FFI Forsvarets forskningsinstitutt

Analyse & Tall

COMMON CONSULTANCY

21/02746

FFI-RAPPORT

Uønsket utenlandsk påvirkning?

– kartlegging og analyse av stortingsvalget 2021

Eskil Grendahl Sivertsen
Lea Bjørgul
Håvard Lundberg [1]
Ingvild Endestad [1]
Tobias Bornakke [1]
Jakob Bæk Kristensen [2]
Nicolai Meldgaard Christensen [3]
Thomas Albrechtsen [3]

[1] Analyse & Tall
[2] RUC/ Analyse & Tall
[3] Common Consultancy

Uønsket utenlandsk påvirkning?
– kartlegging og analyse av stortingsvalget 2021

Eskil Grendahl Sivertsen
Lea Bjørgul
Håvard Lundberg [1]
Ingvild Endestad [1]
Tobias Bornakke [1]
Jakob Bæk Kristensen [2]
Nicolai Meldgaard Christensen [3]
Thomas Albrechtsen [3]

Forsvarets forskningsinstitutt (FFI)
[1] Analyse & Tall
[2] RUC/ Analyse & Tall
[3] Common Consultancy

1. januar 2022

Emneord
Valgpåvirkning
Informasjonspåvirkning
Påvirkningsoperasjoner
Desinformasjon

FFI-rapport
21/02746

Prosjektnummer
5738

Elektronisk ISBN
978-82-464-3381-3

Engelsk tittel
Unwanted foreign influence? Analysis of the Norwegian parliamentary elections 2021

Godkjennere
Stig Rune Sellevåg, *forskningsleder*
Janet Martha Blatny, *forskningsdirektør*

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Sammendrag

Denne studien forsøker å kartlegge hvorvidt stortingsvalget 2021 ble utsatt for uønsket informasjonspåvirkning fra utenlandske aktører. Med «uønsket informasjonspåvirkning» menes her spredning av (des)informasjon og/eller manipulasjon på norske nettsider og i sosiale medier i den antatte hensikt å påvirke valgresultatet, valgdeltakelsen eller tilliten til valget. Valgdagen var 13. september, og kartleggingens hovedfokus er perioden 1. august til 16. september 2021.

Studien er gjennomført av Forsvarets forskningsinstitutt (FFI) i samarbeid med de skandinaviske analysebyråene Analyse & Tall og Common Consultancy. Oppdragsgiver er Kommunal- og moderniseringsdepartementet (KMD).

Vi har tatt utgangspunkt i en hypotese om at uønsket informasjonspåvirkning fra utenlandske aktører *ikke* har funnet sted. Gjennom ulike kvantitative og kvalitative metoder har vi så forsøkt å motbevise denne hypotesen. Dette er gjort ved å kartlegge og analysere spredning av (des)informasjon og propaganda fra utenlandske aktører på norske nettsider, på Facebook og på Twitter. Vi har også undersøkt inautentisk aktivitet på Facebook og Twitter for å identifisere målrettede forsøk på manipulasjon.

Vi har valgt å prioritere Facebook og Twitter fordi en vesentlig del av den offentlige debatten foregår på disse plattformene, og fordi disse plattformene tidligere har blitt brukt i en rekke påvirkningsoperasjoner i og mot andre stater. I tillegg gir disse plattformene tilgang på data som muliggjør kartlegging og analyser. Utenlandsk påvirkning kan forekomme på en rekke andre plattformer, men disse er ikke tatt med grunnet tekniske, juridiske og/eller ressursmessige begrensninger. Rapportens funn og konklusjoner er derfor begrenset til det datagrunnlaget som er undersøkt i gitt tidsperiode. Vi vurderer det imidlertid som lite sannsynlig at en utenlandsk aktør vil kunne oppnå tilstrekkelig effekt på stortingsvalget uten at vi vil finne spor av det på Facebook, Twitter eller norske nettsider.

Gjennom fire omfattende analyser har vi ikke gjort funn som tyder på at utenlandske aktører har forsøkt å påvirke valgresultatet, valgdeltakelsen eller tilliten til valget. Våre funn viser imidlertid at utenlandske, ikke-statlige aktører aktivt forsøker å spre desinformasjon til et norsk publikum. Disse forsøkene oppnår kun et begrenset liv på sosiale medier i Norge, med relativt lite spredning og få interaksjoner. I tillegg har vi funnet to klynger av det som framstår som utenlandske, inautentiske profiler på Twitter som aktivt sprer innhold til et norsk publikum, uten at vi kan knytte aktiviteten direkte til forsøk på valgpåvirkning. Facebook og Twitter er fremdeles godt egnet som plattformer for påvirkningsoperasjoner, til tross for deres egne forsøk på å stoppe inautentisk aktivitet og spredning av desinformasjon.

Vår litteraturgjennomgang viser at uønsket informasjonspåvirkning mot demokratier foregår i betydelig omfang og ofte subtilt med lav intensitet over tid. Basert på omfanget, vurderer vi det som sannsynlig at utenlandske aktører med tilstrekkelig vilje og evne vil kunne utøve påvirkningsoperasjoner mot den norske befolkningen og norske interesser dersom aktøren ser seg tjent med å gjøre dette. Vi anbefaler at fremtidig kartlegging av uønsket informasjonspåvirkning av valg gjøres over et lengre tidsrom enn i dette oppdraget. Karleggingen bør da utvides til å inkludere langsiktig påvirkning av politiske saker og generell svekkelse av tilliten i samfunnet og til demokratiske institusjoner.

Summary

This study aims to investigate whether the Norwegian Parliamentary election 2021 was subject to malign information influence by foreign actors. “Information influence” is defined in this study as the spread of (dis)information and/or manipulation on Norwegian websites and in social media with the presumed intent of influencing the election results, voter participation or trust in the election itself. The Election Day was 13 September, and the investigation focuses on the periode between 1 August – 16 September 2021.

The study was conducted by the Norwegian Defence Research Establishment (FFI), in cooperation with the Scandinavian analysis agencies Analyse & Tall and Common Consultancy, on behalf of the Norwegian Ministry of Local Government and Modernisation.

Our study is based on the hypothesis that malign information influence by foreign actors has *not* taken place. By using different quantitative and qualitative methods, we have attempted to falsify this hypothesis. We have approached this task by mapping and analyzing the spread of (dis)information and propaganda from foreign actors on Norwegian websites, on Facebook and on Twitter. Furthermore, we have investigated inauthentic activity on Facebook and Twitter in order to identify targeted attempts at manipulation. Our study has focused on Facebook and Twitter because a substantial part of the Norwegian public debate takes place on these platforms, and because these platforms have previously been used in influence operations targeting other nations. Furthermore, these platforms provide access to data that makes it possible to conduct this kind of investigation. Foreign influence may take place on several other platforms. However, these are not included due to technical, legal and/or resource limitations. Our findings and conclusions are thus limited to the datasets investigated during the set time period. However, we consider it unlikely that a foreign actor will be able achieve a sufficient effect on the Parliamentary election without leaving traces of influence activities on Facebook, Twitter or Norwegian websites.

Through four in-depth analyses, we have not made any findings that suggest foreign actors attempted to influence the election results, voter participation or trust in the election itself. However, our analyses show that foreign, non-state actors are actively involved in attempts to spread disinformation to a Norwegian target audience, albeit with limited reach. We have also uncovered two clusters of seemingly foreign, inauthentic Twitter profiles spreading content to a Norwegian audience. Facebook and Twitter are still exploitable with regards to conducting influence campaigns, despite the platforms’ attempts to stop inauthentic behaviour and the spread of disinformation.

Our literature review shows that malign foreign influence directed at democracies is ongoing at a significant level, and is often conducted with low intensity over time. Based on the sheer scope, we consider it likely that foreign actors, with sufficient will and capability, may direct influence operations at the Norwegian population or Norwegian interests in a situation where the actor finds this opportune. Consequently, we recommend that future analyses of malign foreign influence aimed at elections should be expanded to include long-term influence directed at specific political issues and attempts to weaken people’s trust in democratic institutions.

Innhold

Forord

I dette oppdraget har FFI, sammen med analysebyråene Analyse & Tall og Common Consultancy, forsøkt å finne ut om stortingsvalget 2021 ble utsatt for uønsket utenlandsk påvirkning. Oppdraget er gjennomført på vegne av Kommunal- og moderniserings-departementet og er avgrenset til informasjonspåvirkning av valgresultat, valgdeltakelse og tilliten til valggjennomføringen, i perioden 1. august til 16. september 2021.

En kartlegging som dette er en krevende øvelse. Vi forsøker å finne noe vi på forhånd ikke vet hvordan ser ut, hvor det forekommer eller om i det hele tatt eksisterer - i et komplekst informasjonsmiljø hvor aktørene stadig utvikler og endrer sine taktikker og metoder som de i tillegg forsøker å holde skjult.

Vi har på forhånd vurdert og definert hvilke metoder og datagrunnlag vi mener er best egnet som grunnlag for kartlegging og analyse. Alle metoder for kartlegging og analyse har imidlertid sine styrker og svakheter. Svakhetene forsøker vi å kompensere for ved å undersøke fenomener med flere ulike metoder, datakilder og analyser. Denne tilnærmingen, samt stadige endringer i aktørers metoder og virkemiddelbruk, gjør at rapporten bør leses som en eksplorativ kartlegging basert på kunnskapen tilgjengelig i det tidsrommet oppdraget ble utført.

Vi ønsker å rette en takk til Kommunal- og moderniseringsdepartementet for oppdraget, støtte i gjennomføringen og et godt samarbeid.

Oslo, 15.12.2021

Eskil Grendahl Sivertsen (FFI)
Lea Bjørgul (FFI)
Håvard Lundberg (Analyse & Tall)
Ingvild Endestad (Analyse & Tall)
Tobias Bornakke (Analyse & Tall)
Jakob Bæk Kristensen (RUC/Analyse & Tall)
Nicolai Meldgaard Christensen (Common Consultancy)
Thomas Albrechtsen (Common Consultancy)

1 Innledning

Utenlandsk innblanding i andre lands offentlige debatter og demokratiske prosesser, inkludert valg, har de siste årene blitt en økende trussel i takt med tiltakende stormaktsrivalisering (Bentzen, 2018; Markay, 2021). Slik uønsket påvirkning er ikke et nytt fenomen, men utviklingen innen spesielt cyberteknologi og sosiale medier har skapt nye muligheter for å oppnå betydelig større effekt i forhold til innsats og risiko. En global kartlegging av 97 nasjonale valg og 31 folkeavstemninger i perioden 2016 til 2019 konkluderte med at 20 land ble utsatt for informasjonspåvirkning og/eller cyberbasert innblanding (Hanson et al, 2019).

Det mest kjente og best kartlagte eksempelet på utenlandsk påvirkning av et annet lands demokratiske valg, er Russlands forsøk på å påvirke det amerikanske presidentvalget i 2016. I etterkant avdekket amerikanske myndigheter en omfattende påvirkningsoperasjon som forsøkte å framprovosere og forsterke politisk og sosial uenighet i USA, manipulere valgsystemet, skade Hillary Clintons kandidatur og forsterke Donald Trumps (Mueller, 2019).

Dette ble startskuddet for de senere års økning i internasjonal oppmerksomhet rettet mot utenlandsk påvirkning og spredning av desinformasjon på internett og i sosiale medier. Forskningsinnsatsen har økt, flere uavhengige faktasjekkere er etablert og de sosiale medieplattformene er under press for å stoppe spredning av desinformasjon og bruk av falske kontoer. I tillegg har både sivile og militære myndigheter i flere land, samt i EU og Nato, etablert ulike former for samarbeid og funksjoner for å i større grad evne å forstå, fange opp og håndtere fremmedstatlige påvirkningsoperasjoner (Rob et al, 2021).

Det finnes lite offentlig kjent kunnskap om omfanget og innretningen av målrettet fremmedstatlig påvirkning mot Norge. SINTEF gjennomførte en kartlegging av mulig utenlandsk informasjonspåvirkning av kommunestyre- og fylkestingsvalget i 2019. I rapporten *På leting etter utenlandsk påvirkning - en analyse av det norske kommunestyre- og fylkestingsvalget 2019*, konkluderes det med at det ikke ble funnet klare tegn på utenlandsk påvirkning. I rapporten ble det imidlertid påvist at flere tilsynelatende norske brukere inngikk i nettverk som systematisk overførte innhold fra ytterliggående nettsider og som forsøkte å kamuflere sin aktivitet. I den sammenheng ble det påpekt at det kan være "særs vanskelig å skille utenlandsk påvirkning fra annen mistenkelig virksomhet på nettet" (Grøtan et al, 2019, s. 1).

Sistnevnte observasjon er et fremtredende kjennetegn ved mange påvirkningsoperasjoner, som i sin natur foregår fordekt og hvor opphavet tåkelegges gjennom intrikate nettverk av falske og ekte kontoer, proxysider og manipulasjon på sosiale medier. I tillegg tilpasser påvirkningsaktører seg, og utnytter det politiske, økonomiske, sosiale og teknologiske mulighetsrommet som er i konstant bevegelse. Å kartlegge operasjoner som forandrer seg over tid, der aktørene bak aktivt forsøker å unngå deteksjon, er en krevende oppgave. Vi har i dette oppdraget derfor tatt i bruk flere ulike kvantitative og kvalitative metoder for å belyse informasjonsmiljøet i Norge fra flere vinkler.

Før det gis en grundigere beskrivelse av metodene brukt i dette oppdraget (kapittel 6), rapportens funn (kapittel 7) og konklusjoner (kapittel 8), redegjøres det for vår forståelse av oppdraget. Kapitlene 2-5 tar for seg begrepsavklaringer, påvirkningsaktører, påvirkningsmetoder og eksisterende kunnskap om utenlandsk påvirkning, samt hvordan vi har benyttet denne kunnskapen til å vurdere hvordan det norske stortingsvalget kan bli forsøkt påvirket.

Om oppdraget

I forbindelse med sametings- og stortingsvalget 2021, utarbeidet Solberg-regjeringen 13 tiltak for å hindre uønsket påvirkning. Et av tiltakene var å gjennomføre et forskningsprosjekt om valgpåvirkning (Kommunal- og moderniseringsdepartementet, 2021).

Kommunal- og moderniseringsdepartementet (KMD) la oppdraget «Forskningsprosjekt om informasjonspåvirkning i forbindelse med det norske stortingsvalget 2021» ut på offentlig anbud på Doffin.no 25.5.21. Oppdraget består av to deler: (1) kartlegging og analyse av målrettede forsøk på informasjonspåvirkning i forkant av og under stortingsvalget og (2) utvikling av scenarioer som skisserer ulike scenarioer for informasjonspåvirkning i forbindelse med et norsk valg (Kommunal- og moderniseringsdepartementet, 2021b, s. 3). FFI, i samarbeid med analyseselskapene Analyse & Tall og Common Consultancy, ble valgt som leverandør 05.07.21. Denne rapporten utgjør leveransen for oppdragets del 1.

Oppdragsgivers beskrivelse:

“Departementet ønsker å få gjennomført en ekstern kartlegging og analyse av målrettede forsøk på informasjonspåvirkning fra internasjonale aktører i forkant av og under det norske valget i 2021. Oppdragstaker skal kartlegge informasjon som blir spredd over internett, med særlig vekt på målrettede kampanjer, både på nettsider, sosiale medier, etablerte og alternative nyhetssider samt nettforum og nettsamfunn. Oppdragstaker skal identifisere hvilke aktører som sprer desinformasjon rettet mot norske innbyggere” (Kommunal- og moderniseringsdepartementet, 2021b, s. 3).

2 Begrepsavklaringer

I det følgende vil vi redegjøre for vår forståelse og presiseringer av kjernebegrepene i oppdragsgivers beskrivelse.

Informasjonspåvirkning er i utgangspunktet verken ulovlig eller problematisk. Politiske partier, interesseorganisasjoner, bedrifter og kommunikasjonsbyråer forsøker alle å påvirke befolkningen gjennom informasjon. Informasjonspåvirkning er sågar kjernen i partienes valgkamp. Dette er en del av demokratiet og ytringsfriheten. Det trenger heller ikke være problematisk at det står en internasjonal eller utenlandsk aktør bak påvirkningsaktiviteten. Denne typen «vanlig» og transparent påvirkning er ikke en del av denne kartleggingen. FFI legger til grunn at oppdraget er å avdekke eventuelle uønskede, utenlandske påvirkningsoperasjoner, som vi beskriver som følger:

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 (Sivertsen et al, 2021, s. 15).

I denne definisjonen brukes ordet "illegitim". Men hva er forskjellen på legitime og illegitime påvirkningsmetoder, og hvor går grensen mellom de to?

Ifølge en ny rapport fra EU Disinfo Lab, *Foreign election interferences: An overview of trends and challenges*, har det australske innenriksdepartementet utviklet en god standard for å vurdere graden av utenlandsk valgpåvirkning ved å skille mellom "foreign influence" og "foreign interference" (Henin, 2021).

"Foreign Influence" handler om åpen og transparent påvirkningsaktivitet utført av en annen stats myndigheter. Et eksempel på slik aktivitet er da Tyrkias president Erdogan åpent oppfordret tyske borgere med tyrkisk opphav til ikke å stemme på Angela Merkels koalisjon under det tyske parlamentsvalget i 2017 (Deutsche Welle, 2017). Denne typen påvirkning *alene* anses ikke som illegitim og omfattes dermed ikke av definisjonen av en påvirkningsoperasjon.

"Foreign interference" handler imidlertid om fordekte aktiviteter som for eksempel å manipulere den offentlige debatten ved hjelp av desinformasjon, falske profiler og inautentisk adferd på sosiale medier og bruk av proxy-aktører for å spre falsk informasjon og tåkelegge opprinnelsen (Henin, 2021). Denne typen påvirkning dekkes av begrepet "illegitim" i vår definisjon.

En påvirkningsoperasjon kan imidlertid benytte metoder både fra "foreign influence" og "foreign interference". Russlands måte å operere på er, ifølge Global Engagement Center i det amerikanske utenriksdepartementet, et eksempel på nettopp dette (GEC, 2020). Som et tenkt eksempel, kan en misvisende eller feilaktig påstand skapes på en russisk proxy-plattform som Strategic Culture (ibid.), gjengis av den statskontrollerte nyhetskanalen Sputnik og spres på internett og i sosiale medier av både ekte og falske profiler og bots (såkalt inautentisk adferd) og

bli ytterligere forsterket gjennom en offentlig uttalelse fra den russiske utenriksministeren. I et slikt tilfelle, hvor den offisielle uttalelsen med sannsynlighetsovervekt kan knyttes til andre og illegitime metoder, vil den omfattes av definisjonen på påvirkningsoperasjon.

Internasjonale aktører kan være så mangt, og inkludere alt fra fremmede stater til multinasjonale selskaper, bistandsorganisasjoner, interessegrupper, medier eller profittbaserte desinformasjonsaktører. Vi legger til grunn at "internasjonale aktører" er aktører som ikke er norske. I denne rapporten bruker vi derfor betegnelsen «utenlandske aktører».

Valget 2021 består av stortingsvalget og sametingsvalget. I tråd med tittelen på oppdraget, *Forskningsprosjekt om informasjonspåvirkning i forbindelse med det norske stortingsvalget 2021,* har vi begrenset oppdraget til å kun omfatte stortingsvalget.

Påvirkning av valg kan ha ulike formål. Noen kan være konkrete i form av å påvirke valgets utfall, mens andre kan være mer generelle som å øke polarisering, kompromittere informasjonssikkerhet og undergrave tilliten til demokratiske institusjoner (Henin, 2021; Karlsen, 2021).

Langsiktig påvirkning for å øke polarisering og undergrave tillit er krevende å kartlegge dette oppdragets korte tidsrom. Basert på eksisterende kunnskap om hvordan valg kan bli forsøkt påvirket i et relativt kort tidsrom[1], har vi i dette oppdraget delt "valgpåvirkning" inn i tre kategorier:

1. Påvirkning av valgets resultat
2. Påvirkning av valgdeltakelse
3. Påvirkning av tilliten til valggjennomføringen

Disse tre kan henge tett sammen. For eksempel kan svekket tillit til valggjennomføringen føre til lavere valgdeltakelse som igjen kan påvirke valgets resultat.

Med **«desinformasjon»** menes her «utvikling og spredning av bevisst feilaktig eller villedende informasjon i den hensikt å påvirke menneskers virkelighetsoppfatning, holdninger og handlinger» (Sivertsen et al, 2021, s. 11).

Identifisering av aktører er ikke uproblematisk**.** For det første stiller Personopplysningsloven, inkludert personvernforordningen (GDPR), strenge krav til personvern. Både behandling av personopplysninger og identifisering av aktører gjøres iht. *Lov om behandling av personopplysninger* (Personopplysningsloven, 2018).

[1] Se eksempler i kapittel 4.3, samt for eksempel: Jamieson, K. (2018). Cyberwar: *How Russian Hackers and Trolls Helped Elect a President – What We Don't, Can't and Do Know.* Oxford University Press Inc.; Select Committee on Intelligence United States Senate. (2020, 10. November). *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election* Vol. I-V. (report no. 116-290). Select Committee on Intelligence United States Senate. Publications | Intelligence Committee (senate.gov)

For det andre, er det krevende å avdekke hvem som står bak en påvirkningsoperasjon all den tid det er et mål i seg selv å ikke bli avslørt. Aktørene bruker avanserte metoder for å unngå å bli oppdaget, og selv om man kan finne eksempler på påvirkningsforsøk, vil det ikke nødvendigvis være mulig å fastslå med sikkerhet hvem som står bak.

Sist, men ikke minst: Å attribuere valgpåvirkning til en fremmed stat kan få politiske og andre konsekvenser for Norge. Det er derfor regjeringen som i så fall beslutter om den fremmede staten offentlig skal identifiseres (attribusjon).

3 Hvem kan forsøke å påvirke stortingsvalget?

Ifølge Etterretningstjenestens ugraderte trusselvurdering 2021, er det Russland og Kina som utmerker seg som de mest sannsynlige aktørene med en interesse av å påvirke det norske stortingsvalget (Etterretningstjenesten, 2021, s. 14-25). Begge har lang erfaring med påvirkningsoperasjoner rettet mot andre lands innbyggere.

I dette oppdraget har vi også lett etter påvirkningsforsøk fra andre aktører uavhengig av statlig tilknytning, men hatt et spesielt fokus på de to aktørene utpekt av tjenestene.

Å skille mellom statlige og ikke-statlige aktører er imidlertid komplisert. Stater kan bruke ikke-statlige aktører som proxy, og tilsynelatende ikke-statlige aktører kan være eid eller kontrollert av en stat eller statlige interesser. Vi viser for øvrig til begrensninger mht. attribusjon beskrevet under «Identifisering av aktører» i kapittel 2.

> *I tillegg til åpne forsøk på å påvirke andre staters politiske beslutningsprosesser gjennom diplomati og forhandlinger, søker enkelte stater å gripe inn i beslutningsprosesser gjennom fordekte påvirkningsoperasjoner. Russland har gjennomført påvirkningsoperasjoner under både europeiske og amerikanske valg. Å spre desinformasjon er en etablert operasjonsmåte for russiske påvirkningsaktører. Også Kina gjør framstøt for å påvirke politiske utfall og beslutninger i vestlige land.*
>
> *Fokus 2021 kommer ut i et valgår. Stortings- og sametingsvalget til høsten er et nærliggende tilfelle der Norge kan bli utsatt for forsøk på påvirkning. Valg i andre land har vært utsatt for påvirkning gjennom blant annet nettverksoperasjoner, provokasjoner og koordinert spredning av desinformasjon. Mer begrensede initiativ kan inkludere skjevt vinklede nyhetssaker og spredning av desinformasjon i sosiale medier (...). Etterretningstjenesten (2021, s. 16)*

4 Hvordan har utenlandske aktører forsøkt å påvirke valg i andre land?

Det mest kjente og best kartlagte eksempelet på fremmede staters valgpåvirkning er Russlands forsøk på å påvirke det amerikanske presidentvalget i 2016. Mueller-rapporten, amerikansk etterretning og flere andre undersøkelser avdekket over 10 millioner twittermeldinger og bilder fra 3 841 falske profiler (Gadde, 2018) og 3 517 Facebook-annonser som til sammen ble sett ca. 146 millioner ganger (Lapowsky, 2018). I en supplerende analyse i 2018, identifiserte Twitter selv 50 258 automatiserte Twitter-kontoer (bots) som de knyttet til Russland og spredning av valgrelatert innhold i løpet av valget (Twitter, 2018). Ifølge USAs National Intelligence Council, forsøkte Russland også å påvirke presidentvalget i 2020 (National Intelligence Council, 2021).

Hensiktene bak staters forsøk på å påvirke andre lands demokratiske prosesser er sannsynligvis å skape fordelaktige forhold for å nå egne strategiske mål. Dette gjøres blant annet gjennom å påvirke valgresultat på flere nivåer, svekke valgdeltakelse, dreie den politiske agendaen på en rekke områder, svekke befolkningens tillit til egne myndigheter, politikere, pressen og hverandre og øke polariseringen i samfunnet gjennom å forsterke konflikter (Hanson et al, 2019, s. 7; Martin, 2020, s. 1).

4.1 Taktikker, teknikker og prosedyrer (TTP)

For å oppnå ovennevnte hensikter, benytter påvirkningsaktører seg av et bredt spekter av taktikker, teknikker og prosedyrer (TTP-er), og disse endres og blir mer sofistikerte over tid (Henin, 2021). I Facebooks rapport, *Threat Report - The State of Influence Operations 2017-2020*, presenteres en liste over de metodene som ble mest brukt på sosiale medier i denne perioden (Gleicher et.al., 2021, s. 19-27). Funnene samsvarer med øvrig forskning og kartlegging (kapittel 4.2-4.3):

- Bruk av brukerdata for å målrette innhold direkte til mottakerne basert på deres personlige preferanser, interesser og politiske syn.
- Utvisking av skillet mellom autentisk offentlig debatt og manipulasjon ved å i større grad evne å etterligne autentiske profiler og rekruttere ekte, lokale mennesker til å spre og forsterke innhold.
- Bruke frykten for påvirknings- og nettverksoperasjoner i seg selv til å skape et falskt inntrykk av utbredt manipulasjon av valgsystemer, selv om det ikke finnes bevis.
- Bruk av kommersielle aktører som mellomledd.
- Økt evne til å skjule egen identitet og hvitvaske informasjon gjennom teknisk tåkelegging og bruk av mellomledd (proxies), inkludert mellomledd som ikke er klar over at de er det.
- Bruk av flere plattformer og medier for å unngå deteksjon og spre risiko.

I tillegg peker EU DisinfoLab på følgende TTP-er ved påvirkningsoperasjoner spesielt knyttet til valg (Henin, 2021, s. 19-27):

- Forfalskede versjoner av etablerte og kjente nettsider, personer (manipulerte bilder eller videoer), eller kontoer på sosiale medier.
- Taktisk lekkasje av ekte eller falsk informasjon anskaffet fra datainnbrudd.

4.2 Omfang av utenlandsk påvirkning

Det australske Strategic Policy Institute publiserte i 2019 en kartlegging av utenlandsk påvirkning av 97 nasjonale valg og 31 folkeavstemninger i perioden 2016 til 2019. Av disse ble det identifisert utenlandsk informasjonspåvirkning og/eller cyberbasert innblanding i 20 land, hvorav 12 var europeiske. Mens Russland ble identifisert som aktøren bak påvirkning i europeiske land og mot USA, var Kina den fremtredende påvirkningsaktøren i Asia, samt Australia. Ifølge kartleggingen, ble også Norge utsatt for påvirkning av Russland, men det eneste eksempelet som oppgis er at Arbeiderpartiet ble utsatt for et dataangrep fra den russiske hackergruppen "Fancy Bear" i 2017 (Hanson et al, 2019, 2. 8-16).

I en nyere rapport fra 2020, *Trends in Online Influence Efforts*, argumenteres det for at minst 30 land ble utsatt for 76 fremmedstatlige påvirkningsoperasjoner i perioden 2013-2019. Mange av operasjonene varte over flere år og Russland sto bak 64% av dem (Martin et al, 2020, s.1, 3). Ifølge Oxford Internet Institute, ble det i 2020 alene kartlagt spredning av politisk propaganda og desinformasjon i 81 land (Norge var ikke med i studien) (Bradshaw et al., 2021a, s. 1-5).

Det er en viktig observasjon at påvirkningsoperasjoner kan pågå over lang tid. I 2019 kartla Atlantic Councils Digital Forensics Lab (DFRLab) det de mener er en stor og langsiktig påvirkningsoperasjon i regi av Russland, med mål om å splitte, diskreditere og distrahere vestlige land. Operasjonen, som ble gitt navnet "Operation Secondary Infektion", spenner over 30 sosiale nettverk og bloggplattformer og inkluderer store mengder falske nyheter og profiler (Aleksejeva et al, 2019, s. 3). Analyseselskapet Graphika fulgte opp dette funnet i rapporten S*econdary Infektion* fra 2020. Her argumenteres det for at operasjonen skal ha pågått siden 2014 og at den fremdeles var pågående da rapporten ble utgitt i 2020. I tillegg til målrettet informasjonspåvirkning mot de amerikanske presidentkandidatene i 2016, skal operasjonen også ha inkludert kampanjer rettet mot valg i blant annet Frankrike, Tyskland og Sverige (Nimmo et al, 2020a, s. 5).

4.3 Konkrete eksempler på påvirkning av valg og demokratiske prosesser

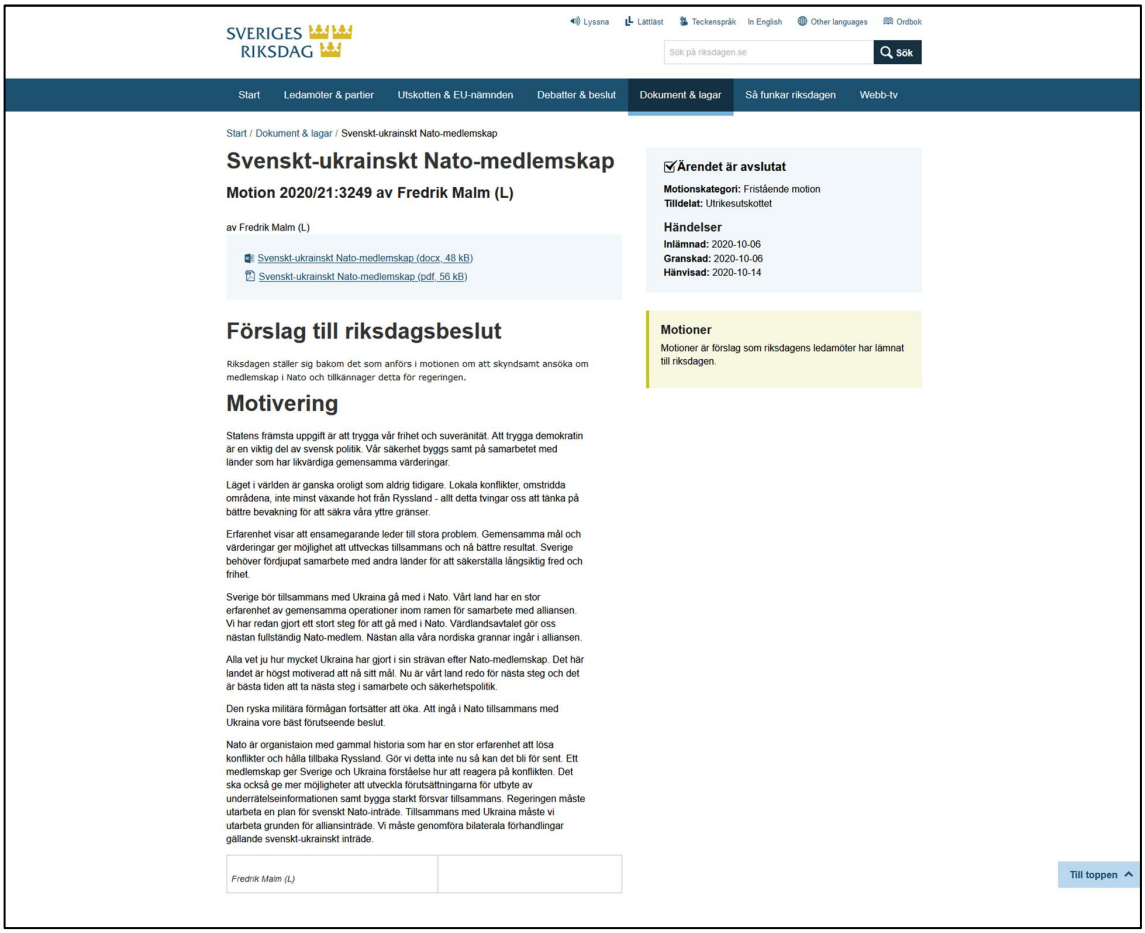
Det er ikke bare statlige aktører som forsøker å påvirke valg. For eksempel, i en rapport publisert av Institute of Strategic Dialogue konkluderes det med at både statlige og ikke-statlige aktører forsøkte å påvirke det tyske valget i 2017. Her fant man at Russland brukte egne statskontrollerte medier til å forsterke konflikter mellom tyske høyre- og venstreradikale grupper. Samtidig ble høyreradikale grupper i Tyskland også støttet av internasjonale høyreradikale nettverk (Applebaum et al, 2017, s. 20).

