-til-russisk-selskap/508363

Pamment, J., Twetman, H., Fjällhed, A., Nothhaft, H., Engelson, H., & Rönngren, E. (2020). *RESIST Counter-disinformation Toolkit* (p. 72). Government Communication Service. https://3x7ip91ron4ju9ehf2unqrm1-wpengine.netdna-ssl.com/wp-content/uploads/2020/03/RESIST-Counter-Disinformation-Toolkit.pdf

Parello-Plesner, J. (2018, October 23). China's LinkedIn Honey Traps. *The American Interest*. https://www.the-american-interest.com/2018/10/23/chinas-linkedin-honey-traps/

Paul, K. (2020, November 13). *Tech companies under pressure to ban far-right forum used for militia organizing*. The Guardian. http://www.theguardian.com/world/2020/nov/13/mymilitia-ban-violence-threats-godaddy-cloudflare

Petty, R. E., & Cacioppo, J. T. (1986). The Elaboration Likelihood Model of Persuasion. In *Advances in Experimental Social Psychology* (Vol. 19, pp. 123–205). Elsevier.

Petty, R. E., Fabrigar, L. R., & Wegener, D. T. (2003). *Emotional factors in attitudes and persuasion.*

Politiets Sikkerhetstjeneste. (2021). *Trusselvurdering 2021*. Politiets Sikkerhetstjeneste. https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/

Ponniah, K. (2020, July 26). How a Chinese agent used LinkedIn to hunt for targets. *BBC News*. https://www.bbc.com/news/world-asia-53544505

Pronin, E., Gilovich, T., & Ross, L. (2004). Objectivity in the eye of the beholder: Divergent perceptions of bias in self versus others. *Psychological Review*, *111*(3), 781.

Psykförsvarsutredningen. (2020). *En myndighet för att stärka det psykologiska försvaret. : Betänkande från Utredningen om en ny myndighet för psykologiskt försvar (Ju 2018:06).* (SOU 2020:29). Statens Offentliga Utredningar. https://www.regeringen.se/49bbbd/contentassets/e3a84a5fd7144c6a95a1eb90a2bbfec0/en-ny-myndighet-for-att-starka-det-psykologiska-forsvaret-sou-2020-29.pdf

Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux, New York.

Romano, A. (2018, October 19). *Twitter released 9 million tweets from one Russian troll farm. Here's what we learned.* Vox. https://www.vox.com/2018/10/19/17990946/twitter-russian-trolls-bots-election-tampering

Rønningen, B. (2016, July 1). Bedehus blir ortodoks kirke. *Sambåndet*. https://sambåndet.no/2016/07/01/bedehus-blir-ortodoks-kirke/

Rosenberg, M., Perlroth, N., & Sanger, D. E. (2020, January 10). 'Chaos Is the Point': Russian Hackers and Trolls Grow Stealthier in 2020. *The New York Times*. https://www.nytimes.com/2020/01/10/us/politics/russia-hacking-disinformation-election.html

Ross, L. (1977). The intuitive psychologist and his shortcomings: Distortions in the attribution process. In *Advances in experimental social psychology* (Vol. 10, pp. 173–220). Elsevier.

Ross, L., Greene, D., & House, P. (1977). The "false consensus effect": An egocentric bias in social perception and attribution processes. *Journal of Experimental Social Psychology*, *13*(3), 279–301.

Sabini, J. (1995). *Social Psychology* (2nd ed.). WW Norton & Company.

Schulz, A., Wirth, W., & Müller, P. (2020). We Are the People and You Are Fake News: A Social Identity Approach to Populist Citizens' False Consensus and Hostile Media Perceptions. *Communication Research*, *47*(2), 201–226. https://doi.org/10.1177/0093650218794854

Schumann, D. W., Kotowski, M. R., Ahn, H.-Y., & Haugtvedt, C. P. (2012). The elaboration likelihood model. In S. Rodgers & E. Thorson (Eds.), *Advertising theory* (pp. 51–68). Routledge.

Seo, H., Blomberg, M., Altschwager, D., & Vu, H. T. (2020). Vulnerable populations and misinformation: A mixed-methods approach to underserved older adults' online information assessment: *New Media & Society*. https://doi.org/10.1177/1461444820925041

Soares, I., & Davey-Attlee, F. (2017, September 13). *The fake news machine: Inside a town gearing up for 2020*. https://money.cnn.com/interactive/media/the-macedonia-story/

Spring, M. (2020, May 27). Coronavirus: The human cost of virus misinformation. *BBC News*. https://www.bbc.com/news/stories-52731624

Staff, A. K. B. (2020). *Datainnbruddet mot Stortinget er ferdig etterforsket*. www.pst.no. https://www.pst.no/alle-artikler/pressemeldinger/datainnbruddet-mot-stortinget-er-ferdig-etterforsket/

Tajfel, H., Turner, J. C., Austin, W. G., & Worchel, S. (1979). An integrative theory of intergroup conflict. *Organizational Identity: A Reader*, *56*(65), 9780203505984–16.

