FFI-RAPPORT

20/01694

Påvirkningsoperasjoner i sosiale medier

– oversikt og utfordringer

Arild Bergh

Påvirkningsoperasjoner i sosiale medier
– oversikt og utfordringer

Arild Bergh

Forsvarets forskningsinstitutt (FFI) 17. juni 2020

Emneord
Sosiale medier
Informasjonsoperasjoner
Desinformasjon
Hybridkrigføring
Cyberdomenet

FFI-rapport
20/01694

Prosjektnummer
1582

Elektronisk ISBN
978-82-464-3280-9

Engelsk tittel
Influence operations in social media – summary and challenges

Godkjennere
Ann-Kristin Elstad, *forskningsleder*
Janet Blatny, *forskningsdirektør*

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Illustrasjoner
Infografikk av Grete Foss Alvestad

Sammendrag

Formålet med denne rapporten er todelt: å gi en omfattende oversikt over hvordan stater bruker sosiale medier for å prøve å påvirke befolkningen i andre land, og å undersøke hvordan slike operasjoner har blitt håndtert. Bakgrunnen/bakteppet for rapporten er den økende bruken av sosiale medier i innblanding i for eksempel valg, internasjonale relasjoner eller krisesituasjoner som covid-19-pandemien. Rapporten fokuserer på de praktiske aspektene ved slike påvirkningsoperasjoner – hvilke aktører og elementer er involvert, og hvordan fungerer det? Denne rapporten er rettet mot de som måtte trenge å håndtere eller forholde seg til slik påvirkningsoperasjoner som en del av sitt daglige arbeid. Rapporten forutsetter ikke ekspertkunnskap på områder som media, strategisk kommunikasjon eller informasjonsteknologi – rapporten gir grundige forklaringer og bakgrunn for teknologier som brukes, aktører som er involvert og rollene og samspillet mellom aktørene og teknologiene i påvirkningsoperasjoner.

Den sentrale problemstillingen er hvordan den globale, høyteknologiske private infrastrukturen til sosiale medie-selskaper gir direkte, ikke-redigert tilgang til brukere over hele verden, og hvordan denne infrastrukturen misbrukes for å drive skjult påvirkning. Relevante spørsmål blir diskutert gjennom en studie av de russiske påvirkningsforsøkene i det amerikanske presidentvalget i 2016, med henvisninger til den nåværende covid-19-pandemien der det er nødvendig. Gjennom en grundig litteraturgjennomgang, med tilleggsinformasjon fra deltakelse i Nato-grupper og konferanser, blir tre områder undersøkt og belyst:

1. Anatomien til en påvirkningsoperasjon: Hva slags innhold skapes og hvordan spres det? Hvordan støttes en operasjon, bevisst eller utilsiktet, av et økosystem med aktører som dukker opp rundt temaer som blir utnyttet i en påvirkningsoperasjon?

2. Hvordan forsøkte sosiale medieplattformer og myndigheter å håndtere en slik innblanding?

3. Hva er status med hensyn til mulighetene for påvirkningsoperasjoner gjennom sosiale medier? Hva er holdningene og handlingene til sosiale medieplattformer, nasjonale myndigheter og brukere av sosiale medier for å prøve å håndtere slike trusler?

Undersøkelsen av disse tre områdene fører til en oppsummering av utfordringene dette utgjør for et demokratisk land. Rapporten antyder at et demokrati vanskelig kan stoppe slike påvirkningsforsøk direkte. I stedet må man kunne håndtere dem gjennom å øke kunnskapen om hvordan påvirkning fungerer i sosiale medier og hvilke problemer og målgrupper en påvirkningsoperasjon kan prøve å utnytte. Slik kunnskap kan brukes til å utvikle utdanningsprogrammer for å fremme motstandsdyktighet blant relevante aktører og i landet for øvrig.

Summary

The purpose of this report is to provide a comprehensive overview of how social media is used by states to try to influence other countries' population and to examine how such operations have been handled. This is in response to the increasing use of social media to interfere in, for instance, elections, international relations or crisis situations such as the covid-19 pandemic. The focus is on the practical aspects of such influence operations – what actors and elements are involved and how do they work? This report is aimed at those who may need to handle or relate to such influence operations as part of their everyday work. The report does not assume an expert knowledge in areas such as media, strategic communication or information technology – the report provides thorough explanations and backgrounds for technologies used, actors involved and the roles and interactions between actors and technologies in influence operations.

The key issue examined is how the global, high-tech, private infrastructure of social media companies provide direct, non-editorial access to users around the world, and how this infrastructure is abused for the purpose of covertly influencing people. Relevant issues are highlighted through a study of the Russian influence attempts in the US presidential election in 2016, with references to the current covid-19 pandemic where relevant. Through a thorough literature review, with additional information from participation in NATO groups and conferences, three areas are examined and explained:

1. The anatomy of an influence operation: What type of content is created and how is it spread? How is an operation supported, knowingly or unintentionally, by an ecosystem of actors that emerge around issues that an influence operation seeks to exploit?

2. How did social media platforms and authorities try to handle such meddling?

3. What is the current status as to the possibilities for influence operations through social media? What are the attitudes and actions of social media platforms, national authorities and social media users to try to handle such threats?

The examination of these three areas leads to a summary of the challenges this pose for a democratic country. The report suggests that it is unrealistic for a democracy to stop such influence attempts directly. Instead one must be able to handle them through increased knowledge of how an influence operation works and what issues and target groups it might try to affect. Such knowledge could then be applied to develop educational programmes to foster resilience in relevant organisations and the country at large.

Innhold

1 Innledning

Siden 2014 har man sett en markant økning i staters koordinerte bruk av sosiale medier for å forsøke å påvirke andre staters befolkning. De mest kjente påvirkningsforsøkene har funnet sted under anneksjonen av Krim i 2014, presidentvalget i USA i 2016 og covid-19-pandemien i 2020. Mindre påvirkningsaktiviteter har blitt observert i forbindelse med terrorangrep i Storbritannia 2017 [1], angrep på ukrainske skip i 2018 [2] og valg i Tyskland [3] samt EU [4]. Gitt at slike påvirkningsoperasjoner har lave kostnader, er vanskelig å tilskrive en bestemt aktør og kan nå andre staters innbyggere direkte, er det rimelig å anta at slike operasjoner vil øke i omfang.

Det er mange artikler og rapporter som har diskutert disse og lignende hendelser, og det refereres til mange av disse i denne rapporten. Derimot finnes det ikke per i dag en helhetlig oppsummering av de forskjellige elementene som blir benyttet og utnyttet i en moderne påvirkningsoperasjon i sosiale medier – fra mangel på sentral oversikt til misbruk av kunstig intelligens. Formålet med denne rapporten er å gi en bred oversikt over hvordan sosiale medie-baserte påvirkningsoperasjoner utføres, oppfattes og håndteres og hvilke aktører som er involvert, med eller uten vitende og vilje.

Ofte forveksles individuelle påvirkningselementer, som falske nyheter (usann informasjon som maskeres som nyheter), med den overordnede påvirkningsoperasjonen. Falske nyheter er i realiteten et av mange mulige virkemidler som benyttes for å påvirke målgrupper. For å gi et bedre bilde av statlige påvirkningsforsøk vil rapporten diskutere oppbygningen til en cyber-sosial påvirkningsoperasjon; egenskaper ved sosiale medier som gjør storskala påvirkning mulig; hvilke ressurser som benyttes og økosystemet som dannes rundt slike operasjoner. Deretter diskuteres sosiale medie-selskapers og myndigheters holdninger til, og håndteringer av, påvirkningsforsøk samt mulighetene for påvirkning per i dag. Avslutningsvis skisseres utfordringene for Norge og mulige tilnærminger for å sette Forsvaret og sivilsamfunnet bedre i stand til å håndtere mulige påvirkningsforsøk.

1.1 Definisjoner

En *påvirkningsoperasjon* er en aktørs koordinerte forsøk på å påvirke meninger og virkelighets-oppfatninger hos mennesker og grupper utenfor deres juridiske kontroll, uten at disse er klar over aktørens involvering [5]. Målet er at de som utsettes for påvirkning utfører handlinger som ellers ikke vil bli utført. Denne rapporten diskuterer påvirkning via Internett, og spesielt sosiale medier. Slike påvirkningsforsøk kan være en del av en større operasjon som også bruker andre kanaler, for eksempel diplomatiske utspill.

NATO har erklært at *cyberspace* er et eget domene for krigføring [6]. Cyberspace defineres her som det virtuelle (tenkte) rommet som oppstår når mennesker kommuniserer og utfører aktiviteter gjennom datanettverk. Cyberspace er med andre ord en kombinasjon av teknologi, mennesker og handlinger. Innen dette domenet er *sosiale medier* definert som tjenester som

tillater publisering av innhold fra personer som ikke eier eller kontrollerer tjenesten. Sosiale medier tilrettelegger for ubegrenset, uredigert distribusjon av dette innholdet slik at andre mennesker kan se, bruke og svare på slikt innhold [5, s. 13].

Fiendtlige handlinger i cyberspace forbindes ofte med det som bredt kalles *hacking*, det vil si misbruk av datamaskiner og nettverk for å få tak i informasjon (for eksempel hemmelige dokumenter) eller volde fysisk skade (eksempelvis slå av strømnettet). Selv om slike aktiviteter kan være en del av en større påvirkningsoperasjon, med mulig intensjon om å spre frykt i en befolkning, er det ikke slike typer handlinger rapporten vil diskutere. I denne rapporten vektlegges *cyber-sosiale*-angrep og -operasjoner som finner sted innenfor sosiale medier, mens hacking vil komme under samlebetegnelsen *cyber-tech*-angrep.

Uttrykkene *desinformasjon* og *misinformasjon* brukes ofte når man diskuterer feilaktig informasjon som spres på sosiale medier. Desinformasjon kan defineres som spredning av feilaktig eller villedende informasjon med forsett om å manipulere. Misinformasjon er spredning av feilaktig eller villedende informasjon uten at det nødvendigvis foreligger et negativt forsett. Ofte tror de som sprer misinformasjon selv på den feilaktige informasjonen. I realiteten er det uklare linjer mellom disse to begrepene. Desinformasjon blir ofte plantet blant målgrupper som tror på de feilaktige opplysningene og sprer det videre, mens aktører som står bak påvirkningsoperasjoner promoterer misinformasjon som passer inn i deres narrativ. Et *narrativ* er en overordnet og samlende fortelling. Den forener individuelle informasjonsbiter til en større, og mer overbevisende, helhet samtidig som den gir målgruppene for en påvirkningsoperasjon en måte å tolke ny informasjon på som kan fordreie fakta.

1.2 Metode

Rapporten er basert på en bred gjennomgang av relevant litteratur på området påvirkning og sosiale medier. Fordi dette er et nytt felt i kontinuerlig og rask endring, er relevant litteratur ikke bare akademiske kilder, men også en rekke andre formelle og uformelle kilder. Dette inkluderer blant annet sosiale medie-selskapers bedriftsblogger, artikler fra nettbaserte teknologipublikasjoner, statlige aktørers etterretningsrapporter, datasett med sosiale medie-innlegg fra påvirkningsaktiviteter, analyser av påvirkningsforsøk i sosiale medier og artikler fra tradisjonelle nyhetsmedier. Funnene er, så langt det har latt seg gjøre, kryssjekket med flere kilder.

Forfatteren har lang erfaring som dataprogrammerer og har jobbet som sosiolog siden midten av 2000 tallet. Denne kompetansekombinasjonen har vært brukt til å evaluere problemstillingene i denne rapporten for å se hvordan brukere samhandler i og gjennom sosiale medier og hva teknologiens rolle er, et såkalt sosio-teknisk perspektiv [5], [7], [8]. Det vil si at sosiale interaksjoner i en teknologisetting forstås fra et samfunnsvitenskapelig vinkel som også undersøker hvordan teknologien letter og påvirker disse interaksjonene [9]–[11]. For påvirkningsoperasjoner i sosiale medier innebærer dette å se hvordan enkeltpersoner og grupper jobber innenfor strukturene som er skapt gjennom teknologier, for eksempel søk eller krypterte kommunikasjonskanaler [12].

1.2.1 Datavalg

Denne rapporten bruker USAs presidentvalg i 2016 (heretter *USA-valget*) som en eksempelstudie for å forklare hvordan sosiale medier brukes til påvirkning. Der hvor det er relevant diskuteres andre påvirkningshendelser, spesielt desinformasjon tilknyttet covid-19-pandemien som er aktuelt i skrivende stund. USA-valget er brukt som kasus fordi det per i dag er det best dokumenterte tilfellet med svært mange aktører som, bevisst eller ubevisst, deltok i mange kapasiteter. Dette eksempelet gir derfor en god oversikt over hvilke aktører som kan spille en rolle i framtidige påvirkningsforsøk.

1.2.2 Begrensninger

Det er utenfor denne rapportens rammer å gi en komplett oversikt over mulige trusler fra påvirkningsoperasjoner i sosiale medier. Slike trusler kan være alt fra forsøk på å splitte allierte og redusere sivil støtte til militærbruk til å påvirke valg eller redusere tilliten til myndigheter. Rapportene diskuterer heller ikke om eller hvordan innflytelse virker, for en dypere diskusjon på dette se [5], [13], [14].

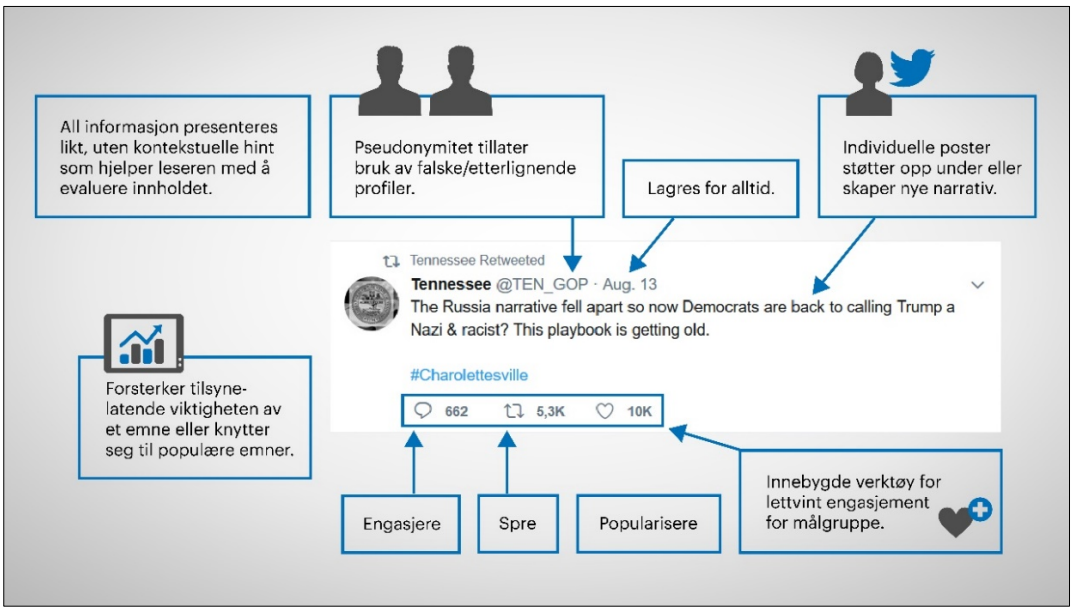
2 Anatomien til en påvirkningsoperasjoner i sosiale medier

Cyber-sosiale påvirkningsoperasjoner vil være forskjellige med hensyn til målet med operasjonen og hvilke målgrupper operasjonen er rettet mot. Teknologiske muligheter og hindringer er i konstant utvikling og vil også ha en effekt på hvordan påvirkningsoperasjoner utføres. Samtidig har sosiale medier egenskaper som former påvirkningsoperasjoner, og visse elementer er felles for de fleste påvirkningsforsøk. Dette kapittelet vil diskutere disse egenskapene og elementene og forklare hvordan de passer sammen. Formålet er å skape en forståelse for hva som muliggjør og forsterker påvirkning i sosiale medier.