Kina benytter seg av en rekke ulike metoder og taktikker for politisk påvirkning, spesielt bruk av økonomiske maktmidler (Hamilton & Ohlberg, 2020). Kinas økonomiske maktmidler er ikke begrenset til utnyttelse av markedsposisjoner, oppkjøp, lånevirksomhet eller strategiske fortrinn i global produksjon, handel og logistikk. For eksempel, i Australia har politikere blitt tilbudt penger for å endre politiske standpunkt og truet med mobilisering av kinesisk-australske velgere for å straffe politiske partier som ikke støtter Kinas politiske preferanser. Blant andre virkemidler brukes for eksempel etablering av egne medier og falske grasrotbevegelser (astroturfing) til støtte for Kinas syn (Searight, 2020).

Ifølge Etterretningstjenesten, benytter kinesiske aktører også sosiale medier mer systematisk til påvirkning og desinformasjon (Etterretningstjenesten, 2021, s. 23). Blant annet skal Kina ha forsøkt å påvirke kanadiske borgere med kinesisk bakgrunn gjennom koordinerte påvirkningskampanjer med spredning av desinformasjon på meldingsappen WeChat i forbindelse med det kanadiske parlamentsvalget i 2021 (Thibaut, 2021).

Et annet og mer hjemlig eksempel kan hentes fra Sverige. I 2020 uttalte en samlet svensk presse at Kina fortsetter å angripe uavhengig journalistikk, svenske medieforetak og svenske forlag. Pressen ba den svenske regjeringen gå sammen med EU for å reagere mot Kinas forsøk på å påvirke pressefriheten (Utgivarna, 2020).

Ett og samme påvirkningsforsøk kan ha flere ulike målgrupper og mål. For eksempel, ifølge Recorded Futures Insikt Group, er det svært sannsynlig at det var Russland som stod bak et forsøk på å påvirke den svenske offentlige debatten om svensk Nato-medlemskap sommeren 2021 (Insikt Group, 2021, s 3). Dette ble gjort blant annet gjennom å spre en forfalsket skjermdump (Figur 4.1) fra den svenske Riksdagens nettside om at Sverige og Ukraina bør gå sammen om å bli medlemmer av Nato. Insikt Groups vurdering er at dette var et forsøk på å svekke den svenske befolkningens tillit til svenske politikere, skape falskt håp blant ukrainere og styrke den negative oppfatningen av Nato i Russland. Forsøket knyttes til Russlands «Operation Secondary Infektion (ibid.).



Figur 4.1 Skjermdump av forfalsket versjon av den svenske Riksdagens nettsider. Ifølge Recorded Futures Insikt Group, var dette høyst sannsynlig en del av Russlands statsstøttede påvirkningsoperasjon «Operation Secondary Infektion» (Insikt Group, 2021, s. 3).

Et ytterligere eksempel på en påvirkningsoperasjon er "Ghostwriter". Dette er navnet på en hacking-operasjon som cyberkriminelle har gjennomført i store deler av Europa siden mars 2017 (Mandiant, 2020; Mandiant, 2021). Ifølge en rapport fra cybersikkerhetsfirmaet Mandiant Threat Intelligence, har Ghostwriter-kampanjen blant annet vært involvert i en anti-Nato-desinformasjonsoperasjon, cyberspionasje og politiske hacking-kampanjer. Mandiant har funnet forbindelser mellom «Ghostwriter» og UNC1151, en cyberaktør som skal være finansiert av Russland (ibid.).

Målgruppen for denne operasjonen har blant annet vært høyt profilerte EU-parlamentarikere, journalister og sivilsamfunnet generelt, som er blitt rammet av cyberangrep som har gitt tilgang på datasystemer og personlige kontoer for epost og sosiale medier. I mange tilfeller har aktøren bak benyttet seg av metoder som for eksempel kompromittering av nettsider og bruk av forfalskede eposter til å spre falske nyhetsartikler, sitater, korrespondanse og fabrikkerte dokumenter angivelig fra politiske og militære ledere i de enkelte land (ibid.). For eksempel ble

kompromitterende bilder av en kvinne som lignet den polske lokalpolitikeren, Ewa Szarzyńska, spredd på Twitter og Instagram av kompromitterte kontoer tilhørende Szarzyńska selv og det polske parlamentsmedlemmet Marek Suski (ibid., s. 6).

Disse eksemplene viser at påvirkningsaktører er aktive i land tett på Norge og at sosiale medier er et hyppig brukt virkemiddel for å skape effekter i en påvirkningsoperasjon.

4.4 Effekter av påvirkningsoperasjoner

At påvirkningsoperasjoner rettet mot demokratiske valg og prosesser gjennomføres i betydelig omfang betyr imidlertid ikke at alle oppnår ønsket effekt. Et eksempel på dette er Russlands forsøk på å påvirke det franske presidentvalget i 2017. Gjennom desinformasjonskampanjer og såkalte «hack-and-release»-operasjoner forsøkte russiske aktører å sverte Emmanuel Macron og fremme mer Russlandsvennlige kandidater som François Fillon (Daniels, 2017). Ifølge det franske forsvarsdepartementet og Center for Strategic & International Studies (CSIS), greide Russland verken å påvirke valget eller å forsterke konflikter i den franske befolkningen (Vilmer, 2018, s. 5).

Det er imidlertid krevende å påvise hvorvidt en påvirkningsoperasjon har hatt effekt eller ikke. Med mindre man har etterretning om hvilken hensikt den har og hvilke effekter den forsøker å skape, kan man ikke vite sikkert hva målet for operasjonen er. Til tross for at det kan fremstå som åpenbart hva den aktuelle aktøren ønsker å oppnå, som for eksempel å forsterke konflikter, er det vanskelig å måle i hvor stor grad effektene man eventuelt ser er et resultat av påvirkningsoperasjonen eller andre forhold. Det finnes lite forskning på effekter av påvirkningsoperasjoner og mottiltak (Empirical Studies of Conflict, 2021).

5 Hvordan kan det norske stortingsvalget påvirkes?

Som beskrevet under "taktikker, teknikker og prosedyrer" finnes det svært mange taktikker, teknikker og prosedyrer (TTP-er) en utenlandsk aktør kan benytte seg av for å forsøke å påvirke et annet lands valgresultat, valgdeltakelse eller tilliten til valggjennomføringen. Det er heller ikke mulig å på forhånd definere alle TTP-er man bør se etter, da kun kreativiteten setter begrensninger for hva en aktør kan forsøke å finne på innenfor det politiske, økonomiske, sosiale og teknologiske mulighetsrommet. Eksemplene som nevnes her er derfor bare det – eksempler.

V*algresultatet* kan påvirkes for eksempel ved at en aktør lekker informasjon som avslører en korrupt, kriminell eller på andre måter alvorlig klanderverdig kandidat tett oppunder valgdagen. Dette kan føre til at kandidatens parti mister stemmer. Informasjonen kan være sann, delvis sann eller usann og underbygges med ekte eller forfalsket dokumentasjon. Å skape tvil hos tilstrekkelig mange om man kan ha tillit til kandidaten kan være nok til å oppnå effekt.

Ett av flere eksempler på slik diskreditering av politikere er Russlands «hack-and-relase-operasjon» under det amerikanske presidentvalget i 2016. Ved å stjele og lekke eposter fra Demokratenes nasjonalkomité (Democratic National Committee), forsøkte russiske aktører å svekke Demokratenes kandidater Bernie Sanders og Hillary Clinton (Mueller, 2019). I Norge kan man se for seg at informasjon fra datainnbruddene på Stortinget av Russland i 2020 (Utenriksdepartementet, 2020) eller Kina i 2021 (Utenriksdepartementet, 2021) kan benyttes i en slik operasjon.

Valgresultatet kan også påvirkes på andre måter. Man kan for eksempel se for seg at en bølge av (des)informasjon om polariserende saker tett opp mot valget kan påvirke hvilke saker som oppleves som viktigst og hvilke partier velgere stemmer på.

Forsøk på å redusere *valgdeltakelsen* kan rettes mot bestemte grupper, for eksempel med mål om å holde et parti under sperregrensen hvor marginene kan være så små at bortfall av et mindre antall velgere kan være nok til å skape ønsket effekt. Man kan også se for seg andre metoder, som for eksempel å påvirke klimabevisste velgere til å boikotte valget i protest over at politikerne ikke gjør nok for å redusere klimagassutslippene.

To eksempler på påvirkning av valgdeltakelse

I 2017 oppfordret Tyrkias president Erdogan tyske velgere med tyrkisk bakgrunn til å ikke stemme på Angela Merkel (Deutsche Welle, 2017).

Rett før det danske kommunal- og regionsvalget i november 2021, gikk den islamske organisasjonen Hizb ut-Tahrir ut og oppfordret alle muslimer i Danmark til å holde seg vekk fra valglokalene med begrunnelse i at det i islam "kun er tillatt å stemme på en person som skal utføre noe som er tillatt i islam" (Grønborg, 2021).

Tilliten til gjennomføringen av valget kan påvirkes for eksempel ved å skape tvil, gjennom rykter og desinformasjon, om hvorvidt man kan stole på opptellingen av forhåndsstemmene eller gjennom påstander om at det har foregått fusk i valglokaler. Det er imidlertid et vesentlig poeng at det sannsynligvis skal mye til for at en utenlandsk aktør skal klare å skape betydelig effekt innenfor et kort tidsrom, og risikoen for å bli oppdaget er større.

6 Metode og datagrunnlag

Som beskrevet innledningsvis, er påvirkningsoperasjoner krevende å avdekke. Aktørene utvikler sine metoder og taktikker kontinuerlig og forsøker aktivt å tåkelegge hva de gjør, hvordan de gjør det og hvem som står bak.

Dersom forsøk på målrettet informasjonspåvirkning skulle rettes mot Norge, tilsier empiriske eksempler fra andre land (kapittel 4.2, 4.3 og 4.4) at vi kan forvente spredning av desinformasjon og skjult manipulasjon på sosiale medier rettet mot å påvirke den norske offentlige samtalen. Vi vet imidlertid ikke på forhånd konkret hva vi leter etter, hvordan det ser ut eller om det i det hele tatt finnes.

Derfor har vi valgt å ta utgangspunkt i en hypotese om at stortingsvalget 2021 ***ikke*** *ble utsatt for forsøk på informasjonspåvirkning fra utenlandske aktører, og forsøker å finne empirisk belegg for at hypotesen kan motbevises.*

Vi har testet hypotesen gjennom følgende veiledende spørsmål:

- *Har innhold fra russiske eller kinesiske påvirkningsnettverk[2] blitt spredd til et norsk publikum på sosiale medier eller norske nettsider i forbindelse med stortingsvalget 2021?*

- *Har det forekommet inautentisk aktivitet[3] på sosiale medier som retter seg mot et norsk publikum i forbindelse med stortingsvalget 2021?*

- *Har valgets integritet blitt forsøkt trukket i tvil på sosiale medier i forbindelse med stortingsvalget 2021?*

- *Har funn fra de ovennevnte spørsmålene karakteristikker som kan være egnet til å påvirke valgresultatet, valgdeltakelsen eller tilliten til valggjennomføringen?*

For å svare på disse spørsmålene, har vi benyttet oss av en kombinasjon av kvantitative og kvalitative metoder til datainnsamling og analyse av åpne kilder. Disse inkluderer norske nettsider, nyhetsmedier, alternative medier og blogger (.no-domener), samt Twitter og åpne grupper og sider på Facebook (se kapittel 6.2 for beskrivelse og begrunnelse for datagrunnlag, og kapittel 6.5 for utfordringer, begrensninger og validitet knyttet til dette). Kort oppsummert, har vi:

[2] Med "påvirkningsnettverk" menes her nettsider eller kontoer på sosiale medier med dokumentert direkte eller indirekte tilknytning til en statlig aktør. Et eksempel er russiske aktører kartlagt av Global Engagement Center (2020). Dette beskrives nærmere i dette kapittelet.
[3] Med "inautentisk aktivitet" menes her aktiviteter og handlinger som ikke er utført av autentiske personer eller kan forklares som naturlig eller organisk. Eksempler er falske kontoer, bots og koordinert aktivitet for å forsterke et budskap. Dette beskrives nærmere i dette kapittelet.

1. Kartlagt spredning av innhold fra dokumenterte russiske og kinesiske påvirkningsnettverk til et norsk publikum på Facebook, Twitter og norske nettsider, nyhetsmedier, alternative medier og blogger (.no-domener).

2. Kartlagt potensiell inautentisk adferd på Facebook og Twitter rettet mot et norsk publikum.

3. Kartlagt innhold som omhandler valgets integritet på Facebook og Twitter.

4. Søkt etter omtale av Norge, norske interesser eller forhold i internasjonale kartlegginger av påvirkningsoperasjoner og spredning av desinformasjon.

Avgrensninger

- **Tid:** I henhold til oppdragsbeskrivelsen, er tidsrommet for undersøkelser primært avgrenset til valgperioden 1. august til 16. september 2021. Vi har inkludert datasett som går opptil to år tilbake i tid for å kunne forstå eventuelle funn i en større kontekst, men analysene er i all hovedsak avgrenset til dette tidsrommet. Der analysene dekker et lengre tidsrom er dette angitt.

- **Aktører:** Kartleggingen av eventuell informasjonspåvirkning fra konkrete, *kjente* statlige aktører er avgrenset til Russland og Kina. Kartleggingen som helhet inkluderer imidlertid også ukjente aktører uavhengig av statstilknytning.

- **Datagrunnlag:** Kartleggingen inkluderer data fra åpne grupper og sider på Facebook, Twitteraktivitet på norsk og innhold fra norske nettsider, nyhetsmedier, alternative medier og blogger (.no-domener). Begrunnelsen for valg av datagrunnlag og betydningen av dette beskrives senere i dette kapittelet.

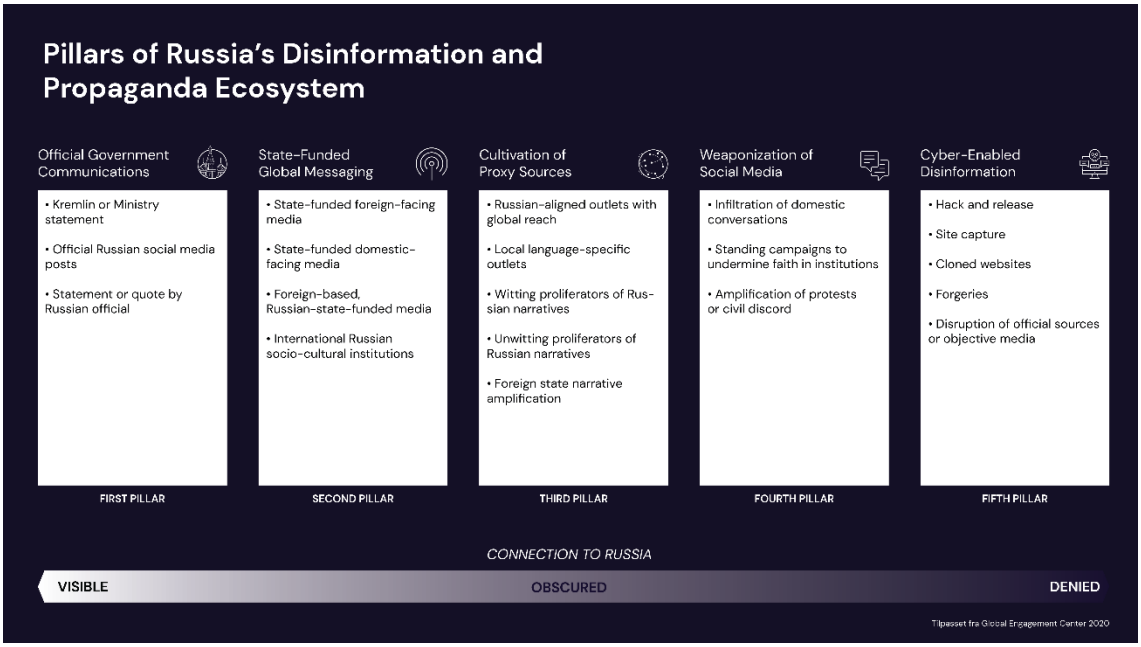
Kapittel 6 har følgende oppbygning: I kapittel 6.1 beskrives det teoretiske rammeverket som danner utgangspunktet for undersøkelsene beskrevet ovenfor. Deretter redegjøres det for valg av datagrunnlag (kapittel 6.2), før vi går nærmere inn på beskrivelser av konkrete metoder i kapittel 6.3 og 6.4, samt redegjør for studiens utfordringer og begrensninger i kapittel 6.5. Da rapporten består av fire selvstendige analyser med hvert sitt datagrunnlag og metodiske tilnærming, gjennomgås metodene for hver enkelt analyse grundigere i kapittel 7 (Analyser og resultater).

6.1 Teoretisk rammeverk for kartlegging av statlige påvirkningsnettverk

Som tidligere nevnt, peker Etterretningstjenesten på statene Russland og Kina som de mest relevante aktørene når det gjelder påvirkningsoperasjoner rettet mot Norge (Etterretningstjenesten, 2021). Vi har derfor forsøkt å kartlegge om innhold fra disse statenes påvirkningsnettverk finner veien til et norsk publikum, og hvorvidt dette innholdet kan knyttes til påvirkning av stortingsvalget 2021. I det følgende beskrives hvordan vi har gått fram.

6.1.1 Russisk påvirkningsnettverk

I rapporten «*Russia's Pillars of Disinformation and Propaganda»,* publisert av Global Engagement Center (GEC), presenteres Russlands økosystem for spredning av desinformasjon og propaganda gjennom fem pilarer som illustrerer hvordan aktiviteter koordineres og forsterkes mellom de ulike pilarene for å maksimere effekt. Videre identifiserer rapporten konkrete aktører som kontrolleres, brukes eller er under innflytelse av den russiske stat og beskriver hvilke metoder som benyttes for å skape en illusjon av troverdighet (GEC, 2020, s. 8; Sivertsen et al., 2021, s. 19). Modellen er gjengitt i Figur 6.1.



Figur 6.1 *Gjengivelse av modellen «Pillars of Russia's disinformation and propaganda ecosystem» utviklet av Global Engagement Center under US Department of State viser hvordan Russland benytter flere plattformer og aktører i spennet mellom åpent og fordekt. Pilarer f.v.: (1) Official government communications, (2) state-funded global messaging, (3) cultivation of proxy sources, (4) weaponization of social media, (5) cyber-enabled disinformation (GEC, 2020).*

Vi vurderer denne modellen, med tilhørende identifiserte aktører, som et egnet teoretisk rammeverk for å kartlegge spredning av russisk propaganda og desinformasjon. For det første presenterer den russiske aktører og metoder i et rammeverk som tar høyde for at

påvirkningsoperasjoner stadig blir mer sofistikerte, samt utføres via et stadig større økosystem av kanaler og aktører. For det andre fungerer modellen godt til å skille mellom ulike former for påvirkningsaktivitet i spennet mellom åpen («foreign influence») og skjult («foreign interference») og for å kunne se disse i sammenheng med hverandre på tvers av digitale plattformer. Modellen gir dermed mulighet til å fremsette hypoteser som kan testes ut med utvalgte metoder og analyseteknikker, som vil beskrives i dette kapittelet.

Det er også noen utfordringer ved å bruke denne modellen. For det første er modellen ikke et etablert, fagfellevurdert rammeverk for kartlegging av russisk påvirkning i alle tenkelige sammenhenger, men en fremstilling av kunnskapen utviklet av GEC ved det amerikanske utenriksdepartementet basert på etterforskningen av Russlands innblanding i det amerikanske valget i 2016 (GEC, 2020). Vi har også vurdert andre rammeverk, som for eksempel det britiske *RESIST 2 Counter Disinformation Toolkit* (Government Communication Service, 2021). De etablerte modellene vi har funnet, inkludert RESIST 2, er imidlertid først og fremst laget for operativ håndtering og analyse av desinformasjon, ikke for kartlegging og analyse av påvirkningsaktiviteter i det omfanget som behøves i dette oppdraget.

En annen utfordring er at bruk av GECs modell, på grunn av dens rom for kompleksitet, forutsetter at vi benytter oss av flere datakilder og metoder. Et enklere rammeverk kunne vært mindre krevende å jobbe med, men sannsynligvis ikke gitt de samme mulighetene til å forstå og beskrive kompleksiteten i hvordan Russland bruker et mangfold av kilder, plattformer og metoder i samspill.

Etter vår gjennomgang av eksisterende litteratur, er det vår vurdering at GECs «Pillars of Russia's disinformation and propaganda ecosystem» er den best egnede modellen til dette oppdragets formål.

6.1.2 Kinesisk påvirkningsnettverk

Vi har ikke funnet en kartlegging av et kinesisk økosystem for informasjonspåvirkning tilsvarende det russiske kartlagt av GEC.[4] Vi har derfor brukt den samme modellen med fem pilarer (Figur 6.1) og gjennomgått et bredt utvalg av kilder, inkludert forskningsrapporter om kinesisk påvirkning, for å identifisere aktører i de ulike pilarene som er tilknyttet, kontrollert eller eid av den kinesiske stat,[5] eller framstår som forsterkere av kinesiske myndigheters narrativ. Denne tilnærmingen er eksperimentell i den forstand at vi ikke på forhånd kan vite om den er egnet. Valget av denne metoden gjør det muligens lettere å identifisere fellestrekk og ulikheter i hvordan de to statene opererer, og vil slik kunne gi ny kunnskap.

[4] En oversikt publisert 19.11.21 gir oppdatert kunnskap om det kinesiske påvirkningsnettverket. Denne kom for sent for denne rapporten, men vi har kvalitetssjekket våre analyser mot denne. Se oversikten her: https://clintwatts.substack.com/p/chinas-propaganda-and-disinformation

[5] Se vedlegg D for oversikt over de konkrete kildene som vår kartlegging baserer seg på.

6.1.3 Metodisk oversikt over russisk og kinesisk påvirkningsnettverk

For å bruke modellen som et metodisk rammeverk til å kartlegge både russisk og kinesisk informasjonspåvirkning, inkludert spredning av desinformasjon og propaganda i Norge, har vi laget en egen modell basert på GECs *"Five pillars of Russia's disinformation and propaganda ecosystem"* tilpasset formålet og avgrensningene i dette oppdraget. Her bruker vi norske betegnelser (Figur 6.2).

Figur 6.2 Metodisk oversikt over russisk og kinesisk påvirkningsnettverk. Basert på GECs «Pillars of Russia's Disinformation and Propaganda Ecosystem» (Figur 6.1).

6.1.4 Beskrivelse av Russland og Kinas påvirkningsnettverk

Pilar 1: Offisiell myndighetskommunikasjon
Den første pilaren inkluderer Russland og Kinas offisielle myndigheter. Det vil si statenes politiske ledelser, ambassader i Oslo, faste representanter i internasjonale organisasjoner og utvalgte departementer som har interesser relatert til Norge (som handel, utenriks og forsvar). Enkelte nøkkelpersoner i sikkerhetsrådet og utenriksdepartementet er også inkludert, samt offisielle myndighetspersoner som har en betydelig rolle.

Pilar 2: Statsfinansierte medier
Den andre pilaren inkluderer statsfinansierte medier basert i Russland og Kina, samt russiske og kinesiske statsfinansierte medier basert i utlandet. Kildene som er brukt har en klar statlig forbindelse i form av statlig finansiering og redaksjonell kontroll, og har i tillegg vært involvert i spredning av desinformasjon og propaganda. Eksempler fra Russland inkluderer de større mediehusene som *Sputnik* og *RT*, som var involvert i blant annet påvirkningsoperasjonen mot det amerikanske presidentvalget i 2016 (DNI, 2017, s 3; GEC 2020, s 34). Også mindre

nyhetssider er inkludert, som for eksempel *Regnum*, som har spredd misvisende informasjon om en rekke EU-land (EUvsDisInfo, 2018).

På grunn av Kinas omfattende statlige kontroll over egne medier, omfatter dette utvalget de viktigste aktørene i det kinesiske medielandskapet. De største er *People's Daily*, *China Daily* og *Bejing Daily*, samt mediekonserner som *Xinhua News Agency* (Cook, 2020; Twitter, u.å.c).

Pilar 3: Kultivering av proxykilder
Proxykilder er nettsider, organisasjoner og personer som fremstår som uavhengige, men som er finansiert, kontrollert eller under innflytelse av russiske eller kinesiske statlige aktører, eller som skaper, sprer eller forsterker innhold som er i tråd med disse to statenes kjente narrativ og strategiske interesser.

Den tredje pilaren omfatter primært kilder basert utenfor Russlands og Kinas grenser, og som distribuerer pro-russiske og pro-kinesiske nyheter rettet mot et internasjonalt publikum. For Russlands del inkluderer det nettsider som *The Strategic Culture Foundation*, som er knyttet til den russiske etterretningstjenesten SVR, og den kanadiske nettsiden *Global Research*, som er vurdert til å ha en sentral rolle i spredning av russisk desinformasjon (GEC, 2020, s. 12). Eksempler på mindre nettsider inkluderer det pseudo-akademiske tidsskriftet *New Eastern Outlook*, som har forsøkt å tilsløre sin forbindelse til russiske institusjoner, samt det Krim-baserte mediet *News Front*, som tilbyr en «alternativ kilde til informasjon» (ibid.). I vår kartlegging har vi utvidet kildegrunnlaget utover GECs kartlegging ved å legge til flere medier og organisasjoner til listen over det vi mener er reelle proxykilder. Tilføyelser er kun gjort der vi har funnet grundige vurderinger fra etablerte og troverdige kilder (vedlegg C og D).

Eksempler på kinesiske kilder i pilar 3 inkluderer den engelskspråklige nettsiden *Gray Zone* som blant annet har avfeiet kritikken mot Kinas behandling av Uighurene i Xinjiang-provinsen (Allen-Ebrahimian, 2020). Et annet eksempel er den kinesiskspråklige nyhetssiden *Guancha*, som blant annet har spredd desinformasjon om BBCs dekning av kinesiske forhold (Zhang et al., 2021, s. 7). Kildegrunnlaget omfatter også utenlandske medier som distribuerer pro-kinesisk propaganda uten en formell tilknytning til den kinesiske stat, som for eksempel de Hong-Kong-baserte mediene *Phoenix TV* og *Oriental Daily*, samt den engelskspråklige *South China Morning Post* (Cook, 2020).

En oversikt over antall unike kilder i de to påvirkningsnettverkene innenfor hver pilar står beskrevet i Tabell 6.1. Se vedlegg C og D for fullstendig oversikt over kildene i hver pilar.

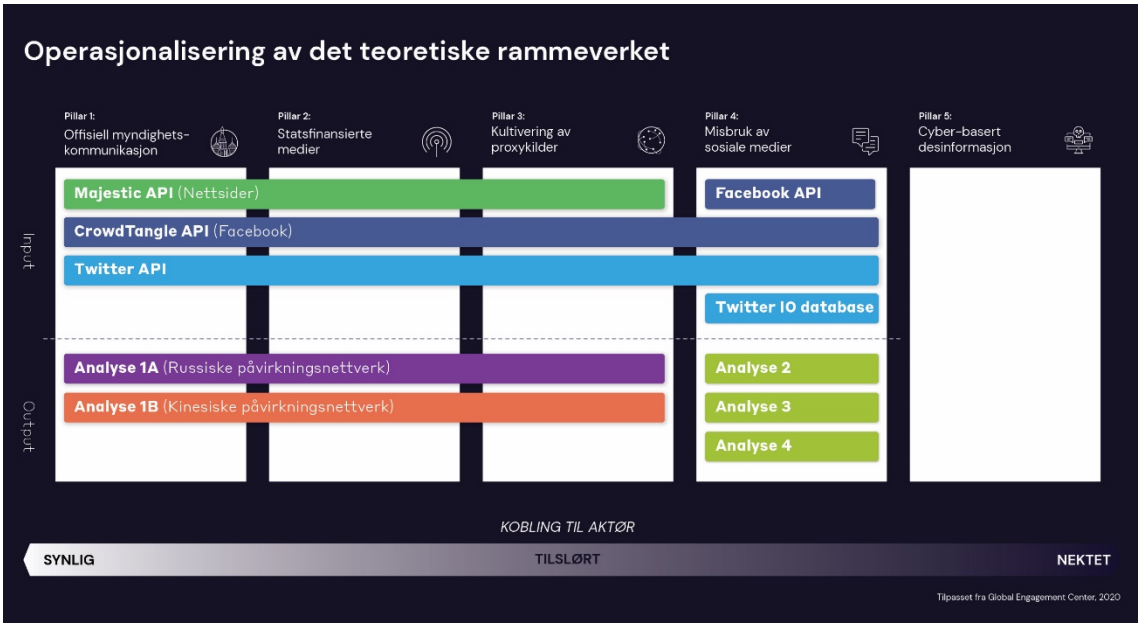
Tabell 6.1 Unike kilder innenfor de tre første pilarene for hver stat. En kilde kan operere med tilstedeværelse på flere plattformer og hjemmesider. Dette fremkommer ikke i denne tabellen. Full oversikt over kilder er å finne i vedlegg C og D.

Stat	**Pilar 1:** Offisiell myndighets-kommunikasjon	**Pilar 2:** Statsfinansierte medier	**Pilar 3:** Kultivering av proxykilder
Russland	13	11	26

Kina	15	32	17

6.1.5 Operasjonalisering av det teoretiske rammeverket

Figur 6.3 viser hvordan vi har benyttet det teoretiske rammeverket for det russiske og kinesiske påvirkningsnettverket (Figur 6.2) til å utføre datainnsamling og analyse. Dette beskrives i de påfølgende underkapitler 6.2 Datagrunnlag, 6.3 Metoder for å avdekke inautentisk adferd og 6.4 Innholdsanalyse.