Tang, J. (2021). *China's Information Warfare and Media Influence Spawn Confusion in Thailand*. Radio Free Asia. https://www.rfa.org/english/news/china/thailand-infowars-05132021072939.html

Tversky, A., & Kahneman, D. (1981). The framing of decisions and the psychology of choice. *Science*, *211*(4481), 453–458.

Utgivarna. (2020). Markera kraftigare mot Kinas försök att påverka pressfriheten. *:Utgivarna*. https://utgivarna.se/artiklar/markera-kraftigare-mot-kinas-forsok-att-paverka-pressfriheten/

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, *359*(6380), 1146–1151. https://doi.org/10.1126/science.aap9559

Walther, S., & McCoy, A. (2021). *US Extremism on Telegram: Fueling Disinformation, Conspiracy Theories, and Accelerationism*. *15*(2), 25.

Warzel, C. (2017, October 4). *Here's How YouTube Is Spreading Conspiracy Theories About The Vegas Shooting*. BuzzFeed News. https://www.buzzfeednews.com/article/charliewarzel/heres-how-youtube-is-spreading-conspiracy-theories-about

Weissmann, M., Nilsson, N., Palmertz, B., & Thunholm, P. (2021). *Hybrid Warfare—Security and Asymmetric Conflict in International Relations*. Bloomsbury Publishing.

Wong, E. (2019, August 27). How China Uses LinkedIn to Recruit Spies Abroad. *The New York Times*. https://www.nytimes.com/2019/08/27/world/asia/china-linkedin-spies.html

Wong, J. C. (2021, April 12). How Facebook let fake engagement distort global politics: A whistleblower's account. *The Guardian*. https://www.theguardian.com/technology/2021/apr/12/facebook-fake-engagement-whistleblower-sophie-zhang

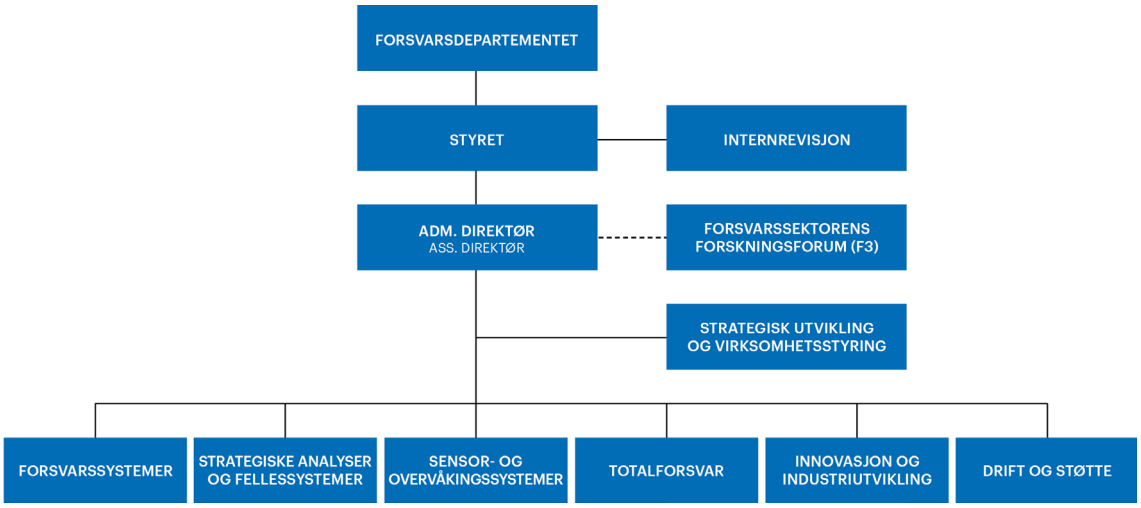
Yurieff, K. (2021). *Before rioters stormed the US Capitol, Trump supporters called for violence online*. CNN. https://www.cnn.com/2021/01/06/tech/protest-violence-online/index.html

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
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

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

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

Office address:
Instituttveien 20
N-2007 Kjeller

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