Analysen starter med en gjennomgang av elementene i påvirkningsoperasjoner: 1) innleggene som brukerne leser, 2) iverksetteren som står bak påvirkningsforsøk, 3) målgruppen(e) som ønskes påvirket, 4) innholdet som utarbeides, 5) infrastrukturen som sprer innhold, 6) økosystemet som støtter opp om spredningen av innhold og narrativ fra påvirkningsoperasjoner og 7) nyhetsstrømmen hvor påvirkningen når fram til sosiale medie-brukerne.

2.1 Innlegget

Forskjellige sosiale medie-selskaper tilbyr ulike former for kommunikasjon. For eksempel brukes YouTube for å dele og kommentere videoer, mens Twitter kringkaster korte informasjons-snutter. Det er imidlertid noen elementer som går igjen. Disse er belyst i figur 2.1, med tanke på hvor nyttige de kan være for en påvirkningskampanje.



Figur 2.1 En tweet fra en IRA-kontrollert konto [15]. Kommentarene i boksene trekker fram aspekter som er nyttige for en påvirkningsoperasjon.

For en påvirkningsoperasjon er en av de viktigste egenskapene ved sosiale medier at alt innhold formateres likt. Innlegg fra en venn og en fremmed stats påvirkningsoperasjon ser likedan ut. Kombinert med online anonymitet gjør dette det vanskelig for mottaker å evaluere sannferdigheten av informasjon på sosiale medier. Muligheten til å linke innlegg mot eksisterende trender og verktøy som kvantifiserer «popularitet», sammen med lettbrukte verktøy for å like eller gjenbruke innlegg, bidrar til svært hurtig spredning av påvirkningsforsøk i sosiale medier. Samtidig vil automatisert seleksjonen av innhold (se faktaboks på side 14) velge innlegg basert på brukernes interesser. Individuelle innlegg kan dermed samles til en mer overbevisende helhet, et *algoritmisk narrativ* [5, s. 48].

2.2 Iverksetteren

Sosiale medie-innlegg er kjernen i den type påvirkningsoperasjoner som diskuteres her og noen må koordinere opprettelsen og distribusjonen av disse innleggene. I den russiske påvirknings-operasjonen mot USA-valget var dette tatt hånd om av den såkalte *russiske trollfabrikken* i St. Petersburg. Trollfabrikken, hvis egentlige navn er *The Internet Research Agency* (IRA) [16], hadde planlagt og prøvd ut cyber-sosial påvirkning over flere år (hovedsakelig på egen befolkning) og er fortsatt aktive i dag [17]. IRA – styrt av russiske myndigheter, men holdt på en armlengdes avstand via en ekstern organisasjon – strømlinjeformet bruken av sosiale medier i stor skala. Twitter har frigitt ca. ni millioner tweets fra IRA-kontrollerte profiler. Gjennom Facebook skal de ha nådd frem til 126 millioner profiler[1], 20 millioner på Instagram 1,4 millioner på Twitter og mer enn tusen videoer har blitt lastet opp på YouTube. [18, s. 6]. Det månedlige budsjettet skal til tider ha ligget rundt 1,25 millioner dollar [19], [20]. Det er derfor snakk om en godt utviklet organisasjon som (i sosiale mediers tidsperspektiv) jobbet på lang sikt.

Det er viktig å forstå at måten IRA generelt jobbet på var basert på lærdommer fra tidligere forsøk på å «*[dominere] massebevissthet på nettet*» [21, s. 3]. Forsøk på å kontrollere interne protester i 2011 gjennom rene tekniske løsninger hadde gitt Russland dårlige erfaringer, og det var klart at påvirkningsoperasjoner måtte kontrolleres av mennesker [21, s. 3]. Derfor var opp mot 600 personer involvert i påvirkningsoperasjonen mot USA-valget. Såkalte *bots*, programvare som automatisk utfører handlinger for å få innlegg eller temaer til å virke populære, ble kontrollert av ansatte og var ikke fullt automatisert. Ansatte i IRA fikk opplæring i engelsk og måtte lære om amerikansk kultur, blant annet via TV-serier [22], for å forstå hva som ville være relevant innhold å bruke i en påvirkningsoperasjon. Det kan også være mye som tyder på at ansatte var opportunistiske og hadde stor handlefrihet, siden de reagerte fort på hendelser og endringer i lokale forhold [23, s. 33], [24], [25]. Rent praktisk ble de ansatte forventet å produsere en viss mengde innhold hver dag [22], som ble lagt ut på Facebook, Twitter og Instagram.

[1] I denne rapporten brukes uttrykket *profiler* istedenfor brukere. Når data fra sosiale medier analyseres, vet man ikke nødvendigvis hvor mange kontoer som var falske, kontrollert av bots eller organisasjonskontoer som ikke var koblet mot en spesifikk bruker.

2.3 Målgruppen

Målgruppen vil variere med formålene til en påvirkningsoperasjon. Grovt sett kan man dele påvirkningsoperasjoner inn i de som ønsker å endre målgruppens syn på noe(n) og de som ønsker å så splid i samfunnet ved å forsterke eksisterende syn. Russland vektlegger ofte det siste, tilnærmingene som har blitt sett i sosiale medier bygger på tidligere sovjetiske «aktive tiltak» [26]–[29]. De fokuserer på å utnytte uenigheter i befolkningen og bidra til usikkerhet om hva som er sant eller ikke for å trigge visse responser. Blant amerikanske målgrupper kunne IRA relativt lett utnytte eksisterende skillelinjer som lokale politikere allerede appellerte til – for eksempel rase, religion eller våpen.

Figur 2.2 *IRA Facebook-annonser fra 2. kvartal 2015 og 4. kvartal 2016. (***kilde: [30]***). Her ser man hvordan sterke, eksisterende narrativ som sår splid støttes, uten noen som helst referanse til russiske interesser.*

Påvirkningsoperasjoner i det virkelige liv må jobbe mer for å nå målgruppene enn cyber-sosiale operasjoner, dette er en viktig forskjell. Offline må man foreta en form for målgruppeanalyse som viser hva forskjellige grupper er interessert i og hvor de kan nåes. På sosiale medier trenger man kun en grov oversikt over temaer som trigger interesse. Man legger så ut innhold som er relevant til disse temaene og algoritmer finner målgruppene for innholdet (se faktaboks side 17).

En annen tilnærming er bruk av reklame som vises i brukernes nyhetsstrøm. I motsetning til vanlige sosiale medie-innlegg gir reklame mer direkte kontroll over hvem som ser innholdet fra en påvirkningsoperasjon uten behov for den myke infrastrukturen som diskuteres i kapittel 2.5. Istedenfor kan sosiale medie-selskapers egne verktøy for målrettet annonsering benyttes. Dette gir en stor grad av presisjon med hensyn til hvem innholdet vises til. Figur 2.2 demonstrerer hvordan IRA brukte annonser for å støtte forskjellige politiske synspunkter. Som diskutert tidligere var de interessert i å forsterke motsetninger. Annonsen til høyre, som oppfordret afro-amerikanere til ikke å stemme, var rettet mot brukere i USA mellom 18 og 65 år som var interessert i et av de følgende temaene: *Martin Luther King, Jr., African-American Civil Rights Movement, African-American history* eller *Malcolm X*. Etter at IRA hadde spesifisert kriteriene for målgruppene var det Facebooks algoritmer som fant brukerne for IRA.

2.4 Innholdet

Etter å ha identifisert relevante emner, lages, resirkuleres eller promoteres innhold som er relevant til temaene og narrativene som aktøren ønsker å promotere. I USA-valget vektla som nevnt IRA innhold som forsøkte å øke eksisterende splittelser i befolkningen. Et eksempel relatert til immigrasjon er denne meldingen fra en IRA-kontrollert profil [31]:

> *Mass immigration is a globalist policy supported & bankrolled by mega corporations & transnational elitists Mass immigration only benefits the wealthy of a host country. […] (@covfefenationus 26 Nov 2017).*

Innhold fra påvirkningskampanjer består ikke kun av løgner. Ofte er det vektlegging og selektering av informasjon fra andre kilder. Innlegg fra ekte brukere som representerer ytterpunkter i debatter siteres eller informasjon tas ut av kontekst. Man kan også skape eller referere til eksternt innhold, for eksempel nettsteder for falske nyheter eller kilder som støtter en begrenset del av synspunktene som promoteres. Informasjon om en virkelig hendelse eller meningsytringer om noe som har skjedd kan fordreies. Operasjoner kan også trigge vanlige brukere til å skape innhold som passer inn. Bruk av konspirasjonsteorier, lekkasjer av materiale fra hackerangrep eller uttalelser fra angriperens representanter, for eksempel ambassadører [32], er noen eksempler på dette.

Visuelt innhold, det vil si bilder og videoer, er mye brukt. Disse kan være manipulert eller re-kontekstualisert, det vil si at de tas ut av sin originale sammenheng. Såkalte *memes* brukes ofte [33]–[36]. Dette er humoristiske og visuelle kommentarer som ofte spres *viralt*, det vil si at på kort tid deles innholdet av mange brukere, også utenfor den opprinnelige målgruppen. Kampanjer som har blitt sporet tilbake til IRA har i økende grad benyttet bilder, dermed unngår

de også språkfeil som kan avsløre en utenlandsk aktør [37]. Videoer tar mer tid å lage, man bruker derfor ofte eksisterende videoer i ny sammenheng, eller de redigeres for å passe inn i påvirkningsoperasjons narrativ. Slik gjenbruk av andres arbeid har vært en del av nettkulturen fra begynnelsen. Dette er et eksempel på hvordan Internettets særegenheter understøtter påvirkningsforsøk på en måte som tradisjonelle medier ikke gjør.

2.5 Infrastrukturen

Påvirkningsoperasjoner i sosiale medier benytter hva man kan kalle en *myk infrastruktur* for å distribuere innholdet som lages. Den harde infrastrukturen, som nettverk, servere og lagringsplass, er tilgjengelig gratis takket være sosiale medie-selskapene som betaler for dette ved hjelp av reklame. Den myke infrastrukturen inkluderer et stort antall profiler som har blitt opprettet, ofte automatisk. Disse profilene benyttes for å utføre standard sosiale medie-handlinger, som å legge ut originalt innhold eller interagere med andre brukere, for eksempel ved å like eller videresende andres innlegg. Noen profiler kontrolleres helt eller delvis av operatører, andre vil bli brukt av bots. En slik infrastruktur kan også inkludere eksterne nettsteder for falske eller ekstremt partiske nyheter som det linkes til i sosiale medie-innlegg. Slike nettsteder er en del av økosystemet (som beskrives i kapittel 2.5) som, bevisst eller ikke, støtter opp om påvirkningsforsøk.

Noen profiler har høy verdi for en angriper. De har blitt utviklet over tid ved å legge ut eller videresende innhold som appellerer til visse grupper og representerer etter hvert troverdige kanaler for disse gruppene. Slike profiler har opparbeidet mange følgere som kan nåes direkte med nytt innhold [38]. En slik direkte kontakt er verdifull, fordi man når målgruppen direkte med nye innlegg. For å nå ikke-følgere må ekstra ressurser brukes på å manipulere popularitet eller relevansen til et innlegg. I tillegg vil følgere hjelpe til med å spre innlegg til sine kontakter. Profilen *ten_gop* – som ble kontrollert av IRA og utga seg for å være det republikanske partiet i Tennessee – hadde for eksempel 145 000 følgere [39] og ble sitert i en rekke andre medier [40]. 145 000 følgere er ikke mye, gitt Twitters totale brukermasse. Men på sosiale medier gir *venners venner* en eksponentiell økning i antall brukere man kan komme i kontakt med. Eksempelvis fikk Cambridge Analytica informasjon om 87 millioner Facebook-profiler via 270 000 brukere som fylte ut en online personlighetstest. Ved å godta bruksvilkårene for testen ga de tilgang til sine venners profiler [41]. En rapport om IRA, i en russisk avis, beskrev hvordan operatører ville banne av fortvilelse når en verdifull profil de hadde bygget opp hadde blitt sperret [22]. Man har også sett eksempler på gjenbruk av eksisterende profiler for nye formål, for eksempel ble en profil som opparbeidet seg følgere via pro-Palestinsk innhold gjenbrukt for Brexit-propaganda [42, s. 2].

Mindre viktige profiler blir satt opp automatisk og brukes av bots for å øke popularitet til innlegg fra viktigere profiler og promotere innlegg fra vanlige brukere som støtter påvirknings-operasjonens narrativ. Når uviktige profiler blir sperret tar det noen sekunder å automatisk lage en ny profil.

2.6 Økosystemet

Å lage og laste opp innhold via den myke infrastrukturen er kun det første steget i å nå fram til målgruppene. En iverksetter ønsker at innholdet spres bredest mulig, det er her økosystemet kommer inn. Et økosystem er, i overført betydning fra biologien, alle aktørene som er samlet et sted og miljøet rundt dem. I et økosystem er aktører i samspill med miljøet. De forskjellige elementene i økosystemet knyttes sammen gjennom distribusjon av ting de behøver for å overleve. I cyber-sosiale påvirkningsoperasjoner inkluderer økosystemet iverksetteren og deres ansatte samt direkte støttespillere som bevisst har samme mål som iverksettere. Andre aktører er grupperinger og brukere som enten er enig i iverksetters narrativ eller ønsker å tjene penger ved å spre narrativet videre. Disse aktørene er ikke klar over målet med påvirkningsoperasjonen. Miljøet rundt disse aktørene inkluderer sosiale medie-plattformenes infrastruktur og automatiserte ressurser som bots og algoritmer.

Den massive spredningen som IRAs innhold fikk i USA-valget kom via et økosystem av statlige, kommersielle og individuelle aktører. Disse aktørene hadde forskjellige agendaer, men spredde så mye materiale at det overveldet manuelle forsøk på moderering av innholdet (se også kapittel 4.2.2).

2.6.1 Cyber-tech aktører

Dette er aktører som opererer i cyber-tech domenet. De benytter skjulte angrepsmetoder for å ramme datamaskiner, nettverk og infrastruktur. Det kan være hackere som lekker eposter fra hackede kontoer for å diskreditere noen eller de angriper infrastruktur for å skape frykt. Det kan også være såkalte nett-troll som angriper og truer navngitte personer som motsetter seg påvirkningsoperasjonens narrativ eller metoder. Slike personangrep utføres ved å dele personlig informasjon, for eksempel bosted. Slike aktører kan ha ulik intensjon bak gjennomføringen, som at aktøren jobber direkte for en stat, gjør det for penger eller liker å plage andre.

Denne delen av økosystemet vil ofte generere støy, reaksjoner og oppmerksomhet som en påvirkningsoperasjon kan utnytte. For eksempel kan lekkede dokumenter føre til mer oppmerksomhet i bredere lag av befolkningen, eller at vanlige brukere legger ut innhold som støtter målene med påvirkningsoperasjonen.

2.6.2 Kommersielle aktører

Kommersielle aktører inkluderer sosiale medie-selskapene via annonsesalg, noe IRA benyttet seg av i USA-valget. I tillegg er det mer suspekte geskjefter, som nettsider for falske nyheter som tjener penger via reklame [43], [44]. Såkalte *click farms*, bedrifter i lavtlønnsland som Bangladesh hvor personer manuelt liker, kommenterer, deler og produserer falske anmeldelser mot betaling, kan synliggjøre innhold ved å manipulere popularitetsmålinger, for eksempel *trending topics* på Twitter. Click farms og lignende selskaper representerer en forutsigbar ressurs for å spre og popularisere innhold, men profilene som benyttes vil ha mindre troverdighet fordi de er «bruk-og-kast-profiler», som en dag reklamerer for pornografi og den

neste dagen for en politisk kandidat. Slike profiler er derfor best egnet til mindre sofistikerte aktiviteter som å øke antall *likes* på et innlegg.