Figur 6.3 Operasjonalisering av det teoretiske rammeverket vist i Figur 6.2.

6.2 Datagrunnlag

Sosiale medier spiller en viktig rolle i påvirkningsoperasjoner. Analyser av sosiale medier har følgelig vært en sentral del av dette prosjektet. For å kunne kartlegge påvirkningsoperasjoner innenfor prosjektets tids- og ressursbegrensninger, har det vært avgjørende å prioritere hvilke sosiale medier som skal analyseres. Basert på en helhetsvurdering av hvordan kjente påvirkningsoperasjoner er blitt utført (se kapittel 4, og oversikt i vedlegg A), samt hvilke tekniske og juridiske begrensninger som eksisterer for tilgang på data, ble det i begynnelsen av prosjektet gjennomført en prioritetsvurdering av plattformer og andre kilder (vedlegg B).

Ifølge IPSOS SoMe-tracker for Q3 2021, er de sosiale mediene med flest *daglige* brukere over 18 år i Norge: Facebook (68%), Snapchat (49%), Instagram (41%) og YouTube (30%). Twitter ligger på 10% (IPSOS, 2021).

Til tross for at andelen av daglige brukere på Facebook har falt noe de siste årene, er dette fortsatt den desidert største plattformen i Norge, hvor 82% av alle nordmenn over 18 år har en profil og 68% bruker den daglig (ibid.). Facebook er derfor en avgjørende plattform å følge med på i forbindelse med et valg.

I en norsk kontekst er Twitter en liten plattform. 27% av alle nordmenn over 18 år har en profil, og 10% bruker den daglig (ibid.). Twitter er likevel interessant fordi mye politisk debatt foregår her, og fordi plattformen er mye brukt av utenlandske påvirkningsaktører. Facebook og Twitter er også fremdeles de plattformene som brukes mest i utenlandske påvirkningsoperasjoner (Shapiro et al, 2020, s. 10).

Med bakgrunn i dette har vi prioritert to av de viktigste sosiale mediene i Norge som oftest har blitt benyttet i kjente påvirkningsoperasjoner: Facebook og Twitter.

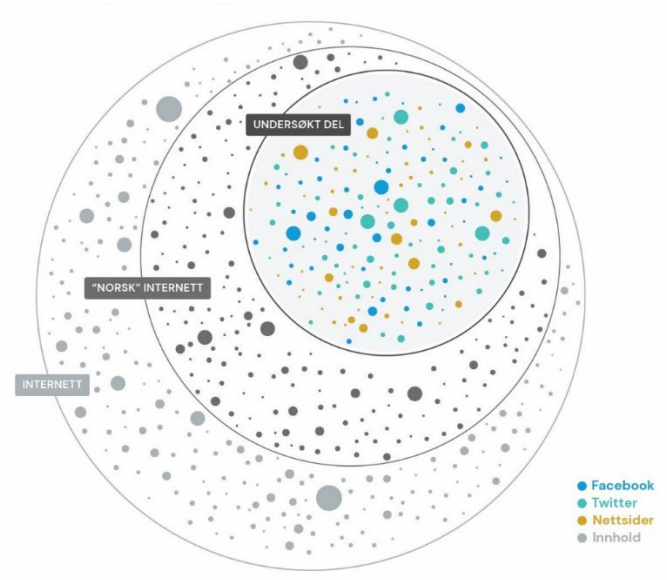
Vi har i tillegg undersøkt innhold fra norske nettsider. Dette inkluderer redaksjonelle nyhetsmedier, alternative medier, blogger, forum og andre åpne nettsider med .no-domene.

Avgrensninger

For å kartlegge og analysere fenomener på internett og i sosiale medier, må man foreta avgrensninger for at datagrunnlaget skal være relevant og håndterbart. I tillegg til egne avgrensninger, finnes det en rekke tekniske og juridiske begrensninger for hvilke data man har mulighet til å samle inn.

En felles avgrensning for alle tre kildene (Facebook, Twitter og norske nettsider) er at vi kun har sett på åpne kilder. I tillegg har vi avgrenset datainnsamlingen fra Facebook og Twitter ved å definere målgruppen som norsk. Vi har derfor kun undersøkt åpne Facebook-grupper og -sider hvor det hovedsakelig deles innhold på norsk og ved å søke etter innhold på Twitter forfattet på norsk (se Figur 6.4 for illustrasjon av denne avgrensningen).

Utfordringer og begrensninger, inkludert validitetsvurderinger av datagrunnlaget, beskrives i kapittel 6.5.



Figur 6.4 Forenklet illustrasjon av datagrunnlaget som rapporten bygger på.

6.2.1 Facebook

Vi har samlet inn data fra Facebook ved hjelp av Facebooks Graph API[6] og CrowdTangles API. Facebooks Graph API (Facebook, u.å.) gir oss adgang til innhold som publiseres på offentlige Facebook-sider. Vi har innsamlet aktivitet som har foregått på 356 norske mediers[7] Facebook-sider og 2 520 norske partipolitiske[8] Facebook-sider (Tabell 6.1). Innlegg og kommentarer til disse er innhentet i perioden 1. januar - 1. oktober 2021. Facebooks API anonymiserer kommentarer som er skrevet til disse offentlige innleggene.

Ved hjelp av CrowdTangles API (CrowdTangle, u.å.a) har vi undersøkt delinger av innhold fra kilder i det russiske og kinesiske påvirkningsnettverket i offentlige Facebook-grupper og sider. Dette gjør det mulig å analysere hvordan innhold deles og interageres med i en digital offentlighet. CrowdTangle er eid av Meta (tidligere Facebook) og oppgir selv at de følger over 7 millioner[9] Facebook-grupper og sider. CrowdTangle inkluderer ikke private grupper eller personlige Facebook-profiler (CrowdTangle, u.å.b). Hverken Facebook eller CrowdTangle oppgir hvor mange grupper og sider som totalt finnes på plattformen, eller som hovedsakelig inneholder norsk innhold.

Per 8. juni 2021 oppgir CrowdTangle (CrowdTangle, u.å.b) at de har en dekningsgrad på 99,64% av alle sider (med registrert aktivitet innenfor perioden 19-28. juni 2021) som har mer

[6] Application Programming Interface, eller programmeringsgrensesnitt på norsk, gir brukere adgang til bestemte data.
[7] Nasjonale, regionale og lokale medier
[8] Sider på nasjonalt, regionalt og lokalt nivå som representerer 17 politiske partier er med. Utover partiene som var representert på Stortinget før valget, har vi også inkludert Alliansen, Demokratene, Folkeaksjonen nei til mer bompenger, Helsepartiet, Industri og Næringspartiet, Liberalistene, Partiet De Kristne og Sentrum.
[9] https://help.crowdtangle.com/en/articles/4201940-about-us

enn 25 000 følgere. Denne andelen faller dramatisk for sider med mellom 500 og 2500 følgere (7,86%). Totalt oppgir CrowdTangle at de dekker 1,9% av alle sider på Facebook. CrowdTangle oppgir ikke hvordan dekningen er for grupper (ibid.). Dette har påvirket våre muligheter til å bruke CrowdTangle til å innsamle delinger på mindre sider og grupper, da CrowdTangle antakeligvis ikke dekker disse. Det finnes dog ingen tilgjengelig oversikt til å vurdere omfanget av dette. Vi har innsamlet informasjonen (Tabell 6.2) over en toårsperiode (september 2019 – september 2021). Informasjonen ble innhentet 5. oktober 2021.

6.2.2 Twitter

Vi har samlet inn data fra Twitter ved hjelp av Twitters API (Twitter, u.å.a). Programmeringsgrensesnittet gjør det mulig å søke etter spesifikt innhold ved hjelp av søkeord.

På grunn av det store volumet av innhold som produseres på Twitter, har vi hatt behov for å filtrere ut irrelevant innhold fra datagrunnlaget for analyse. I 2013 rapporterte Twitter selv at det ble publisert 500 millioner twittermeldinger hver dag på plattformen (Twitter, 2013). Vi har ikke funnet oppdaterte tall fra plattformen siden da, men det er god grunn til å anta at dette tallet har steget de siste 8 årene i takt med at plattformen har vokst.

På grunn av de enorme datamengdene som hver dag blir publisert på plattformen har vi benyttet oss av to strategier for å finne frem til relevant innhold. Ved hjelp av Twitters API har vi kun søkt etter innhold som Twitter, ved hjelp av språkgjenkjenningsalgoritmer, selv har kategorisert som norsk (Twitter, u.å.b). Deretter har vi søkt etter innhold som enten ved bruk av emneknagger eller spesifikke ord omtaler relevante norske tema, medier, partier eller politikere. En nærmere beskrivelse av disse kategoriene finnes i vedlegg F. Fordi vi kun har hatt mulighet til å hente ut innhold som vi allerede kan beskrive, inneholder ikke dette datagrunnlaget alle twitttermeldingene som er forfattet på norsk. Det inneholder heller ikke twittermeldinger som er forfattet på andre språk, men som handler om Norge og norske forhold.

Innhold fra Twitter er innhentet for perioden 1. august - 16. september 2021. Vedlegg G viser omfanget av data som ble innsamlet på de ulike temaene vi har undersøkt. Utover dette har vi innsamlet delinger og medfølgende interaksjoner fra spesifikke lenker til kilder fra de kinesiske og russiske påvirkningsnettverkene[10] over en toårsperiode (september 2019 - september 2021).

6.2.3 Norske nettsider

Det finnes ingen tilgjengelig database over alt innhold som publiseres på norskspråklige nettsider. Vår datainnsamling fra norske nettsider er derfor avgrenset til norske nettsider som inneholder lenker til kilder som er knyttet til Russlands og Kinas påvirkningsnettverk.

Lenker til innhold på norske nettsider, som inneholder lenker til de to påvirkningsnettverkene, er innhentet ved bruk av tjenesten Majestic (Majestic, 2021). Majestic indekserer innhold på internett og inneholder blant annet informasjon om hvordan spesifikke lenker på internett lenker til andre nettsider. Ved hjelp av Majestics API (Majestic, u.å.) har vi samlet inn data for norske

[10] Se vedlegg C og D for hvilke kilder som er med.

nettsider (Tabell 6.2). Data ble innsamlet 5. oktober 2021. Majestic oppgir ikke når innholdet ble publisert eller endret, kun når innholdet ble indeksert. Derfor kan innhold som er samlet inn her være publisert før 2021. Vi har likevel inkludert dette, da gammelt innhold kan få nytt liv på sosiale medier i lang tid etter opprinnelig publisering.

Tabell 6.2 Dataomfang i prosjektet og hvilket datagrunnlag som benyttes i de ulike analysene (analysene beskrives i kapittel 7).

Analyse	Datakilder	Antall	Tidsperiode for datainnsamling
Analyse 1	Innhold på norske nettsider som lenker til kilder fra de to påvirkningsnettverkene	6 241	september 2019 - september 2021
Analyse 1	Delinger av lenker til påvirkningsnettverkene på Twitter	1 031	september 2019 - september 2021
Analyse 1	Delinger av lenker til påvirkningsnettverkene på Facebook	413	september 2019 - september 2021
Analyse 2 og 3	Norske twittermeldinger i valgperioden	360 473	1. august - 16. september 2021
Analyse 2	Norske diskusjonsgrupper på Facebook	325	n.a.
Analyse 2	Innlegg i norske diskusjonsgrupper på Facebook	320 059	1. januar - 1. oktober 2021
Analyse 3	Facebook-sider for norske medier	3756	n.a.
Analyse 3	Norske partipolitiske Facebook-sider	2 520	n.a.
Analyse 3	Innlegg på norske medier sine Facebook-sider i 2021	441 218	1. januar - 1. oktober 2021
Analyse 3	Innlegg på norske partipolitiske Facebook-sider i 2021	171 545	september 2019 - september 2021
Analyse 3	Facebook kommentarer i 2021 til norske mediers sider og partipolitiske sider.	12 455 621	1. januar - 1. oktober 2021
Analyse 4	Twittermeldinger fra offentliggjorte påvirkningsnettverk fra Twitter	137 940 427	2009 - 2020

6.3 Metoder for å avdekke inautentisk adferd

Forskningsresultater, rapporter og vitenskapelig litteratur om påvirkningsoperasjoner gjennomgått til denne rapporten viser at inautentisk adferd på sosiale medier er et gjennomgående virkemiddel for påvirkning - uavhengig av aktør (Giglietto, 2020; Graham et al, 2020; Weber & Neumann, 2021).

Med «inautentisk adferd» menes aktiviteter og handlinger som ikke er utført av autentiske personer eller kan forklares som naturlig eller organisk (DiResta, 2018). Eksempler er falske kontoer, bots og koordinert aktivitet. Vi har derfor sett spesielt etter inautentisk adferd i dette

oppdraget. Dette er en egnet tilnærming for å fange opp både kjente og ukjente aktører, uavhengig av om de er statlige eller ikke-statlige.

Våre undersøkelser av denne adferden baserer seg på tre forhold: Koordinering, kontekstuelle anomalier og digitale fingeravtrykk. Disse beskrives kort i Tabell 6.3.

Tabell 6.3 Metoder for å identifisere inautentisk aktivitet.

Inautentisk aktivitet	Teknikker for å undersøke	Eksempel på bruk av teknikk
Koordinering	Vi identifiserer inautentisk aktivitet som bl.a. er automatisert.	Kan vi se at flere kontoer opptrer koordinert ved å dele samme type innhold samtidig?
Kontekstuelle anomalier	Vi identifiserer inautentisk aktivitet basert på kontekstuelle avvik. For eksempel hvor den digitale aktiviteten ikke passer inn i normale, menneskelige adferdsmønstre.	Kan vi finne aktivitet fra kontoer som virker unormal med tanke på publiseringstidspunkt, volum og intensitet?
Digitale fingeravtrykk	Vi identifiserer inautentisk aktivitet ut fra innholdsmessige likheter.	Bruker forskjellige kontoer identisk språk som kan avsløre at det er den samme aktøren som står bak innholdet uten å opplyse om dette?

Å studere inautentisk adferd er svært utfordrende, hovedsakelig på grunn av tre utfordringer:

- Tilgangen på relevant og anonymisert brukerdata fra plattformene begrenset, men også håndhevet på forskjellige måter av de ulike plattformene. Svært mange studier av inautentisk adferd, som bot-aktivitet, er laget på Twitter. Ikke nødvendigvis fordi plattformen er mest relevant for det man ønsker å undersøke, men fordi denne plattformen deler mer data enn det for eksempel Facebook gjør. Mangel på tilgang vanskeliggjør arbeidet med å identifisere denne type adferd for eksterne aktører, og våre studier av aktivitet på Facebook er derfor begrenset til å se på koordinert deling av innhold.

- Identifikasjon av inautentisk adferd må foregå innenfor strenge etiske og juridiske rammer. Fordi man leter etter aktivitet man i utgangspunktet ikke kjenner til, vil analyser som forsøker å avdekke inautentisk aktivitet også kunne inkludere analyse av autentisk aktivitet. Ingen analyseteknikker er feilfrie, og produktet vil kunne være falske negative (inautentisk aktivitet som ikke fanges opp) eller falske positive (autentiske aktivitet som feilaktig kategoriseres som inautentisk). Dette kan forsøkes løses ved at analyser ikke kun ser på profiler, men også analyserer relevant aktivitet, samt at kvantitative og tekniske analyser følges opp med kvalitative undersøkelser.

- Fenomenet inautentisk aktivitet er i stadig utvikling. Det er mange aktører som har interesse av å påvirke mennesker på sosiale medier. En stor del av dette er aktører som er kommersielt motivert, da det er mange penger å tjene på datatrafikk. Markedet for å

kjøpe inautentisk aktivitet på sosiale medier er i dag så stort at NATO Strategic Communications Center of Excellence (heretter NATO StratCom CoE) omtaler dette som *"the digital manipulation industry"* (Fredheim et al., 2020, s. 38). Mens plattformene løpende forsøker å styrke sitt forsvar mot denne typen aktivitet, har manipulasjonsindustrien sterke insentiver for å innovere for å sikre opprettholdelse av falske profiler og innhold på plattformene. Resultatet er et våpenkappløp mellom plattformene og manipulasjonsindustrien, som innebærer at en tredjeparts forsøk på å avdekke inautentisk aktivitet (som i dette prosjektet) også må evne å fange opp stadig nye og mer sofistikerte metoder (Henin, 2021). En naturlig konsekvens av dette kappløpet er at det ikke vil være mulig å gi et komplett overblikk over all inautentisk aktivitet til enhver tid.

I møte med disse utfordringene har vi i dette prosjektet hovedsakelig valgt å studere inautentisk aktivitet ved å undersøke hvordan innhold deles og spres. Overordnet sett har vi gjort dette på to måter:

- Undersøkt tilstedeværelse av potensielle bots
- Undersøkt om det har forekommet koordinert deling av innhold

Botometer

For å undersøke potensiell bot-aktivitet har vi benyttet oss av verktøyet "Botometer" (Botometer, u.å.a), som er en samling av algoritmer som er utviklet ved The Observatory on Social Media (OsoME) ved Indiana University, i samarbeid med Network Science Institute ved samme universitet. Algoritmene er trent opp til å beregne sannsynligheten for at en konto er en bot.

Treningsdata har, ifølge OsoMe, bestått av titusenvis av annoterte eksempler. Når algoritmen brukes til å undersøke en anonymisert konto, ser den på *"tusenvis av karakteristika som beskriver kontoens profil, venner, sosiale nettverksstruktur, tidsavhengige aktivitetsmønstre, språkbruk og sentiment"* (Botometer, u.å.b).

Botometer har likevel en rekke begrensninger. Algoritmer som er utviklet med bestemte datasett kan være vanskelig å gjenbruke i andre kontekster. Rauchfleisch & Kaiser peker blant annet på at dette kan gjøre det vanskelig å fange opp innhold som ikke er forfattet på samme språk som algoritmene er trent på (Rauchfleisch & Kaiser, 2020). De viser også til at verktøyet generelt har en høy andel av falske negative og falske positive i deres forsøk på å estimere tilstedeværelse av bot-aktivitet. En annen studie peker på at verktøyet i deres eksperiment ikke klarte å fange opp 4 av 5 forskjellige typer bots (Torusdağ et al, 2020). Dette viser hvor utfordrende det er å fange opp denne typen aktivitet, og understreker behovet for videre utvikling innenfor området. Vi har diskutert våre funn ved bruk av denne metoden, samt begrensninger av disse, i kapittel 7.2.1.

Koordinert deling av innhold

I 2018 begynte både Twitter (Gadde, 2018) og Facebook (Gleicher, 2018) å kommunisere utadrettet om det de kaller *koordinert inautentisk adferd*. Nathaniel Gleicher ved Facebook definerer begrepet på følgende måte: *"grupper med sider eller mennesker som samarbeider for å villede andre om hvem de er eller hva de gjør"* (ibid.). Fordelen ved å kun undersøke aktiviteten som gjennomføres er at plattformene ikke nødvendigvis må ta stilling til innholdet som spres. Begrepet "koordinert inautentisk adferd" har imidlertid aldri blitt formelt definert, og teknikkene det rommer, samt datamaterialet som benyttes, varierer fra plattform til plattform (Grégoire, 2021). Til tross for at dette er et forholdsvis nytt begrep, har temaet mottatt økt forskningsinteresse de siste årene, noe som har bidratt til å operasjonalisere hvordan eksterne aktører kan undersøke fenomenet på de store plattformene (Giglietto, 2020; Weber & Neumann, 2021).

For å undersøke om det har forekommet koordinert deling av innhold har vi benyttet oss av *Coordination Network Toolkit*, som er utviklet ved Queensland University of Technology (Graham, 2020). Konkret har vi undersøkt om det er forekommet koordinert deling av lenker på sosiale medier innenfor korte tidsrom, og om dette er en adferd som forekommer gjentatte ganger i tidsperioden. Vi har benyttet denne metoden for å veie opp for noen av de begrensningene som er funnet ved Botometer.

6.4 Innholdsanalyse

Delinger av lenker til kilder fra de to påvirkningsnettverkene har blitt gjennomgått manuelt for å undersøke om innhold fra disse kildene har vært brukt i den hensikt å påvirke valget. Totalt fant vi 7 685 delinger og referanser til de to påvirkningsnettverkene (de tre øverste linjene i Tabell 6.2).

6.4.1 Twitter og Facebook

På Twitter og Facebook har vi undersøkt samtlige 1444 lenkedelinger som vi har identifisert fra det russiske og kinesiske påvirkningsnettverket i perioden 1. september 2019 – 15. september 2021 (rad 2 og 3 i Tabell 6.1). Dette har vi gjort ved å kvalitativt vurdere innholdet i selve artikkelen som er lenket til fra en kilde i påvirkningsnettverkene, samt teksten i innlegget eller twittermeldingen den er delt sammen med. Videre har vi undersøkt hvor mange totale interaksjoner (kommentarer, delinger, likes) hvert innlegg har fått.

6.4.2 Nettsider

Lenker på norske nettsider til nettsider i det russiske og kinesiske påvirkningsnettverket utgjør den største delen av datasettet vårt (rad 1 i Tabell 6.1). Av hensyn til prosjektets tidsramme har vi ikke gjennomgått alle disse lenkedelingene, men begrenset oss til tidsrommet 1.august – 15. september 2021.

Fordi datagrunnlaget fra Majestic ikke inneholder publiseringsdato, men indekseringsdato (kapittel 6.2.3), har vi først manuelt gjennomgått materialet for å utelukke de artiklene som ikke er publisert i de aktuelle tidsrommet. Deretter har vi kvalitativt lest igjennom de artiklene det

lenkes til og kodet dem ut fra om de nevner det norske valget eller norske politikere (ja/nei) og om innholdet kan ansees som forsøk på valgpåvirkning (ja/nei).

6.4.3 Kategorisering av innhold

For å skaffe en oversikt over tematikken i innholdet som spres på Facebook, Twitter og norske nettsider, er delingene blitt kategorisert i følgende tema:

- Forsvars- og sikkerhetspolitikk
- Internasjonal politikk
- Helse
- Migrasjon/religion (inkludert spørsmål om identitetspolitikk og minoriteter)
- Teknologi (inkludert medier og sosiale medier)
- Klima- og miljø

Temaene ble identifisert ved gjennomlesning av et tilfeldig utvalg på 100 delinger av innhold fra det russiske og kinesiske påvirkningsnettverket. Delingene ble også kategorisert i "sekundærtema" som sier noe mer om hva innholdet handler om. Eksempelvis har mange delinger fått hovedtema "helse" og sekundærtema "korona".

I tilfeller der lenken viser til slettet innhold, eller der det ikke har vært mulig å se hvilket innhold det opprinnelig har vært lenket til (eksempelvis dersom det lenkes til en forside som stadig oppdateres), har kategoriseringen vært foretatt på bakgrunn av innholdet i innlegget som lenken er delt sammen med, samt tittelen til lenken der denne har vært tilgjengelig. I de tilfeller hvor artikkelens innhold og teksten den publiseres sammen med ikke har vært samsvarende, er kategoriseringen gjort på bakgrunn av innholdet i artikkelen som det er lenket til.

I tillegg til å systematisere innholdet etter tema, er alle lenkedelingene kategorisert ut fra hvordan den som publiserer innholdet forholder seg til kilden som lenken viser til. Dersom profilen deler en lenke fra en kilde uten å kritisk forholde seg til kilden, kategoriseres delingen som positiv. Delinger som stiller spørsmål ved kildens legitimitet eller tar avstand til kilden den lenker til, kodes som negativ.

6.5 Utfordringer og begrensninger

Det er flere utfordringer knyttet til å undersøke potensiell utenlandsk valgpåvirkning i et digitalt demokrati generelt. I tillegg er det flere spesifikke validitets- og reliabilitetsutfordringer knyttet til denne studien konkret, samt juridiske, opphavsrettslige og etiske krav og begrensninger. Her beskriver vi de viktigste.

6.5.1 Generelle utfordringer

For det første finnes det et stort antall digitale plattformer med ulike egenskaper, bruksområder og demografiske brukergrupper. (IPSOS, 2021). Dette fører med seg en rekke utfordringer. Det er ressurskrevende å undersøke mange plattformer, og det vil alltid være digitale plattformer og miljøer som det av ulike årsaker ikke er mulig å undersøke. Dette kan være fordi man enda ikke

kjenner til dem, fordi tilgang er vanskelig å oppnå, eller fordi juridiske eller tekniske rammer umuliggjør undersøkelser. Videre er det et poeng at fordi strategier og teknikker for valgpåvirkning vil endre seg i takt med teknologiutvikling og -bruk i befolkningen, vil også metodene for å forsøke å avdekke slik påvirkning måtte utvikle seg. Et slikt kappløp vil alltid være gjeldende, men fordi (deler av) påvirkningsoperasjoner av natur er fordekte, vil det være vanskelig å vurdere hvor godt man faktisk ligger an.

For det andre er det utfordringer knyttet til at valgpåvirkning ofte skjer mer indirekte gjennom langsiktige og mer subtile metoder for å skape splittelse, svekke tillit eller påvirke velgeres virkelighetsoppfatning og holdninger til bestemte tema over tid. En endring av velgeres holdninger til bestemte saker vil kunne påvirke hvilket parti de stemmer på, og en svekkelse av tillit til politikere og/eller demokratiske institusjoner vil kunne svekke valgdeltakelsen og tillitten til valgresultatet. Det er svært ressurskrevende å samle inn og analysere de store datamengdene som kreves for å gjennomføre en slik kartlegging. Videre er det vanskelig å skaffe seg tilstrekkelig oversikt over (og kunnskap om) hvilke tema man burde inkludere i denne typen undersøkelser. I tillegg er det en utfordring at jo mer indirekte påvirkningen er, jo vanskeligere vil det være å påvise en årsakssammenheng mellom påvirkningen og dens eventuelle effekt på for eksempel valgdeltakelse.

Avslutningsvis må vi nevne at denne type undersøkelser (uavhengig av tidsperioden som blir undersøkt), i svært stor grad er prisgitt de store teknologiplattformenes villighet til å dele relevant data. Det er store forskjeller på hvordan disse plattformene tilnærmer seg disse spørsmålene, og hvor åpne de er om sine tiltak for å motvirke problematisk adferd på sine plattformer. I august 2021 ble forskere fra New York University, som undersøkte hvordan feil- og desinformasjon ble spredd gjennom annonseringer på Facebook, utestengt av plattformen (Edelson & McCoy, 2021). I september medgikk Facebook at de ved en feil hadde utelatt store mengder data til en rekke samfunnsforskere gjennom sitt akademiske flaggskip-samarbeid *Social Science One* (Timberg, 2021). I oktober 2021 publiserte Twitter resultater fra egen forskning som viser at innhold fra det de kaller «political right» og «right leaning media» opplever algoritmisk fremhevning på plattformen (Twitter, 2021a). Hvordan disse plattformene fortsetter å håndheve adgangen til data for eksterne organisasjoner, og i hvor stor grad de gir innsyn i interne tiltak, prosesser og forskning, vil være avgjørende for fremtidig forskning innenfor dette feltet.

6.5.2 Validitets- og reliabilitetsutfordringer

Det er noen validitets- og reliabilitetsutfordringer knyttet til denne studiens avgrensinger og metodevalg, beskrevet i kapittel 6.2.

Tid: Tidsrommet for våre undersøkelser i avgrenset til perioden 1. august til 16. september 2021. Som beskrevet i foregående underkapittel skjer valgpåvirkning ofte mer indirekte, gjennom langsiktige og mer subtile metoder, for å skape splittelse eller påvirke velgeres virkelighetsoppfatning og holdninger på bestemte tema over lang tid. Å undersøke data i en så kort tidsperiode som 1. august til 16. september vil følgelig kunne svekke studiens validitet. For

å styrke validiteten, har vi inkludert datasett som går opptil to år tilbake i tid på Facebook og Twitter.

Aktører: Kartleggingen av eventuell informasjonspåvirkning fra kjente aktører er avgrenset til Russland og Kina. Det betyr at vi ikke kan utelukke at andre kjente aktører som vi ikke har undersøkt direkte kan ha forsøkt å påvirke valget. Dette kan svekke studiens validitet. For å styrke validiteten, har vi kartlagt inautentisk aktivitet på Facebook og Twitter. I tillegg har vi, på de samme plattformene, søkt etter ord og uttrykk som kan være egnet til å så tvil om valgets integritet. Disse metodene er egnet til å fange opp andre aktører, uavhengig av om de på forhånd er kjent eller ikke.

Datagrunnlag: Kartleggingen inkluderer data fra åpne grupper og sider på Facebook, Twitteraktivitet på norsk og innhold fra norske nettsider, inkludert nyhetssider, «alternative medier» og blogger. Noen validitetsutfordringer knyttet til dette er:

Språk: Denne studien har vært avgrenset til å undersøke innhold på de nevnte plattformene som er forfattet på norsk. Vi har dermed ikke fanget opp innhold som er skrevet på andre språk. Påvirkning kan rettes mot diaspora-grupper med andre morsmål. Fordi en vesentlig del av kartlegging av informasjonspåvirkning er basert på språk, vil eventuelle målrettede påvirkningsforsøk mot fremmedspråklige grupper i Norge bare i begrenset grad kunne fanges opp. En annen utfordring tilknyttet språk er at vi i denne undersøkelsen kun har sett på skriftlig formidling av innhold. Dette fører med seg en annen viktig blindsone, nemlig identifisering av innholdet i videoer og «memes» (bilder med integrert tekst). Med mindre videoer eller memes har blitt delt sammen med en norsk tekst som inneholder relevante søkeord og/eller lenker som viser til kilder til det russiske eller kinesiske påvirkningsnettverket, vil vi ikke fange opp dette. Vi vil imidlertid kunne fange opp dette innholdet dersom innholdet er blitt delt gjennom inautentisk aktivitet, eller dersom innholdet er videredelt med norsk tekst.

Utvalg av plattformer: En viktig validitetsutfordring er knyttet til utvalget av plattformer. Det finnes en rekke andre sosiale medier (for eksempel Instagram, TikTok og YouTube) som vi av ressursmessige årsaker har utelatt. Vi kan ikke utelukke at det har foregått forsøk på påvirkning på disse plattformene. Dette kan svekke studiens validitet. Et annet relevant forhold er at aldersdemografien varierer fra plattform til plattform. Dette kan medføre at vi i mindre grad har fanget opp representativ aktivitet som den yngste velgergruppen i Norge kan ha blitt utsatt for.

Videre finnes det utfordringer knyttet til de enkelte plattformene. På Facebook har det, på grunn av juridiske og tekniske begrensninger, kun vært mulig å undersøke data fra åpne grupper og sider. Vi kjenner ikke til hvor mange lukkede, norske grupper som finnes på Facebook, og kan derfor ikke utelukke at det har foregått informasjonspåvirkning i disse. Facebook offentliggjør heller ingen informasjon om hvor mange norske Facebook-grupper og -sider som finnes totalt sett, så vi vet derfor ikke hvor stor «andel» av det offentlige Facebook for norske brukere vi har undersøkt.

Det er også utfordringer knyttet til studiens analyse av Twitter. Vi har kun undersøkt innhold som enten omhandler spesifikke tema (basert på en egenprodusert liste med søketema og søkeord), eller som inneholder lenker til bestemte kilder. For det første, kan vi ikke være sikre på at denne listen inkluderer *alle* relevante temaer og ord for å kunne fange opp *alt* innhold som omhandler valget, eller at alle relevante meldinger inneholder lenker til bestemte kilder. Dette kan påvirke studiens validitet.