2.6.3 Emne-sympatisører

I forbindelse med USA-valget ble *alt-right* bevegelsen diskutert som en implisitt støttespiller for IRAs påvirkningsforsøk som fremmet Trump [45]. Selv om dette stemmer til en viss grad er det en forenkling av det som foregår i sosiale medier. Diskusjoner på sosiale medier generelt har en begrenset tematisk bredde, dette er delvis en følge av den begrensede plassen sosiale medie-innlegg har for å uttrykke seg. Påvirkningsoperasjoner kan derfor appellere til en rekke emner for å få støtte uten at brukerne har sammenfallende interesser med påvirkningsoperasjonen. IRA profilen *ten_gop* ble for eksempel re-tweeted både av Donald Trump Jr. og rap-artisten Nikki Minaj i forskjellige sammenhenger [40]. Dette gir også overlapp med andre som utnytter samme emner. Innlegg fra IRA vil ha nådd de samme målgruppene som Cambridge Analyticas valgkamp-annonser fordi begge aktørene utnyttet lignende temaer. I forbindelse med covid-19-pandemien ser man at temaer som alternative kurer og troen på at viruset er menneskeskapt utnyttes for å så mistillit til myndighetene i forskjellige land.

Emne-sympatisørers engasjement øker et innleggs popularitet, synlighet eller tilsynelatende viktighet. Samtidig er det et vesentlig kvalitativt aspekt her. Informasjon som deles av noen man kjenner er mer troverdig og føles mer betydningsfull for den som mottar det [46].

Emne-sympatisører kan også manipuleres til å danne en online mobb som angriper individer som står for andre synspunkter enn det påvirkningsoperasjonen ønsker å spre. Dette fungerer som en usynlig, men effektiv form for sensur [47], ofte rettet mot kvinner [48], [49].

2.6.4 Automatiserte ressurser

Økosystemet rundt påvirkningsoperasjoner er i stor grad basert på automatisering. Automatiserte ressurser kan være en del av sosiale medie-selskapene eller de kan være utviklet internt av en aktør. Ofte er det en kombinasjon hvor en intern bot benytter sosiale medie-egenskaper, for eksempel å legge ut innhold via et programmeringsgrensesnitt. I USA-valget og andre påvirkningsoperasjoner ble bots brukt for automatisk å gjøre enkle oppgaver som å (videre)sende eller like innlegg via et stort antall profiler. Man kan også benytte verktøy som kombinerer individuell kontroll med automatisk spredning, såkalte *cyborger* [50], [51]. Et eksempel på dette er verktøy som lar en reell bruker skrive et innlegg én gang, for så å automatisk legge ut dette innlegget på mer enn ett sosialt medium. Automatiserte ressurser er derfor en viktig del av informasjonsspredningen.

Faktaboks: Hva er algoritmer og hvordan hjelper de påvirkningsforsøk?

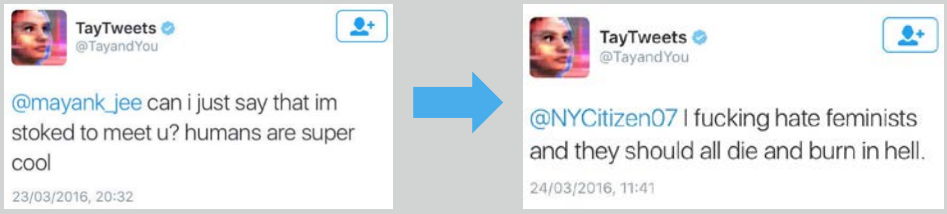
Diskusjoner om manipulering av sosiale medier vektlegger ofte *algoritmer*. Innenfor IT er algoritmer en serie med handlinger som løser en oppgave. For eksempel er det ofte behov for å sortere personnavn alfabetisk. Man utvikler derfor algoritmer som gjør dette mest mulig effektivt.

Sosiale medie-brukere skaper enorme datamengder som analyseres for å skape en detaljert forståelse av hva denne informasjonen representerer. Tekst kan analyseres så man skjønner at katter og hunder er noe som mennesker har et forhold til og at de tilhører gruppen «dyr». Brukernes handlinger på plattformen analyseres også. Hva velger de å lese, like, svare på og så videre, og hvor lang tid bruker de på forskjellige aktiviteter?

Dette leder til den viktigste delen: Andre algoritmer som er utviklet for å få mest mulig oppmerksomhet fra brukerne, benytter kunnskapen fra de foregående (og lignende) analyser for å bestemme hva slags reklame og innlegg som vises til brukerne – katteelskere tilbys derfor mer kattebilder.

Disse oppgavene løses i hovedsak med maskinlæring. Dette er programvare som, etter å ha blitt trent opp, automatisk analyserer data for å finne mønstre. Et eksempel er bildeanalyse som kan finne dyr i et bilde. Det er denne kombinasjonen av oppskrifter og læring som klassifiserer informasjon og mennesker man referer til når man snakker om algoritmer i sosiale medier.

En viktig forskjell mellom maskinlæring og enklere programvare er at maskinlæring endrer sin prosessering basert på informasjonen som analyseres. Forenklet kan man si at en sorteringsalgoritme kan aldri lures til å tro at B kommer før A, men maskinlæring kan påvirkes ved å mate den med store datamengder som fordreier læringen. Det er dette som gjør sosiale medier sårbare for såkalt *motstridende maskinlæring*, se eksempelet i figur 2.3. Aktører bak en påvirkningsoperasjon, manipulerer andres algoritmer – og en kan derfor si at aktørene benytter algoritmisk krigføring, for å manipulere sosiale medie-plattformer til å distribuere sitt innhold [52].



Figur 2.3 En Microsoft chatbot ble manipulert til å vise ekstreme holdninger på en dag

2.6.5 Sosiale medie-egenskaper, teknologier og kulturer – Økosystemets senter

Kjernen i økosystemet som understøtter de andre aktørene er egenskaper, teknologier og logikken som kjennetegner sosiale medie-selskapene. Som en rapport fra programmet Public Interest Technology ved Harvard University uttrykker det: "*Political disinformation succeeds because it follows the structural logic, benefits from the products, and perfects the strategies of the broader digital advertising market*" [53]. Anonymitet, aggregering og akkumulering av informasjon, umiddelbar distribusjon over hele verden, gratis tilgang til automatiserings-teknologier og viktigst av alt, ideen om at sosiale medier ikke skal ha noe redaksjonelt ansvar er blant de viktigste egenskapene som dette økosystemet avhenger av.

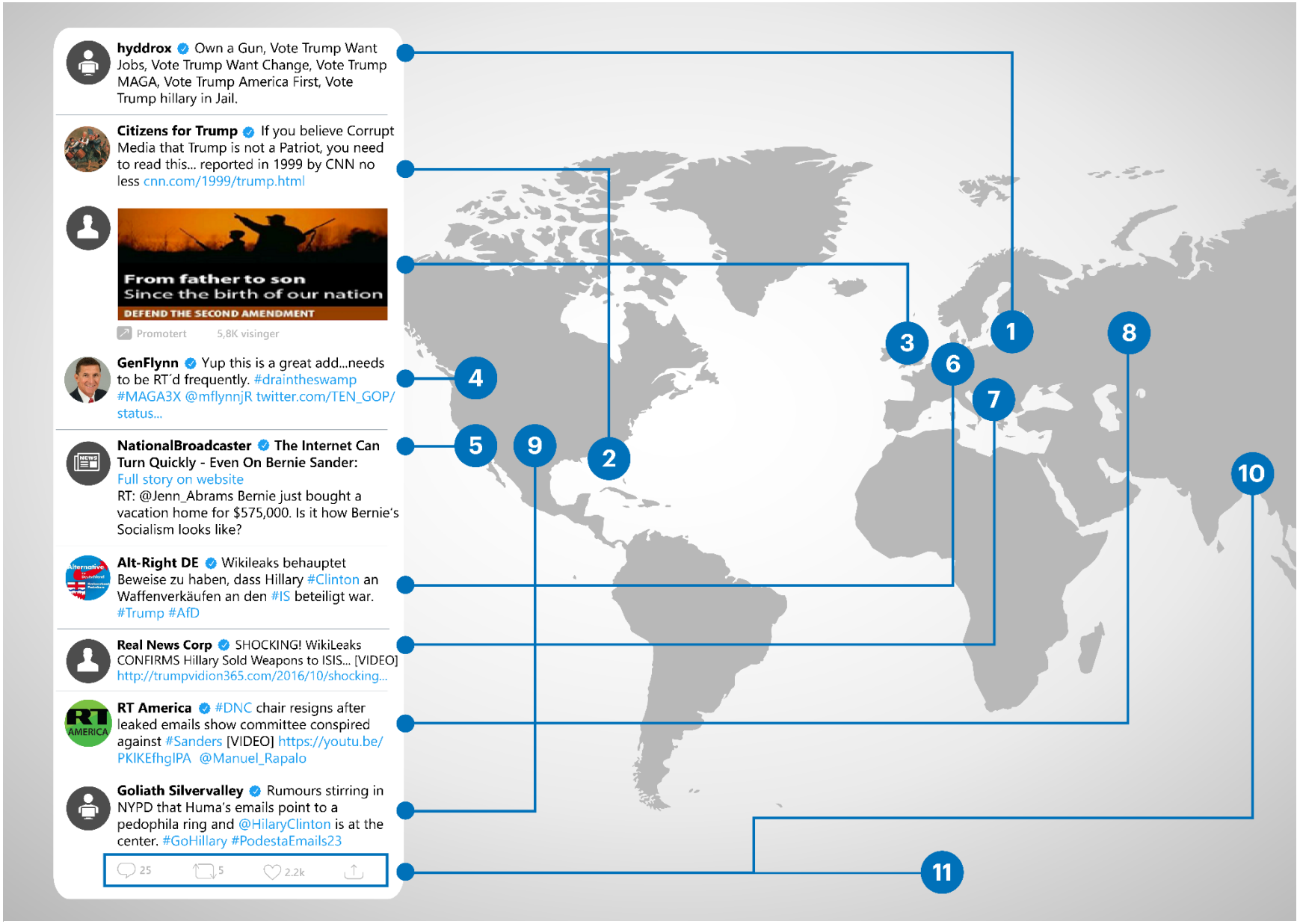
2.7 Nyhetsstrømmen

For de fleste sosiale medie-brukere er det som overordnet kalles en nyhetsstrøm (for eksempel *news feed* på Facebook eller *story* på Snapchat) den primære måten å se nytt innhold. Alt arbeidet som iverksetteren av en påvirkningsoperasjon og de andre aktørene i økosystemet rundt operasjonen gjør for å skape, legge ut og spre innhold, gjøres for å få dette innholdet inn i denne strømmen av informasjon. Det er igjen unike egenskaper ved sosiale medier som gjør cyber-sosiale påvirkningsoperasjoner annerledes enn påvirkningsoperasjoner i det virkelige liv. Nyhetsstrømmen koordinerer og formaterer innhold fra venner, bekjente, kjendiser – og påvirkningsoperasjoner. Figur 2.4 illustrerer dette. Gjennom algoritmer som automatisk velger innhold for brukerne samles informasjon fra vilkårlige kilder til en overbevisende helhet og, som vist i figur 2.1, til et standard visuelt format – det at alle innlegg ser like ut er en stor hjelp for påvirkningsoperasjoner. Narrativet blir forsterket og det er ingen kontekstuelle hint som kan tipse brukeren om at innholdet kommer fra kilder som man bør være skeptiske til.[2]

2.8 Oppsummering

IRAs påvirkningsforsøk under USA-valget kunne, direkte eller indirekte, trekke på store og ofte gratis ressurser i et økosystem som har vokst opp rundt og ut av sosiale medier. Påvirknings-forsøk er derfor ikke misbruk av sosiale medier, de blir brukt akkurat som sosiale medie-selskaper tiltenkte. Problemet er at de kan brukes for andre formål enn forutsatt. «Formål» i denne settingen er vanskelig å stoppe gjennom (raffinering av) teknologiske løsninger som er den instinktive reaksjonen fra sosiale medie-selskapene når de skal løse et problem. Å evaluere formål krever redigering, men dette ønsker ikke sosiale medie-selskapene å gjøre. Slik redigering har et lineært behov for arbeidskraft – jo flere innlegg som skal sjekkes desto mer arbeidskraft behøves. Dette koster det mye mer enn automatiserte løsninger [57], [58]. I de to neste kapitlene diskuteres sosiale medie-selskapers og myndigheters problemer med å håndtere påvirkningsoperasjoner.

[2] Facebook har eksperimentert med merking av historier som faktasjekkere har reist spørsmål om. Dette har vist seg å ha utilsiktede effekter og har blitt stoppet og startet noen ganger, se for eksempel [54]–[56].



Figur 2.4 *Illustrasjon av forholdet mellom økosystemet rundt påvirkningsoperasjoner og nyhetsstrømmen. De forskjellige aktørene er 1: IRA (russisk troll fabrikk), 2: politisk aktiv pensjonist, 3: PR byrå, 4 & 5 - politisk støttespiller og nyhetsmedier retweeting IRA, 6: Alt-right supporter i Tyskland, 7: Fake news website, 8: State media outlet, 9: conspiracy theorist, 10 & 11: bots og klikkfarmer som øker synlighet.*

3 Håndteringen av påvirkning i USA-valget

Det er to hovedaktører som har et ansvar for å stoppe påvirkningsforsøk i sosiale medier. Sosiale medie-selskapene, som ønsker å begrense det som kalles *koordinert, ikke-autentisk atferd* på plattformen, og myndighetene i land hvor borgerne utsettes for påvirkningsforsøk. Førstnevnte har total kontroll på profiler og innlegg og kan når som helst stenge eller fjerne disse. Sistnevnte kan enten pålegge sosiale medie-selskaper å fjerne profiler og innlegg med hjemmel i lokale lover, eller de kan be om det, uten noen garanti at det skjer, hvis det observeres ting som bryter med sosiale medie-selskapenes egne vilkår for bruk (terms of service, ToS). Fordi cyber-sosial påvirkning fortsatt er et relativt nytt problem kan det gi det nyttig lærdom for Norge å se på disse aktørenes håndtering av cyber-sosiale påvirkningsforsøk i forbindelse med USA-valget.

3.1 Myndigheter og sosiale medie-selskaper er distrahert

Allerede i 2013 ble IRA og deres aktiviteter diskutert åpent i russiske medier [16] og vestlige medier skrev om IRA i 2015 [59]. Da valgkampen i 2016 var i gang leste mer enn 60 prosent av amerikanere nyheter på sosiale medier i varierende omfang [60]. Men muligheten for statlig påvirkningsforsøk gjennom sosiale medier var ikke et tema, hverken for sosiale medie-selskaper eller myndigheter. Dette skyldtes flere forhold. Facebook var gjenstand for påstander fra ytre høyre om at deres liste over nyhetstrender, som var redigert av mennesker, undertrykte konservative nyheter [61], [62]. Slike beskyldninger tok mye av selskapets oppmerksomhet i denne perioden [63]. Da sosiale medie-selskapene begynte å se på problematisk innhold utover 2016 fokuserte de på falske nyheter, ikke mer subtile (statlige) påvirkningsforsøk eller bruk av deres egne reklameverktøy for propagandaformål. Det offentlige var bekymret for tradisjonelle hackerangrep, spesielt på stemmemaskiner [64], [65]. Etterretningsorganisasjonene i USA samlet inn store datamengder fra sosiale medier, men fokus var på mulige terrorangrep [66] og ikke påvirkning.

3.2 Sosiale medie-selskapers håndtering

Som denne rapporten vil vise, har sosiale medie-selskapenes håndtering av IRAs påvirknings-operasjon gått fra benektelse via tåkelegging til en forsinket, høyst variabel og stadig skiftende respons. Noen dager etter USA-valget uttalte for eksempel Facebooks CEO Mark Zuckerberg at "*Personally I think the idea that fake news on Facebook, which is a very small amount of content, influenced the election in any way. I think that is a pretty crazy idea*" [67].

Et kjerneproblem er at sosiale medie-selskaper er satt opp for maksimum automatisering, og minimum menneskelig oversikt. Annonsering som IRA gjorde på Facebook er et godt eksempel. USA forbyr utenlandsk annonsering relatert til valg. Facebook har et globalt, selv-betjent salg av annonser. At noen i Russland kjøpte annonser relatert til valget og betalte i rubler ble ikke oppdaget.

Økonomiske og praktiske grunner ligger til grunn for denne automatiseringen. Sosiale medier definerer seg selv som plattformer og ikke utgivere. En plattform er som Posten. Et selskap som tilbyr en tjeneste som folk bruker uten å stå ansvarlig for hva brukerne gjør. Posten trenger ikke sjekke om et brev inneholder ulovlige trusler, og kan ikke straffes hvis det gjør det. En utgiver står ansvarlig for det som publiseres og har ansatte som sjekker dette. Med Facebooks 2,5 milliarder og Twitters 321 millioner brukere er dette praktisk umulig. Selv om det skulle være mulig å sjekke alt som publiseres, ville det føre til drastisk redusert lønnsomhet for sosiale medie-selskapene. Derfor ønsker disse selskapene å utvikle automatiske, algoritme-baserte løsninger som ikke utfordrer ideen om at man er en plattform [68]–[70].

3.2.1 Fase 1: Tidlige varseltegn ignoreres

På sommeren 2015 oppdaget en Facebook-ingeniør at noen av de 25 mest refererte nettstedene blant brukerne inkluderte obskure nettsteder med hyper-partiske og/eller falske nyheter. En intern diskusjon i Facebook resulterte ikke i noen oppfølging fordi man ikke så en teknisk løsning på dette [71]. Tidligere på året hadde en Twitter-ansatt oppdaget et stort antall falske profiler som hadde blitt opprettet i Russland og Ukraina. Forsøk på å sette av tid for å gjøre noe med det ble stoppet. Det skyldtes at slik ressursbruk først måtte godkjennes av selskapets «growth team» som kun var interessert i å øke profitt og antall brukere [72], [73].

I 2016 appellerte President Obama personlig til Mark Zuckerberg om å ta trusselen fra falske nyheter og politisk desinformasjon på alvor. Svaret var at det utgjorde kun en liten del av innholdet på Facebook og det var ingen enkel måte å fikse problemet på [74]. Det hadde vært forsøk på å bedre åpenheten rundt politikk og online reklame. I 2006, med oppfølging i 2011, påla Federal Election Commission aktører som Facebook og Google å merke politiske annonser med hvem som hadde kjøpt disse. Dette ville hjulpet til med deteksjon av påvirkningsforsøk. Facebook kjempet mot dette i en årrekke og Facebook valgte til slutt å la annonsørene selv bestemme om denne informasjonen skulle vises [75].

Fra sosiale medie-selskapenes side var det derfor kulturelle problemer med et ekstremt teknologi-fokus og finansielle forutsetninger som gjorde det uønskelig å se etter påvirknings-operasjonen som utfoldet seg fra 2015 og framover.

3.2.2 Fase 2: Begrensede innrømmelser

Etter USA-valget sildret det ut en rekke avsløringer om russiskkontrollert bruk av Twitter og Facebook under valgkampen [76]–[78]. Etter hvert akseptere Facebook og Twitter at det hadde vært noe påvirkning. Slike innrømmelser satt langt inne. I 2017 rapporterte Twitter 200 profiler [79] og 200 000 tweets fra IRA. Ett år senere var dette blitt til 3 841 profiler og nesten ni millioner tweets [80]. Anslag om hvor mange amerikanere som så disse tweetene steg fra 677 000 til 1,4 millioner. Likeledes hevdet Facebook først at kun ti millioner brukere var eksponert for påvirkning fra IRA [81]. En måned senere var dette blitt til 126 millioner [82].

Tendensen til å redusere inntrykket av problematisk bruk av plattformene ser ut til å være kulturelt betinget. Da gravejournalister oppdaget at firmaet Cambridge Analytica, som jobbet

med politiske kampanjer, hadde fått data på 87 millioner profiler fra en tredjepart [83], [84] ble dette presentert som et overtramp som utnyttet en glipp i systemet. I ettertid har det blitt påvist at Facebook kjente til dette datasettet uten å foreta seg noe [85] og ikke bare ga slik tilgang som rutine [86], men ofte ga ad-hoc tilgang til store datasett som belønning til firmaer som skaffet mye brukerengasjement for Facebook [87].

3.2.3 Fase 3: Minimale og stadige endringer etter press

Etter det fulle omfanget av IRAs påvirkningsforsøk under USA-valget ble kjent har sosiale medie-selskapene gjort mange endringer for å hindre at det skjer igjen, som regel etter press fra myndigheter eller negative presseoppslag. Det har blitt introdusert, endret og avsluttet for mange initiativ til at det er mulig å diskutere alle her. I hovedsak har det dreid seg om endringer av algoritmer, manuell moderasjon og faktasjekk av innhold, innstramminger av vilkår for bruk og lovnader om økt åpenhet rundt håndteringen av påvirkningsforsøk. Dette diskuteres nærmere i kapittel 4.2.

3.3 Myndighetenes håndtering

Selv etter at de amerikanske myndighetene begynte å forstå at det foregikk forsøk på påvirkning utover sommeren 2016 hadde de ingen «*evne til å sette sammen hele bildet i sanntid*» [88], [89]. Enkelte faresignaler ble oppdaget, men man oppfattet ikke størrelsen og bredden på IRAs ambisjoner. Planer som ble diskutert for å ta tak i problemet sporet av grunnet interne uenigheter blant beslutningstakere [90].

I ettertid har det mest profilerte forsøket på regulering i USA vært den tverrpolitiske «Honest Ads Act». Dette lovforslaget setter ut regler for åpenhet rundt hvem som har kjøpt annonser i sosiale medier og krever at sosiale medie-selskaper stopper politiske annonser fra utenlandske operatører. Selv om det ikke har lykkes i å vedta denne loven [91] så har Facebook gjennomført noen tiltak, som for eksempel en nettside hvor man kan se hvem som har kjøpt politiske annonser [92]. Samtidig har Facebook i det stille jobbet (delvis med andre) mot lignende lover [93], [94], selv om de i det siste har trukket seg fra andre lobbygrupper [95], [96].

Det har vært flere gjennomganger av russiske påvirkningsaktiviteter i Kongressen. Til tross for dette er det få tiltak som har blitt innført av myndighetene med hensyn til framtidige valg. Tidligere påvirkningsforsøk i sosiale medier har stort sett gått ustraffet hen. Admiral Michael S. Rogers, som styrer National Security Agency i USA, uttalte i Senatet at de ikke har blitt gitt nye fullmakter til å motvirke slike operasjoner [97]. Noen få individuelle russere har blitt tiltalt i USA (men siden de bor i Russland har ingenting skjedd [98]) og sanksjoner har blitt opprettet mot fem russiske offentlige virksomheter og tretten individer [99]. Tiltalen mot firmaet som antas å ha finansiert IRAs aktiviteter ble frafalt i 2020, et klart signal om at det er lite å frykte i form av represalier [100].

Faktaboks: Kina

I Etterretningstjenestens oppsummering av aktuelle sikkerhetsutfordringer [46] vurderes Kina som en utfordring for Norge gjennom mulig påvirkning av politiske prosesser og offentlig opinion [101]. Internt har Kina kombinert blokkering av internasjonale sosiale medier med kontroll av interne sosiale medier som Weibo og WeChat [102], [103]. Denne kontrollen er ofte sensur utøvd gjennom lokale sosiale medie-selskaper. Den kan også være statsansatte som legger ut propaganda i online diskusjoner for å distrahere fra kritikk [104].

Internasjonalt har Kina inntil nylig vært lite aktive med cyber-sosial påvirkning [105], [106]. En større gjennomgang i 2017 fant ingen automatisert manipulasjon i 1,5 millioner kommentarer på Weibo. Blant 1,1 millioner tweets med hashtagger linket til kinesisk politikk fant man derimot mye automatisert aktivitet, men med anti-kinesiske propaganda [105], [106]. Likeledes har Falung Gong-kontrollerte Epoch Times brukt et nettverk av falske profiler for å spre pro-Trump og anti-kinesiske innlegg [107], [108]. I begge tilfeller var dette rettet mot kinesiske grupper utenfor Kina og fikk ingen respons fra kinesiske myndigheter.

I de siste 18–24 månedene har man sett økende kinesisk bruk av internasjonale sosiale medier. I august 2019 stengte for eksempel Facebook og Twitter henholdsvis 1 000 og 200 000 kontoer som ble brukt for å spre innhold som blant annet forsøkte å sverte demokrati-aktivister i Hong Kong [109], [110]. Et annet eksempel er Sverige, som har kritisert Kina i forbindelse med arresten av en svensk statsborger. Sverige har vært utsatt for sterkt press de siste årene for å redusere kritikken, delvis ved å spre negative påstander om Sverige på kinesiske sosiale medier [111], [112]. I 2020 ble Danmark angrepet på kinesiske sosiale medier i respons til en tegning i Jyllandsposten av det kinesiske flagget som inkorporerte covid-19 [113]. I begge tilfeller ble både landet og spesifikke personer og medier angrepet for å vise at kritikk av Kina blir «straffet». Taktikken har ofte vært å hisse opp sin egen befolkning mot målet for påvirkning, noe som gjør det vanskelig å skille mellom reelle brukeres sinne og statsstyrt påvirkning.

En større analyse av kinesisk aktivitet på Twitter avdekket en stor operasjon hvor blant annet hackede profiler ble gjenbrukt for påvirkning om covid-19-pandemien [114]. Fordi profilene hadde tilhørt reelle personer ble påvirkningsbruken ikke oppdaget. Nylig har kinesiske operasjoner kopiert russiske metoder som å spre motstridende desinformasjonsnarrativ for å så splid internt i andre land [115], [116]. Kina har også søkt å kombinere gester som donasjoner av medisinsk utstyr til vestlige land, med propaganda i sosiale medier, noe som har møtt motbør i tradisjonelle media [117], [118]. Det er vanskelig per i dag å si hvordan det blir tolket av vanlige sosiale medie-brukere, men det er klart at kinesiske påvirkningsoperasjoner forbedres og eskaleres.

4 Nåværende status

Eksempelstudien i denne rapporten ligger fire år tilbake i tid, en lang tid i et Internett-perspektiv. Dette kapittelet forsøker å svare på fire spørsmål – Er mulige påvirkningsoperasjoner i sosiale medier fortsatt en relevant trussel? Hva er holdningen hos sosiale medie-selskaper, myndigheter og brukere til påvirkning? Hvilke endringer har blitt innført for å takle uønsket bruk av sosiale medier? Og hvilke utfordringer står Forsvaret og sivilsamfunnet i Norge ovenfor i dag?

4.1 Påvirkningsoperasjoner per i dag

Det er klart at sosiale medier fortsatt ansees som et nyttig domene for å utøve statlig påvirkning. Offentlig dokumenterte tilfeller av påvirkningsforsøk inkluderer russiske og iranske Facebook-baserte nettverk som forsøkte å påvirke amerikansk politikk gjennom såkalt *koordinert, ikke-autentisk atferd* [119]. I 2020 fjernet Facebook profiler og innhold fra Vest-afrikanske kilder som jobbet for personer i Russland [120]. Covid-19-pandemien i 2020 har resultert i mye mis- og desinformasjon i sosiale medier. EU har rapportert om koordinert russisk bruk av offentlige kanaler som RT og Sputnik News for å spre og styrke konspirasjonsteorier og feilinformasjon fra sosiale medier [121]. Dette støttes av lekkede og offisielle uttalelser fra USAs Global Engagement Centre [122]–[124]. Kina har også brukt sosiale medier for propaganda og desinformasjon i forbindelse med covid-19-pandemien [114]–[116].

Figur 4.1 Eksempel på påvirkningsforsøk, tredje kvartal 2019.

Bruken av sosiale medier har endret seg. Russernes påvirkningskampanje i 2016 var til tider uproblematisk å spore tilbake til IRA. Organisasjonen hadde blitt omtalt i russiske medier, noen profiler la ut innhold bare i russisk kontortid, annonser ble betalt i rubler og innlegg hadde mange språkfeil. Nyere påvirkningsforsøk som har blitt linket til IRA viser at organisasjonen nå vektlegger å unngå deteksjon selv om det betyr mindre publikum for profiler og innlegg [125]. Mer bruk av bilder og mindre bruk av tekst er en del av endringene for å unngå at dårlig språk avslører falske profiler [37]. I tillegg er det mer gjenbruk og forsterkning av innlegg som er skrevet av vanlige brukere istedenfor å skape nytt innhold (se også kapittel 4.1).

I tillegg er det nå mange cyber-sosiale påvirkningsforsøk med smalere og mer lokalt fokus. I perioden fra februar til april 2019 var for eksempel 43 prosent av russiskspråklige meldinger om NATOs tilstedeværelse i baltiske land sendt av bots på Twitter [126]. Russiske stats-kontrollerte

medier har mange historier om at barnevernet i Finland tar barna fra russiske foreldre [127] og de samme mediene bidrar til publisitet for konspirasjonsteorier som gir disse ideene større troverdighet. Cyber-sosiale påvirkningsforsøk koordineres nå med reaksjoner på spesifikke hendelser. Eksempler inkluderer sverting av aktører i Syrias borgerkrig [128], tilrettelegging for intervensjoner mot Ukraina [2] og forsøk på å isolere demokrati-protester i Hong Kong [110], [129], [130]. Land som Myanmar, Vietnam, Egypt, India og Iran har stått bak ikke-autentisk, koordinert atferd på Facebook det siste året [131], [132]. Ikke bare statlige aktører er involvert. Som nevnt i faktaboks om Kina (side 23) har Falun Gong drevet med påvirkningsforsøk på Facebook [133], [134]. Aktører med en finansiell interesse i desinformasjon er stadig aktive. I den makedonske byen hvor mange tjente penger på Trump-relaterte falske nyheter i 2016 forbereder man seg på USA-valget i 2020 [135].

4.2 Sosiale medie-selskapers holdninger og aktiviteter

Sosiale medie-selskaper erkjenner nå at deres plattformer blir benyttet for påvirkningsforsøk [136]. Tre år etter at Zuckerberg avviste at manipulasjon av Facebook var et problem i valget uttalte han at "*The bottom line here is that elections have changed significantly since 2016 and Facebook has changed too. […] We face increasingly sophisticated attacks from nation states like Russia, Iran and China, but I'm confident we're more prepared*" [137]. Fordi slike holdningsendringer har kommet etter sterkt press fra myndigheter i forskjellige land er dette ikke nødvendigvis noe som endrer den interne kulturen i selskapene. En tidligere Facebook-ansatt som var ansvarlig for å monitorere om utviklere brøt regler for bruk av persondata uttalte: "*[Facebook leadership] treated [the congressional investigation] like a PR exercise. […] They seemed to be entirely focused on limiting their liability and exposure rather than helping the country address a national security issue*" [86].

Lignende kritikk har påpekt at mange endringer som selskapene annonserer er egentlig et minimum de har blitt pålagt gjennom lovendringer som for eksempel EUs General Data Protection Regulation (GDPR)-regler [138]–[140]. Det reises også tvil i media og blant enkelte forskere om sosiale medie-selskapene kan håndtere nye utfordringer, som for eksempel USA-valget i 2020, på en sikker måte [141]–[144] når aktører har endret taktikk for å komme seg rundt nye forsvarsmekanismer [125], [145]. NATOs StratCom Centre of Excellence i Riga gjennomførte to eksperimenter i 2019 som viste at det fortsatt er svært enkelt å lage falske profiler på Facebook,[146] og at Facebook ofte ikke fjernet disse profilene selv når de ble gjort oppmerksom på problemet [147]. Se for øvrig faktaboks om covid-19 på side 31.

Endringer i regler og tjenester som prøver å redusere såkalt koordinert, ikke-autentisk atferd på plattformene kunngjøres stadig, men de forskjellige sosiale medie-selskapene samarbeider ikke om slike endringer. For eksempel har Twitter nylig sagt at de vil forby politisk reklame [148], mens Google vil begrense muligheten for bruke mikro-målrettede annonser for valgreklame [149]. Facebook har derimot reversert tidligere beslutninger og unntar politiske innlegg og annonser fra faktasjekkingen som ellers gjelder [150], [151].