Vi vurderer likevel at datagrunnlaget vårt er relevant og tilstrekkelig for å kunne fange opp eventuelle utenlandske forsøk på å påvirke stortingsvalget 2021, fordi plattformene vi har undersøkt når ut til en stor andel av befolkningen, er de mest brukte til politisk debatt og fordi empiriske eksempler fra andre land viser at disse to plattformene har blitt brukt i flere påvirkningsoperasjoner tidligere.

I vår kartlegging har vi forsøkt å finne ulike former for informasjonspåvirkning. Det at en aktør gjennomfører aktiviteter for å forsøke å påvirke noen, er imidlertid ikke det samme som at disse faktisk blir påvirket. Vi har ikke gjort funn av påvirkningsforsøk som vi kan knytte til valget 2021, og har følgelig ikke hatt et grunnlag for å vurdere effekt.

En sentral *reliabilitetsutfordring* er at undersøkelsene våre er basert på data som tredjepartleverandører har gitt oss tilgang til. Denne tilgangen kan til enhver tid endres fra leverandørenes side. Profiler og innhold kan også slettes fra plattformene, enten av brukerne selv, av de som administrerer grupper og sider eller av plattformene. Dette vil kunne vanskeliggjøre innsamling av et tilsvarende datamateriale som denne rapporten bygger på.

Vi måler også i stor grad på delinger, interaksjoner og videre spredning av innhold basert på måleenheter som plattformene selv har utviklet og implementert. Disse kan endres over tid ved at plattformene endrer struktur eller gjennom måten brukere interagerer med innhold. Innhold som vi har målt i løpet av 2021 vil også kunne ha mottatt nye interaksjoner og delinger etter våre målinger ble gjennomført. I sum vil dette kunne redusere undersøkelsens etterprøvbarhet.

6.5.3 Personvern, opphavsrett og etikk

I dette oppdraget har vi samlet inn data fra åpne kilder på nettsider og sosiale medier. I datasettene kan det finnes persondata, selv om vi ikke aktivt samler inn dette. Dette er en utfordring i slike prosjekter, da innsamling og behandling av persondata er underlagt strenge krav jfr. Lov om behandling av personopplysninger (2018).

For å ivareta kravene har vi benyttet både intern og ekstern juridisk rådgivning, FFIs personvernombud og Datatilsynets veileder for ivaretakelse av grunnleggende personvernprinsipper beskrevet i personvernforordningen (Datatilsynet, 2019). Prosedyrer for behandling, lagring, deling og sletting av persondata er definert i en egen databehandleravtale mellom partene i prosjektet (FFI, Analyse & Tall og Common Consultancy). Databehandleravtalen følger Datatilsynets veiledere «Hvordan lage en databehandleravtale» (Datatilsynet, 2019a) og «Behandlingsansvarlig og databehandler» (Datatilsynet, 2019b), og skal sikre at personopplysninger blir behandlet i samsvar med regelverket og setter en klar ramme for hvordan databehandleren kan behandle opplysninger. Det er også utarbeidet en egen

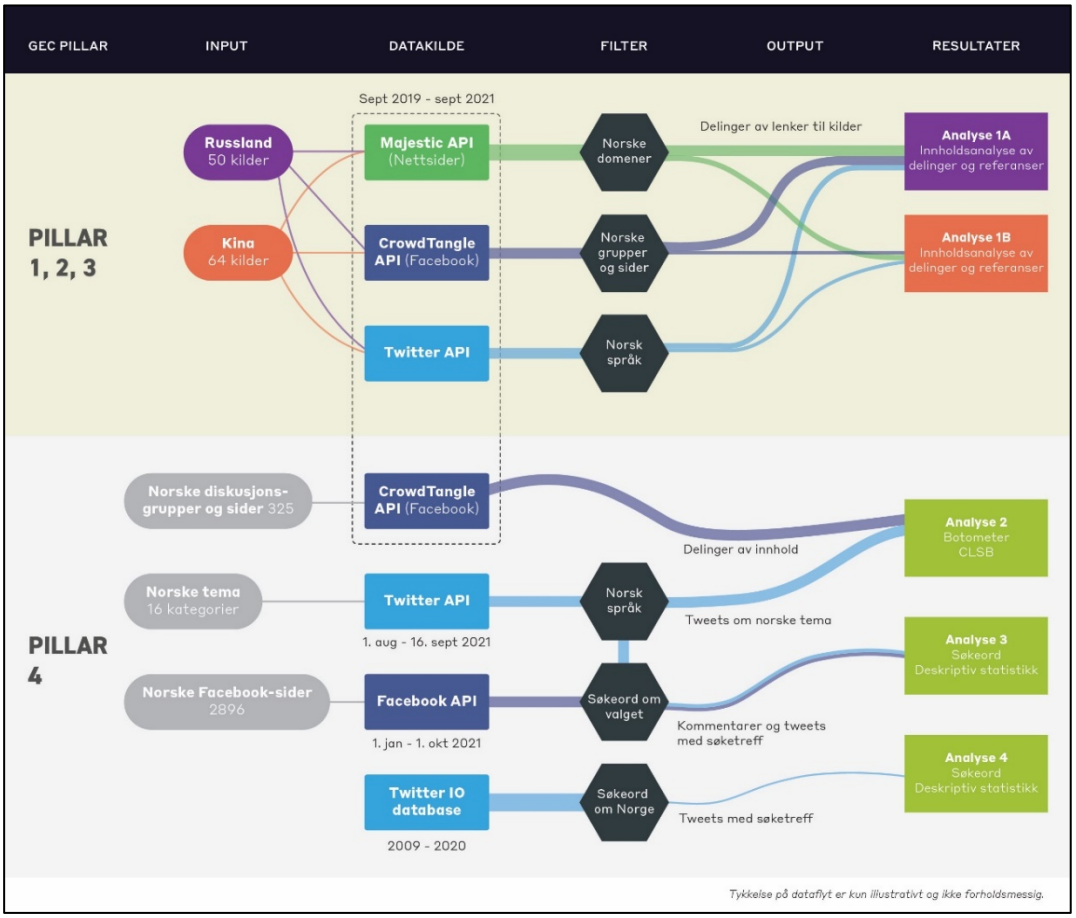
risikovurdering og protokoll for behandling av persondata. Databehandleravtalen, risikovurderingen og protokollen for behandling av persondata er godkjent av FFIs personvernombud.

Vi har i dette prosjektet ikke lastet ned, lagret eller offentliggjort materiale som er omfattet av opphavsrett, jfr. Lov om opphavsrett til åndsverk m.v. (2018).

En sentral del av dette oppdraget har vært innsamling og behandling av data fra norske nettsider og sosiale medier. Dette har vært gjort iht. til strenge krav til ivaretakelse av personvern. For å sikre gode etiske vurderinger i prosessen og i skrivingen av denne rapporten, har vi benyttet *Forskningsetisk veileder for internettforskning* (Den nasjonale forskningsetiske komité for samfunnsvitenskap og humaniora, 2019). Hensikten har vært å avklare eventuelle etiske dilemmaer og fremme god vitenskapelig praksis gjennom arbeidet. De mest sentrale etiske vurderingene som har vært relevante for dette oppdraget er skillet mellom offentlig og privat, ansvaret for konfidensialitet og anonymitet og deling av data, åpne data og stordata.

7 Analyser og resultater

For å få en god oversikt over mulig utenlandsk påvirkning og sikre en bred og grundig avdekning av fenomenene undersøkt i studien, består rapporten av fire selvstendige analyser med hvert sitt datagrunnlag og metodisk tilnærming. Analysene følger logikken i GEC-rammeverket (kapittel 6.1). Datagrunnlag og filtrering av data til de ulike analysene illustreres i Figur 7.1.



Figur 7.1 Oversikt over datainnsamling, filtrering og anvendelse av datamateriale i de fire selvstendige analysene i prosjektet.

Kapittel 7 har følgende struktur:

Kapittel 7.1 avdekker hvorvidt kilder fra det russiske eller kinesiske påvirkningsnettverket er blitt brukt til å spre desinformasjon i forbindelse med valget, diskreditere politiske kandidater eller partier eller påvirke oppslutningen rundt valget. Vi har undersøkt hvordan innhold fra disse kildene blir spredt på norsk eller til et norsk publikum.

Kapittel 7.2 redegjør for undersøkelsene av misbruk av sosiale medier og cyber-basert desinformasjon. Her har vi tatt i bruk flere teknikker for å avdekke bruk av inautentisk aktivitet for å påvirke den norske befolkningen i forbindelse med stortingsvalget 2021. Disse teknikkene er designet for å kunne avdekke inautentisk adferd uavhengig av aktør, og vil derfor kunne fange opp både statlig og ikke-statlig aktivitet fra både kjente og ukjente aktører.

Kapittel 7.3 undersøker det om valgets integritet har vært gjenstand for diskusjoner i sosiale medier. Her har vi sett etter utslag i måten valget har blitt omtalt på i kommentarfelt på åpne, norske Facebook-grupper og –sider, samt i norske twittermeldinger på Twitter.

Kapittel 7.4, beskriver gjennomførte søk etter omtale av Norge i databaser over kjente påvirkningsoperasjoner, eksisterende kartlegginger av spredning av desinformasjon og kjente tilfeller av koordinert inautentisk adferd.

7.1 Analyse 1: Spredning fra det russiske og kinesiske påvirkningsnettverket i Norge

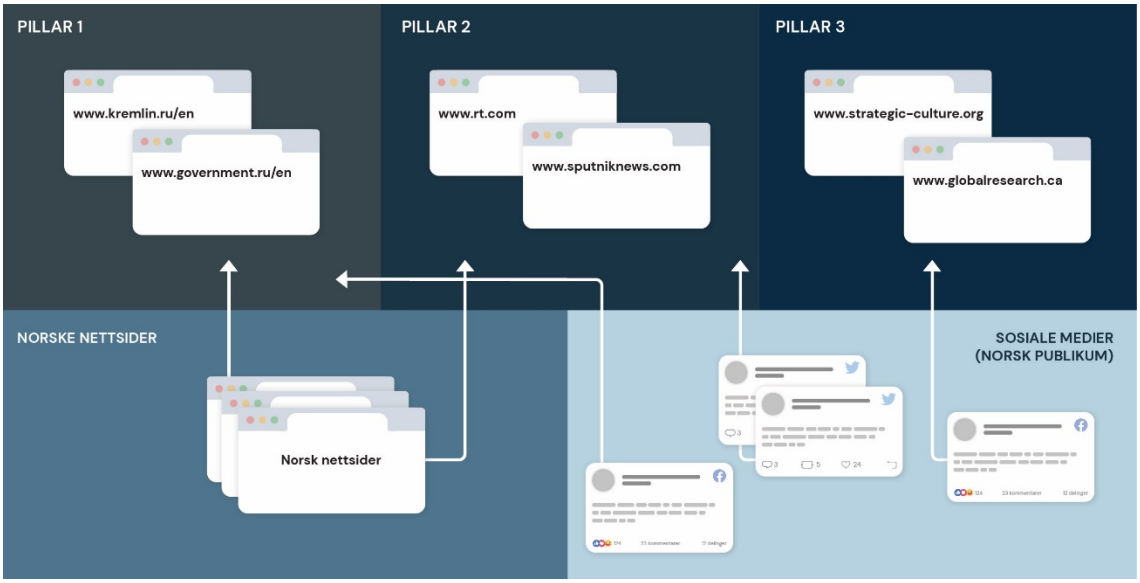
Analyse 1 består av analysene 1A (Russland) og 1B (Kina). Her gjennomgås hvor mye innhold fra kilder (vedlegg C og D) i det russiske og det kinesiske påvirkningsnettverket som har blitt spredd til et norsk publikum via Facebook, Twitter og norske nettsider i perioden 1. september 2019 – 15. september 2021. Tabell 7.1 viser hvor mange lenker til nettsider i det russiske og det kinesiske påvirkningsnettverket som har blitt delt på de ulike plattformene i perioden.

Tabell 7.1 Oversikt over samtlige referanser til kilder i de to påvirkningsnettverkene. Tabellen viser delinger på Facebook og Twitter av lenker til kilder i det russiske og kinesiske påvirkningsnettverket (Pilar 1-3) og referanser til de samme kildene på norske nettsider. (Pilar 1: Offisiell myndighetskommunikasjon, Pilar 2: Statskontrollerte medier, Pilar 3: Proxykilder).

		Antall referanser/delinger av lenker			
Påvirkningsnettverk	**Plattform**	**Pilar 1**	**Pilar 2**	**Pilar 3**	**Sum**
Russland	Facebook	10	180	155	345
	Twitter	8	400	325	733
	Nettsider	573	1903	992	3468
	Sum	591	2483	1472	4546
Kina	Facebook	0	28	40	68
	Twitter	7	72	219	298
	Nettsider	324	1730	719	2773
	Sum	331	1830	978	3139

I løpet av det siste året fram mot stortingsvalget 2021, har lenker til kilder i det russiske påvirkningsnettverket blitt delt til sammen 4 546 ganger i norske, åpne grupper og sider på Facebook, blant norskspråklige brukere på Twitter og på norske nettsider. For det kinesiske påvirkningsnettverket er det samme tallet 3 139. Mer detaljer om spredningen omtales i analyse 1A (det russiske påvirkningsnettverket) og analyse B (det kinesiske påvirkningsnettverket).

Måten delingen foregår på illustreres forenklet i Figur 7.2, som viser hvordan både norske nettsider og innlegg på Facebook og Twitter lenker til kilder i de to påvirkningsnettverkenes tre pilarer «offisiell myndighetskommunikasjon» (pilar 1), «statskontrollerte medier» (pilar 2) og «proxykilder» (pilar 3).



Figur 7.2 *Illustrasjon av hvordan datamaterialet for analyse 1A og 1B er bygget opp. Delinger og lenker til kilder fra pilar 1 (offentlig myndighetskommunikasjon), pilar 2 (statskontrollerte medier) og pilar 3 (kultivering av proxykilder) er innsamlet for perioden 1. september 2019 – 15. september 2021.*

Vår vurdering av datasettet er at den største andelen av delingene som er registrert foregår organisk i digitale miljøer der det finnes en etterspørsel etter nyheter og innhold fra andre kilder enn norske redaksjonelle medier. *I vår gjennomgang har vi ikke funnet eksempler på aktivitet som vi mener at kan kategoriseres som forsøk på valgpåvirkning.*

Vurderingen er basert på resultatene av analyse 1A og 1B.

7.1.1 Analyse 1A: Spredning fra det russiske påvirkningsnettverket

I det følgende vil vi redegjøre for hvor mange delinger av lenker til kilder i det russiske påvirkningsnettverket som vi har identifisert i løpet av de siste to årene, som ble rettet mot et norsk publikum. *Kort oppsummert har vi ikke funnet innhold som direkte omhandler det norske stortingsvalget i det russiske datasettet*. I det følgende beskrives delingsmønstrene på de ulike plattformene.

7.1.1.1 Delinger på Twitter

I vårt datasett finner vi 733 delinger av lenker til kilder i det russiske påvirkningssystemet på Twitter i perioden september 2019 – september 2021. Til sammenligning fant vi 11 533 norske twittermeldinger i perioden 1. august – 16. september 2021 som nevnte det norske valget[11]. Delingene fordeler seg på følgende måte: 8 delinger stammer fra offisielle russiske

[11] Ved bruk av følgende søkeord: #valg, #valg21, #valg2021, #2valg, #nrkvalg, stortingsvalg, stortingsvalg2021, stortingsvalg21

kommunikasjonskanaler (1. pilar). 400 delinger med lenker til statseide medier eller medier med tilknytning til den russiske stat (2. pilar). 325 delinger av lenker til kilder som kan karakteriseres som proxykilder (3. pilar). Samlet har de 733 delingene (alle på norsk) mottatt 1 896 interaksjoner. På Twitter defineres interaksjoner som likes, kommentarer (replies) og retweets.

RT International er det russiske mediet som har fått flest delinger til et norsk publikum på Twitter. Innhold fra RT International har 268 delinger i vårt datasett. Deretter følger det konspiratoriske amerikanske mediet Zero Hedge (159), det russiske nyhetsbyrået TASS (86), Global Research (49) som er en kanadisk hjemmeside som ifølge GEC er "dypt innviklet" i det russiske påvirkningsnettverket (GEC, 2020) og The Russophile/Russia News Now (47).

Vi har undersøkt hvilke tema fra disse mediene som oftest er bakgrunnen for delingen. På Twitter er det primært temaene internasjonal politikk (182), helse (172) og forsvars- og sikkerhetspolitikk (142), men det deles også innhold som handler om migrasjon/religion (73) og klima- og miljø (51). *Vi har ikke funnet eksempler på delinger som omhandler det norske stortingsvalget, og vi finner ingen delinger som fremstår som forsøk på å påvirke valgresultatet, valgdeltakelsen eller tilliten til valget.*

7.1.1.2 Kontekst for delinger på Twitter

Den største andelen av delingene av kilder fra det russiske påvirkningsnettverket blir delt av norskspråklige profiler som fremstår kritiske til den norske mediedekningen, og som ønsker seg alternative perspektiver på aktuelle hendelser. De 10 mest aktive profilene i datasettet står for 348 av 733 delinger. Disse delingene har totalt mottatt 828 interaksjoner. Dette tyder på at delinger av innhold fra det russiske påvirkningsnettverket foregår i et forholdsvis lite digitalt miljø på Twitter, og at delingene ikke når bredt ut til et norsk publikum. Ingen av de 733 delingene har oppnådd noe som kan klassifiseres som viral spredning.

7.1.1.3 Delinger på Facebook

I den samme tidsperioden finner vi 345 delinger av lenker til kilder i det russiske påvirkningsnettverket til et norsk publikum på Facebook (til sammenligning delte 356 norske medier 833 581 lenker i samme tidsperiode på sine Facebook-sider). 10 av disse delingene kommer fra offisielle russiske kilder (1. pilar). 180 delinger inneholder lenker til statseide medier eller medier med tilknytning til den russiske stat (2. pilar). 155 delinger er av lenker til kilder som kan karakteriseres som proxykilder (3. pilar). Samlet har de 345 delingene mottatt 6 986 interaksjoner. Det er vanskelig å sammenligne interaksjonstall mellom de to plattformene, men denne forskjellen kan tyde på at Facebook er en bedre egnet plattform for å nå ut til et norsk publikum.

RT International er også den mest delte kilden på Facebook. Av de 345 delingene kommer 129 fra RT International. Deretter følger Global Research (51) og Fort Russ News (50), Zero Hedge (40) og Sputnik News (31). De resterende delingene i datamaterialet fordeler seg på 14 ulike kilder.

På Facebook er det helse som er det desidert største temaet (122), og det er særlig koronaviruset, pandemihåndtering og vaksiner som utgjør den største delen av dette. Deretter kommer internasjonal politikk (87) og forsvars- og sikkerhetspolitikk (46). *Vi har ikke funnet eksempler på delinger som omhandler det norske stortingsvalget, og vi finner ingen delinger som fremstår som forsøk på å påvirke valgresultatet, valgdeltakelsen eller tillitten til valget.*

Det er verdt å nevne at vi finner 45 delinger fra kilder i det russiske påvirkningsnettverket, hvor enten Norge, norske politikere eller norske forhold direkte tematiseres i artiklene det lenkes til eller i teksten hvor lenken deles. Av disse handler 20 om forsvars- og sikkerhetspolitikk, 15 om internasjonal politikk, 4 om klima- og miljø, 2 om migrasjon/religion eller identitetspolitikk, 2 om teknologi og 2 om helse. Delingene som er kategorisert som forsvars- og sikkerhetspolitikk handler i hovedsak om grenseområdene mellom Russland og Norge eller Svalbard. I kategorien internasjonal politikk spenner temaene bredt, og handler om alt fra menneskerettigheter, handelsavtaler, diplomati og skattepolitikk. Også i denne kategorien er det i hovedsak forholdet mellom Norge og Russland som er temaet i kilden eller delingen av denne.

7.1.1.4 Kontekst for delinger på Facebook

328 av de 345 delingene vi finner på Facebook foregår i åpne grupper. I det følgende ser vi nærmere på hva som kjennetegner disse gruppene generelt sett.

Selv om både Facebook-grupper og Facebook-sider er offentlige og har moderatorer, skiller grupper seg fra sider ved at også medlemmer av gruppen kan publisere innhold på lik linje med moderatorene. Facebook-sider er i hovedsak profiler hvor moderator kommuniserer til et publikum, mens Facebook-grupper kan betraktes som interessefellesskap hvor medlemmene kommuniserer og diskuterer med hverandre.

At nesten alle lenkedelingene forekommer i åpne grupper på Facebook passer godt inn i utviklingen på plattformen i senere år, hvor Facebook har endret sine algoritmer til å promotere grupper til sine brukere (Zuckerberg, 2018). Men ut fra et scenario om utenlandsk påvirkning er det likevel verdt å merke seg denne fordelingen. Facebook-grupper er avgrensede fellesskap hvor forskere og analytikere har mer begrenset adgang til å undersøke innholdet enn på Facebook-sider. Dette gjør det vanskeligere for uavhengige organisasjoner å undersøke om og hvordan utenlandsk påvirkning foregår i Facebook-grupper. Samtidig er tanken med Facebook-grupper at likesinnede brukere skal kunne møtes og utveksle ideer og informasjon med relevante fellesskap. Dette kan øke risikoen for at aktive medlemmer av slike Facebook-grupper utvikler eller styrker forutinntatte meninger i grupper som oftest består av en homogen medlemsmasse (Van Raemdonck, 2019).

Når vi ser nærmere på de gruppene som har delt lenker til kilder fra det russiske påvirkningsnettverket, finner vi flere grupper som Faktisk.no, i en tidligere kartlegging, har kategorisert som ‘systemkritisk’, ‘generell’ eller ‘nasjonalistisk’ (Dahlback, 2021). Innholdet som deles i disse gruppene har i stor grad det til felles at de stiller seg kritisk til myndigheter og redaksjonelle medier, og at det deles innhold fra norske og utenlandske alternative medier og blogger.

I gruppene finner vi også eksempler på at delinger til lenker fra kilder i det russiske påvirkningsnettverket brukes til å understøtte medlemmenes synspunkter om at myndighetene enten ikke har håndtert koronapandemien på en god måte, eller at Norges syn på Russland bygger på falske premisser. De 10 gruppene som sammenlagt har flest delinger i datasettet vårt har totalt 41 761 medlemmer[12] og står for 170 av 345 lenkedelinger, nesten halvparten av alle delingene i utvalget.

7.1.1.5 Eksempler på potensiell problematisk adferd

I flere tilfeller har vi funnet at lenker til kilder i det russiske påvirkningsnettverket blir delt i mange forskjellige grupper i løpet av en kort tidsperiode. Et eksempel på slike delinger er en artikkel fra S*putnik News* (2. pilar) som ble publisert 12. mars 2020, med tittelen "*Escaping Pandemic: World's Rich Head Off to Bunkers Amid the Outbreak of Coronavirus"* (Sputnik News, 2020). Lenken er delt i fem ulike norske Facebook-grupper 15. mars samme år, i løpet av 22 sekunder. To av delingene foregår innenfor samme sekund. Teksten som følger med delingen er identisk i alle fem innlegg. Gruppene det er snakk om har sammenlagt 28 715 medlemmer og lenkedelingene har totalt mottatt 97 interaksjoner. På grunn av personvern, har vi ikke undersøkt hvem som står bak disse delingene.

Eksempelet ovenfor fra Sputnik News anses ikke som direkte relevant for stortingsvalget 2021. Det viser imidlertid hvordan profiler som ønsker å spre informasjon om et emne, eller påvirke i en sak, relativt lett kan nå et stort publikum ved å benytte seg av flere forskjellige Facebook-grupper. Det viser også hvor utfordrende det er å skille mellom inautentisk og autentisk aktivitet for uavhengige organisasjoner som ikke har tilgang til de samme datapunktene som de sosiale medieplattformene har.

7.1.1.6 Lenkedelinger på sosiale medier i valgperioden

I perioden fra 1. august til 16. september fant vi totalt 56 delinger av lenker til kilder fra det russiske påvirkningsnettverket. Av disse er 54 prosent fra statskontrollerte medier (2. pilar) og 46 prosent fra proxysider (3. pilar). Vi finner ingen delinger fra kilder i 1. pilar, offisiell myndighetskommunikasjon, i dette utvalget. 43 av lenkedelingene forekom på Twitter og 13 på Facebook. Totalt mottok delingene 236 interaksjoner på de to plattformene.

Kun to av delingene omhandler Norge eller norsk politikk. Den ene er en artikkel fra TASS om russisk oljeproduksjon og det norske firmaet Rystad Energy. Den andre er en artikkel om konflikt mellom Tyskland og Russland om Nord Stream 2, hvor Norge ikke tematiseres i selve artikkelen, men i delingen fra profilen. Majoriteten av artiklene i denne perioden handler om helse og korona, henholdsvis 61% på Facebook og 40% på Twitter. Deretter utgjør forsvars- og sikkerhetspolitikk og internasjonal politikk de resterende kategoriene, totalt 17 lenkedelinger.

[12] En Facebook-profil kan være medlem av flere grupper, så det samlede tallet over individuelle profiler som er medlem i disse gruppene kjenner vi ikke til, men det er sannsynligvis lavere.

Kort oppsummert finner vi ikke endret aktivitet i valgperioden verken i hvilke profiler som er aktive eller hvilke tema innleggene handler om. Vi finner ikke innhold som fremstår som forsøk på å påvirke valgresultatet, valgdeltakelsen eller tillitten til valget.

7.1.1.7 Lenker på norske nettsider i valgperioden

Som en del av kartleggingen har vi identifisert norske nettsider som lenker til kilder i det russiske påvirkningsnettverket. Til sammen har vi identifisert 398 unike artikler/nettsider (av totalt 3 468) som ble indeksert etter 1. august 2021. 139 av disse viste seg å ha blitt publisert før 1. august og er derfor holdt utenfor vår kvalitative gjennomgang. 43 av lenkene var ikke lenger tilgjengelig fordi nettsiden de viste til enten var slettet eller det dynamiske innholdet de viste til (for eksempel en nyhetsstrøm) ikke lenger var tilgjengelig. De resterende 216 lenkedelingene er kategorisert kvalitativt.

Av disse fant vi 3 lenker som nevner det norske valget og som samtidig refererer til kilder i det russiske påvirkningsnettverket. To av disse kritiserer forskning.no for å drive med valgpåvirkning i et oppslag om hvilke saker Russland ønsker at nordmenn skal stemme på, og beskriver både RT og forskning.no som propagandanettsteder. Den andre lenken er publisert på en norsk nettside om globale nyheter og kritiserer lederen av Demokratene for å drive valgkamp på RT (Færseth, 2021; Karlsen, T, 2021).

7.1.2 Analyse 1B: Spredning fra det kinesiske påvirkningsnettverket

I det følgende redegjøres det for hvor mange delinger av lenker til kilder i det kinesiske påvirkningsnettverket som vi har identifisert i løpet av de siste to årene, som ble rettet mot et norsk publikum. *Kort oppsummert har vi ikke funnet innhold som direkte omhandler det norske stortingsvalget i det kinesiske datasettet.*

7.1.2.1 Delinger på Twitter

Som med det russiske datasettet, er det viktig å presisere at delingene det henvises til i denne delen av rapporten kun gjelder twittermeldinger der det er en direkte lenke i twittermeldingen til en av kildene i det kinesiske påvirkningsnettverket.

I datasettet finner vi 298 delinger på Twitter. 7 stammer fra offisielle kinesiske kanaler (1. pilar). 72 delinger lenker til kinesiske statsstyrte medier eller medier med tilknytning til den kinesiske stat (2. pilar). 219 delinger stammer fra kilder som kan karakteriseres som proxykilder (3. pilar). South China Morning Post er det mediet som er delt flest ganger (163), etterfulgt av Gray Zone (55), Global Times (36), Xinhua News Agency (13) China Daily (12).

Innholdet som deles handler i de fleste tilfellene om internasjonal politikk (113) og helse (98). Samtlige av artiklene som handler om helse handler om korona. Resterende innhold (87) handler om tematikk knyttet til sikkerhets- og forsvarspolitikk, teknologi, samt klima og miljø.

7.1.2.2 Kontekst for delinger på Twitter

Det er 174 profiler som står bak de 298 delingene på Twitter. Av disse er det 143 (82%) som kun har delt én lenke. Det er kun 6 profiler som har delt fem eller flere lenker, og disse har til sammen 20 721 følgere. Majoriteten av disse (18 897 følgere) tilhører to norske journalister og en bot som utelukkende retweeter norske journalister (599 følgere). De resterende tre profilene (totalt 1824 følgere) som deler hyppigst på Twitter ser ut til å være privatpersoner (med åpne kontoer), som publiserer innhold som handler om internasjonal politikk og helse (korona).

7.1.2.3 Delinger på Facebook

På Facebook har vi funnet 68 delinger av kilder fra det kinesiske påvirkningsnettverket. 28 av delingene på Facebook stammer fra statsstyrte medier eller medier med tilknytning til den kinesiske stat (2. pilar). 40 delinger stammer fra proxykilder (3. pilar).

Av de 68 delingene er det South China Morning Post (28) som er den største kilden til delinger. Deretter følger Xinhua News Agency (14), Gray Zone (11), Global Times (9) og China Daily (4), China Global Television Network (1) og Ming Pao (1). På Facebook er det mest omtalte tema internasjonal politikk (45), etterfulgt av helse (12), innenrikspolitikk (7) og klima og miljø (4).

7.1.2.4 Kontekst for delinger på Facebook

10 av de 68 delingene vi har funnet på Facebook er delt av den offisielle Facebook-siden til den kinesiske ambassaden i Norge. I tillegg til ren informasjon om ambassadens aktiviteter, handler disse delingene om Kina som destinasjon for turisme og som foregangsland i utviklingen av teknologi, jordbruk og transport. Facebook-siden har 3 921 følgere og de ti delingene har til sammen mottatt 449 interaksjoner.

De profilene som har delt flere lenker fra det kinesiske nettverket er i hovedsak norske Facebook-grupper eller sider som er kritiske til Kinas politikk på regionale eller nasjonale forhold. Her finner vi også Facebook-sidene til to norske partiledere som har delt hvert sitt innlegg om demokratibevegelsen i Hongkong. Det er også kritikken av kinesiske myndigheter som har gitt flest interaksjoner. Blant de resterende profilene ser vi et overlapp mellom myndighetskritiske og mediekritiske grupper som også har delt lenker til kilder fra det russiske påvirkningssystemet. I disse gruppene spres det også lenker fra norske alternative medier og artiklene som spres handler i hovedsak om korona.

7.1.2.5 Lenkedelinger på sosiale medier i valgperioden

I valgperioden (august-september 2021) fant vi totalt 13 delinger av lenker på Facebook og Twitter. 11 av disse er delt på Twitter og 2 på Facebook. Kun én av disse kom fra offisielle kinesiske kanaler (1. pilar), 5 fra statsstyrte medier eller medier med tilknytning til det kinesiske stat (2. pilar). 7 kom fra proxykilder (3. pilar). Vi finner ikke noe innhold som kvalifiserer som valgpåvirkning i denne perioden.

7.1.2.6 Lenker på norske nettsider i valgperioden

Til sammen har vi identifisert 187 lenker til kilder i det kinesiske påvirkningsnettverket på norske nettsider som ble indeksert etter 1. august 2021. 136 av disse var enten publisert før 1. august eller var slettet/ikke tilgjengelig, og er derfor holdt utenfor vår kvalitative gjennomgang. Vi har utført en kvalitativ gjennomgang av det resterende innholdet, og ikke funnet tegn til valgpåvirkning. Det norske valget blir heller aldri nevnt i dette innholdet.