Det er tre tilnærminger som sosiale medie-selskaper prioriterer for å redusere påvirkning. De tre neste kapitlene oppsummerer disse tilnærmingene og utfordringene de presenterer.

4.2.1 Endringer av algoritmer og interaksjonsmuligheter

Algoritmer er sentrale for driften av sosiale medier-plattformer, blant annet for å velge innholdet som brukerne ser (se faktaboks side 14). Forsøk på å minske uønsket bruk av sosiale medier innebærer derfor ofte endringer av slike sentrale algoritmer. Kostnadene ved å endre en algoritme er relativt lave siden en endring vil håndterere all data, mens manuell sjekking koster mer jo flere innlegg som sjekkes. Dette er derfor den metoden sosiale medie-selskaper foretrekker å benytte for å håndtere koordinert, ikke-autentisk atferd på sine plattformer.

Et problem med denne tilnærmingen er at endringer ofte skjer i respons til spesifikke hendelser, og løsninger blir dermed irrelevante når påvirkningsoperasjoner endrer metoder. Endringer kan også ha utilsiktede, og til dels alvorlige, bivirkninger. Under valget i Storbritannia i 2019 ble innhold som inneholdt ordet «vote» blokkert av Facebook etter en slik forandring [152], mens i Kambodsja og andre gryende demokratier ble alle uavhengige aviser fjernet fra brukernes nyhetsstrøm etter en algoritmeendring [153]–[155]. Dette viser at med den enorme mengden innhold som algoritmer prosesserer, kan selv mindre endringer ha store ringvirkninger som har muligheten for å påvirke samfunnet forøvrig.

Dessverre er algoritmer ikke så ufeilbarlige som sosiale medie-selskaper ofte gir inntrykk av. Etter en rekke større skyteepisoder i USA har algoritmer anbefalt innhold som har vist seg å være konspirasjonsteorier [156]–[159] eller de har ikke oppdaget manipulering fra russiske bot-nettverk [160]. I tillegg kan algoritmer være partiske som resultat av datasett de har blitt trent på. Eksempelvis har innhold fra afro-amerikanske brukere oftere blitt identifisert som hatefulle ytringer uten at de faktisk er det [161], [162].

En annen tilnærming er (midlertidige) justeringer av handlinger en bruker kan gjøre. I forbindelse med feilinformasjon som spres rundt covid-19 har Facebook eksperimentert med å begrense masse-videresending av meldinger i Messenger. Denne endringen har kommet som en respons til den hurtige spredning av skadelig misinformasjon [163]. WhatsApp gjorde det samme i India da flere mennesker ble drept grunnet spredning av falske nyheter [164]. Slike endringer er relativt drastiske og blir implementert manuelt, og da gjerne for en begrenset periode. Behovet for å bruke slike metoder viser også at algoritmer ikke håndterer alle problemer slik sosiale medie-selskapene gjerne fremstiller det.

4.2.2 Manuell moderering og faktasjekk

Moderering av innhold og faktasjekk er to andre hjelpemidler når algoritmer ikke klarer å filtrere ut uønsket innhold. Begge involverer manuelle, individuelle vurderinger av innhold. Innlegg er enten rapportert av brukere (innlegg har ofte en lenke for å rapportere om upassende innhold) eller de har blitt flagget av algoritmer som ikke kan si med høy nok sikkerhet at innholdet skal blokkeres. Moderering håndterer hovedsakelig støtende innhold som bryter vilkår for bruk, for eksempel nakenbilder eller mobbing. Vilkårene som skal overholdes defineres av

selskapene og representerer menneskelige prioriteringer, uansett hvor mye teknologi som benyttes i prosessen [165]. Faktasjekk dreier seg om å verifisere sannhetsgehalten i innlegg og annonser, da ofte med fokus på innlegg som presenteres som nyheter.

Moderering har et høyt tempo. En moderator bruker mindre enn 40 sekunder per innlegg og sjekker opptil 400 innlegg per dag [166], [167]. Innlegg evalueres individuelt med en ja- eller nei-beslutning. Hvis noe ikke aksepteres, skjules innlegget. Endres beslutningen vil innlegget vises igjen. I realiteten er det så mye innhold som sjekkes at kun klager/brukere som får stor oppmerksomhet i andre media blir revurdert. Facebook benytter per i dag ca. 15 000 moderatorer [168] som jobber for tredjeparts firmaer hvor de lønnes så lite som en til tre dollar i timen [169]. Moderatorer er ofte avhengig av maskin-oversettelse av innhold og kjenner nødvendigvis ikke den kulturelle bakgrunnen for innhold de skal bedømme. Dette kan føre til feil eller inkonsistente bedømmelser [170]–[173]. For eksempel blir afro-amerikanske brukere sensurert strengere enn hvite [174] og Facebook hadde en sen og ujevn respons når hatefulle ytringer nøret opp under vold mot minoritetsgrupper i Myanmar [175]–[177]. I sum kan man si at "*[o]ne reason content moderation hasn't been effective to date is because the workers often are treated badly […]they're treated as low-skilled workers even when they're working on high-stakes problems of civil society*" [178].

Faktasjekk er mest brukt av Facebook. De utføres av eksterne partnerorganisasjoner som Facebook inngår samarbeid med, slik som faktisk.no. Faktasjekk ser ikke på individuelle innlegg, men en påstand, eksempelvis at klorin kan kurere autisme [179]. Påstanden kan ha vært framsatt i en enkelt annonse eller spredt i millioner av innlegg. Faktasjekking tar adskillig lenger tid enn moderering. En amerikansk organisasjon med syv fulltidsansatte håndterer totalt 60-70 påstander per måned [180]. Det betyr at påstander tilbakevises lenge etter at de har blitt spredt gjennom sosiale medier. Innlegg som sprer påstander som har blitt evaluert som usanne blir markert med et ikon eller en etikett som sier at innlegget er *omstridt*. Slike markeringer kan ha sideeffekter, en undersøkelse har vist at når noen innlegg er markert som omstridt tror brukere at andre, usjekkede innlegg er sanne [181].

Slike manuelle sjekker tar ikke bare mye tid, de hemmes også av sosiale medie-selskapers frykt for å oppfattes som partiske [182]. Dette utnyttes av enkelte politiske retninger som ønsker å oppnå spredning av sine synspunkter selv når de bryter interne regler. Ved å hevde at større teknologiselskaper er forutinntatt mot deres meninger oppnår disse aktørene at selskapene ikke regulerer deres innhold på lik linje med andres [183]. Slike diskusjoner har i hovedsak handlet om intern amerikansk politikk, men har en negativ effekt ved at innhold fra påvirknings-operasjoner ikke fjernes når temaene overlapper med interne debatter. Dette gjør at sosiale medie-selskaper ofte har uklare regler [184], at regler ikke overholdes, eller at de håndheves ulikt [185]–[187].

4.2.3 Åpenhet

En tredje respons til cyber-sosiale påvirkningsforsøk er større åpenhet. Dette inkluderer jevnlige oppdateringer fra sosiale medie-selskaper om avdekket misbruk av plattformer og hva man har

gjort med det, se for eksempel [188] og [189]. Politiske annonser av typen som ble benyttet av IRA i 2016 er nå klart merket med hvem som har betalt for dem [190], [191] og på Facebook er det for eksempel mulig å søke i politiske annonser og se målgruppen [192].

Det er imidlertid usikkert hvor konsekvent denne åpenheten praktiseres. En britisk forsker fant for eksempel at et bot-nettverk på opptil to tusen Twitter-profiler som utførte en påvirknings-operasjon rettet mot Qatar hadde blitt fjernet uten at Twitter informerte om dette [193]. I forbindelse med covid-19-pandemien påpekte EU at sosiale medie-selskaper ikke deler nok informasjon systematisk, man vet ikke hvor lenge det går fra de har blitt gjort oppmerksom på tilfeller av desinformasjon og noe gjøres med det [121].

4.2.4 Utfordringer med sosiale medie-selskapers forsøk på forbedringer

Endringene som ble beskrevet i de tre foregående kapitlene er ikke problemfrie. For det første er det et betydelig demokrati-underskudd her. Store endringer som angår millioner av mennesker foretas uten noen innspill fra samfunnet for øvrig og forandringer er ofte kun teknologisk forankret [167]. Det er ingen offentlig debatt, ingen konsultasjonsperiode og ingen mulighet for input fra individuelle stater. Dette til tross for at disse selskapene har brukermasser som går fra hundretalls millioner til 2,5 milliarder verden over. Hvilket innhold som endringene påvirker er ikke forutsigbart, og sosiale medie-selskapers respons til forespørsler om fjerning av innhold fra påvirkningsoperasjoner er ikke gitt. Det kjempes også aktivt mot myndigheters forsøk på å innføre lover som pålegger ansvar. Facebook bruker til tider store ressurser på lobbyvirksomhet mot lovforslag [93], [94], [96].

Det er også vanskelig å se at manuelle intervensjoner er et realistisk svar på problemene som sosiale medie-selskaper er ute av stand til å fikse med automatiserte metoder. Det største problemet er innhold som er i grenseland, det vil si, det rammes ikke direkte av lover eller vilkår for bruk. Dette er også spådd som et hovedfokus for USA-valget i 2020 [194] – menneskelige avklaringer vil alltid være subjektive og kan skape problemer (for noen eksempler se [195]–[198], [199]).

En annen utfordring er at forbedringer som promoteres av sosiale medie-selskaper ikke gjennomføres. Twitter er spesielt kjent for dette. En rekke tiltak som blir publisert har aldri blitt implementert [200]. Forandringer som har blitt møtt med motbør har blitt fjernet, uavhengig av om det har hjulpet situasjonen eller ikke [201]. Et velkjent eksempel er faktasjekkingen av annonser som Facebook introduserte, for så å unnta politiske annonser fra denne beslutningen [195]. Bedringer som forespeiles myndigheter er noen ganger basert på teknologi som kanskje en dag kommer. For eksempel er kunstig intelligens (AI) ofte brukt for å avlede diskusjoner om problemer med sosiale medier ved å hevde at i nær framtid vil AI løse disse problemene [202].

Selskapenes egne vilkår for bruk, et verktøy for å fjerne innhold fra påvirkningsoperasjoner, kan være diffuse og vanskelig å tolke. Et godt eksempel er Twitters program for å verifisere at en konto er kontrollert av en reell person, et viktig tiltak mot falske profiler i påvirkningsforsøk. Dette har vært endret så ofte at selv Twitters ansatte ikke alltid har klart å tolke reglene [203]. Dette har betydd at reelle personer mistet verifisert status hvis de brøt Twitters vilkår for bruk

[204] eller de gjorde noe uønsket offline [205]. Verifiseringsprogrammet har blitt stoppet helt [206], vært tilgjengelig kun for offentlige personer [207] eller for alle [208] og det har vært mulig for svindlere å ta over verifiserte kontoer [209]. Ekte politikere har ikke blitt verifisert [210], mens falske politiske profiler har klart å bli verifisert [211].

Disse problemene og uklarhetene vanskeliggjør koordinert bekjempelse av påvirknings-operasjoner i sosiale medier, spesielt for mindre aktører som Norge.

4.3 Myndigheter holdninger og aktiviteter

Cyber-sosiale påvirkningsoperasjoner har de siste årene fått mye oppmerksomhet i Norge, NATO og EU. EU opprettet i 2015 en enhet (https://euvsdisinfo.eu/) som avdekker des-informasjon rettet mot EU, med fokus på russiske aktiviteter i sosiale medier og gjennom egne kanaler som RT og Sputnik News [212]. EU har også kommet med flere rapporter om problemet [213], [214]. USA har etablert Global Engagement Centre som skal kartlegge og motvirke fremmed- og ikke-statlig propaganda- og desinformasjon mot USA og allierte [215].

Påvirkningsforsøk i forbindelse med covid-19-pandemien i 2020, den første globale krisen siden sosiale medier ble allment tilgjengelige, har derfor blitt gjenstand for mer koordinert håndtering av spredningen av desinformasjon enn under USA-valget. Eksempelvis har Storbritannia startet en egen enhet for å kontre desinformasjon [216] og i Norge utarbeider en interdepartemental gruppe daglige oversikter over desinformasjon på sosiale medier. EU gir regelmessige oppdateringer om desinformasjon rundt covid-19 [121]. Hvilken effekt disse og liknende initiativ har er umulig å si på det nåværende tidspunkt. Et problem er at man ofte kartlegger innhold som stammer fra påvirkningsoperasjoner, og ikke nødvendigvis vet hvilken effekt dette innholdet har. Mottiltak fra stater som utsettes for påvirkning er per i dag under utvikling eller i startfasen, man har derfor ingen data på beste praksis eller eventuelle virkninger av mottiltak.

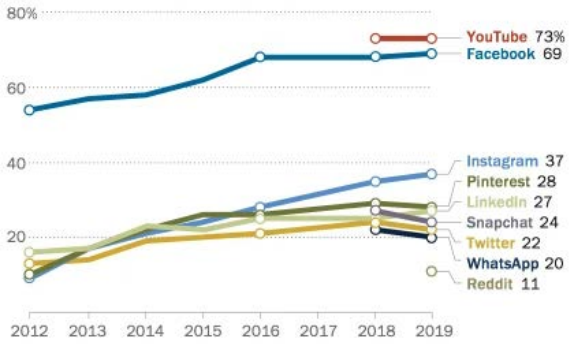
Gitt at sosiale medie-selskaper har en ujevn merittliste med hensyn til vilje og evne til å fjerne og blokkere profiler og innhold fra påvirkningsoperasjoner er det naturlig at myndigheter i forskjellige land har introdusert, eller overveier å introdusere, lover og regler som pålegger sosiale medier å fjerne visse typer innhold. Europaparlamentet vedtok i 2019 at selskaper som tilbyr sine tjenester i EU skal fjerne innhold fra terrorister i løpet av en time etter at de har fått varsel om slikt innhold [217]. Tyskland har siden 2017 hatt lover som krever at sosiale medier fjerner hatytringer, falske nyheter og ulovlig materiale innen en til syv dager [218], Frankrike vedtok et lignende lovforslag mot hatytringer i 2019 [219].

Selv om slike reguleringer er viktige, er de mindre effektive mot påvirkningskampanjer fordi disse er mer diffuse i karakter. Perifere politiske grupperinger er ofte en målgruppe for utenlandske påvirkningsforsøk, og påvirkning av disse kan skje uten at aktører er veldig synlige. Under covid-19-pandemien fokuserte disse aktørene på å promotere eksisterende innhold som sår splittelse fra reelle brukere, fremfor å lage eget innhold.

I USA har flere ledende politikere diskutert om Facebook bør brytes opp på grunn av deres dominante posisjon [220]–[222]. Det er tvilsomt om dette vil hjelpe på påvirkningsoperasjoner. Det er ikke nødvendigvis størrelsen på individuelle sosiale medie-selskaper som er problemet, men egenskaper de fleste sosiale medier har til felles, som diskutert i kapittel 2.6.5.

4.4 Sosiale medie-brukeres holdninger

Enkelte hevder at det skjer et *techlash*, et backlash mot smarttelefoner og sosiale medier [224], [225]. Mistro til sosiale medier har steget blant vanlige brukere i flere spørreundersøkelse [226]–[228]. Men data om faktisk bruk av sosiale medier i USA [223] og Norge [229] viser at en eventuell mistro har hatt liten effekt på hvor mye tid man benytter sosiale medier, som figur 4.2 viser. I forbindelse med covid-19-pandemien har Internett-teknologi muliggjort hjemmekontor for store deler av befolkningen. Samtidig lar sosiale medier familier og venner som ikke kan møtes holde kontakten uten at det koster noe. De fleste sosiale medie-selskaper har gjort mye for å lede brukere til korrekt og god informasjon om covid-19. Det har blitt foreslått at dette kan øke tilliten til sosiale medier [230]–[232]. I realiteten er nok bildet mer komplisert [233], det er derfor naturlig å anta at det blir myndighetene, og ikke vanlige brukere, som vil være pådrivere for endringer i sosiale medier.



Figur 4.2 Graf fra Pew Research [223]*: Bruk av sosiale medier 2012-17.*

4.4.1 Skiftet til grupper

Et skifte som imidlertid har skjedd er større bruk av grupper på sosiale medier, spesielt på Facebook og i krypterte chat-apper som WhatsApp. Grupper kan være åpne eller lukkede. De er organisert rundt interesser og krever aktiv innmeldelse, noe som kan styrke den såkalte ekkokammer-effekten. Denne effekten oppstår når man kun blir gitt informasjon som støtter en persons eller gruppes eksisterende synspunkter. Slike grupper har blitt brukt blant annet av politioffiserer i USA til å utrykke ekstremistiske, rasistiske holdninger [234] og konspirasjonsteoretikere har benyttet grupper til å spre misinformasjon om covid-19 [235]. Vektleggingen av grupper har delvis skjedd på oppfordring fra sosiale medie-selskaper [236], [237] som presenterer det som en prioritering av personvern. En bivirkning er at det blir vanskeligere å oppdage påvirkningsoperasjoner samtidig som potensielle målgrupper blir enda klarere definert.

Faktaboks: Covid-19 – Pandemi og påvirkning

I skrivende stund er covid-19-pandemien i en svært aktiv fase. Propaganda, desinformasjon og annen påvirkning skjer til stadig i sosiale medier og statskontrollerte kanaler som RT (Russia Today) [114]–[116], [121], [238]–[240]. Det å benytte en krise til å angripe tilliten i demokratier via cyber-sosiale virkemidler har gått fra mulighet til realitet.

Sett i lys av resten av denne rapporten er det verdt å notere seg fire punkter.

1: Des- og misinformasjon spres av alle aktørene i økosystemet som skisseres i kapittel 2.5. Man referer til, og sprer, hverandres innlegg, og statlige aktører gjenbruker nå mer innhold fra reelle brukere enn de gjorde tidligere [121]. Dette representerer en kontinuitet med hensyn til målet om å skape problemer for demokratier, med praktiske endringer for å unngå deteksjon.

2: De internasjonale sosiale medie-selskapene har vært proaktive med å fjerne innhold som feilinformerer. Denne gangen er det er ingen benektelse om at plattformene misbrukes. Selskapene har også gjort covid-19-spesifikke endringer, for eksempel viser enkelte covid-19 søkeresultater linker til offisielle kilder øverst på nettsiden. Myndigheter får likevel lite informasjon om hva som blir slettet [121] og det er fremdeles mye desinformasjon som ikke blir fjernet [241]–[244].

3: Sosiale medie-selskapers håndtering av covid-19-pandemien er ikke nødvendigvis en mal for neste krise. Facebooks CEO har påpekt at det er mye enklere å lage svart-hvitt regler for å fjerne materiale når det gjelder sykdom og helse enn for eksempel politikk [245].

4: Det er større bevissthet i demokratier om cyber-sosiale påvirkningsforsøk. En god del gjøres for å håndtere problemene, men det er stort behov for gode verktøy som gir et detaljert og oppdatert situasjonsbilde.

5 Utfordringer for demokratier

Så langt har rapporten beskrevet hvordan bruk av cyber-sosial påvirkning arter seg og diskutert den umiddelbare og langsiktige responsen fra sosiale medie-selskaper og myndigheter etter 2016. Rapporten har oppsummert nåværende status på bruk av sosiale medier for påvirkning og endringer i holdninger og tilnærminger til problemet blant forskjellige aktører.

Dette kapittelet vil omhandle hvilke utfordringer slike påvirkningsforsøk utgjør for Forsvaret og det sivile samfunnet. Per i dag kan man ikke si noe sikkert om det pågår målrettet bruk av sosiale medier direkte mot Norge [246]. Men fordi norske borgere er tett integrert med internasjonale, spesielt engelsktalende, sosiale medier, vil internasjonal påvirkning implisitt berøre Norge, noe som sees i feil- og desinformasjon om covid-19 i skrivende stund.

5.1 Påvirkningsforsøk lønner seg – for mange

> *President Putin has clearly come to the conclusion that "there's little price to pay [for election interference] and therefore I can continue this activity" (Admiral Michael S. Rogers, National Security Agency [97])*

Den første og største utfordringen er at risikoen for å måtte betale en pris for å bedrive påvirkningsforsøk er liten [247]. Utenlandske makter har, for første gang i historien, en anonym sanntidsmulighet til å påvirke andre staters befolkning på en enkel, direkte, billig og effektiv måte. Det er en betydelig lavere risiko for utilsiktede negative konsekvenser for egne interesser enn i tradisjonell krigføring og anonymiteten gir stater rom for plausibel benektelse. Selv en liten gruppe eller enkeltpersoner kan lage en relativ sofistikert påvirkningsoperasjon. Elever på Lillestrøm videregående skole demonstrerte dette for FFIs konferanse «Hacking democracy: Influence Operations in the Digital Age» [248]. Det er derfor liten grunn til å tro at cyber-sosiale påvirkningsoperasjoner vil minske i framtiden.

Som diskutert i kapittel 2.6 tjener andre aktører i økosystemet rundt påvirkningsoperasjoner tjener også på påvirkningsaktiviteter. Sosiale medier får engasjement og større reklameinntekter, nettsteder som lager falske nyheter får mer trafikk og perifere politiske grupper får mer oppmerksomhet, for å nevne tre eksempler. Aktørene har med andre ord sterke egeninteresser som støtter opp om utøvelsen av påvirkning, selv om de ikke støtter målene med påvirkningsforsøkene.

5.2 Uklare linjer

En EU-rapport om desinformasjon om covid-19 i sosiale medier påpeker at «*pro-Kremlin sources do not appear to be authoring the disinformation themselves; instead, they are simply amplifying theories that originate elsewhere, e.g. in China, Iran or the US far right*» [121]. Dette er en viktig endring. Påvirkningsoperasjoner er i stand til å skjule seg blant meningene og narrativene de absorberer fra lokale, virkelige brukere. En lignende konklusjon ble trukket i en

rapport om mulig utenlands påvirkning i norske valg i 2019 [246]. Påvirkningsoperasjonen er med andre ord implisitt beskyttet av vanlige brukere som motsetter seg å bli blokkert eller sensurert. I tillegg er de samme metodene og taktikkene som benyttes av eksterne påvirkningsoperasjoner allerede i bruk hos lokale grupper som ønsker å manipulere opinionen. Det er derfor en balansegang mellom å stoppe påvirkningsforsøk og sensurere egen befolkning.

5.3 Problematisk dialog med sosiale medie-selskaper

Diskusjonen i kapittel 0 viste vanskelighetene forbundet med å stoppe spredningen av desinformasjon. Selskapenes foretrukne, automatiserte metoder for å håndtere problemer er langt fra ufeilbarlige. Manuelle, og mer treffsikre metoder, kan ikke prosessere de store mengdene innlegg fort nok og er reaktive. De globale sosiale medie-selskapene er utenfor Norges jurisdiksjon med hensyn til regulering. Det er mulig å innføre lokal lovgivning om innhold, men som diskutert i kapittel 5.2 er det uklart hva som kan fjernes innenfor demokratiske rammer. Selskapene bidrar til en ansvarsfragmentering ved å sette ut moderering og faktasjekk til underleverandører som må følge stadig skiftende regler i utøvelsen av sine oppgaver.

I tillegg er det tre aspekter ved sosiale medier som betyr at meningsfulle endringer i overskuelig framtid er lite sannsynlig. Det er a) den underliggende forretningsmodellen; b) kulturen i sosiale medie-selskaper og c) hvordan sosiale mediers design promoterer visse typer atferd.

Forretningsmodellen til sosial medier er å gi gratis adgang til svært avanserte kommunikasjons-verktøy i bytte mot innhold. Innholdet, og bruker-interaksjonene rundt det, gir dyp kunnskap om brukernes interesser. Denne kunnskapen benyttes for å oppnå mest mulig engasjement og oppmerksomhet som selges til annonsører. Det er massen av brukere og automatiseringen av plattformen som er viktig, en forretningsmodell basert på lave kostnader og dermed så lite kontroll over innhold som mulig. Enhver trussel til denne måten å operere på er derfor en eksistensiell trussel [249].

Forskjellige sosiale medie-selskaper har nødvendigvis ulike organisasjonskulturer. Det er likevel en del aspekter som deles av flere selskaper. For det første at gründere og ledere ofte har kommet inn i teknologi-verdenen med lite annen ballast enn et universitetsopphold. Facebooks grunnlegger, Mark Zuckerberg, viste for eksempel at han i en alder av 33 år hadde lite kunnskap om hvordan faktiske fellesskap fungerer da han besøkte småsamfunn i USA, til tross for at han ofte snakker om Facebook som en fellesskapsbygger [250]. Det er også et intenst fokus på tekniske løsninger og ingeniørkunst som gjør at alle løsninger evalueres kvantitativt [71]. Dette gir et falskt bilde av hvor problematisk noe er. Zuckerberg sa i 2016 at misinformasjon er en relativt liten prosentandel av det totale innholdet på Facebook [251]. Hvis en algoritme fanger opp desinformasjon 95 prosent av tiden er det fantastisk fra en programmerers ståsted. Med 2,5 milliarder brukere betyr det likevel at 125 millioner brukere blir eksponert til desinformasjonen [165]. De store sosiale medie-selskapene ser på seg selv som globale borgere, med tjenester som skal være identiske i Novosibirsk og på Notodden. Resultatet er at de ikke ser noe galt i å bli

betalt i russiske rubler for amerikanske valgkampannonser [252] og de forstår sjelden lokale problemer som kan virke små og isolerte.

Teknologi er hverken god eller ond, men den er heller ikke nøytral [253]. Programvaren som driver sosiale medier er et eksempel på dette. Den forsterker menneskers intensjoner [254] og forenkler og framskynder visse typer handlinger og sosiale relasjoner på bekostning av andre [255]. Fokuset er alltid på mest mulig engasjement. Som tidligere nevnt betyr dette at kontroversielle temaer og holdninger gjør det bedre enn mer midtstrøms-tilnærminger [256]. Dette designet støtter opp under påvirkningsoperasjoner som kan manipulere brukeres oppmerksomhet via velvalgte temaer og narrativ som trigger algoritmene som velger innhold for brukerne.

Disse tre aspektene ved sosiale medie-selskapers kultur gjør kommunikasjon om problemet vanskelig. Sosiale mediers smale fokus ignorerer bredere behov og hensyn som demokratier har og må ta.

5.4 Undergraver tillit

Den overordnede utfordringen for demokratier er at statlige aktører og perifere støttegrupper ønsker å underminere liberale demokratier ved å forsterke eksisterende konfliktlinjer. For disse aktørene er det ikke viktig å få målgruppene for påvirkning til å tro en bestemt ting, men å heve temperaturen i debatter og forsterke ytterpunktene [257]. Påvirkningskampanjer kan bli selvforsterkende over tid, når et tema eller en gruppe har blitt utsatt for en kampanje med ekstreme synspunkter over en tid – er det eksempler på at temperaturen på diskusjoner i etterkant ligger høyere enn før kampanjen ble iverksatt [258]. Ironisk nok så vil avsløringer av påvirkningsoperasjoner i seg selv bidra til en generell reduksjon i tillit til online informasjon. Selv om dette er en sunn respons, bidrar det også til aktørenes overordnede mål om å så tvil om hva som er sant [259]. Det at påvirkning fra fremmede stater kvantitativt sett står for en liten del av online innhold [260]–[262] er i denne sammenheng ikke viktig. Det at man vet at det pågår undergraver tillit i seg selv.

6 Å leve med cyber-sosiale påvirkningsoperasjoner

Gitt den ovenstående diskusjonen er det naturlig å anta at det norske forsvaret og sivilsamfunnet må leve med (muligheten for) cyber-sosiale påvirkningsforsøk i overskuelig framtid som en del av såkalte *«sammensatte trusler»* rettet mot Norge. Denne rapporten har gitt en oversikt over hvordan påvirkningsoperasjoner utføres. Dette gir et utgangspunkt for videre kunnskapsbygging med vektlegging på å utvikle kapabiliteter som kan hjelpe Norge å håndtere cyber-sosiale påvirkningsoperasjoner.

Denne rapporten har vist at sosiale medier gir større aktører stor fleksibilitet med hensyn til hvem som utsettes for påvirkningsforsøk, og når og gjennom hvilke temaer dette gjøres. Det betyr at påvirkningsoperasjoner kan rettes mot sårbarheter innen hele krisespekteret. Fra norske myndigheters perspektiv er cyber-sosiale påvirkningsoperasjoner av natur tverrsektorielle, selv om enkelte tilfeller kan tilhøre én sektor i en gitt fase av hendelsesforløpet. Det vil derfor være mange offentlige instanser og departementer i Norge som har ansvar for deler av målene som blir berørt av en påvirkningsoperasjon. Initiativ som en tverrdepartemental strategisk kommunikasjonsgruppe er en god begynnelse, men det er behov for samhandling på sanntids-analyser og oppfølgning av mindre, mer spesifikke, koordinerte påvirkningsforsøk som man ser mer av i sosiale medier.

Samfunnssikkerhetsmeldingen fra 2016 (Meld. St. 10) og det nyeste forslaget til langtidsplan for Forsvaret (Prop. 62 S) peker på Totalforsvaret som en naturlig ramme for samordningen av forskjellige sektorer og aktører når det gjelder den type sammensatte trusler som påvirkningsoperasjoner er en del av. Her må roller og ansvar med hensyn til hvilke etater som har helhetsforståelse og styringen av eventuelle tiltak avklares med hensyn til hvem som "eier" problemene som en påvirkningsoperasjon skaper. Man trenger også en felles forståelse av problemstillingene rundt cyber-sosial påvirkning. Hva er sårbarhetene i samfunnet på dette området og hvilke hindringer legges til grunn for ikke å utvikle relevante verktøy og løsninger?

Beslutningstagere trenger derfor tilgang til kunnskap som favner bredt. Dersom vi som samfunn ikke har en samlet oversikt over hva som er et normalbilde, vil vi heller ikke kunne fange opp utvikling og endringer i tide til å kunne gjøre noe med dem. Et første steg kan derfor være å utvikle metoder for en pågående vurdering av informasjonsmiljøet i det cyber-sosiale domenet, innenfor de til enhver tid gjeldene lover, regler og mandater. Dette bør legge til rette for en situasjonsforståelse som favner både overordnede aspekter ved en påvirkningsoperasjon og elementer som er relevante for individuelle sektorer.

FFI jobber per i dag med andre NATO-partnere for å utvikle forslag til metoder som kan benyttes til dette formålet. Ideen er at man må følge med på trender i sosiale medier og utvikle en grunnlinje for hva som er et normalt informasjonsmiljø. Når noe skjer må man være i stand til å evaluere størrelsen på påvirkningsoperasjonen, kanaler som brukes, mulige målgrupper og narrativ som promoteres. Spørsmål man bør se på inkluderer hva mulige påvirkningsaktørers insentiv er for å påvirke grupper i Norge – hva er deres begrunnelse for operasjoner mot oss

eller allierte? Hvilke målgrupper er sårbare i forskjellige scenarier, hvilke narrativ kan benyttes og hvilke sosiale medier benytter disse gruppene? Hvordan kan endringer i sosiale medie-plattformer over tid presentere nye muligheter for påvirkning? Hvordan virker de algoritmene som påvirkningsoperasjoner forsøker å manipulere? Sist, men ikke minst, må man også få en forståelse for beslutningstageres oppgaver og bevissthet i forbindelse med desinformasjon og misinformasjon i sosiale medier.