7.1.2.7 Forskjell på spredning fra det russiske og kinesiske påvirkningsnettverket

Da vi undersøkte spredning fra det russiske påvirkningsnettverket fant vi at lenkene i hovedsak publiseres for å videreformidle innholdet eller budskapet i artiklene, eller for å underbygge et argument. De fleste publiseringene var videreføring av budskapet fra kilden og vi fant i liten grad kritikk av russiske myndigheter eller russisk presse.

I innleggene der det lenkes til det kinesiske påvirkningsnettverket ser vi derimot at profilene/innleggene er kritiske til kinesiske myndigheter. Lenkedelingene brukes for eksempel i innlegg som støtter demokratibevegelsen i Hongkong, Tibet eller minoriteter i Kina som står i opposisjon mot kinesiske myndigheter. Dette kan tyde på at de aktørene vi har identifisert i liten grad har potensial til å fungere som kanaler for påvirkning fra Kina fordi de i utgangspunktet er kritiske til kinesiske myndigheter.

7.1.3 Konklusjon, analyse 1A og 1B

Denne analysen har hatt som formål å avdekke hvorvidt innhold fra russisk eller kinesisk påvirkningsnettverk har blitt spredd til et norsk publikum på Facebook, Twitter eller på norske nettsider i forbindelse med stortingsvalget 2021. Mer spesifikt har vi undersøkt hvorvidt kilder fra disse nettverkene er blitt brukt til å spre desinformasjon som er egnet til å påvirke valgresultatet, valgdeltakelse eller tilliten til valggjennomføringen.

Analysen viser at innhold fra både det russiske og kinesiske påvirkningsnettverket når ut til et norsk publikum via sosiale medier og norske nettsider. Informasjon fra det russiske påvirkningsnettverket spres jevnlig i miljøer som er kritiske til norske myndigheter og tradisjonelle medier, og som ønsker et annet perspektiv på aktuelle begivenheter. Vi finner eksempler på spredning av informasjon fra det russiske påvirkningsnettverket som foregår med aktivitet som fremstår som inautentisk. Vi kan ikke knytte denne spredningen til bestemte aktører, og informasjonen som spres handler ikke om stortingsvalget. Informasjon fra det kinesiske påvirkningsnettverket oppnår ikke samme spredning på sosiale medier, og deles som oftest i forbindelse med kritikk av den kinesiske regjeringen. Det analyserte innholdet vurderes ikke som egnet til å påvirke valgresultatet, valgdeltakelse eller tilliten til valggjennomføringen.

7.2 Analyse 2: Inautentisk aktivitet på sosiale medier

Vår andre analyse har forsøkt å detektere inautentisk aktivitet i forbindelse med stortingsvalget 2021. Vi har valgt denne fremgangsmåten da den vil kunne avdekke påvirkningsaktivitet gjennom problematisk adferd uten å på forhånd måtte kjenne til hvilke aktører som kan stå bak. Som beskrevet i kapittel 6.3, er inautentisk aktivitet en kompleks størrelse som dekker flere elementer.

7.2.1 Undersøkelse av bot-aktivitet på Twitter

I analysen har vi undersøkt hvordan 84 474 norske twittermeldinger som er innsamlet ved bruk av 16 tematiske søkeordlister kan være utsatt for bot-aktivitet. Anonymiserte profiler som har tweetet, liket eller retweetet de originale twittermeldingene har blitt undersøkt ved hjelp av algoritmene i Botometer (Botometer, u.å.a). Algoritmene rangerer profiler på en skala fra 0 til 5, hvor 0 betyr mest 'human-like' og 5 betyr mest 'bot-like' (Botometer, u.å.a).

I første omgang kategoriserte Botometer 14 456 twittermeldinger til å være utsatt for bot-aktivitet, ved at profiler som enten hadde tweetet, liket eller retweetet hadde en score på 4 eller mer. Ved kvalitativ kvalitetssjekk av disse resultatene, kunne vi imidlertid fastslå at algoritmene har en meget høy grad av falske positive resultater. Dette kan komme av at innholdet vi har undersøkt er forfattet på norsk, som tidligere omtalt i kapittel 6.3. Vi valgte derfor å heve terskelen for vurdering av hvilke twittermeldinger som potensielt var utsatt for bot-konti, ved å kun inkludere twittermeldinger hvor algoritmene mente at tre eller flere bot-konti hadde deltatt (fortsatt med en score på 4 eller mer).

Dette resulterte i at 1 148 twittermeldinger ble kategorisert til å være utsatt for bot-aktivitet. *Av disse fant vi ingen tegn på aktivitet som fremstår som forsøk på å påvirke valgresultatet, valgdeltakelsen eller tillitten til valget.*

Det er viktig å understreke at disse resultatene ikke kan tolkes som at det er en høy grad av tilstedeværelse av bot-kontoer i vårt datamateriale. Fordi verktøyet har kjente begrensninger (beskrevet i kapittel 6.3), har vi kun brukt resultatene som en filtreringsmekanisme for videre analyser. Her fant vi to kontoer som etter nærmere undersøkelse viste seg å være en del av et kjent ikke-statlig påvirkningsnettverk. Aktiviteten er verken knyttet til den kinesiske stat eller til påvirkning av stortingsvalget, men er egnet som en illustrasjon på en ikke-statlig påvirkningsaktør. Vi har derfor beskrevet disse funnene som en egen casestudie på side 57.

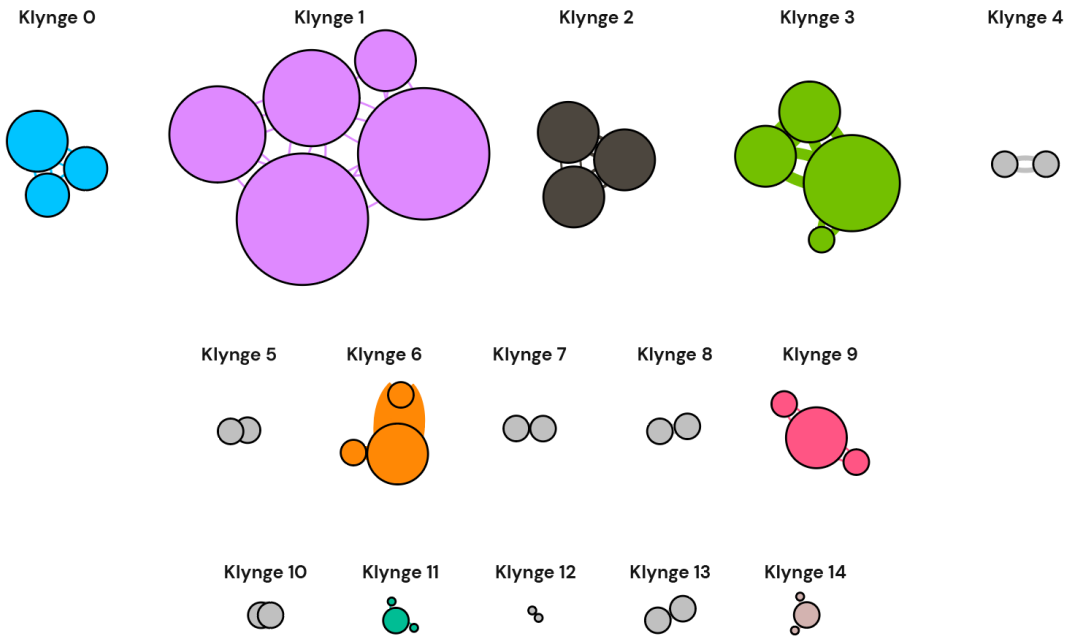
Til tross for at metoden produserte en rekke falske positive resultater, avdekket den aktivitet som med stor sannsynlighet er inautentisk. Om det er en effektiv metode for å avdekke inautentisk aktivitet generelt, og i en norsk kontekst spesielt, er imidlertid usikkert, som tidligere diskutert i kapittel 6.3.

7.2.2 Undersøkelse av koordinert lenkedeling på Twitter

Vi har undersøkt om det har foregått koordinert deling av de samme lenkene på Twitter i løpet av tidsperioden 1. august - 16. september 2021. Datagrunnlaget kommer fra 16 tematiske

søkeordlister for å kartlegge relevante tema på Twitter, benevnelser av de daværende partilederne for partiene som var representert på Stortinget før valget eller partiene og nasjonale og regionale medier i Norge. Analysen er basert på 360 473 originale twittermeldinger, retweets, replies og quotes som omhandler utvalgte tema (vedlegg F og G).

For å undersøke om det har foregått koordinert lenkedeling fra flere profiler, har vi undersøkt om to eller flere profiler deler de samme lenkene i sine twittermeldinger eller retweets innenfor et tidsvindu på 60 sekunder. Heretter omtales dette som «samdelinger». Det er ikke unormalt at flere profiler deler samme lenker, men ved å undersøke om dette skjer innenfor et svært kort tidsrom (60 sekunder) og gjentatte ganger med forskjellige lenker, er det mulig å danne seg et bilde av aktivitet som potensielt kan komme fra koordinerte nettverk. Figur 7.3 viser 15 klynger med profiler hvor vi har avdekket denne type adferd.



Figur 7.3 Avdekkede klynger av profiler som har delt en eller flere av de samme lenkene innenfor en tidsperiode på 60 sekunder. Størrelsen på nodene illustrerer hvor mange koblinger profilene har til andre profiler («degree»), mens tykkelsen på trådene mellom nodene illustrerer hvor mange ganger to profiler har delt det samme innholdet («weight»).

.

7.2.3 Falske positive

Av de 15 identifiserte klyngene finner vi flere profiler som ikke utviser noen form for inautentisk aktivitet. Av disse kan nevne for eksempel klynge 6, som består av to kontoer som er tilknyttet en av Norges største nettaviser, samt en uavhengig profil som deler siste nytt fra norske nettaviser. Klynge 6 er et godt eksempel på flere av klyngene vi avdekker med denne metoden, hvor det ser ut til at to eller flere profiler deler det samme innholdet fordi profilene

enten representerer samme organisasjon eller fordi profilene åpenlyst er koblet sammen. Klynge 1 er et eksempel på hvordan fremmedspråklige profiler er kommet med i datasettet fordi Twitter har feiltolket innholdet som norsk. I dette tilfellet er innholdet forfattet på nederlandsk og stammer fra flere medier som er eid av samme mediegruppe.

7.2.4 Tegn på inautentisk adferd

Flere klynger av profiler viser likevel tegn på inautentisk adferd. Vi har sett nærmere på to klynger som vi mener både utviser tegn på inautentisk aktivitet (høy andel av samdeling av lenker) i tillegg til at selve profilene fremstår som inautentiske.

Klynge 2 består av tre profiler. Vi bruker her betegnelsene «Profil 1», «Profil 2» og «Profil 3». Profil 1 og Profil 2 har det samme personnavnet som eier av profilene. Vi har her pseudonymisert det til «John Smith» (tilfeldig valgt eksempel) (Figur 7.4). De tre profilene har til sammen 632 delinger av norsk innhold i tidsperioden, og kommer opp i våre analyser fordi de hyppig deler de samme lenkene innenfor en periode på 60 sekunder.

I tillegg finnes det ytterligere to profiler med det samme navnet som Profil 1 og 2. Disse ble ikke avdekket gjennom undersøkelse av koordinert lenkedeling, men av kvalitative undersøkelser basert på funnene av Profil 1, 2 og 3. Vi kaller de to ytterligere profilene «Profil 4» og «Profil 5».

De fem profilene er knyttet sammen med en rekke fellestrekk. I tillegg til at Profil 1, 2 og 3 hyppig deler de samme lenkene innenfor korte tidsrom (60 sekunder), kan de viktigste forbindelsene mellom kontoene kort oppsummeres som følgende:

- Profil 1, 2, 4 og 5 ble alle opprettet i mars 2009 og har samme navn.
- Profilbildene på Profil 1, 2, 4 og 5 ser ut til å være av samme person.
- Brukernavnet (handle) til Profil 1 og Profil 2 har et tematisk slektskap.
- Profil 1s oppgitte Facebookside har samme brukernavn som Profil 2s Twitterprofil.
- Profil 2 og Profil 4 har det samme profilbildet, men med justert lys og utsnitt, som kan ha vært gjort for å unngå at Twitter oppdager at de bruker samme bilde.
- Navnet til Profil 3 er det samme som brukernavnet til Profil 4.
- En overfladisk, kvalitativ gjennomgang viser at profilene ser ut til å tvitre mest på engelsk, men skifter tidvis språk til både norsk, svensk, dansk, fransk, russisk og færøysk.
- Temaene varierer noe, men internasjonal politikk er en fellesnevner.

Figur 7.4 De tre profilene i klynge 2 (Profil 1, 2 og 3) deler fellestrekk med ytterligere to profiler (Profil 4 og 5). Kontoene utviser inautentisk aktivitet, blant annet rettet mot et norsk publikum. Navn og brukernavn er her pseudonymisert. Eventuelle likheter med ekte navn og brukernavn er tilfeldig.

«John Smith-nettverket» er ikke bare interessant fordi det viser tydelige tegn på inautentisk aktivitet rettet mot (blant annet) et norsk publikum. En av profilene (Profil 1) har tidligere fungert som kilde til en artikkel på den russiske proxykilden *Strategic Culture Foundation* (GEC, 2020, s. 12) og har flere ganger vært engasjert i diskusjoner om Nato.

Nettverkets Twitteraktivitet kan virke autentisk ved første øyekast, men ved nærmereundersøkelser fremstår det som autogenerert og derfor inautentisk. Det ser ut til at profilene i stort omfang innsamler innhold fra en rekke nettsider som de omsetter til en twittermelding med lenke til artikkelen. Dette fremstår som rimelig enkle metoder for å skape innhold rettet inn mot ulike målgrupper.

Klynge 3 består av fire forskjellige profiler som til sammen har 365 delinger av norsk innhold i tidsperioden. Klyngen består av profilene "The News Yard" (@thenewsyard) "News Bht" (@newsbht1), "Best Hindi Tech" (@BestHindiTech1) og "Galla Go" (@galla_go).

Profilene deler norsk innhold i sine twittermeldinger med lenker til nettsidene https://thenewsyard.com, https://olive92.com, https://besthinditech.com og https://usa366.com/, som alle har tilsvarende oppsett og utforming. Innholdet som er publisert på disse nettsidene ser ut til å være kopiert fra en rekke norske medier (bl.a. Aftenposten, E24 og Nettavisen) og handler alle om norsk innenriks- og utenrikspolitikk. Mellom disse fire profilene finner vi parvis samdeling av lenker innenfor en tidsperiode på 60 sekunder varierende fra 40 til 69 ganger.

Svært mange av delingene foregår innenfor en tidsperiode på 2-3 sekunder, noe som får delingene til å fremstå som koordinert. Vi har ikke funnet aktivitet fra nettverket som tyder på forsøk på valgpåvirkning og innholdet som er delt har ikke fått videre spredning eller liv på plattformen.

Det kan virke som nettverket har et kommersielt motiv ved å forsøke å drive trafikk til de omtalte nettsidene som videreformidler innhold som er kopiert fra norske medier. Dette stemmer godt overens med modus operandi fra lignende clickbait-nettverk i Myanmar som Graphika tidligere har beskrevet (Ronzaud et.al., 2020) og som MIT Technology Review dekket i dybden i november 2021 (Hao, 2021).

Kort oppsummert, har vi funnet avgrensede klynger av profiler på Twitter som utviser inautentisk adferd. Klyngenes aktivitet fremstår som koordinert fordi samdelinger av lenker mellom profilene foregår innenfor et kort tidsvindu og gjentatte ganger gjennom analyseperioden. Til tross for at profiler i noen klynger i tidsperioden deler norsk innhold, fremstår de ikke som norske da de generelt deler mye innhold på andre språk, noe som forsterker mistanken om inautentisk adferd. *Vi har ikke funnet innhold som tyder på valgpåvirkning.* Innholdet som deles oppnår svært lav spredning og interesse på plattformen.

7.2.5 Undersøkelse av koordinert inautentisk adferd på Facebook

På Facebook har vi ikke mulighet til å undersøke om spesifikke profiler fremstår som inautentiske, da vi kun har adgang til offentlige grupper og sider. Derfor har vi kun undersøkt om vi kan finne lignende mønster med koordinert lenkedeling i offentlige grupper og sider på Facebook.

Fordi Facebook har en relativt større brukerbase enn Twitter i Norge, som igjen fører til betraktelig mer innhold som teoretisk sett kan deles samtidig, har vi valgt å redusere tidsvinduet hvor vi leter etter samdelinger fra 60 sekunder til 1 sekund. Ved hjelp av CrowdTangles API har vi undersøkt 320 059 delinger som har forekommet over en toårsperiode (september 2019 - september 2021) i 325 norske Facebook-grupper og -sider som diskuterer politikk og samfunnsspørsmål. På grunn av personvern har vi ikke undersøkt hvilke profiler som står bak disse delingene.

Vi fant 118 unike delinger av samme lenker innenfor samme sekund. De fleste delingene foregår i par, altså at samme lenke blir delt i to forskjellige grupper eller sider innenfor samme sekund. I det tilhørende datamaterialet (tekst som følger med lenkedelingen) har vi *ikke funnet tegn til aktivitet som fremstår som forsøk på å påvirke valgresultatet, valgdeltakelsen eller tillitten til valget.*

Denne formen for samdeling kan teoretisk forekomme tilfeldig ved at to forskjellige profiler på plattformen deler samme lenke i hver sin side eller gruppe på Facebook på nøyaktig samme tidspunkt. Det virker likevel usannsynlig at dette kan skje gjentatte ganger, og vår vurdering er at disse samdelingene av samme innhold i forskjellige deler av Facebook fremstår som inautentisk.

Det har ikke vært mulig for oss å gjenskape denne type adferd ved å dele identisk innhold gjennom en vanlig Facebook-konto i to forskjellige grupper. Vi kan bare konstatere at denne formen for aktivitet vil være mulig å gjennomføre ved hjelp av programmatiske verktøy og at den ikke har blitt stanset av Facebooks sikkerhetssystemer.

Case 1: Inautentisk adferd på Facebook?

CASE 1: Inautentisk adferd på Facebook?

De siste årene har Facebook kommunisert hyppig om at de gjør mye for å demme opp for falske kontoer på plattformen. Noen av tiltakene kan ha vært vellykket, men det er fortsatt mange aktører som lykkes i å utnytte Facebook til manipulasjon. I mai 2021 kunne den engelske virksomheten Comparitech meddele at de hadde funnet en ubeskyttet server som inneholdt en bot-farm med 13 775 aktive Facebook-kontoer (Bischoff, 2021). Kontoene var konfigurert ved hjelp av Selenium, en programvare som gjør det mulig å forhåndsdefinere bestemte handlinger, som for eksempel å logge seg inn på Facebook og dele innhold.

Kontoene delte innhold 15 ganger i måneden, som resulterte i at 205 625 innlegg ble delt av en rimelig enkel form for kunstig intelligens i løpet av én måned. Da Comparitech publiserte sin artikkel, påpekte de at Facebook på daværende tidspunkt kun hadde fjernet 10 av profilene som var avdekket av Comparitech (ibid.).

Disse funnene er sammenlignbare med analyser som tidligere er offentliggjort av NATO StratCom CoE (Fredheim et. al., 2020). Her undersøkte de hvordan flere sosiale medier, inkludert Facebook, arbeidet for å begrense falske kontoer. I Facebook sitt tilfelle klarte virksomheten å fjerne 9 av 100 falske kontoer etter tre uker. Facebooks halveringstid var i 2020 på 146 dager, omlag 4,5 måneder. Det betyr at om 10 000 falske kontoer ble opprettet i dag, ville 5000 av dem fortsatt være aktive etter 4,5 måned. I rapporten fra NATO StratCom CoE skriver forfatterne:

"Ultimately, however, none of the protection measures currently in place are robust enough to stop persistent users or organisations from creating inauthentic accounts on any of the platforms we studied. The continued low cost and effectiveness of manipulation services is proof of this" (Fredheim, et. al., 2020, s. 18).

11. november 2021 publiserte den engelske tenketanken, Institute for Strategic Dialogue, en analyse som viste at aktørerer som sprer desinformasjon stadig klarte å omgå Facebook sine sikkerhetssystemer med relative enkle metoder (Thomas, 2021). På den måten har for eksempel News Front, en nyhetsorganisasjon med tilholdssted på Krimhalvøya, klart å dele innhold på Facebook - til tross for at de er utestengt fra plattformen. News Front ble sanksjonert av USA i april 2021, etter anklager om å ha deltatt i forsøk på å påvirke det amerikanske valget i 2020. Det samme gjelder for aktørnettverket som omtales som «Spamouflage», som blant annet har hacket SoMe-kontoer og brukt falske kontoer for å spre pro-kinesisk innhold under protestene i Hong-Kong i 2019 (Graphika, 2019).

Dette viser at aktører som sprer desinformasjon klarer å forbigå Facebook sine sikkerhetssystemer og at dette også vil kunne skje i forbindelse med forsøk på valgpåvirkning. Vi har ikke funnet eksempler på at dette har skjedd i forbindelse med det norske stortingsvalget 2021, men de seneste avsløringer understreker at dette fortsatt er et risikoscenario for Norge og andre demokratiske stater.

7.2.6 Konklusjon, analyse 2

Denne analysen har undersøkt hvorvidt det har forekommet inautentisk aktivitet på sosiale medier som retter seg mot et norsk publikum, og om denne aktiviteten eventuelt har karakteristikker som kan være egnet til å påvirke valgresultatet, valgdeltakelse eller tilliten til valggjennomføringen. *Vi finner tegn på inautentisk aktivitet både på Facebook og Twitter*.

Grunnet tekniske og juridiske begrensninger, er det ikke mulig å undersøke disse funnene med formål om attribuering. På Twitter virker noe av aktiviteten til å være overlappende med russiske interesser og narrativer, mens den øvrige aktiviteten synes å ha kommersielle formål. Av samme årsak som tidligere nevnt, er attribuering i begge tilfeller ikke mulig. *Vi finner ingen aktivitet som faller inn under vår forståelse av valgpåvirkning i dette oppdraget.*

Case 2: «Guo Wengui's Online Whistleblower Movement»

CASE 2: «Guo Wengui's Online Whistleblower Movement»

Selv om vi ikke fant inautentisk aktivitet som faller inn under vår forståelse av valgpåvirkning, gjorde vi et interessant funn. Da vi undersøkte bot-aktivitet på Twitter, fant vi to bots som hadde vært aktive i å spre desinformasjon på norsk. Etter grundigere undersøkelser ser det ut til at disse kontoene er en del av et kjent ikke-statlig påvirkningsnettverk som den kinesiske forretningsmannen Guo Wengui står bak (Graphika, 2021a). Nettverket ble først kartlagt og beskrevet i en rapport fra mai 2021 av analyseselskapet Graphika (ibid).

Rapporten beskriver dette nettverket som *«a vast network of interrelated media entities which have disseminated online disinformation…»* (ibid., s. 2). Det beskrives hvordan disse entitetene er bygget opp, hvor Gnews og GTV er nettverkets to mediekanaler.

Vi bestemte oss følgelig for å bruke den metodiske logikken fra GEC-rammeverket (Figur 6.1) til å undersøke om vi kunne finne flere kontoer med tilknytning til dette nettverket, ved å undersøke hvordan lenker til Gnews og GTV blir delt på norsk (vedlegg F). Ved å undersøke hvordan lenker til disse to mediene har blitt delt, fant vi Twitter-aktivitet rettet mot et norsk publikum. Denne aktiviteten ser ut til å være en del av det omfattende nettverket beskrevet i Graphikas rapport.

Aktiviteten vi har identifisert i vårt materiale samsvarer med rapporten fra Graphika på tre punkter:

- Tematikk som trekkes frem i rapporten gjenspeiles i aktiviteten vi har funnet. Sentrale eksempler er: utstrakt feilinformasjon angående covid-19 (inkludert vaksinemotstand), negative holdninger til Kinas Kommunistiske Parti (heretter KKP) og sympati for den politiske situasjonen til Taiwan og Hongkong, samt Qanon-narrativer. Dette er tema som også sammenfaller med amerikanske høyreorienterte holdninger. Aktiviteten samsvarer med Graphikas beskrivelser av nettverkets aktivitet:

  «Criticism of the CCP is often focused on territorial and human rights disputes with international significance, including those relating to «Taiwan, Hong Kong, Xinjiang, and Tibet. Members of the network express solidarity with groups oppressed or targeted by the CCP, and use their struggle to amplify their own cause» (Graphika, 2021a, s. 20).

- Flere av emneknaggene det henvises til i rapporten brukes, som for eksempel: #takedowntheccp, #whitleblowermovement og #NewFederalStateofChina (ibid., s. 9, 19). Noe av innholdet vi har identifisert publiseres på norsk, spesielt i august og september 2021.

Dette innholdet har budskap som omhandler vaksineskepsis/motstand og anklager om at Kina har utviklet Covid-19. Denne informasjonen ble også publisert på fransk, tysk, engelsk, spansk, kinesisk og i ett tilfelle på ungarsk. Vi har ikke funnet indikasjoner på at dette innholdet spres på noen av de andre skandinaviske språkene.

- Vi finner innhold som omhandler «artemisin», som fremsettes som en kur på covid-19 og et alternativ til vaksinering. Graphika har tidligere avdekket hvordan dette nettverket sprer denne formen for desinformasjon på sosiale medier (Graphika, 2021b). og majoriteten av aktiviteten er på kinesisk. I perioder skifter språket til bl.a. norsk, som er bakgrunnen for at vi finner disse i vårt materiale.

Til sammen fant vi 54 kontoer som deler innhold fra Gnews og GTV på norsk. Vi vurderer at minst 50 av disse er en del av Guo Wenguis nettverk av twitterkontoer. Dette baserer vi på en samlet vurdering av følgende: (1) kontoene deler hyppig lenker til Guo Wenguis organisasjoner, (2) de utviser de inautentisk adferd, da de ikke bruker egne profilbilder, (3) mange av dem bruker anti-KKP-bilder, bilder av Guo Wengui alene eller sammen med Steve Bannon og (4) profiltekstene er ofte på kinesisk. Kontoene er aktive på flere språk og majoriteten av aktiviteten er på kinesisk. I perioder skifter språket til bl.a. norsk, som er bakgrunnen for at vi finner disse i vårt materiale.

I tillegg til innhold som er kritisk til KKP og delinger av direktesendinger fra «Miles Wengui», fremstår det som at nettverkets primære formål er å skape mistillit til vaksineutvikling, samt å promotere alternative behandlingsformer for korona.

I datasettet finner vi 74 delinger til Gnews og GTV, hvorav 9 er fra 2020 og 65 er fra 2021. De første delingene er fra april 2020. Forskjellen i antall delinger i 2020 og 2021 kan være et tegn på at aktivitetsnivået har økt, men dette kan også være et resultat av at Twitter fjernet deler av nettverkets aktivitet i 2020. Den største aktiviteten ser vi den 22. juni 2021, hvor en twittermelding fra kontoen «Sakura2064» retweetes 34 ganger og får 36 likes. «Sakura2064» er en aktiv konto på Twitter, men har på tidspunktet for rapporten ikke tweetet siden 30. september. Figur 7.5 viser et eksempel på en twittermelding fra «Sakura2064» (Ukjent, 2021a):

Figur 7.5 *Twittermelding fra kontoen «Sakura2064» 22. juni, 2021. Profilen vurderes som inautentisk og tilknyttet Guo Wenguis nettverk som sprer anti-KKP-innhold og desinformasjon om covid-19 og vaksiner.*

De to mest aktive kontoene på norsk i datasettet vårt er «tiansha» med 11 delinger og «tianyexiang» (田野香) med 8 delinger. Begge kontoene er primært engasjert i anti-KKP aktivitet på norsk, men deler også innhold om vaksiner. Figur 7.6 viser et eksempel på en twittermelding fra «tianyexiang» (Ukjent, 2021b):

Figur 7.6 *Twittermelding fra kontoen «tianyexiang» 25. august 2021. Profilen vurderes som inautentisk og tilknyttet Guo Wenguis nettverk som sprer anti-KKP-innhold og desinformasjon om Covid-19 og vaksiner.*

Med unntak av «Sakura2064»s twittermelding fra 22. juni 2021, mottar twittermeldinger fra nettverket få eller ingen interaksjoner. De interaksjonene som finnes, ser ut til å være skapt av nettverket selv. Det er følgelig vår vurdering at spredningen av innhold fra nettverket enn så lenge ikke har oppnådd bred spredning blant nordmenn.

Innholdet beskrevet i dette caset indikerer ikke noen form for statlig aktivitet eller valgpåvirkning, men det viser at ikke-statlige aktører er aktive i å spre desinformasjon rettet mot et norsk publikum. Formålet med aktiviteten, utover å spre negativt innhold om KKP, ser ut til å være å påvirke nordmenns holdning til vaksiner. Vi vurderer at effekten av aktiviteten fra nettverket som vi har avdekket sannsynligvis har vært svært begrenset, målt i spredning og interaksjoner.

Likevel viser disse funnene at Twitters sikkerhetssystemer kan omgås av internasjonale, ikke-statlige aktører med et formål om å forsøke å påvirke et norsk publikum. Aktøren som omtales her har tilgang til språkteknologier som gjør det mulig å rette kampanjeaktivitet mot nordmenn. Det kan ikke utelukkes at dersom denne aktøren er i stand til dette, er det naturlig at andre vil være i stand til det samme. Til tross for at effekten av spredningen vurderes til å være begrenset, er omfanget av kontoer som er aktive på norsk av en betydelig størrelse.

En viktig implikasjon av disse funnene er at verktøy for å drive med spredning av desinformasjon er tilgjengelige, også for andre organisasjoner enn stater. Dette utvider landskapet av aktører som kan tenkes å ville påvirke både demokratiske og kommersielle prosesser i land som Norge.

7.3 Analyse 3: Diskusjoner om valgets integritet

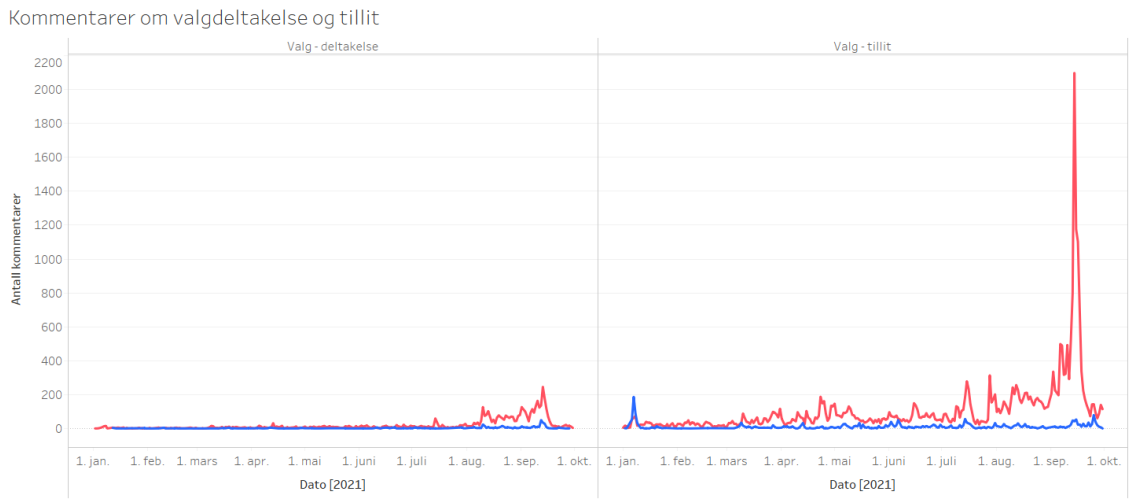
Vi har undersøkt om det har vært økt interesse for gjennomføringen av valget i norske kommentarer på Facebook og Twitter, og om disse kommentarene kan ha hatt som (antatt) hensikt å påvirke valgdeltakelsen eller tilliten til valget.