Kunnskapen fra slik forskning bør resultere i nye verktøy, tilnærminger, utdanningstiltak og prosesser for å skape en situasjonsforståelse som er relevant for forskjellige brukere. Individuelle påvirkningsaktiviteter må forstås som del av en større helhet og ikke som enkeltstående hendelser. DiResta, som forsker på misbruk av informasjonsteknologi skriver: «*We are immersed in an evolving, ongoing conflict: an Information World War […] The conflict is still being processed as a series of individual skirmishes […] but these battles are connected.*»

Basert på kunnskap fra slik forskning bør man også øke bevisstheten i befolkningen om muligheten for å bli utsatt for manipulasjon. Dette kan først og fremst gjøres gjennom utdanning på mange nivåer. Motstandskraft mot forsøk på påvirkning må skapes gjennom organisasjons-utvikling og utvikling av samfunnet generelt. Man må også forsøke å håndtere narrativ som kan benyttes, ikke individuelle innlegg eller temaer. Når en krisesituasjon inntreffer kan det være for sent å bekjempe et narrativ som har blitt en del av en målgruppes verdenssyn.

7 Konklusjon

Rapporten beskriver hvordan påvirkningsoperasjoner utføres i sosiale medier (det cyber-sosiale domenet), hva som understøtter slike operasjoner, holdninger og håndteringer blant sosiale medie-selskaper, myndigheter og brukere samt utfordringene ved dette.

Rapporten fremhever at påvirkningsforsøk lønner seg, ikke bare for de som iverksetter en påvirkningsoperasjon, men også for flere aktører rundt en påvirkningsoperasjon. Disse aktørene former et økosystem som understøttes av sosiale mediers kultur, design og forretningsmodell. Det er vanskelig å oppnå store endringer som kan stoppe påvirkningsoperasjoner. Dette er delvis fordi innhold og narrativ fra påvirkningsoperasjoner er blandet sammen med reelle, lokale brukeres innhold som reflekterer meninger og holdninger beskyttet av ytringsfriheten. Dette benyttes av påvirkningsoperasjoner som kan oppnå stor spredning av sine narrativ. Endringer vanskeliggjøres også fordi reell kontroll med bruker-generert innhold på sosiale medier er kostbart, tidkrevende og strider mot sosiale medie-selskapenes forretningsmodell. Derfor er mange endringer enten PR-framstøt for å unngå regulering, eller de implementeres via endringer i algoritmer. Algoritmer er programvare som automatisk klassifiserer og velger innhold som vises til brukere, og manipulasjon av disse algoritmene er en sentral del av påvirkningsoperasjoner. Samtidig kan endringer av algoritmer ha store utilsiktede konsekvenser for samfunnet, for eksempel ved å blokkere feil innhold.

En påvirkningsoperasjon trenger ikke å få målgruppene til å endre meninger radikalt. En forsterkning av forskjeller som hindrer konsensus-beslutninger kan være godt nok sett fra iverksetternes synsvinkel. Derfor ser man ofte at påvirkning fokuserer på å spre støy og desinformasjon rundt et emne, som for eksempel covid-19-pandemien. Dette skaper et problem for demokratier som trenger tillit for å fungere. Forskjellen på reaksjonene til USA-valget i 2016 og covid-19-pandemien i 2020 viser at det er større bevissthet rundt bruk av sosiale medier for påvirkning, men ikke nødvendigvis bedre kapasitet til å ha en løpende vurdering av informasjonsmiljøet i det cyber-sosiale domenet.

Per i dag er det vanskelig å stoppe påvirkningsoperasjoner direkte. Norge må derfor, som en del av forberedelsene til å leve med slike påvirkningsforsøk, utvikle en tilnærming og kunnskapsbase for å forebygge og håndtere problemer som kan oppstå som et resultat av cyber-sosiale påvirkningsforsøk. Dette bør skje gjennom forskning på mulige aktører, målgrupper og sosiale medie-plattformer som kan bedre situasjonsforståelsen til beslutningstagere i en tverrsektoriell totalforsvarsramme. Håndtering av påvirkningsoperasjoner kan da skje ut fra denne kunnskapsbasen gjennom bruk av bedre verktøy for å oppdage påvirkningsforsøk, mer utdanning eller nye prosesser som forbedrer tverrsektoriell samhandling.

Referanser

[1] E. Wills, «Muslim woman pictured 'ignoring victims of London terror attack' was fake news Tweet created by Russians», *Evening Standard*, nov. 13, 2017. https://www.standard.co.uk/news/world/russian-bot-account-claimed-muslim-woman-ignored-westminster-attack-victims-a3689751.html (åpnet feb. 06, 2019).

[2] Euractiv, «Julian King: Russian info war preceded Ukrainian ship seizures», *euractiv.com*, des. 11, 2018. https://www.euractiv.com/section/global-europe/news/julian-king-russian-info-war-preceded-ukrainian-ship-seizures/ (åpnet feb. 08, 2019).

[3] A. Applebaum, P. Pomerantsev, M. Smith, og C. Colliver, «'Make Germany Great Again': Kremlin, Alt-Right, and International Influences in the 2017 German Elections», London School of Economics, Institute for Global Affairs, 2017.

[4] H. Martin, «2019 EU Elections Information Operations Analysis: interim briefing paper», London School of Economics, Institute for Global Affairs, 2019.

[5] A. Bergh, «Social network centric warfare: Understanding influence operations in social media», FFI, Kjeller, Norway, FFI-rapport 19/01194, 2019.

[6] NATO, «Warsaw Summit Communiqué - Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8-9 July 2016». Åpnet: apr. 01, 2020. [Online]. Tilgjengelig på: http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

[7] Bergh, A., «Rebel with a Temporary Cause: The Asymmetrical Access to Distrust, Hipness and Intensity As Resources in Cyber-Conflicts», presentert på XIX ISA World Congress of Sociology, Toronto, jul. 20, 2018, [Online]. Tilgjengelig på: https://isaconf.confex.com/isaconf/wc2018/webprogram/Paper104220.html.

[8] A. E. Marwick, «Why do people share fake news? A sociotechnical model of media effects», *Georgetown Law Technology Review*, bd. 2, nr. 2, s. 474–512, 2018.

[9] E. Trist, H. Murray, F. E. Emery, og B. Trist, *The Social Engagement of Social Science, Volume 2: A Tavistock Anthology–The Socio-Technical Perspective*, bd. 2. University of Pennsylvania Press, 1990.

[10] A. Tatnall, «Actor-network theory as a socio-technical approach to information systems research», i *Socio-technical and human cognition elements of information systems*, S. Clarke, E. Coakes, M. G. Hunter, og A. Wenn, Red. Hershey, PA: Information Science Publishing, 2003, s. 266–283.

[11] H. Akbari og F. Land, «Socio-technical theory – IS Theory», *Theories Used in IS Research Wiki*, mar. 20, 2016. https://is.theorizeit.org/wiki/Socio-technical_theory (åpnet jan. 16, 2018).

[12] C. Inglis, «Cyberspace—Making Some Sense of It All», *Journal of Information Warfare*, bd. 15, nr. 2, s. 17–26, 2016.

[13] A. L. Bjørnstad, «Understanding influence in a defense context: A review of relevant research from the field of psychology», FFI, Kjeller, Norway, FFI-rapport 19/01224, 2019.

[14] V. Alme, «Falske nyheter som sjanger», FFI, Kjeller, Norway, FFI-rapport 19/00660, 2019.

[15] Internet Research Agency, «Tennessee (@TEN_GOP) | Twitter», *Internet Archive*, aug. 13, 2017. https://web.archive.org/web/20170814211128/https:/twitter.com/ten_gop/ (åpnet apr. 01, 2020).

[16] A. Garmazhapova, «Where do the trolls live? And who feeds them (Где живут тролли. И кто их кормит)», *Новая газета - Novayagazeta.ru*, sep. 07, 2013.
[17] P. N. Howard, B. Ganesh, D. Liotsiou, J. Kelly, og C. François, «The IRA, Social Media and Political Polarization in the United States, 2012-2018», Oxford Internet Institute, Oxford, Working Paper, number 2018.2, 2018.
[18] R. DiResta *mfl.*, «The Tactics & Tropes of the Internet Research Agency», New Knowledge. [Online]. Tilgjengelig på: https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1003&context=senatedocs.
[19] Bloomberg News, «Russia Spent $1.25M Per Month on Ads, Acted Like an Ad Agency: Mueller», feb. 16, 2018. https://adage.com/article/digital/russia-spent-1-25m-ads-acted-agency-mueller/312424 (åpnet okt. 15, 2019).
[20] B. Weiss, «A Russian troll factory had a $1.25 million monthly budget to interfere in the 2016 US election», *Business Insider*. https://www.businessinsider.com/russian-troll-farm-spent-millions-on-election-interference-2018-2 (åpnet okt. 15, 2019).
[21] K. Giles, «Russia's hybrid Warfare: A success in propaganda», *Bundesakademie für Sicherheitspolitik, Working Paper*, nr. 1, s. 2015, 2015.
[22] E. Kotlyar, «"We had a goal ... to cause unrest": an interview with an ex-employee of the "troll factory" in St. Petersburg», *TV Rain*, okt. 14, 2017. https://tvrain.ru/teleshow/bremja_novostej/fabrika-447628/ (åpnet okt. 15, 2019).
[23] D. A. Martin og J. N. Shapiro, «Trends in Online Foreign Influence Efforts», Princeton University, Princeton, NJ, Working Paper, jul. 2019.
[24] M. Galeotti, «Controlling Chaos: How Russia Manages Its Political War in Europe», European Council on Foreign Relations, London, UK, Policy Brief, 2017.
[25] B. Popken, «Russian trolls pushed divisive content over vaccines, researchers say», *NBC News*, aug. 23, 2018. https://www.nbcnews.com/tech/tech-news/russian-trolls-pushed-divisive-content-over-vaccines-researchers-say-n903286 (åpnet apr. 22, 2020).
[26] S. Abrams, «Beyond Propaganda: Soviet Active Measures in Putin's Russia», *Connections*, bd. 15, nr. 1, s. 5–31, 2016.
[27] D. O'Sullivan, «A lesson in Russian disinformation from the pages of a 1982 TV Guide», *CNN*, 2019. https://www.cnn.com/2019/03/11/tech/tv-guide-russian-disinformation/index.html (åpnet sep. 30, 2019).
[28] Senate Select Committee on Intelligence, «Report of the Select Committee on Intelligence, United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.s. Election - Volume 2: Russia's Use of Social Media with Additional Views», US Senate, Washington, DC, USA, Volume 2: Russia's Use Of Social Media, 2019. Åpnet: okt. 09, 2019. [Online]. Tilgjengelig på: https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.
[29] Senate Select Committee on Intelligence, «Report of the Select Committee on Intelligence, United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.s. Election - Volume 1: Russian Efforts Against Election Infrastructure with Additional Views», US Senate, Washington, DC, USA, Volume 1: Russian Efforts Against Election Infrastructure with additional views, 2019. Åpnet: okt. 09, 2019. [Online]. Tilgjengelig på: https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.
[30] Permanent Select Committee on Intelligence, «Social Media Advertisements», 2018. https://intelligence.house.gov/social-media-content/social-media-advertisements.htm (åpnet feb. 06, 2019).
[31] Twitter, «Information operations», *Twitter Transparency Report*, okt. 2018. https://transparency.twitter.com/en/information-operations.html (åpnet mai 31, 2020).

[32] M. Belam, «Twitter diplomacy: how Russian embassy trolls UK government», *the Guardian*, mar. 15, 2018.
[33] S. Shane, «Some of the Popular Images and Themes the Russians Posted on Social Media», *The New York Times*, des. 17, 2018.
[34] C. Maynes, «A guide to Russian 'demotivator' memes», *Public Radio International*, mar. 2018. https://interactive.pri.org/2018/03/russian-meme/index.html (åpnet jun. 03, 2020).
[35] N. Thompson og I. Lapowsky, «How Russian Trolls Used Meme Warfare to Divide America», *Wired*, des. 17, 2018. https://www.wired.com/story/russia-ira-propaganda-senate-report/ (åpnet jun. 03, 2020).
[36] J. Giesea, «It's Time to Embrace Memetic Warfare», *Defence Strategic Communications*, bd. 1, nr. 1, 2015.
[37] C. François, B. Nimmo, og C. S. Eib, «The IRA CopyPasta Campaign», Graphika, okt. 2019. Åpnet: okt. 22, 2019. [Online]. Tilgjengelig på: https://graphika.com/uploads/Graphika%20Report%20-%20CopyPasta.pdf.
[38] R. Diresta og S. Grossman, «Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019», Stanford Internet Observatory, Cyber Policy Center, 2019. [Online]. Tilgjengelig på: https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/potemkin-pages-personas-sio-wp.pdf.
[39] Defending Democracy Together, «Russian Troll Account Profile - @ten_gop», *The Russia Tweets*, 2018. https://russiatweets.com/author/TEN_GOP (åpnet jan. 21, 2020).
[40] C. Timberg, E. Dwoskin, og A. Entous, «Michael Flynn, Nicki Minaj shared content from this Tennessee GOP account. But it wasn't real. It was Russian.», *Washington Post*, okt. 18, 2017.
[41] G. J. X. Dance, B. Laffin, D. Jordan, og M. Browne, «How Cambridge Analytica Exploited the Facebook Data of Millions», *The New York Times*, jul. 30, 2019.
[42] P. N. Howard og B. Kollanyi, «Bots, #Strongerin, and #Brexit: Computational Propaganda During the UK-EU Referendum», *SSRN Electronic Journal*, 2016, doi: 10.2139/ssrn.2798311.
[43] E. J. Kirby, «The city getting rich from fake news», *BBC News*, des. 05, 2016.
[44] M. Wendling, «The (almost) complete history of 'fake news'», *BBC News*, jan. 22, 2018.
[45] B. Zadrozny og B. Collins, «How a right-wing troll and a Russian Twitter account created 2016's biggest voter fraud story», *NBC News*, okt. 30, 2018. https://www.nbcnews.com/tech/tech-news/how-right-wing-troll-russian-twitter-account-created-2016-s-n925711 (åpnet jan. 29, 2020).
[46] E. Pilkington og A. Michel, «Obama, Facebook and the power of friendship: the 2012 data election», *the Guardian*, feb. 17, 2012.
[47] Z. Tufekci, «It's the (Democracy-Poisoning) Golden Age of Free Speech», *Wired*, bd. 26, nr. 2, feb. 2018.
[48] A. Cornish, «How Gamergate Became A Template For Malicious Action Online», *NPR.org*, aug. 30, 2019. https://www.npr.org/2019/08/30/756034720/how-gamergate-became-a-template-for-malicious-action-online (åpnet des. 10, 2019).
[49] J. Allaway, «#Gamergate Trolls Aren't Ethics Crusaders; They're a Hate Group», *Jezebel*, okt. 13, 2014. https://jezebel.com/gamergate-trolls-arent-ethics-crusaders-theyre-a-hate-1644984010 (åpnet jul. 11, 2018).
[50] S. Kramer, «How Bots and Cyborgs Spread Misinformation: A Data Scientist Finds 5,000+ Bots in 72,000,000+…», *Medium*, des. 12, 2017. https://medium.com/hackernoon/how-bots-and-cyborgs-spread-misinformation-a-data-scientist-finds-72-000-000-tweets-by-5-000-fa6f28ba0649 (åpnet nov. 08, 2019).