7.3.1 Kommentarer på Facebook

Vi har søkt igjennom anonymiserte kommentarer som er skrevet til innlegg på Facebook-sidene til norske medier, politiske partier og politikere i perioden 1. januar - 1. oktober 2021[13]. Til sammen har vi søkt gjennom 12,45 millioner kommentarer. Hovedandelen av kommentarene er skrevet til innlegg fra norske medier (79%), mens kommentarer til norske partier og politikeres sider utgjør til sammen 21 prosent. Totalt finner vi 38 426 kommentarer som nevner relevante søkeord i perioden 1. januar - 1. oktober 2021. Dette tilsvarer 3 promille av totale antall kommentarer i perioden.

Figur 7.7 viser antall Facebook-kommentarer som omhandler valgdeltakelse (grafen til venstre) og tillit til valget (grafen til høyre).

[13] Kommentarene stammer fra 356 Facebook-sider som representerer norske medier og 2 520 Facebook-sider som representerer partiorganisasjoner eller kandidater fra 17 norske politiske parti (omtalt i kapittel 6.2.1).



Figur 7.7 *Antall kommentarer (per dag) til innlegg på Facebook-sider tilhørende norske medier, politiske partier og politikere. Grafen til venstre viser antall kommentarer som omhandler valgdeltakelse. Grafen til høyre viser antall kommentarer som omhandler tillit til valg. Den røde linjen viser antall kommentarer som er nøytrale i den forstand at de inneholder ord som f.eks. «valglokale» eller «sperregrense», men **ikke** ord eller uttrykk som f.eks. «valgfusk» eller «valget er rigget». Den blå linjen viser antall kommentarer som inneholder formuleringer som f.eks. «ikke stem», «valgfusk» eller «valget er rigget».*

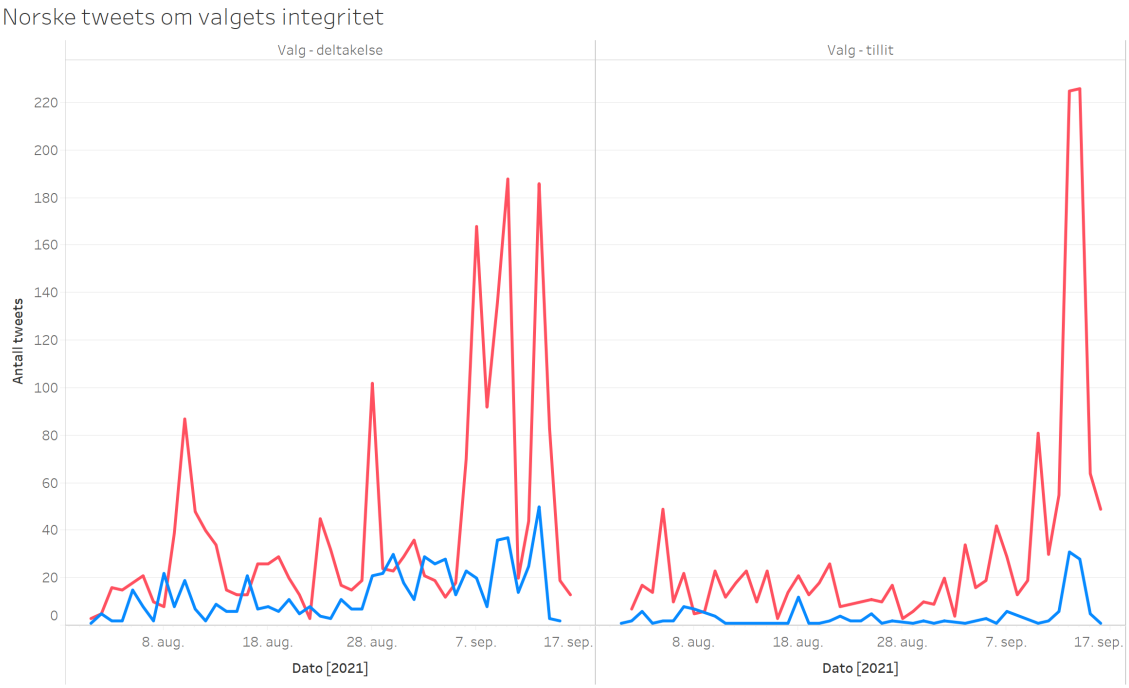
Den røde linjen i Figur 7.7 kan best beskrives som «generell omtale av valg». Ikke overraskende finner vi en økt interesse for valg i tidsperioden fra begynnelsen av august til slutten av september 2021. I perioden 1. september til 20. september ser vi en spesielt stor økning i økning i antall kommentarer som nevner ord som blant annet *valgkort*, *valglokale*, *stemmelokale*, *sperregrense*, *valgresultat*, *valgprognose*, *valgopptelling*, *valgdistrikt*, *distriktsmandat* og *utjevningsmandat*. Dette får en topp rundt valgdagen 13. september.

Den blå linjen i Figur 7.7 viser omtale av valg som inneholder ord og uttrykk som blant annet *valgfusk*, *valgjuks*, *ugyldig valg*, *ugyldig valgresultat* og at *valget er rigget*, *stjålet* eller *kuppet.* I den første uken av 2021 ser vi en liten økning i antall kommentarer (380). Kommentarene omhandler primært det amerikanske valget og stormingen av den amerikanske kongressen 6. januar, 2021. Til sammenligning finner vi henholdsvis 232 og 222 av denne typen kommentarer i uke 37 og 38 i 2021, i forbindelse med avviklingen av stortingsvalget.

7.3.2 Kommentarer på Twitter

Som på Facebook, er det på Twitter økende interesse for valget frem mot valgdagen 13. september 2021. (Figur 7.8). Andelen twittermeldinger som omhandler valggjennomføring og valgresultat utgjør en begrenset andel av de norske twittermeldingene vi har undersøkt, med en samlet andel på 1,1 prosent. Vi observerer en økning i twittermeldinger som omhandler valgsystemet og gjennomføring (rød linje i Figur 7.8) frem mot valgdagen. Twittermeldinger

som nevner ord som «valgfusk» etc. (blå linje i Figur 7.8) får en liten økning på valgdagen (81 twittermeldinger), men som på Facebook finner vi ingen store utslag.



Figur 7.8 *Tidslinje over norske twittermeldinger (per dag) som omhandler valg. Grafen til venstre viser antall twittermeldinger som omhandler valgdeltakelse. Grafen til høyre viser antall twittermeldinger som omhandler tillit til valg. Den røde linjen viser antall twittermeldinger som er nøytrale i den forstand at de inneholder ord som f.eks. «valglokale» eller «sperregrense», men ikke ord eller uttrykk som f.eks. «valgfusk» eller «valget er rigget». Den blå linjen viser antall kommentarer som inneholder formuleringer som f.eks. «ikke stem», «valgfusk» eller «valget er rigget».*

Det er viktig å understreke at den blå linjen med ord som «valgfusk» og «valget er rigget» ikke viser antallet kommentarer hvor dette nødvendigvis påstås, men antallet kommentarer og twittermeldinger som inneholder slike ord og uttrykk. Den blå linjen viser altså i hvor stor grad mistillit til valget har vært et tema som har blitt diskutert, ikke hvor mange kommentarer og twittermeldinger som har uttrykt mistillit til valget.

Dersom den blå linjen hadde vist store utslag, ville det vært en indikasjon på at det foregikk mye debatt om valgets integritet. Våre funn viser at dette ikke er tilfellet. Dersom det *hadde* vært tilfelle, ville en ytterligere undersøkelser av aktiviteten vært nødvendig for å vurdere hva debatten handlet om og hvorvidt den kunne vært en effekt av utenlandsk påvirkning.

Den viktigste begrensninger i denne typen undersøkelse er bruken av søkeord. Undersøkelsen er basert på søkeord vi vurderer som sannsynlig å bruke for å omtale valget og valgets integritet.

Man kan se for seg at tema som valgdeltakelse og tillit til valget omtales på andre måter, uten bruk av ordene man søker etter.

7.3.3 Konklusjon, analyse 3

Denne analysen har hatt som formål å undersøke om valgets integritet er blitt forsøkt trukket i tvil på sosiale medier. Vi har ikke funnet noen betydelig økning i antall kommentarer eller twittermeldinger som inneholder ord og uttrykk vi vurderer som sannsynlige å bruke for å fremsette påstander som undergraver tilliten til valgets integritet. Kommentarene og twittermeldingene som av ulike grunner inneholder slike ord og uttrykk fremstår ikke som en del av en større kampanje eller som koordinert aktivitet. *Vi har ikke funnet tegn på at utenlandske aktører har forsøkt å påvirke valgdeltakelsen eller spre mistillit til valgets gjennomføring eller resultat*.

7.4 Analyse 4: Internasjonale kartlegginger av påvirkningsoperasjoner og spredning av desinformasjon

Vi har gjennomført søk etter norske tilfeller i databaser over kjente påvirkningsoperasjoner, eksisterende kartlegginger av spredning av desinformasjon og kjente tilfeller av koordinert inautentisk adferd. Det er viktig å presisere at materialet vi har undersøkt her inkluderer manipulerende innhold i bred forstand, og er *ikke* er avgrenset til kun valgpåvirkning.

7.4.1 Facebook

Meta (tidligere Facebook) publiserer månedlige rapporter om funn fra deres arbeid med å fjerne koordinert inautentisk adferd fra Facebook og Instagram. De månedlige rapportene i perioden januar til og med oktober 2021 omtaler ikke at plattformene har tatt grep for å fjerne norske kontoer, grupper eller sider som har utvist det Facebook selv definerer som koordinert, inautentisk adferd (Meta, 2021). Dette er konsistent med Metas gjennomgang av denne type aktivitet på Facebook i perioden 2017 - 2020 (Gleicher et.al., 2021). Gjennomgangen av disse rapportene finner heller ingen omtale av funn rettet mot Norge[14]. Dette betyr ikke nødvendigvis at denne type aktivitet ikke foregår på Facebook. Fordi Facebook ikke offentliggjør det spesifikke innholdet (for eksempel. innlegg og kommentarer) som de *har* fjernet, er det umulig å lage en ekstern vurdering av om noe av dette innholdet har vært rettet mot Norge, norske interesser eller forhold.

7.4.2 Twitter

I motsetning til Meta, har Twitter siden 2018 offentliggjort datamateriale over profiler og twittermeldinger som de mener er knyttet til statlige påvirkningskampanjer (Twitter, 2021b). Frittstående analytikere har tidligere pekt på mangler i dette materialet (Basel, et. al., 2020),

[14] Meta har tilgjengeliggjort en oversikt over de spesifikke operasjonene som de har fjernet: https://about.fb.com/wp-content/uploads/2021/05/2017-2021-IO-Threat-Report-Takedown-List.xlsx

men det er likevel det beste tilgjengelige materialet for å undersøke kjente påvirkningsoperasjoner på plattformen (Bradshaw et.al. 2021b, s. 5; Freelon et.al., 2020, s. 6).

Twitters siste offentliggjøring av nettverk ble publisert i februar 2021, og inneholder derfor ikke materiale som er relevant for det norske stortingsvalget i 2021[15]. Vi har likevel valgt å søke gjennom deres arkiver fra 2020 og 2021, for å se om Norge, norske interesser eller forhold blir nevnt i materialet[16]. Materialet inneholder nettverk fra 18 påvirkningsoperasjoner, med tilknyttet aktivitet som spenner fra 2009 - 2020. Våre funn er summert i Tabell 7.2.

Tabell 7.2 Oversikt over Twitters offentlige arkiver over 18 nettverk som knyttes til statlige påvirkningskampanjer som plattformen har oppdaget og fjernet i perioden 2020-2021.

Datasett	Stater identifisert av Twitter	Tidsperiode for aktivitet i nettverket (åååå-mm-dd)	Antall profiler fjernet	Totalt antall twittermeldinger i datasettet	Antall twitter-meldinger om Norge, norske interesser og forhold
Februar 2021	Iran	2009-09-06 - 2020-12-27	130	560 571	100
Februar 2021	Armenia	2014-08-06 - 2020-11-25	35	72 960	33
Februar 2021	Russland (GRU)	2013-12-06 - 2020-11-21	69	26 684	11
Februar 2021	Russland (IRA)	2009-07-06 - 2020-12-27	31	68 914	59
Oktober 2020	Iran	2020-01-08 - 2020-07-01	104	2 450	0
Oktober 2020	Russland (IRA)	2019-12-25 - 2020-08-21	5	1 368	0
Oktober 2020	Thailand	2015-10-12 - 2020-07-20	926	21 385	0
Oktober 2020	Saudi Arabia	2010-07-29 - 2020-06-14	33	220 254	9
Oktober 2020	Kuba	2010-09-06 - 2020-07-31	526	4 802 243	323
Juni 2020	Kina	2018-01-11 - 2020-04-17	23 750	348 608	34
Juni 2020	Tyrkia	2009-05-19 - 2020-04-21	7 340	36 948 536	5 285
Juni 2020	Russland	2009-05-19 - 2019-12-12	1 152	3 434 792	229
April 2020	Egypt	2009-02-27 - 2020-01-29	2 541	7 935 329	1 454
April 2020	Honduras	2009-07-02 - 2020-01-08	3 104	1 165 019	63
April 2020	Indonesia	2009-02-27 - 2020-01-31	795	2 700 296	19
April 2020	Serbia	2009-07-15 - 2020-01-30	8 558	43 067 074	21 180
April 2020	Saudi Arabia	2008-04-17 -	5 350	36 523 980	2 924

[15] Twitter offentliggjorde et nytt arkiv av nettverk i desember 2021, men dette kom for sent til å bli inkludert i denne rapporten.

[16] Søk i twittermeldinger med søkeord som dekker omtale av Norge på relevante språk (Norge og norsk oversatt), norske selskap som Telenor og Equinor, norske medier, emneknagger om norsk politikk, norske partier og partiledere, samt statsministre, forsvarsministre og utenriksministre i perioden 2013-2021.

	(KSA, Egypt, UAE)	2020-01-22			
Mars 2021	Nigeria / Ghana	2014-04-04 - 2020-02-29	71	39 964	4

En dyptgående analyse av innholdet som ser ut til å omhandle Norge, har ligget utenfor dette prosjektets rammer, da aktivitetene forekom før 2021 og dermed ikke er relevant for stortingsvalget 2021. Det er likevel interessant at Norge, norske forhold og interesser opptrer i dette materialet. Disse forekomstene kan ha mange årsaksforklaringer. For eksempel finner vi at noe av innholdet handler om norsk natur, norske turistmål, norske kunstnere og artister. Annet innhold viser til Norge som foregangsland innenfor fornybar energi, tilstanden for fiskeri i Norge eller utviklingen av olje- og gassindustrien. Dette kan handle om at profilene har behov for å skape innhold som vil gjøre dem attraktive å følge for sine spesifiserte målgrupper.

Vi finner imidlertid også omtale av norske hendelser som terrorangrepet 22. juli 2011, moskéangrepet i Bærum ved Al-Noor Islamic Centre, SIANs demonstrasjoner mot islam eller daværende stortingspolitiker Guri Melbys nominasjon av folket i Hongkong til Nobels fredspris. Vi finner også delinger som omhandler Norges rolle i andre land og regioner, som for eksempel Oslo-avtalen fra 1993, fredsprosessene i Colombia og Venezuela-samtalene. Generelt sett bærer ikke disse delingene preg av å forsøke å nå ut til et norsk publikum.

Vi har ikke funnet innhold som er forfattet på norsk. I datasettet fra februar 2021 finner vi dog en profil som hevder å være fra Norge. Twitter har attribuert profilens aktivitet til Russland (GRU). Profilen har vært aktiv i tidsperioden juli 2017 til mars 2020, hvor den har publisert 4 608 twittermeldinger. Profilen hadde 6 502 følgere før den ble fjernet av Twitter. Til tross for at profilen hevder å være norsk, skriver profilen kun på engelsk. Over halvparten av innholdet som profilen står bak, handler om Syria. Profilen er tidligere omtalt av både Graphika (Nimmo, 2020b) og Stanford Internet Observatory (DiResta et al, 2021). I Stanford Internet Observatory sin rapport kommer det frem at profilen har brukt et bilde av den norske skuespilleren Josefine Frida Pettersen (DiResta et al, 2021, s. 6).

I det samme datasettet finner vi to andre profiler som skriver om norsk sikkerhetspolitikk, og da særlig Nato-medlemskap og militære øvelser i nordområdene.

Alliance for Securing Democracy og Graphika har utviklet en søkbar database hvor noe av materialet fra Twitter er tilgjengeliggjort (IO-ARCHIVE, 2021). Databasen ser ikke ut til å være oppdatert siden august 2019.

Utover plattformenes egne rapporteringer på innhold og profiler som de selv har fjernet, finnes det flere initiativ som, basert på egen eller andres forskning, følger med på påvirkningsoperasjoner eller spredning av desinformasjon. Vi har undersøkt om Norge opptrer i disse databasene.

Disinfoindex

Disinfoindex er en offentlig tilgjengelig database som inneholder informasjon om kjente desinformasjonkampanjer. Prosjektet er støttet av Berkman Klein Center ved Harvard University (DISINFOINDEX, 2020a). 1. november 2021 gjennomførte vi søk etter «Norway»

og «Norwegian» i databasen, men dette ga ingen resultat. Et utvidet søk etter Nato-land ga et resultat over et lite nettverk av profiler og sider på Instagram og Facebook, som Facebook fjernet i 2020 (DISINFOINDEX, 2020b). Nettverket så ut til å forsterke innhold fra blant annet Strategic Culture Foundation og Oriental Review, som begge er identifisert som russiske proxy-aktører (GEC, 2020).

EUvsDisinfo database

EU East StratCom Task Force står bak prosjektet EUvsDisinfo, som ble opprettet i 2015. Formålet med prosjektet er å blant annet å følge med på, og avdekke, hvordan desinformasjon som stammer fra det de omtaler som pro-Kremlin medier spres i EUs medlemsland (EUvsDisinfo, 2021). Søk som ble gjennomført 1. november 2021 etter «Norway» og «Norwegian» gir ingen relevante treff, men Norge nevnes indirekte gjennom oppføringer som omhandler vestlige land og Skandinavia.

7.4.3 Konklusjon, analyse 4

Gjennom søk i de nevnte databasene *finner vi ingen eksempler på at Norge har vært mål for kjente påvirkningsoperasjoner fra andre stater. Likevel ser vi at Norge, norske interesser og forhold blir omtalt i påvirkningsoperasjoner fra 18 nettverk som Twitter selv har attribuert til forskjellige stater i 2020 og 2021*. Våre begrensede søk i disse arkivene har avdekket profiler som skriver om bl.a. norsk utenrikspolitikk, sikkerhetspolitikk, energipolitikk, innenrikspolitiske tema eller som også hevder å være norsk.

8 Konklusjon

På oppdrag fra Kommunal- og moderniseringsdepartementet (KMD) har Forsvarets forskningsinstitutt (FFI), sammen med de skandinaviske analysebyråene Analyse & Tall og Common Consultancy, forsøkt å kartlegge hvorvidt det norske stortingsvalget 2021 ble utsatt for uønsket informasjonspåvirkning fra utenlandske aktører i perioden 1. august – 16. september 2021.

Vi har tatt utgangspunkt i en hypotese om at uønsket informasjonspåvirkning fra utenlandske aktører *ikke* har funnet sted. Gjennom ulike kvantitative og kvalitative metoder har vi så forsøkt å motbevise denne hypotesen. Dette er gjort ved å kartlegge og analysere spredning av (des)informasjon og propaganda av utenlandske aktører på norske nettsider, på Facebook og på Twitter. Vi har også undersøkt inautentisk aktivitet på Facebook og Twitter for å identifisere målrettede forsøk på manipulasjon.

Gjennom fire omfattende analyser har vi ikke funnet indikasjoner på at stortingsvalget 2021 ble utsatt for uønsket informasjonspåvirkning fra utenlandske aktører. Vi har med andre ord ikke motbevist hypotesen som var utgangspunktet for denne studien.

Våre analyser viser imidlertid at utenlandske, ikke-statlige aktører er aktive i å spre desinformasjon til et norsk publikum. Disse forsøkene oppnår kun et begrenset liv på sosiale medier i Norge, med relativt lite spredning og få interaksjoner. Vi har også funnet tidligere aktive nettverk som har spredd desinformasjon om Norge til et utenlandsk publikum. I tillegg har vi funnet to klynger av det som framstår som utenlandske, inautentiske profiler på Twitter som aktivt sprer nyheter og politisk innhold til et norsk publikum. Aktiviteten fremstår imidlertid ikke som direkte forsøk på å påvirke valgets resultat, valgdeltakelse eller tillit til valget. Det er også verdt å merke seg at innhold fra spesielt det russiske påvirkningsnettverket deles på norske nettsider og i sosiale medier. Den største andelen av delingene gjøres av norskspråklige profiler som fremstår som kritiske til den norske mediedekningen.

Et tydelig funn er at relativt billige og tilgjengelige teknologier, samt usofistikerte og lett detekterbare manipulasjonsteknikker, brukes av flere aktører for å forsøke å påvirke et norsk publikum. Facebook og Twitter er fremdeles godt egnet som plattformer for påvirkningsoperasjoner, til tross for deres egne forsøk på å stoppe inautentisk aktivitet og spredning av desinformasjon. Selv om aktiviteten fra nettverket tilknyttet kinesiske Guo Wengui ikke har oppnådd stor spredning i Norge, er dette et illustrerende eksempel på en ikke-statlig aktør som er aktiv i å spre desinformasjon rettet mot et norsk publikum. Det er også en viktig observasjon at kontoene tilknyttet dette nettverket (ca. 50 stk.) har hatt muligheten til å operere helt siden Graphika publiserte sin rapport i mai 2021, uten at kontoene er blitt stengt av Twitter.

Å undersøke potensiell utenlandsk valgpåvirkning i et demokrati som Norge er underlagt flere juridiske og tekniske begrensninger. På grunn av et strengt personvern er det kun anledning å samle inn data fra åpne kilder. I tillegg er det store forskjeller i hvor mye data de ulike plattformene er villige til å dele med eksterne aktører. I dette oppdraget har vi også gjort nødvendige avgrensninger med hensyn til tidsperioden for undersøkelsene, hvilke aktører og

taktikker vi har kartlagt, samt datagrunnlaget analysene våre baserer seg på. I sum skaper disse faktorene potensielle blindsoner.

Det kan ikke utelukkes at andre plattformer enn de vi har undersøkt har vært benyttet i påvirkningsforsøk av stortingsvalget 2021. Det kan heller ikke utelukkes at det har foregått påvirkningsforsøk i lukkede grupper eller via private profiler på Facebook. For å lykkes i å påvirke valget med merkbar effekt, må en aktør imidlertid nå en tilstrekkelig stor andel norske velgere. Vi vurderer det derfor som lite sannsynlig at man vil kunne oppnå tilstrekkelig effekt uten at vi hadde funnet spor av dette på Facebook, Twitter eller norske nettsider. Det er også viktig å understreke at vår kartlegging er avgrenset til målrettet påvirkning av valgresultatet, valgdeltakelsen og tilliten til valget. Vi har følgelig ikke hatt mulighet til å undersøke alle tenkelige påvirkningsoperasjoner som *kan* være rettet mot Norge. Det kan derfor ikke utelukkes at det foregår målrettet utenlandsk påvirkning i Norge som faller utenfor rapportens fokus på valgpåvirkning. Våre funn viser at utenlandske påvirkningsforsøk av den norske befolkningen forekommer innenfor enkelte saker og politikkområder. Fordi disse funnene ikke har vært knyttet til stortingsvalget 2021, har vi ikke undersøkt dem nærmere.

Vår gjennomgang av tidligere kartlagte påvirkningsoperasjoner viser at utenlandsk påvirkning av valg i demokratiske stater i stor grad skjer indirekte og subtilt over lang tid, gjennom gradvis påvirkning av befolkningens holdninger og virkelighetsoppfatning. Dette kan på sikt få implikasjoner for hvilke partier folk velger å stemme på, eller hvor stor grad av tillit de har til politikere, myndighetene og demokratiske institusjoner. Vi anbefaler derfor at norske myndigheter innretter fremtidige undersøkelser av valgpåvirkning på en slik måte at de kan fange opp påvirkning av nordmenns virkelighetsoppfatning, verdier og tillit over tid. Fremtidig kartlegging av valgpåvirkning bør dermed gjennomføres over et lenger tidsrom og inkludere flere plattformer og vurderingsparametre enn det som var mulig innenfor dette oppdragets rammer.

Referanser

Akerbæk, E. Skiphamn, S. (2021, 20. september). *Flere ubegrunnede spekulasjoner om valgfusk*. Faktisk.no https://www.faktisk.no/artikler/jxm3w/flere-ubegrunnede-spekulasjoner-om-valgfusk

Aleksejeva, N., Andriukaitis, L., Bandeira, L., Barojan, D., Brookie, G., Buziashvili, E., Carvin, A., Karan K., Nimmo, B, Robertson, I, Sheldon, M. (2019). *Operation "Secondary Infection" - A suspected Russian intelligence operation targeting Europe and the United States.* Atlantic Council, Digital Forensics Lab. https://www.atlanticcouncil.org/wp-content/uploads/2019/08/Operation-Secondary-Infektion_English.pdf

Allen-Ebrahimian, B. (2020). *The American blog pushing Xinjiang denialism.* Axios. https://www.axios.com/grayzone-max-blumenthal-china-xinjiang-d95789af-263c-4049-ba66-5baedd087df4.html

Amnesty International (2017). *China's Deadly Secrets.* Amnesty International: https://amnesty.dk/wp-content/uploads/media/2980/embargo-11-april-chinas-deadly-secrets-eng.pdf

Applebaum, A., Pomerantsev, P, Smith, M., Colliver, C. (2017). *Make Germany great again - Kremlin, Alt-Right and International Influences in the 2017 German Elections.* Institute of Strategic Dialogue. https://www.isdglobal.org/wp-content/uploads/2017/12/Make-Germany-Great-Again-ENG-081217.pdf

Avelar, D. (2019, 30. oktober). *WhatsApp fake news during Brazil election 'favoured Bolsonaro'.* The Guardian. https://www.theguardian.com/world/2019/oct/30/whatsapp-fake-news-brazil-election-favoured-jair-bolsonaro-analysis-suggests

Basel, S., Suiche, M. (2020, 12. februar). *Twitter's Information Operations - An OSINT Analysis.* https://si.ma/tw-io/

BBC (2018, 6. mars). *China profile - Media.* BBC. https://www.bbc.com/news/world-asia-pacific-13017881

BBC (2019, 4. november). *Powerful 'Putin's chef' Prigozhin cooks up murky deals.* BBC. https://www.bbc.com/news/world-europe-50264747

BBC (2021, 8. juni). *Russia profile - Media.* BBC. https://www.bbc.com/news/world-europe-17840134

Bentzen, N. (2018). *Foreign influence operations in the EU.* European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625123/EPRS_BRI(2018)625123_EN.pdf

Bhatnagar, P. (2020, 5. august). *Foreign State-sponsored Media Outlets and Presence on Reddit.* Foreign Policy Research Institute. https://www.fpri.org/fie/foreign-state-sponsored-media-outlets-reddit/

Bischoff, P. (2021, 10. mai). *Inside a Facebook bot farm that pumps out 200k+ political posts per month.* Comparitech. https://www.comparitech.com/blog/information-security/inside-facebook-bot-farm/

Blackburn, J. (2018, 16. februar). *How 4chan and The_Donald Influence the Fake News Ecosystem*. inCyber. https://incyber.fr/en/how-4chan-and-the_donald-influence-the-fake-news-ecosystem-by-jeremy-blackburn-university-of-alabama-at-birmingham/

Bogle, A. (2019, 20. januar). *Instagram spreads political misinformation and Australian elections are vulnerable.* ABC News. https://www.abc.net.au/news/science/2019-01-20/instagram-australian-federal-election-russian-misinformation/10717034

Botometer. (u.å.a). *Botometer*. https://botometer.osome.iu.edu/

Botometer. (u.å.b). *FAQ*. https://botometer.osome.iu.edu/faq

Bradshaw, S., Bailey, H., & Howard, P. (2021a). *Industrialized Disinformation: 2020 Global Inventory of Organised Social Media Manipulation.* Oxford Internet Institute, Oxford University. https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/127/2021/01/CyberTroop-Report-2020-v.2.pdf

Bradshaw, S., Henle, A. (2021b). *The Gender Dimensions of Foreign Influence Operations.* International Journal of Communication 15 (2021). https://ijoc.org/index.php/ijoc/article/view/16332

Brooking, E. T. & Kianpour, S. (2020). *Iranian digital influence efforts: Guerrilla broadcasting for the twenty-first century.* Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2020/02/IRAN-DIGITAL.pdf

Brown, A. (2020, 20. juni). *Discord Was Once The Alt-Right's Favorite Chat App. Now It's Gone Mainstream And Scored A New $3.5 Billion Valuation.* Forbes. https://www.forbes.com/sites/abrambrown/2020/06/30/discord-was-once-the-alt-rights-favorite-chat-app-now-its-gone-mainstream-and-scored-a-new-35-billion-valuation/?sh=73acfb35b6b2

Cheng, K. (2019, 25. juli). *Hong Kong gov't orders pro-Beijing newspaper to remove giant sign on building following complaints.* Hong Kong Free Press. https://hongkongfp.com/2019/07/25/hong-kong-govt-orders-pro-beijing-newspaper-remove-giant-sign-building-following-complaints/

Coffey, L. (2019, 8. februar). *Russia exploits "yellow vest" turmoil in France.* The Heritage Foundation. https://www.heritage.org/europe/commentary/russia-exploits-yellow-vest-turmoil-franc

Cook, S. (2020). *Special Report 2020: Beijing's Global Megaphone*. Freedom House: https://freedomhouse.org/report/special-report/2020/beijings-global-megaphone#footnote8_40knrr0

Crime and Security Research Institute [CSRI] (2020). '*Perception Infections': Tactics and Techniques of a Russian Information, Influence and Interference Operations (IIIO) Methodology*. Cardiff University: https://static1.squarespace.com/static/57875c16197aea2902e3820e/t/5f1068441a1a876727648ed2/1594910815803/Perception+Infection+Report.pdf

Crime and Security Research Institute [CSRI] (2021). *How a Kremlin-Linked Influence Operation is Systematically Manipulating Western Media to Construct & Communicate Disinformation.* Cardiff University: https://www.cardiff.ac.uk/__data/assets/pdf_file/0007/2551849/final-report.pdf

CrowdTangle. (u.å.a). *CrowdTangle API*. https://help.crowdtangle.com/en/articles/1189612-crowdtangle-api

CrowdTangle. (u.å.b) *What data is CrowdTangle tracking?* https://help.crowdtangle.com/en/articles/1140930-what-data-is-crowdtangle-tracking

Cush, A. (2015, 20. august). *Emails Link Kremlin Troll Farm to Bizarre New York Photography Exhibit.* StopFake. https://www.stopfake.org/en/emails-link-kremlin-troll-farm-to-bizarre-new-york-photography-exhibit/

Dahlback, M. (2021, 17. juni). *Her er ekkokammeret som gjør alternative medier til virale vinnere.* Faktisk.no https://www.faktisk.no/artikler/0q4rw/her-er-ekkokammeret-som-gjor-alternative-medier-til-virale-vinnere

Daniels, L. (2017, 23. april). *How Russia hacked the French Election.* Politico. https://www.politico.eu/article/france-election-2017-russia-hacked-cyberattacks/

Datatilsynet (2019). *Grunnleggende personvernprinsipper*. Datatilsynet. https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/

Datatilsynet (2019a). *Hvordan lage en databehandleravtale?* Datatilsynet. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/databehandleravtale/hvordan-lage-en-databehandleravtale/

Datatilsynet (2019b). *Behandlingsansvarlig og databehandler.* Datatilsynet. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/databehandleravtale/behandlingsansvarlig-og-databehandler/

Den nasjonale forskningsetiske komité for samfunnsvitenskap og humaniora (2019). *Forskningsetisk veileder for internettforskning*. De nasjonale forskningsetiske komiteene. https://www.forskningsetikk.no/retningslinjer/hum-sam/forskningsetisk-veileder-for-internettforskning/

Der Spiegel (2014), 30. mai). *How Russia Is Winning the Propaganda War.* Der Spiegel. *https://www.spiegel.de/international/world/russia-uses-state-television-to-sway-opinion-at-home-and-abroad-a-971971.html*

Deutsche Welle. (2017, 18. august). *Erdogan tells German Turks not to vote for Angela Merkel*. Deutsche Welle. https://www.dw.com/en/erdogan-tells-german-turks-not-to-vote-for-angela-merkel/a-40149680

DFRLab (2020, 8. oktober). *Facebook removed inauthentic network connected to United Russia party.* Medium. https://medium.com/dfrlab/facebook-removed-inauthentic-network-connected-to-united-russia-party-6b9cfd2332de

Diamond, L. & Schell, O. (2018). *Chinese Influence & American Interests: Promoting Contructive Vigilance.* The Hoover Institution: https://www.hoover.org/sites/default/files/research/docs/00_diamond-schell_fullreport_2ndprinting_web-compressed.pdf

DiResta, R. (2018). *Free Speech in the Age of Algorithmic Megaphones*. Wired. https://www.wired.com/story/facebook-domestic-disinformation-algorithmic-megaphones/

Diresta, R., Miller, C., Molter, V., Pomfret, J., & Tiffert, G. (2020). *Telling China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives*. Stanford Internet Observator.

DiResta, R., Grossman, S. (2021). *Fronts & Friends: An Investigation into Two Twitter Networks Linked to Russian Actors*. Standford Internet Observatory. https://raw.githubusercontent.com/stanfordio/publications/main/russia_twitter_takedown_feb_23_2021.pdf

DISINFO INDEX. (2020a) *Disinfo Index Database.* Disinfo Index. https://disinfodex.org/

DISINFO INDEX. (2020b) *Network FB-RU-0920-C*. Disinfo Index. https://disinfodex-new-frontend-production-e2kyhghera-ue.a.run.app/5f949a94043369786f267153

Dizikes, P. (2018, 8. mars). *Study: On Twitter, false news travels faster than true stories.* Massachusetts Institute of Technology (MIT). https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308

DNI (2017). *Assessing Russian Activities and Intentions in Recent US Elections.* Office of the Director of National Intelligence: https://www.dni.gov/files/documents/ICA_2017_01.pdf

Doncheva, T. (2020, 30. april). *Tracking Russia's Narratives in the Western Balkan Media*. NATO StratCom COE. https://stratcomcoe.org/publications/tracking-russias-narratives-in-the-western-balkan-media/53

Edelson, L. & McCoy, D. (2021, 14. august). *Facebook is obstructing our work on disinformation. Other researchers could be next.* The Guardian. https://www.theguardian.com/technology/2021/aug/14/facebook-research-disinformation-politics

Etterretningstjenesten. (2021). *Fokus 2021 - 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

EuvsDisinfo (2017, 16. oktober). *Self-Help Via Pro-Kremlin Disinformation*. EUvsDisinfo. https://euvsdisinfo.eu/self-help-via-pro-kremlin-disinformation/

EUvsDisinfo (2018, 31. mai). *Figure of the week: 6.4%.* EUvsDisinfo. https://euvsdisinfo.eu/figure-of-the-week-6-4/

EUvsDisinfo (2019). *Election Meddling and Pro-Kremlin Disinformation.* EUvsDisinfo: https://euvsdisinfo.eu/uploads/2019/10/PdfPackage_EUvsDISINFO_2019_EN_V2.pdf

EUvsDisinfo. (2021). *Disinfo Database*. https://euvsdisinfo.eu/disinformation-cases/

Empirical Studies of Conflict. (2021). *Review of Literature on Effect of Influence Operations.* Empirical Studies of Conflict Project. https://esoc.princeton.edu/publications/review-literature-effect-influence-operations

Facebook. (u.å.) *Graph API*. https://developers.facebook.com/docs/graph-api/

Fredheim, R., Bay, S., Dek, A., Dek, I. (2020, 21. desember). *Social Media Manipulation Report 2020.* NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/social-media-manipulation-report-2020/21

Freelon, D., Bossetta, M., Wells, C., Lukito, J., Xia, Y., Adams, K. (2020) *Black Trolls Matter: Racial and Ideological Asymmetries in Social Media Disinformation*. European Journal of Women's Studies. April 2020:282-287. https://doi.org/10.1177/1350506814529900a

Færseth, J. (2021, 11. september). *Demokratene-leder bidrar på russisk propagandakanal.* Johnfaerseth.no. https://johnfaerseth.no/2021/09/12/demokratene-leder-bidrar-pa-russisk-propagandakanal/

Gadde, V., & Roth, Y. (2018, 17. oktober). *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

GEC. (2020). *GEC Special Report: Russia's Pillars of Disinformation and Propaganda*. U.S. Departement of State. https://www.state.gov/russias-s-of-disinformation-and-propaganda-report/

Giglietto, F., Righetti, N., Rossi, L., & Marino, G. (2020). *It takes a village to manipulate the media: coordinated link sharing behavior during 2018 and 2019 Italian elections*. Information, Communication and Society, 1–25. https://doi.org/10.1080/1369118X.2020.1739732

Gleicher, N. (2018, 6. desember). *Coordinated Inauthentic Behavior Explained*. Facebook. https://about.fb.com/news/2018/12/inside-feed-coordinated-inauthentic-behavior/

Gleicher, N et al. (2021, mai). *Threat Report - The State of Influence Operations 2017-2020*. Facebook. https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf

Government Communication Service. (2021). *Resist 2: Counter-disinformation toolkit*. Government Communication Service. RESIST 2 Counter-disinformation toolkit (netdna-ssl.com)

Graham, T. (2020). *Coordination Network Toolkit*. QUT Digital Observatory. Queensland University of Technology. (Software) https://doi.org/10.25912/RDF_1632782596538

Graham, T. Bruns, A., Zhu, G., Campbell, R. (2020). *Like a virus: the coordinated spread of coronavirus disinformation*. Centre for Responsible Technology. https://apo.org.au/node/305864

Graphika. (2021a, mai). *Ants in a Web: Deconstructing Guo Wengui's Online "Whistleblower Movement."* Graphika. https://public-assets.graphika.com/reports/graphika_report_ants_in_a_web.pdf

Graphika. (2021b, september). *Artemisinin: Guo Wengui Is Borrowing Anti-Vaxx Tactics to Promote a New "Miracle Cure"*. Grapika. https://graphika.com/posts/artemisinin-guo-wengui-is-borrowing-anti-vaxx-tactics-to-promote-a-new-miracle-cure/

Graphika, IFTF & IRI (2020). *Detecting Digital Fingerprints: Tracing Chinese Disinformation in Taiwan*. Graphika, IFTF & IRL. https://www.iftf.org/fileadmin/user_upload/downloads/ourwork/Detecting_Digital_Fingerprints_-_Tracing_Chinese_Disinformation_in_Taiwan.pdf

Graphika Team. (2020). *Step into My Parler*. Graphika. https://public-assets.graphika.com/reports/graphika_report_step_into_my_parler.pdf

Grégoire, A. (2021, 7. september). *CIB Detection Tree: 4th Branch - The Authenticity Assessment.* EU Disinfo Lab. https://www.disinfo.eu/publications/cib-detection-tree-4th-branch/

Grønborg, M. (2021, 15. november). *Hizb ut-Tahrir vækker vrede med valg-opfordring: «Det er jo vanvittigt!»* B.T. https://www.bt.dk/samfund/hizb-ut-tahrir-vaekker-vrede-med-valg-opfordring-det-er-jo-vanvittigt

Grøtan, T.O. et al. (2019). *På leting etter utenlandsk informasjonspåvirkning - en analyse av det norske kommunestyre- og fylkestingsvalget 2019*. SINTEF Digital. https://www.regjeringen.no/contentassets/4d850821991746ecbcd9477a475baf73/sintef-rapport_2019-01292_gradering_apen.pdf

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

Hanke, D. R. (2020, 28. januar). *TikTok national security problem: Don't ignore the lessons of 2016.* The Hill. https://thehill.com/opinion/cybersecurity/480251-the-tiktok-national-security-problem-dont-ignore-the-lessons-of-201

Hansen, H. Elgaaen, V. (2021, 13. september). *Fant ikke partiets stemmeseddel:- Det er dumt.* VG. https://www.vg.no/nyheter/innenriks/i/9KqkOW/fant-ikke-partiets-stemmeseddel-det-er-dumt

Hanson, F., O'Connor, S., Walker, M. & Courtois, L. (2019). *Hacking democracies: Cataloguing cyber-enabled attacks on elections* (Rapport nr. 16). The Australian Strategic

Policy Institute. https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-05/Hacking%20democracies.pdf

Hao, K. (2021, 20. november). *How Facebook and Google fund global misinformation.* MIT Technology Review. https://www.technologyreview.com/2021/11/20/1039076/facebook-google-disinformation-clickbait/

Hathaway, Tim. (2007, 9. november). *A Journalist in China.* Asia Media Archives. https://web.archive.org/web/20100718220855/http:/asiamedia.ucla.edu/article.asp?parentid=81687

Henin, N. (2021, 18. oktober). *Foreign election interferences: An overview of trends and challenges.* EU Disinfo Lab. https://www.disinfo.eu/publications/foreign-election-interferences-an-overview-of-trends-and-challenges/

Hille, K. (2019, 17. juli). *Taiwan primaries highlight fears over China's political influence.* Financial Times. *https://www.ft.com/content/036b609a-a768-11e9-984c-fac8325aaa04*

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*. Project on Computational Propaganda, Oxford Internet Institute. https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/The-IRA-Social-Media-and-Political-Polarization.pdf

Insikt Group. (2021, 26. oktober). *Cyber Threat Analysis - Russia*. Recorded Future. https://go.recordedfuture.com/hubfs/reports/cta-2021-1026.pdf

IO-ARCHIVE. (2021). *Informations Operations Archive*. https://www.io-archive.org/

IPSOS. (2021). *Ipsos SoMe-tracker Q3'21.* IPSOS. https://www.ipsos.com/nb-no/ipsos-some-tracker-q321

Jacobsen, G. U. (2021). *I'm fighting an election in Norway next week to stop equality before the law and freedom of speech being stolen from us by stealth.* Russia Today. https://www.rt.com/op-ed/534515-election-norway-eu-eea/

Joske, A. (2020, 9. juni). The party speaks for you: *Foreign interference and the Chinese Communist Party's united front system.* Australian Strategic Policy Institute. https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-06/The%20party%20speaks%20for%20you_0.pdf?gFHuXyYMR0XuDQOs_6JSmrdyk7MralcN=

Karlsen, G. H. (2021, mars). *Hvordan kan vi beskytte valg mot fremmed påvirkning? Internasjonal politikk* – Skandinavisk tidsskrift for internasjonale studier. https://tidsskriftet-ip.no/index.php/intpol/article/view/2309

Karlsen, T. (2021, 13. september). *Demokratene-leder bidrar på russisk propagandakanal.* Transit Magasin. https://www.transitmag.no/2021/09/13/demokratene-leder-bidrar-pa-russisk-propagandakanal/

Kazer, W. (2013, 27. september). *New Warning Issued on China Local Government Debt.* The Wall Street Journal. https://www.wsj.com/articles/no-headline-available-1380304883

Kliman, D., Kendall-Taylor, A., Lee, K., Fitt, J., & Nietsche, C. (2020). *Dangerous Synergies: Countering Chinese and Russian Digital Influence Operations.* Center for a New American Security. https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS-Report-Dangerous-Synergies-May-2020-DoS-Proof.pdf?mtime=20200506164642&focal=none

Kommunal- og moderniseringsdepartementet (2021, 1. juni). *Tiltak for å hindre uønsket påvirkning i valget.* Regjeringen Solberg. https://www.regjeringen.no/no/dokumentarkiv/regjeringen-solberg/aktuelt-regjeringen-solberg/kmd/pressemeldinger/2021/tiltak-for-a-hindre-uonsket-pavirkning-i-valget/id2854721/

Kommunal- og moderniseringsdepartementet (2021). *Forskningsprosjekt om informasjonspåvirkning i forbindelse med det norske stortingsvalget 2021 - konkurransegrunnlag.* Regjeringen Solberg. https://eu.eu-supply.com/app/rfq/publicpurchase_docs.asp?PID=302751&LID=355198&AllowPrint=1

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/

Lee, E. & Sheng, W (2021, 26. juli). *Chinese edtech upended by sweeping regulations.* TechNode. https://technode.com/2021/07/26/chinese-edtech-upended-by-sweeping-regulations/

Majestic. (u.å.). *Your first 5 minutes with the Majestic API.* https://developer-support.majestic.com/

Majestic. (2021). *SEO Backlink Checker & Link Building Toolset*. https://majestic.com/

Mandiant (2020). *Ghostwriter influence campaign.* Mandiant. https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/Ghostwriter-Influence-Campaign.pdf

Mandiant. (2021). *Ghostwriter update: Cyber Espionage Group UNC1151 Likely Conducts Ghostwriter Influence Activity.* Mandiant.

Markay, L. (2021). *China increases spending 500% to influence America.* AXIOS. https://www.axios.com/china-foreign-influence-spending-317a9be4-8ead-4abf-8ac4-3f27974d7a9d.html

Martin, D. A., Shapiro, J. N., Ilhardt, J. G. (2020). *Trends in online influence efforts*. Empirical Studies of Conflict. https://esoc.princeton.edu/publications/trends-online-influence-efforts

Martineau, P. (2018, 17. desember). *How Instagram Became the Russian IRA's Go-To Social Network.* Wired. https://www.wired.com/story/how-instagram-became-russian-iras-social-network/

Meta. (2021). *Coordinated Inauthentic Behavior*. https://about.fb.com/news/tag/coordinated-inauthentic-behavior/

Miller, C. (2015, 1. maj). *Russia's pro-Putin media darling loves his new life in Brooklyn -- minus the hipsters.* Mashable. https://mashable.com/archive/russia-lifenews-founder-loves-nyc

Milosevich-Juaristi, M. (2017, 20. November*). The 'combination': An instrument in Russia's information war in Catalonia.* The Elcano Royal Institute. http://www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/ari92-2017-milosevichjuaristi-combination-instrument-russia-information-war-catalonia

MITRE (2019). *Informational Conflict: Ukraine-Russia Relations 2014-2015.* The Mitre Corporation: https://tac.nist.gov/2019/SM-KBP/guidelines/Ukraine-Russia-Relations-Scenario-Document_2019-02-15_v1.2.1.pdf

Mueller, R. (2019). *Report on the investigation into Russian interference in the 2016 Presidential Election - volume I of II.* U.S. Department of Justice. https://www.justice.gov/archives/sco/file/1373816/download

Nasjonal sikkerhetsmyndighet. (2021). *Risiko 2021 - helhetlig sikring mot sammensatte trusler*. Nasjonal sikkerhetsmyndighet. https://nsm.no/getfile.php/136419-1616673370/Filer/Dokumenter/Rapporter/NSM_Risiko_2021_web_enkeltside_1203.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

Ng, G. (2017, 11. desember). *Snapchat Addresses the "fake news" Problem.* NYU Stern Center for Business and Human Rights. https://bhr.stern.nyu.edu/blogs/2019/1/29/snapchat-addresses-the-fake-news-problem

Ni, V. (2018). *Is Shanghai's Sixth Tone a New Model for China's Overseas Propaganda?* Westminster Papers in Communication and Culture*, 13*(1), 37-40. https://doi.org/10.16997/wpcc.282

Nimmo, B., Eib, S. & Tamora L. (2019, september). *Cross-Platform Spam Network Targeted Hong Kong Protests*. Graphika. https://public-assets.graphika.com/reports/graphika_report_spamouflage.pdf

Nimmo, B. et al. (2020a). *Secondary Infektion*. Graphika. https://secondaryinfektion.org/downloads/secondary-infektion-report.pdf

Nimmo, B. et al. (2020b). *GRU and the Minions*. Graphika. https://public-assets.graphika.com/reports/graphika_report_gru_minions.pdf

Nimmo, B. (2020c). *UK Trade Leaks and Secondary Infektion*. Graphika. https://public-assets.graphika.com/reports/graphika_report_uk_trade_leaks_&_secondary_infektion.pdf

Overly, S. (2020, 27. oktober). *Facebook removes foreign accounts targeting U.S. election.* POLITICO. https://www.politico.com/news/2020/10/27/facebook- removes- foreign- accounts-targeting-election-432843

Pamuk, H. & Brunnstrom, D. (2020). *Pompeo says U.S. designates six more Chinese media firms as foreign missions*. Reuters. https://www.reuters.com/article/us-usa-china-pompeo-idUSKBN2762D0

Personopplysningsloven. (2018). *Lov om behandling av personopplysninger.* (LOV-2018-06-15-38). Lovdata. https://lovdata.no/dokument/NL/lov/2018-06-15-38

Peter, A., Chen, M. & Carrasco, S. (2016). *Power interplay and newspaper digitization: Lessons from the Pengpai experiment*. Global Media and China, *1*(4), 497–510.

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

Purkiss, J. (2018, 28. september). *Russian warriors and British PR firms: Macedonia's information war*. The Bureau of Investigative Journalism. https://www.thebureauinvestigates.com/stories/2018-09-28/russian-warriors-and-british-pr-firms-macedonias-information-wa

Rauchfleisch, A., Kaiser, J. (2020). *The False positive problem of automatic bot detection in social science research.* PLOS ONE 15(10): e0241045. doi: https://doi.org/10.1371/journal.pone.0241045

RFE/RL (2021, 31. oktober). *Belarus Blocks Pro-Kremlin Russian News Agency Regnum.* Radio Free Europe/Radio Liberty. https://www.rferl.org/a/belarus-blocks-regnum-website/31538008.html

RFE/RL (2014, 1. april). *The 20 Russian News Outlets You Need To Read Before They Get The Ax.* Radio Free Europe/Radio Liberty. https://www.rferl.org/a/twenty-russian-news-outlets-you-need-to-read-before-they-get-the-axe/25317371.html

Rob, J. T., Shapiro, J.N. (2021). *A brief history of online influence operations.* Lawfare. https://www.lawfareblog.com/brief-history-online-influence-operations

Ronzaud, L., Eib C., François C., Chandra A., Rio, V., Thu, M. (2020, 22. oktober). *Myanmar Inauthentic Behavior Takedown*. Graphika. https://public-assets.graphika.com/reports/graphika_report_myanmar_inauthentic_behavior_takedown.pdf

Rosenberger, L. (2018, 31. juli). *Foreign influence operations and their use of social media platforms.* Alliance for Securing Democracies. https://securingdemocracy.gmfus.org/foreign-influence-operations-and-their-use-of-social-media-platforms/

Schachtel, J. (2021, 5. september). *'COVID Zero' New Zealand Has Completed Its Transformation Into a Full-Blown Police State.* Strategic Culture. https://www.strategic-culture.org/news/2021/09/05/covid-zero-new-zealand-has-completed-its-transformation-into-full-blown-police-state/

Searight, A. (2020). *Countering China's Influence Operations: Lessons from Australia*. Center for Strategic & International Studies. https://www.csis.org/analysis/countering-chinas-influence-operations-lessons-australia

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

Sputnik News. (2020). *Escaping Pandemic: World's Rich Head Off to Bunkers Amid the Outbreak of Coronavirus.* https://sputniknews.com/20200312/escaping-pandemic-worlds-rich-head-off-to-bunkers-amid-the-outbreak-of-coronavirus-1078547835.html

Stanford Internet Observatory (2020). *Telling China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives*. The Hoover Institution: https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/sio-china_story_white_paper-final.pdf

StopFake (2016, 20. august). *Les médias russes ont faussé les résultats d'un sondage réalisé en Ukraine.* StopFake. https://www.stopfake.org/fr/les-medias-russes-ont-fausse-les-resultats-d-un-sondage-realise-en-ukraine/

Svetova, Z. (2012, 27. august). *Тени из прошлого [Shadows from the past].* The New Times. https://newtimes.ru/articles/detail/56351

Thibaut, K. (2021). *China-linked WeChat accounts spread disinformation in advance of 2021 Canadian election.* Atlantic Council Digital Forensics Lab. https://medium.com/dfrlab/china-linked-wechat-accounts-spread-disinformation-in-advance-of-2021-canadian-election-cb5a8389049

Thomas, E. (2021, 11. november). *What's new (and What's not) with News Front.* ISD. https://www.isdglobal.org/isd-publications/whats-new-and-whats-not-with-news-front/

Timberg, C. (2021, 10. september). *Facebook made big mistake in data it provided to researchers, undermining academic work.* The Washington Post. https://www.washingtonpost.com/technology/2021/09/10/facebook-error-data-social-scientists/

Torusdağ, M. B., Kutlu, M., Selçuk, A. A. (2020). *Are We Secure from Bots? Investigating Vulnerabilities of Botometer*. 2020 5th International Conference on Computer Science and Engineering (UBMK), s. 343-348, doi: 10.1109/UBMK50275.2020.9219433

Twitter. (u.å.a). *Twitter API*. https://developer.twitter.com/en/docs/twitter-api

Twitter. (u.å.b). *Building queries for Search Tweets.* https://developer.twitter.com/en/docs/twitter-api/tweets/search/integrate/build-a-query#iterative

Twitter. (u.å.c). *About government and state-affiliated media account labels on Twitter.* https://help.twitter.com/en/rules-and-policies/state-affiliated-china

Twitter. (2013, 16. August). *New Tweets per second record, and how!* https://blog.twitter.com/engineering/en_us/a/2013/new-tweets-per-second-record-and-how

Twitter (2018, 19. januar). *Update on Twitter's review of the 2016 US election.* https://blog.twitter.com/en_us/topics/company/2018/2016-election-update

Twitter (2019, 19. august). *Information operations directed at Hong Kong.* Twitter. https://blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong

Twitter. (2021a, 21. oktober). *Examining algorithmic amplification of political content on Twitter.* https://blog.twitter.com/en_us/topics/company/2021/rml-politicalcontent

Twitter. (2021b). *Information Operations.* https://transparency.twitter.com/en/reports/information-operations.html

Ukjent. [sakura2064]. (2021a, 22. juni). *Advarsel til Verden Igjen – Miles Guo sin Direktesending den 20. Juni 2021 #GNEWS* [Miniatyrbilde med lenke vedlagt] [Tweet]. Twitter. https://twitter.com/sakura2064/status/1407152044012490752

Ukjent. [sakura2064]. (2021b, 25. august). *Miles Guo sa at piggproteinet i vaksinen vil forårsake myokarditt, perikarditt, hjerneinfarkt og andre sykdommer etter å ha kommet inn* [Miniatyrbilde med lenke vedlagt] [Tweet]. Twitter. https://twitter.com/tianyexiang/status/1430323370659176456

U.S. Intelligence Committee (2020). *Russian active measures campaigns and interference in the 2016 U.S. election.* U.S. Senate. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

Utenriksdepartementet. (2020, 13. oktober*). Datainnbruddet i Stortinget*. Utenriksdepartementet. https://www.regjeringen.no/no/dokumentarkiv/regjeringen-solberg/aktuelt-regjeringen-solberg/ud/pressemeldinger/2020/pm_inbrudd/id2770135/

Utenriksdepartementet. (2021, 18. juli). *Datainnbruddet i Stortingets e-postsystem*. Utenriksdepartementet. https://www.regjeringen.no/no/dokumentarkiv/regjeringen-solberg/aktuelt-regjeringen-solberg/ud/pressemeldinger/2021/pm_datainnbrudd/id2866410/

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

Van Raemdonck, N. (2019, 22. desember). *The Echo Chamber of Anti-Vaccination Conspiracies: Mechanisms of Radicalization on Facebook and Reddit.* Institute for Policy, Advocacy and Governance (IPAG) Knowledge Series, Forthcoming. https://ssrn.com/abstract=3510196

Velch, V. (2021, 26. februar). *Telegram: A Growing Social Media Refuge, for Good and Ill.* Just Security. https://www.justsecurity.org/74947/telegram-a-growing-social-media-refuge-for-good-and-ill

Vilmer, JB. J. (2018) *Successfully countering Russian electoral interference – 15 lessons learned from the Macron Leaks.* Center for Strategic & International Studies (CSIS). https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180621_Vilmer_Countering_russiam_electoral_influence.pdf

Wang, Haiyan., Sparks, Colin. & Yu, Huang. (2018). *Popular journalism in China: A study of China Youth Daily.* Journalism, 19 (9-10), 1203-1219. doi:10.1177/1464884917691987

Wang, B. & Wong, T. C. (2018). The Landscape of Newspapers in Hong Kong. In Huang, Yu & Song, Y. (eds.). *The Evolving Landscape of Media and Communication in Hong Kong.* City University of Hong Kong Press: 13–30.

Watts, C. (2021, 23. april). *Russia's Disinformation Ecosystem - A Snapshot.* Selected Wisdom. Clint Watts. https://clintwatts.substack.com/p/russias-disinformation-ecosystem

Weber, D., Neumann, F. *Amplifying influence through coordinated behaviour in social networks*. Soc. Netw. Anal. Min. 11**,** 111 (2021). https://doi.org/10.1007/s13278-021-00815-2

Whalen, J., Timberg, C. & Dou, E. (2021, 17. mai*). Chinese businessman with links to Steve Bannon is driving force for a sprawling disinformation network, researchers say*. The Washington Post. https://www.washingtonpost.com/technology/2021/05/17/guo-wengui-disinformation-steve-bannon/

Zhang, A., Wallis, Dr J. & Bogle, A. (2021). *Trigger warning: The CCP's coordinated information effort to discredit the BBC.* Australian Strategic Policy Institute. https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2021-05/Trigger%20warning.pdf?VersionId=QRr29MQArn7M7BWwP0twcHnF1JM2q8Rp

Zhang, X. (2014). *Public Access to Primary Legal information in China: Challenges and Opportunities.* Legal Information Management, 14(2), 132-142.

Zuckerberg, M. (2018). Facebook post announcing algorithm change Facebook. https://www.facebook.com/zuck/posts/10104413015393571

Åndsverkloven (2018). *Lov om opphavsrett til åndsverk.* (LOV-2021-05-28-49 fra 01.09.2021, LOV-2021-06-04-58 fra 01.07.2021). Lovdata. https://lovdata.no/dokument/NL/lov/2018-06-15-40

Vedlegg

A Kjente påvirkningsoperasjoner på digitale plattformer

Liste over kjente påvirkningsoperasjoner med tilhørende kilder. Norske brukertall (brukere over 18 år) er hentet fra IPSOS SoMe Tracker fra 3. kvartal 2021 (IPSOS, 2021).

Sosiale medier (utstrakt bruk i Norge)	Eksempler på hendelser	Kilde
Facebook Norge: 68% bruker daglig	Russian active measures campaigns and interference in the 2016 U.S. Election.	(U.S. Intelligence Committee, 2020, s. 6)
	Russian interference in the 2017 Catalan crisis.	(Milosevich-Juaristi, 2017)
	Accusations of Chinese interfering in the Taiwan information environment.	(Graphika, IFTF & IRI, 2020, s. 7)
Twitter Norge: 10% bruker daglig	Chinese information operations directed at Hong Kong.	(Twitter, 2019)
	British PR firms have helped the Macedonian government "divide the opppostion".	(Purkiss, 2018)
	Russian influence on the 2018 "Yellow West" turmoil in France.	(Coffey, 2019)
	Accusations of Chinese interfering in the Taiwan information environment.	(Graphika, IFTF & IRI, 2020, s. 7)
	Russian and Venezuelian influence on the 2018 Brazil elections.	(Ruediger & Grassi, 2019, s. 16)
YouTube Norge: 30% bruker daglig	Russian active measures campaigns and interference in the 2016 U.S. Election.	(U.S. Intelligence Committee, 2020, s. 6)
	Accusations of Chinese interfering in the Taiwan information environment.	(Graphika, IFTF & IRI, 2020, s. 7)
Instagram Norge: 41% bruker daglig	Russian active measures campaigns and interference in the 2016 U.S. Election.	(U.S. Intelligence Committee, 2020, s. 48)
	Iranian- and Russian-affiliated accounts targeting the 2020 U.S. election.	(Overly, 2020)
	Fear of Russian-linked political misinformation ahead of 2019 Australia elections.	(Bogle, 2019)
	How Instagram Became the Russian IRA's Go-To Social Network	(Martineau, 2018)
Tik Tok Norge: 15% bruker daglig	Fears of Chinese meddling in foreign elections (no known cases yet).	(Hanke, 2020)
LinkedIn Norge: 4% bruker daglig	Russian active measures campaigns and interference in the 2016 U.S. Election.	(U.S. Intelligence Committee, 2020, s. 62)
Snapchat Norge: 49% bruker daglig	No cases found.	(Ng., 2017)
Sosiale medier (utland)	**Eksempler på hendelser**	**Kilde**

Gab, Parler og MeWe	Russian disinformation campaign to promote reelection of Trump.	(Graphika Team 2020a, s. 1)
	"Anti-establishment"news targeted towards far-right U.S. communites by Russia.	(Graphika Team 2020a, s. 1)
Vkontakte	Russian active measures campaigns and interference in the 2016 U.S. Election.	(U.S. Intelligence Committee, 2020, s. 25)
Weibo	State-controlled accounts "guiding the opinion" of the Chinese domestic audience.	(Diresta et al., 2020, s. 12)
	Fake imagery of Chinese bombers promoted to install fear in the Taiwanese public.	(Rosenberger, 2018)
Forum	**Eksempler på hendelser**	**Kilde**
Reddit	Russian active measures campaigns and interference in the 2016 U.S. Election.	(U.S. Intelligence Committee, 2020, s. 16)
	Russian accounts amplifying a high-profile leak of UK government documents.	(Nimmo, 2020c, s. 2)
	Russian, Iranian, and Chinese sponsored content during the 2016 U.S. election	(Bhatnagar, 2020)
	Iranian digital influence on the Syrian civil war.	(Brooking & Kianpour, 2020)
4chan	Russian active measures campaigns and interference in the 2016 U.S. Election.	(U.S. Intelligence Committee, 2020, s. 16)
	High diffusion of misinformation - influence in elections can be expected.	(Blackburn, 2018)
Discord	Platform used for organizing Alt-Right movements events.	(Brown, 2020)
Blogger og posterboards	**Eksempler på hendelser**	**Kilde**
Pinterest, Tumblr og Medium	Russian active measures campaigns and interference in the 2016 U.S. Election.	(U.S. Intelligence Committee, 2020, s. 16, 62)
Meldingstjenester	**Eksempler på hendelser**	**Kilde**
WhatsApp Norge: 11% bruker daglig	Disinformation during the 2018 Brazil elections (foreign influence unknown).	(Avelar, 2019)
Telegram	Ukraine finding several channels connected to Russian intelligence services.	(Velch, 2021)
	Massive volume of Russia-linked covid-19 disinformation in Spain.	(GEC, 2020, s. 36)
WeChat	Chinese state actors meddling in Canada's 2019 federal election.	(Kilman et al., 2020, s. 22)
	Chinese censorship of U.S. messages about Hong Kong.	(Kilman et al., 2020, s. 5)
	Mobilisation of Chinese diasporas oversees, e.g. in Australia.	(Joske, 2020, s. 3)
LINE	Accusations of Chinese interfering in the Taiwan information environment.	(Graphika, IFTF & IRI, 2020, s. 16)

B Prosjektets prioritering av medier

Plattform	Vurdering	Prioritet	Datatilgang
Facebook	Facebook er brukt i en rekke påvirkningsoperasjoner og er et populært sosialt medium i Norge med en stor brukermasse.	Høy	Offentlig API
Twitter	Facebook er brukt i en rekke påvirkningsoperasjoner og er et populært sosialt medium i Norge blant politikere, journalister og andre samfunnsdebattanter.	Høy	Offentlig API
Alternative medier, blogger og nettsider	Alternative medier blir ofte utilsiktede ofre for påvirkningsoperasjoner og de seneste årene har Norge fått et stort tilfang av denne type medier. Flere av disse når også bredt ut, eller utgjør en viktig del av informasjonsdietten til mindre miljø.	Høy	Indeksering
YouTube	YouTube har blitt brukt i noen påvirkningsoperasjoner og er et populært sosialt medium i Norge, særlig blant en yngre målgruppe.	Middels	Offentlig API
Reddit	Reddit har særlig blitt brukt ved såkalte hack-and-release kampanjer, men bruken av plattformen er ikke spesielt utbredt i Norge.	Middels	Web-scraping
Redaksjonelle medier	Spredning av feilinformasjon og desinformasjon gjennom redaksjonelle medier har potensialet til å nå ut til store deler av befolkningen. Samtidig er risikoen for dette betydelig lavere. Det finnes likevel eksempler på hvordan feilinformasjon har blitt viderebragt i redaksjonelle medier.	Middels	Indeksering
Instagram	Der er flere kjente forsøk på påvirkningsoperasjoner på Instagram, men norsk lov og den europeiske persondataforordning begrenser mulighetene for stordata-analyse på plattformen.	Lav	Emneknagg og søkeord på offentlige innlegg og kommentarer

Snapchat	Til tross for at Snapchat er et populært sosialt medium er det inntil videre ingen kjente eksempler på påvirkningsoperasjoner på Snapchat. Dette kommer nok av måten appen er bygget opp rundt direkte kommunikasjon eller med mindre grupper, som gjør den mindre egnet for påvirkningsoperasjoner.	Lav	Tilgang til database over politisk annonsering
Meldingstjenester	Eksempler på disse er Telegram, WhatsApp, WeChat og Signal. Det er svært utfordrende å undersøke disse tjenestene fordi de er bygget rundt lukket meldingsutveksling og ofte kryptert.	Lav	Må avklares for den konkrete tjenesten
Forum, posterboards, videodelingstjenester og free-speech plattformer	I forbindelse med at de største plattformene har begynt å moderere innholdet sitt har vi sett en oppblomstring av andre plattformer som promoterer seg selv som free-speech plattformer. Utover Reddit som er behandlet for seg selv over, kan man nevne 4chan, 8kun, Gab, MeWe, Parler, Gettr, Rumble og WIMKIN. Disse vurderes som lite brukt i Norge.	Lav	Må avklares for de konkrete forumene

C Kilder i det russiske påvirkningsnettverket

Pillar	Name	Language	Facebook	Twitter	Domain	YouTube	Source
1. pillar	president_of_russia	rus		kremlinrussia	http://kremlin.ru	https://www.youtube.com/user/kremlin	(GEC, 2020, s. 8)
1. pillar	president_of_russia	eng		kremlinrussia_e	http://en.kremlin.ru	https://www.youtube.com/user/kremlin	(GEC, 2020, s. 8)
1. pillar	mfa_russia	rus	midrussia	mid_rf	https://www.mid.ru	https://www.youtube.com/midrftube	(GEC, 2020, s. 8)
1. pillar	mfa_russia	eng	midrussia	mfa_russia	https://www.mid.ru/en	https://www.youtube.com/midrftube	(GEC, 2020, s. 8)
1. pillar	government_of_russia	rus		pravitelstvo_rf	http://government.ru	https://www.youtube.com/user/pravitelstvoRF	(GEC, 2020, s. 8)

1. pillar	government_of_russia	eng		governmentrf	http://government.ru/en		(GEC, 2020, s. 8)
1. pillar	embassy_of_russia_in_norway	rus	rusembno	rusembno	https://norway.mid.ru/ru		(GEC, 2020, s. 8)
1. pillar	embassy_of_russia_in_norway	eng	rusembno	rusembno	https://norway.mid.ru/en		(GEC, 2020, s. 8)
1. pillar	embassy_of_russia_in_norway	norw			https://norway.mid.ru/no		(GEC, 2020, s. 8)
1. pillar	dmitry_medvedev	rus	dmitry.medvedev	medvedevrussia			(GEC, 2020, s. 8)
1. pillar	dmitry_medvedev	eng	dmitry.medvedev	medvedevrussiae			(GEC, 2020, s. 8)
1. pillar	defence_ministry_russia	rus	mod.mil.rus	mod_russia	https://mil.ru	https://www.youtube.com/channel/UCQGqX5Ndpm4snE0NTjyOJnA	(GEC, 2020, s. 8)
1. pillar	defence_ministry_russia	eng	mod.mil.rus	mod_russia	http://eng.mil.ru/en/index.htm		(GEC, 2020, s. 8)
1. pillar	ministry_of_industry_and_trade_russia	rus	minpromtorg	minpromtorg_rus	https://minpromtorg.gov.ru	https://www.youtube.com/channel/UCxIN1ojWy-Pnw7FUPoKVWlA	(GEC, 2020, s. 8)

1. pillar	ministry_of_industry_and_trade_russia	eng			https://minpromtorg.gov.ru/en		(GEC, 2020, s. 8)
1. pillar	ministry_of_agriculture_russia	rus	minselhoz	mcx_rf	https://mcx.gov.ru		(GEC, 2020, s. 8)
1. pillar	ministry_of_agriculture_russia	eng		mcx_rf_eng	https://mcx.gov.ru/en		(GEC, 2020, s. 8)
1. pillar	ministry_of_sport_russia	rus	minsportrf		http://minsport.gov.ru	https://www.youtube.com/user/minsportrus	(GEC, 2020, s. 8)
1. pillar	maria_zakharova	rus	maria.zakharova.167				(GEC, 2020, s. 8)
1. pillar	russian_mission_eu	rus	russianmissioneu	rusmission_eu	https://russiaeu.ru/ru		(GEC, 2020, s. 8)
1. pillar	russian_mission_eu	eng	russianmissioneu	rusmission_eu	https://russiaeu.ru		(GEC, 2020, s. 8)
1. pillar	russian_mission_nato	rus	russiansatnato		https://missiontonato.mid.ru		(GEC, 2020, s. 8)

1. pillar	russian_mission_nato	eng	russiansatnato	natomission_ru	https://missiontonato.mid.ru/web/nato-en/		(GEC, 2020, s. 8)
1. pillar	russian_rep_un	rus	russiaun	russiaun	https://russiaun.ru		(GEC, 2020, s. 8)
1. pillar	russian_rep_un	eng	russiaun	russiaun	https://russiaun.ru/en		(GEC, 2020, s. 8)
2. pillar	sputnik_news	eng	sputniknews	sputnikint	https://sputniknews.com	https://www.youtube.com/c/SputnikInternational	(DNI, 2017, s.3); GEC, 2020, s. 34)
2. pillar	rt_international	eng	rtnews	rt_com	https://www.rt.com	https://www.youtube.com/channel/UCpwvZwUam-URkxB7g4USKpg	(DIN, 2017, s. 3); (GEC, 2020, s. 34)
2. pillar	vesti / russia-24	rus	vesti.ru	vesti_news	https://www.vesti.ru	https://www.youtube.com/Russia24TV	(GEC, 2020)
2. pillar	ria_novosti	rus	rianru	rianru	https://ria.ru	https://www.youtube.com/user/rianovosti	(GEC, 2020)

2. pillar	tass	rus	tassagency	tass_agency	https://tass.ru	https://www.youtube.com/channel/UCEyGP84v6qbsZy9-pL6Jx2g	(GEC, 2020, s. 34)
2. pillar	tass	eng	tassagency	tassagency_en	https://tass.com		(GEC, 2020, s. 34)
2. pillar	pervyj_kanal	rus	1tvru	rianru			(GEC, 2020, s. 9)
2. pillar	regnum	rus	regnum.ru	ia_regnum	https://regnum.ru	https://www.youtube.com/regnum_na	(EUvsDisInfo, 2018)
2. pillar	ruptly	rus			https://www.ruptly.tv/ru		(Der Spiegel, 2014); (RFL/RE, 2021)
2. pillar	ruptly	eng	ruptly	ruptly	https://www.ruptly.tv/en	https://www.youtube.com/user/RuptlyTV	(Der Spiegel, 2014); (RFL/RE, 2021)
2. pillar	redfish	eng	redfishstream	redfishstream	https://redfish.media	https://www.youtube.com/redfishstream	(Watts, 2021)
2. pillar	tv_zvezda	rus	tvzvezda	zvezdanews	https://tvzvezda.ru	https://www.youtube.com/user/tvZvezda	(Watts, 2021)

2. pillar	tsargrad_tv	rus	tsargradtv	tsargradtv	https://tsargrad.tv		(Watts, 2021)
3. pillar	global_research	eng			https://www.globalresearch.ca		(GEC, 2020, s. 12)
3. pillar	strategic_culture_foundation	eng			https://www.strategic-culture.org		(GEC, 2020, s. 12)
3. pillar	new_eastern_outlook	rus			https://ru.journal-neo.org		(GEC, 2020, s. 12), (Watts, 2021)
3. pillar	new_eastern_outlook	eng			https://journal-neo.org		(GEC, 2020, s. 12), (Watts, 2021)
3. pillar	news-front	rus			https://news-front.info		(GEC, 2020, s. 12)
3. pillar	news-front	eng			https://en.news-front.info		(GEC, 2020, s. 12)
3. pillar	southfront	rus			https://ru.southfront.org		(GEC, 2020, s. 13)
3. pillar	southfront	eng			https://southfront.org		(GEC, 2020, s. 13)
3. pillar	katehon	rus	katehoncom		https://katehon.com		(GEC, 2020, s. 13)

3. pillar	katehon	eng	katehoncomnews		https://katehon.com/en		(GEC, 2020, s. 13)
3. pillar	geopolitica	rus			https://www.geopolitica.ru		(GEC, 2020, s. 13)
3. pillar	geopolitica	eng			https://www.geopolitica.ru/en		(GEC, 2020, s. 13)
3. pillar	united_world	eng	independentanalyticalcenter	uw_inter	https://uwidata.com		(Watts, 2021)
3. pillar	peacedata	eng			http://peacedata.net		(Watts, 2021)
3. pillar	ria-fan	rus			https://riafan.ru	https://www.youtube.com/channel/UC6m5az_cmJco-ULgoWvFRfg	(Watts, 2021)
3. pillar	russia_insider	eng	russiainsider	russiainsider	https://russia-insider.com/en		(Watts, 2021)
3. pillar	russia_insider	rus			https://russia-insider.com/ru		(Watts, 2021)
3. pillar	zero_hedge	eng			https://www.zerohedge.com/		(Watts, 2021)

3. pillar	the_russophile	eng	therussophiles	therussophile	https://therussophile.org/	https://www.youtube.com/c/Therussophile	(Watts, 2021)
3. pillar	the_duran	eng	thedurancom		https://theduran.com/	https://www.youtube.com/theduran	(Watts, 2021)
3. pillar	the_unz_review	eng	unzreview	unzreview	https://www.unz.com/		(Watts, 2021)
3. pillar	the_saker	eng	vineyardsaker	vineyardsaker	https://thesaker.is		(Watts, 2021)
3. pillar	usa_really	eng	usa-really-443352362741431	really_usa	https://usareally.com/		(Watts, 2021)
3. pillar	center_for_syncretic_studies	eng	syncreticstudies		https://syncreticstudies.com/		(Watts, 2021)
3. pillar	fort_russ_news	eng	officialfortruss	fortrussnews	https://fort-russ.com/		(Watts, 2021)
3. pillar	arms_watch	eng	armswatchnews	armswatch_	https://armswatch.com/		(Watts, 2021)
3. pillar	veterans_today	eng	vtveteranstodaynetwork	veteranstoday	https://www.veteranstoday.com/	https://www.youtube.com/channel/UC2Vba5-IAh9kxID8ExsikFw	(Watts, 2021)

3. pillar	oriental_review	eng			https://orientalreview.org/		(Watts, 2021)
3. pillar	rebel_inside	eng		rebelprotests	https://reblins.com/	https://www.youtube.com/channel/UC9wKZ82qGTTtjDocC83fFqQ	(Watts, 2021)
3. pillar	one_world	eng	oneworldglobalthinktank	oneworldgtt	https://oneworld.press/		(Watts, 2021)
3. pillar	infobrics	multi	bricsmedia	bricsmedia	http://infobrics.org/		(Watts, 2021)
3. pillar	inforos	rus			https://inforos.ru		(Watts, 2021)
3. pillar	inforos	eng			https://inforos.ru/en		(Watts, 2021)

D Kilder i det kinesiske påvirkningsnettverket

Pillar	Name	Facebook	Twitter	Domain	YouTube	Source
1. pillar	China Mission to the EU	chinaeumission	chinaeumission	http://www.chinamission.be	https://www.youtube.com/channel/UCuuhPbzNlWAw1ePgWHFRilw	Egen vurdering
1. pillar	China Mission to the UN		chinamission2un	http://chnun.chinamission.org.cn	https://www.youtube.com/channel/UCcv_r4ktJVNrV6chO1CVhTw	Egen vurdering
1. pillar	China Amb to the UN		chinaambun			Egen vurdering
1. pillar	Chinese Emb in Norway	chinainnorway		http://www.chinese-embassy.no		Egen vurdering
1. pillar	State Council			https://english.www.gov.cn		Egen vurdering

1. pillar	State Council Info Office	chinascio	chinascio	http://english.scio.gov.cn	chinascio	Egen vurdering
1. pillar	Hu Chaoming (CPC)		spokespersonhzm			Egen vurdering
1. pillar	Ministry of Foreign Affairs	mfa.chn	mfa_china	https://www.fmprc.gov.cn	https://www.youtube.com/channel/UCZflnMvKRR0P_7jV9cYbxbg	Egen vurdering
1. pillar	Hua Chunying (MFA)		spokespersonchn			(Stanford Internet Observatory, 2020, s. 13)
1. pillar	Zhao Lijian (MFA)		zlj517			(Stanford Internet Observatory, 2020, s. 13)
1. pillar	Ministry of Commerce			http://english.mofcom.gov.cn		Egen vurdering
1. pillar	Ministry of Defence			http://eng.mod.gov.cn		Egen vurdering
1. pillar	Ministry of Culture & Tourism	chinaculturеorg	chinaculturеorg	http://en.chinaculture.org/ministry.html	chinaculturеorg	Egen vurdering
1. pillar	Ministry of Sci & Tech			http://en.most.gov.cn		Egen vurdering

1. pillar	Ministry of Agriculture & RA			http://english.moa.gov.cn		Egen vurdering
2. pillar	China Education Daily			http://www.jyb.cn		(Lee & Sheng, 2021)
2. pillar	China Public Security Daily			http://www.cpd.com.cn		(Hathaway, 2007)
2. pillar	Xinhua News Agency	xinhuanewsagency	xhnews	http://www.xinhuanet.com	https://www.youtube.com/channel/UCHBDXQDmqnaqlEPdEapEFVQ	(Cook, 2020)
2. pillar	China Central Television	cctvcom	cctv	https://english.cctv.com	https://www.youtube.com/channel/UCT8RMFbTJV5ILaVykrluOQg	(Cook, 2020)
2. pillar	People's Daily	peoplesdaily	pdchina	https://en.people.cn	https://www.youtube.com/channel/UCT90pCh-cwFGxjl4uOfiIPw/featured	(Cook, 2020)
2. pillar	China News Service	echinanews	echinanews	https://www.ecns.cn		(Cook, 2020)
2. pillar	Beijing Daily		dailybeijing	https://www.bjd.com.cn		(Twitter., u.å.c)

2. pillar	Jiefang Daily			https://www.jfdaily.com		(Pamuk & Brunnstrom, 2020)
2. pillar	Global Times	globaltimesnews	globaltimesnews	https://www.globaltimes.cn	https://www.youtube.com/user/GlobalTimesNews	(Cook, 2020)
2. pillar	Hu Xijin (Global Times)		HuXijin_GT			(Stanford Internet Observatory, 2020, s. 13)
2. pillar	China Global Television Network	chinaglobaltvnetwork	cgtnofficial	https://www.cgtn.com	https://www.youtube.com/CGTN	(Cook, 2020)
2. pillar	China Daily	chinadaily	chinadaily	https://www.chinadaily.com.cn	https://www.youtube.com/channel/UCahujLjSL34EPNxtwKRi_vg	(Cook, 2020)
2. pillar	China Military Online		china_military	http://eng.chinamil.com.cn		Egen vurdering basert på 5-P rammeverket (2020, s. 8)
2. pillar	Ta Kung Pao	takungpao		http://www.takungpao.com		(Cheng, 2019)
2. pillar	Wen Wei Po	wenweipo		https://www.wenweipo.com		(Wang & Wong, 2018, s. 14)

2. pillar	China Economic Daily	ednewschina	ednewschina	http://en.ce.cn		(Pamuk & Brunnstrom, 2020)
2. pillar	China Youth Daily			http://www.cyol.net		(Wang, Sparks & Yu, 2018)
2. pillar	Economic Information Daily			http://jjckb.xinhuanet.com		(Kazer 2013)
2. pillar	Legal Daily			http://www.legaldaily.com.cn		(Zhang, 2014, s. 135)
2. pillar	People's Court Daily			http://rmfyb.chinacourt.org		(Zhang, 2014, s. 138)
2. pillar	Reference News			https://www.cankaoxiaoxi.com		(BBC, 2018)
2. pillar	The Beijing News			https://www.bjnews.com.cn		(Amnesty International, 2017, s. 11)
2. pillar	China National Radio	chinanationalradio	cnr_news	http://china.cnr.cn		(BBC, 2018)
2. pillar	The Paper	thepapernews	thepapercn	https://www.thepaper.cn	https://www.youtube.com/channel/UCzdgh34HFyN8v2k3ZZA5uNA	(Peter et al., 2016)

2. pillar	Sixth Tone	sixthtone	sixthtone	https://www.sixthtone.com	https://www.youtube.com/c/SixthTone	(Ni, 2018)
2. pillar	Yicai Global	yicaiglobal	yicaichina	https://www.yicaiglobal.com	https://www.youtube.com/c/yicaiglobal	(Pamuk & Brunnstrom, 2020)
2. pillar	Beijing Review	bjreview	beijingreview	https://www.bjreview.com	https://www.youtube.com/c/BeijingReview	(Pamuk & Brunnstrom, 2020)
2. pillar	CSS Today			http://www.csstoday.com		(Pamuk & Brunnstrom, 2020)
2. pillar	China times		china_times	https://thechinatimes.com		(Hille, 2019)
3. pillar	Gray Zone	thegrayzone	thegrayzonenews	https://thegrayzone.com	https://www.youtube.com/channel/UCEXR8pRTkE2vFeJePNe9UcQ	(Zhang et al., 2021, s. 10)
3. pillar	Guancha		realguancha	https://www.guancha.cn	https://www.youtube.com/channel/UCJncdiH3BQUBgCroBmhsUhQ	(Zhang et al., 2021, s. 7)
3. pillar	South China Morning Post	scmp	scmpnews	https://www.scmp.com	https://www.youtube.com/channel/UC4SUWizzKc1tptprBkWjX2Q	(Cook, 2020)

3. pillar	Phoenix TV	phoenixtvhk	phoenixtvhk	https://phtv.ifeng.com	https://www.youtube.com/c/鳳凰衛視PhoenixTV	(Cook, 2020)
3. pillar	Phoenix TV U.S.	phoenixtv	phoenixtvusa	https://ifengus.com		(Cook, 2020)
3. pillar	Oriental Daily			https://orientaldaily.on.cc	https://www.youtube.com/channel/UCjIEhfJnHqL0oO-K_MyfM8g	(Cook, 2020)
3. pillar	Rumor Shredder				https://www.youtube.com/channel/UCF6wQ8wn36-_8v7m0PJHjTQ/featured	(Nimmo et al., 2019, s. 1)
3. pillar	Michael Welsh				https://www.youtube.com/user/SomersetSavings	(Nimmo et al., 2019, s. 6)
3. pillar	Miss Aiello				https://www.youtube.com/channel/UCMg-RKk_axydF91L6XSgoUg	(Nimmo et al., 2019, s. 8)
3. pillar	Qiao Bao / The China Press	qiaobaowang	usqiaobao	http://www.uschinapress.com	https://www.youtube.com/user/nyusqiaobao	(Stanford Internet Observatory, 2020, s. 13)

3. pillar	Sino Vision	sinovisionofficial		https://www.sinovision.net		(Diamond & Schell, 2018, s. 85)
3. pillar	Ming Pao	mingpaoinews	mingpaocom	https://news.mingpao.com	https://www.youtube.com/channel/UCk8a6ogkkg1EcVysur1Wb9A	(Diamond & Schell, 2018, s. 87)
3. pillar	World Journal	worldjournalnews	nyworldjournal	https://www.worldjournal.com	https://www.youtube.com/channel/UCkohPTwjkan3z7_cPylpTKg	(Diamond & Schell, 2018, s. 87)

E Kilder i det ikke-statlige påvirkningsnettverket

Pillar	Name	Twitter	Domain	YouTube	Source
3. pillar	Gnews	Gnews101064	https://gnews.org	https://youtube.com/channel/UCO3pO3ykAUybrjv3RBbXEHw	(Whalen et al., 2021)
3. pillar	GTV		https://gtv.org		(Whalen et al., 2021)
3. pillar	Rule of Law Foundation	rolfiii	https://rolfoundation.org		(Whalen et al., 2021)
3. pillar	Rule of Law Society	rolsocietyiv	https://rolsociety.org		(Whalen et al., 2021)

F Søkeordlister for å avgrense relevant innhold

Vi har utviklet søkeordslister for å avgrense relevant innhold på Facebook og Twitter. Tilsvarende undersøkelser som vår har brukt samme metode. Da NATO StratCom COE skulle undersøke hvordan russiske narrativ ble videreformidlet av medier i landene på Balkanhalvøya, benyttet de seg av samme metode (Doncheva, 2020). SINTEF benyttet seg av samme metode da de på oppdrag av KMD skulle kartlegge eventuell utenlandsk informasjonspåvirkning i forbindelse med kommunestyre- og fylkestingsvalget (Grøtan et al, 2019).

I vårt arbeid har vi utviklet søkeord-lister for en rekke tema som kan tenkes å være utsatt for utenlandske påvirkningsforsøk. Totalt har vi arbeidet med 16 avgrensede kategorier:

1. Anti-establishment
2. Barnevern
3. Bompenger, veiavgifter og drivstoffpriser
4. By og land
5. Innvandring og asyl
6. Internasjonalt (samarbeid)
7. Islam
8. Klima
9. Korona og pandemihåndtering
10. Likestilling og inkludering
11. Olje- og gassutvinning
12. Sikkerhetspolitikk og Nato
13. Vaksiner
14. Valg - deltakelse
15. Valg - tillit
16. Vindkraft

Vi har operert med to typer av søkeord-lister for hvert avgrenset tema.

Den første typen (tematikk) inneholder deskriptive ord av temaet, relevante begrep eller entiteter som personer og organisasjoner som ofte nevnes i forbindelse med temaet. Formålet med denne har vært å kunne gi et overblikk over hvor mye bestemte tema har blitt omtalt og diskutert i den analyserte tidsperioden.

Den andre typen listen (ladede ord) inneholder språklige uttrykk som slang, ladede ord og stammespråk som er blitt observert brukt i forbindelse med omtale av temaet i sosiale medier. Formålet med denne har vært å skape et overblikk over potensiell polariserende omtale av de samme tematikkene.

Utover de 16 kategoriene har vi også utviklet 3 ytterligere søkeord-lister:

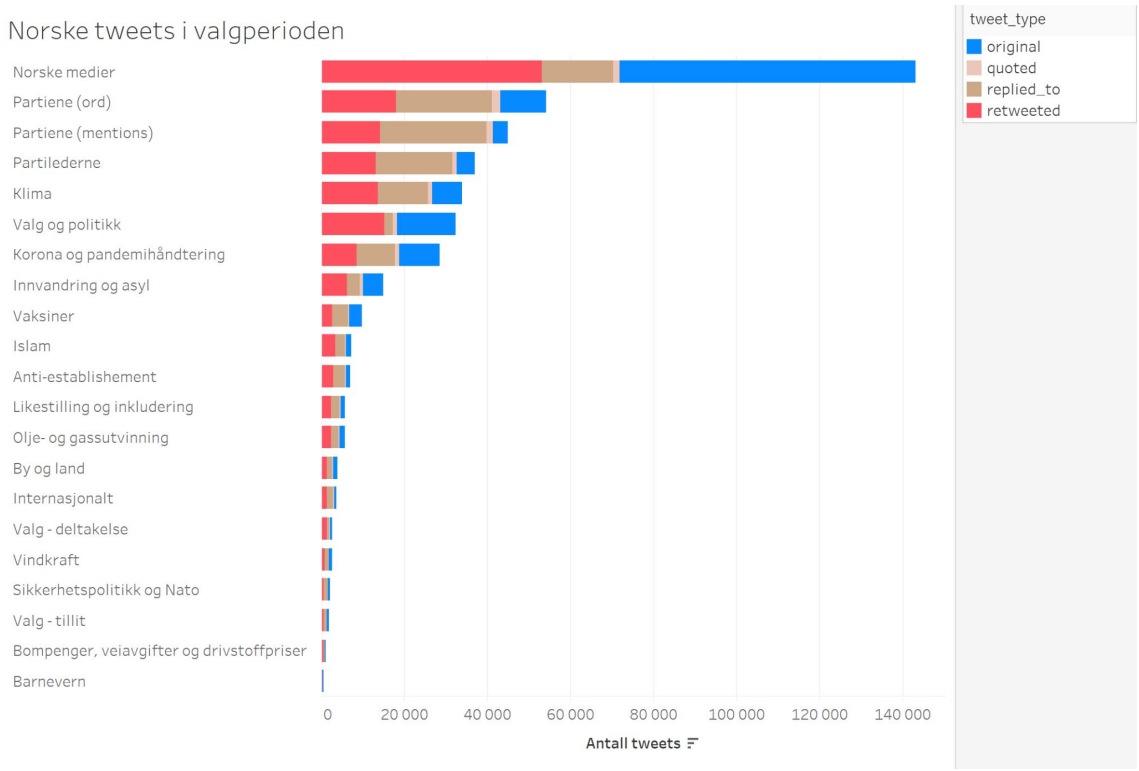
- Vanlig brukte emneknagger for norsk politikk og det norske valget

- Partier som var representert på Stortinget før valget og deres daværende partiledere (navn og brukernavn på Twitter)
- Nasjonale og regionale medier i Norge (navn og brukernavn på Twitter)

En twittermelding kan inneholde søkeord som hører inn under flere av tematikkene vi har ønsket å fange opp. Oversikten i vedlegg F viser kun den første kategorien som en twittermelding ble tilordnet. Innsamlingen ble gjennomført ved å først søke etter de to valg temaene (tillit og deltakelse), deretter er søket gjennomfør alfabetisk. Dette betyr at dersom en twittermelding inneholder søkeord som både faller inn under anti-establishment og vindkraft, så vil twittermeldingen kun telle under den første kategorien.

Søk som dette har noen begrensninger. For det første vil vi kun fange opp innhold som vi antar at vi kjenner til hvordan omtales på forhånd. Man kan se for seg at tema er blitt omtalt på andre måter, uten bruk av ordene vi har søkt etter. Metoden tar ikke høyde for konteksten ord brukes i, eller meningsinnholdet i teksten som ordene inngår i. Ord kan for eksempel inngå i en satirisk eller ironisk kontekst, noe denne metoden ikke vil kunne fange opp. Det må derfor understrekes at resultatene av denne metoden alene ikke kan brukes til å kvantifisere det totale omfanget av et tema, eller holdningene til temaet.

G Twittermeldinger funnet med søkeordlister for relevant innhold



Figur G.1 *Oversikt over antall twittermeldinger som ble fanget opp med de spesifiserte søkeordslistene i perioden 1. august – 16. september 2021. Totalt ble det innsamlet 360 473 twittermeldinger (originale, retweets, replies og quotes). Se vedlegg F for beskrivelse av hva som inngår i de ulike temaene.*

Om FFI

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

FFIs formål

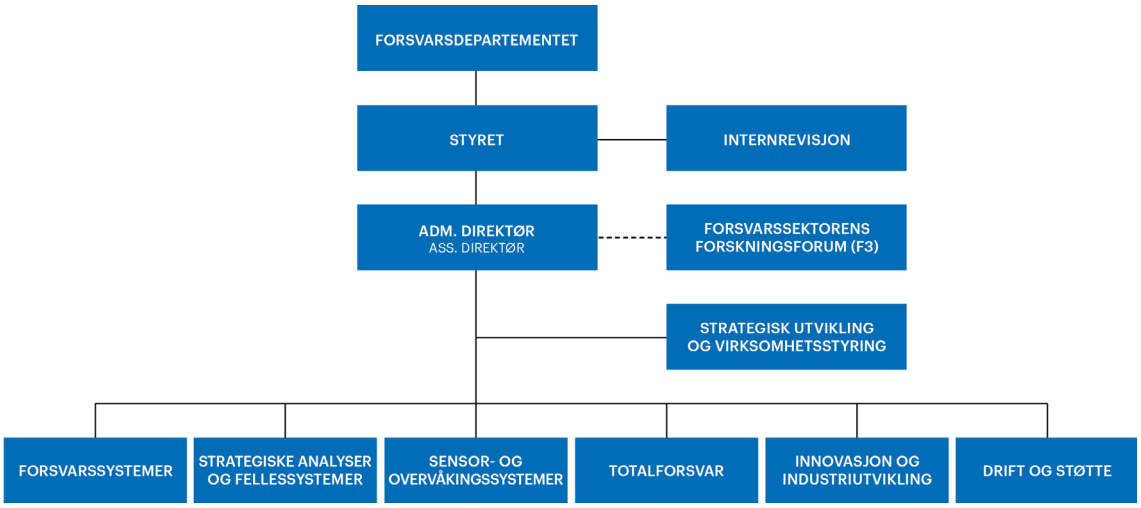
Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som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