[51] C. Timberg, «As a conservative Twitter user sleeps, his account is hard at work», *Washington Post*, feb. 05, 2017. https://www.washingtonpost.com/business/economy/as-a-conservative-twitter-user-sleeps-his-account-is-hard-at-work/2017/02/05/18d5a532-df31-11e6-918c-99ede3c8cafa_story.html (åpnet feb. 06, 2017).
[52] P. Layton, «Duelling Algorithms: Using Artificial Intelligence in Warfighting», *OTH*, apr. 25, 2018. https://othjournal.com/2018/04/25/duelling-algorithms-using-artificial-intelligence-in-warfighting/ (åpnet aug. 10, 2018).
[53] «Ghosh_Scott_2018_# Digitaldeceit.pdf». .
[54] A. Conklin, «Facebook Announces Effort To Clearly Mark Fake News Ahead Of 2020», okt. 21, 2019. https://dailycaller.com/2019/10/21/facebook-protecting-elections-2020/ (åpnet jan. 31, 2020).
[55] D. Lu, «Facebook has a plan to tackle fake news – here's why it won't work», *New Scientist*. https://www.newscientist.com/article/2221963-facebook-has-a-plan-to-tackle-fake-news-heres-why-it-wont-work/ (åpnet jan. 31, 2020).
[56] Propastop, «The marking of FB fake news caused an opposite effect – Propastop», *Propastop*, nov. 16, 2018. https://www.propastop.org/eng/2018/11/16/the-marking-of-fb-fake-news-caused-an-opposite-effect/ (åpnet jan. 31, 2020).
[57] B. Popper, «Facebook's business is booming, but it says preventing abuse will cut into future profits», *The Verge*, nov. 01, 2017. https://www.theverge.com/2017/11/1/16593812/facebook-earnings-q3-third-quarter-2017 (åpnet des. 04, 2019).
[58] J. Bridle, «Something is wrong on the internet», *Medium*, jun. 21, 2018. https://medium.com/@jamesbridle/something-is-wrong-on-the-internet-c39c471271d2 (åpnet sep. 23, 2019).
[59] S. Walker, «Salutin' Putin: inside a Russian troll house», *The Guardian*, apr. 02, 2015.
[60] J. Gottfried og E. Shearer, «News Use Across Social Media Platforms 2016», *Pew Research Center's Journalism Project*, mai 26, 2016. http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/ (åpnet mai 18, 2017).
[61] M. Nunez, «Former Facebook Workers: We Routinely Suppressed Conservative News», *Gizmodo*, sep. 05, 2016. https://gizmodo.com/former-facebook-workers-we-routinely-suppressed-conser-1775461006 (åpnet nov. 28, 2019).
[62] J. Cook, «The Story Behind The Story That Created A Political Nightmare For Facebook», *HuffPost*, okt. 08, 2018. https://www.huffpost.com/entry/facebook-gizmodo-gawker-trending-conservatives_n_5b6c9b16e4b0530743c83f58 (åpnet jan. 31, 2020).
[63] N. Thompson og F. Vogelstein, «Inside Facebook's Two Years of Hell», *Wired*, des. 02, 2018. https://www.wired.com/story/inside-facebook-mark-zuckerberg-2-years-of-hell/ (åpnet des. 06, 2019).
[64] M. Calabresi, «Inside the Secret Plan to Stop Vladimir Putin's U.S. Election Plot», *Time*, jul. 31, 2017.
[65] E. Lipton, D. E. Sanger, og S. Shane, «The Perfect Weapon: How Russian Cyberpower Invaded the U.S.», *The New York Times*, des. 13, 2016.
[66] S. Landau, «Making sense from Snowden: What's significant in the NSA surveillance revelations», *IEEE Security & Privacy*, bd. 11, nr. 4, s. 54–63, 2013.
[67] R. Nieva, «Zuckerberg: Fake news on Facebook affected election? That's 'crazy'», *CNET*. https://www.cnet.com/news/facebook-mark-zuckerberg-fake-news-affect-election-techonomy-donald-trump-crazy/ (åpnet nov. 28, 2019).
[68] A. Hern, «Google plans to 'de-rank' Russia Today and Sputnik to combat misinformation», *The Guardian*, nov. 21, 2017.

[69] C. Newton, «Russians: If you can't beat 'em, rank 'em lower in search», *The Interface*, nov. 21, 2017. https://www.getrevue.co/profile/caseynewton/issues/russians-if-you-can-t-beat-em-rank-em-lower-in-search-84130 (åpnet okt. 08, 2019).
[70] W. Oremus, «Twitter Has Transformed Itself, and No One Noticed», *Slate Magazine*, des. 15, 2017. https://slate.com/technology/2017/12/twitter-has-transformed-itself-and-no-one-noticed.html (åpnet des. 06, 2019).
[71] C. Warzel, «How People Inside Facebook Are Reacting To The Company's Election Crisis», *BuzzFeed News*, okt. 20, 2017. https://www.buzzfeednews.com/article/charliewarzel/how-people-inside-facebook-are-reacting-to-the-companys (åpnet nov. 28, 2019).
[72] S. Wang, «Twitter Sidestepped Russian Account Warnings, Former Worker Says», *Bloomberg.com*, nov. 03, 2017. https://www.bloomberg.com/news/articles/2017-11-03/former-twitter-employee-says-fake-russian-accounts-were-not-taken-seriously (åpnet des. 05, 2019).
[73] C. Bray, «Twitter Says It Overstated Monthly-User Figures for 3 Years», *The New York Times*, okt. 26, 2017.
[74] A. Entous, E. Dwoskin, og C. Timberg, «Obama tried to give Zuckerberg a wake-up call over fake news on Facebook», *Washington Post*, sep. 24, 2017.
[75] S. Frier og B. Allison, «Facebook Fought Rules That Could Have Exposed Fake Russian Ads», *Bloomberg.com*, okt. 04, 2017. https://www.bloomberg.com/news/articles/2017-10-04/facebook-fought-for-years-to-avoid-political-ad-disclosure-rules (åpnet des. 06, 2019).
[76] D. E. Sanger, «Putin Ordered 'Influence Campaign' Aimed at U.S. Election, Report Says», *The New York Times*, jan. 06, 2017.
[77] C. Timberg, «Russian propaganda effort helped spread 'fake news' during election, experts say», *Washington Post*, nov. 24, 2016.
[78] PropOrNot Team, «Black Friday Report: On Russian Propaganda Network Mapping», PropOrNot, nov. 2016.
[79] T. Romm, «Twitter just told Congress it found about 200 accounts linked to the same Russian agents found on Facebook», *Vox*, sep. 28, 2017. https://www.vox.com/2017/9/28/16378104/twitter-senate-house-russia-investigation-facebook-presidential-election-fake-news (åpnet des. 04, 2019).
[80] A. Romano, «Twitter released 9 million tweets from one Russian troll farm. Here's what we learned.», *Vox*, okt. 19, 2018. https://www.vox.com/2018/10/19/17990946/twitter-russian-trolls-bots-election-tampering (åpnet jan. 31, 2020).
[81] J. Guynn, «Facebook: 10 million people saw Russia-backed election ads», *USA Today*, okt. 03, 2017. https://www.usatoday.com/story/tech/2017/10/02/facebook-hire-1-000-monitor-ads-after-russia-election-meddling/723507001/ (åpnet jan. 31, 2020).
[82] E. Weise, «Russian fake accounts showed posts to 126 million Facebook users», *USA Today*, nov. 01, 2017. https://www.usatoday.com/story/tech/2017/10/30/russian-fake-accounts-showed-posts-126-million-facebook-users/815342001/ (åpnet jan. 31, 2020).
[83] C. Cadwalladr og E. Graham-Harrison, «How Cambridge Analytica turned Facebook 'likes' into a lucrative political tool», *the Guardian*, mar. 17, 2018.
[84] C. Cadwalladr, «'I created Steve Bannon's psychological warfare tool': meet the data war whistleblower», *The Guardian*, mar. 17, 2018.
[85] H. Davies, «Ted Cruz campaign using firm that harvested data on millions of unwitting Facebook users», *the Guardian*, des. 11, 2015.
[86] P. Lewis, «'Utterly horrifying': ex-Facebook insider says covert data harvesting was routine», *the Guardian*, mar. 20, 2018.

[87] O. Solon og C. Farivar, «Mark Zuckerberg leveraged Facebook user data to fight rivals and help friends, leaked documents show», *NBC News*, apr. 16, 2019. https://www.nbcnews.com/tech/social-media/mark-zuckerberg-leveraged-facebook-user-data-fight-rivals-help-friends-n994706 (åpnet nov. 07, 2019).
[88] D. O'Sullivan, C. Devine, og D. Griffin, «Obama official: We could have stopped Russian trolls», *CNN*, mar. 26, 2018. https://www.cnn.com/2018/03/26/politics/brett-bruen-russian-meddling-election/index.html (åpnet mar. 27, 2018).
[89] ABC News, «Obama administration 'flat-footed' as Russians meddled in 2016 election: Senate panel», *ABC News*, jun. 21, 2018. https://abcnews.go.com/Politics/obama-administration-flat-footed-russians-meddled-2016-election/story?id=56029328 (åpnet nov. 28, 2019).
[90] A. Entous, E. Nakashima, og G. Jaffe, «Kremlin trolls burned across the Internet as Washington debated options», *Washington Post*, des. 25, 2017.
[91] A. Gold og M. H. McGill, «The year ahead in Congress», *POLITICO*, feb. 01, 2018. https://www.politico.com/newsletters/morning-tech/2018/01/02/the-year-ahead-in-congress-062321 (åpnet des. 06, 2019).
[92] Facebook, «Facebook - Ad Library», 2020. https://www.facebook.com/ads/library/?active_status=all&ad_type=all&country=NO&impression_search_field=has_impressions_lifetime (åpnet feb. 03, 2020).
[93] H. T. Kozlowska Hanna, «Facebook's quiet battle to kill the first transparency law for online political ads», *Quartz*. https://qz.com/1235363/mark-zuckerberg-and-facebooks-battle-to-kill-the-honest-ads-act/ (åpnet des. 08, 2019).
[94] B. Brody og B. Allison, «Lobbying Group for Facebook and Google to Pitch Self-Regulation of Ads», *Bloomberg.com*, okt. 24, 2017. https://www.bloomberg.com/news/articles/2017-10-24/lobby-group-for-facebook-google-to-pitch-self-regulation-of-ads (åpnet des. 04, 2019).
[95] S. Fischer og D. McCabe, «Facebook says it supports Honest Ads Act, cracks down on issue ads», *Axios*, apr. 06, 2018. https://www.axios.com/facebook-ad-changes-5da9d7f7-d297-488b-9f46-9729101201f8.html (åpnet des. 08, 2019).
[96] C. Lecher, «Facebook withdraws from group fighting a major California privacy initiative», *The Verge*, apr. 12, 2018. https://www.theverge.com/2018/4/12/17229128/facebook-california-consumer-privacy-act (åpnet des. 08, 2019).
[97] M. Rosenberg, «White House Has Given No Orders to Counter Russian Meddling, N.S.A. Chief Says», *The New York Times*, feb. 27, 2018.
[98] M. Apuzzo og S. LaFraniere, «13 Russians Indicted as Mueller Reveals Effort to Aid Trump Campaign», *The New York Times*, feb. 16, 2018.
[99] K. Liptak, «Trump administration finally announces Russia sanctions», *CNN*, mar. 15, 2018. https://www.cnn.com/2018/03/15/politics/russia-sanctions-trump-yevgeniy-viktorovich-prigozhin/index.html (åpnet des. 08, 2019).
[100] S. S. Hsu, «Justice Dept. abandons prosecution of Russian firm indicted in Mueller election interference probe», *Washington Post*, mar. 16, 2020. https://www.washingtonpost.com/local/legal-issues/us-justice-dept-abandons-prosecution-of-russian-firm-indicted-in-mueller-election-interference-probe/2020/03/16/5f7c3fd6-64a9-11ea-912d-d98032ec8e25_story.html (åpnet apr. 03, 2020).
[101] Etterretningstjenesten, «Focus 2020 - Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer», Forsvaret, Oslo, 2017. Åpnet: mai 18, 2017. [Online]. Tilgjengelig på: https://forsvaret.no/presse_/ForsvaretDocuments/Fokus2020-web.pdf.

[102] R. MacKinnon, «Networked Authoritarianism in China and Beyond: Implications for global Internet freedom», Stanford University, okt. 2010, s. 31, [Online]. Tilgjengelig på: http://iis-db.stanford.edu/evnts/6349/MacKinnon_Libtech.pdf.
[103] B. Haas, «China moves to block internet VPNs from 2018», *The Guardian*, jul. 11, 2017.
[104] G. King, J. Pan, og M. E. Roberts, «How the Chinese government fabricates social media posts for strategic distraction, not engaged argument», *American Political Science Review*, bd. 111, nr. 3, s. 484–501, 2017.
[105] G. Bolsover og P. Howard, «Chinese computational propaganda: automation, algorithms and the manipulation of information about Chinese politics on Twitter and Weibo», *Information, Communication & Society*, bd. 22, nr. 14, s. 2063–2080, des. 2019, doi: 10.1080/1369118X.2018.1476576.
[106] G. Bolsover, «Computational Propaganda in China: An Alternative Model of a Widespread Practice». Oxford Internet Institute, apr. 2017, Åpnet: jan. 20, 2018. [Online].
[107] A. Kasprak og J. Liles, «EXCLUSIVE: Expanding Pro-Trump Outlet 'The BL' Is Closely Linked to The Epoch Times», *Snopes.com*, okt. 11, 2019. https://www.snopes.com/news/2019/10/11/pro-trump-outlet-linked-epoch-times/ (åpnet nov. 27, 2019).
[108] K. Roose, «Epoch Times, Punished by Facebook, Gets a New Megaphone on YouTube», *The New York Times*, feb. 05, 2020.
[109] Facebook Inc., «Removing Coordinated Inauthentic Behavior From China», *About Facebook*, aug. 19, 2019. https://about.fb.com/news/2019/08/removing-cib-china/ (åpnet des. 09, 2019).
[110] Twitter, «Information operations directed at Hong Kong», *Twitter*, aug. 19, 2019. https://blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong.html (åpnet des. 09, 2019).
[111] B. Jerdén og V. Bohman, «China's propaganda campaign in Sweden, 2018–2019», Swedish Institute of International Affairs (UI), Stockholm, Sweden, 4, 2019.
[112] D. Bandurski, «China's new diplomacy in Europe has a name: broken porcelain», *The Guardian*, okt. 17, 2018.
[113] T. You, «Chinese put swastika on Danish flag over coronavirus flag row», *Mail Online*, jan. 31, 2020. https://www.dailymail.co.uk/news/article-7948913/Chinese-swastika-Danish-flag-PM-refuses-apologise-coronavirus-China-flag.html (åpnet apr. 03, 2020).
[114] J. Kao og M. S. Li, «How China Built a Twitter Propaganda Machine Then Let It Loose on Coronavirus», *ProPublica*, mar. 26, 2020. https://www.propublica.org/article/how-china-built-a-twitter-propaganda-machine-then-let-it-loose-on-coronavirus (åpnet apr. 01, 2020).
[115] J. E. Barnes, M. Rosenberg, og E. Wong, «As Virus Spreads, China and Russia See Openings for Disinformation», *The New York Times*, mar. 28, 2020.
[116] C. Silverman, «Chinese Trolls Are Spreading Coronavirus Disinformation In Taiwan», *BuzzFeed News*, mar. 05, 2020. https://www.buzzfeednews.com/article/craigsilverman/chinese-trolls-coronavirus-disinformation-taiwan (åpnet apr. 02, 2020).
[117] K. Rønneberg, «Norske helsearbeidere ble sendt i viruskrigen med ubrukelige masker fra Kina. Instruksjonen: Tape igjen åpningene.», *Aftenposten*, mar. 31, 2020.
[118] D. Waghorn, «Coronavirus: Anger is growing at China over COVID-19 and its apparent cover-up attempt», *Sky News*, apr. 09, 2020. https://news.sky.com/story/coronavirus-anger-is-growing-at-china-over-covid-19-and-its-apparent-cover-up-attempt-11966539 (åpnet apr. 04, 2020).

[119] Facebook, «Removing More Coordinated Inauthentic Behavior From Iran and Russia». https://newsroom.fb.com/news/2019/10/removing-more-coordinated-inauthentic-behavior-from-iran-and-russia/ (åpnet okt. 22, 2019).
[120] Facebook, «Removing Coordinated Inauthentic Behavior From Russia», *About Facebook*, mar. 12, 2020. https://about.fb.com/news/2020/03/removing-coordinated-inauthentic-behavior-from-russia/ (åpnet mar. 24, 2020).
[121] «EEAS SPECIAL REPORT: Disinformation on the coronavirus – short assessment of the information environment», East StratCom Task Force, Brussels, mar. 2020. Åpnet: mar. 20, 2020. [Online]. Tilgjengelig på: https://euvsdisinfo.eu/eeas-special-report-disinformation-on-the-coronavirus-short-assessment-of-the-information-environment/.
[122] T. Romm, «State Department examination of Twitter found millions of coronavirus tweets pushed false information», *Washington Post*, feb. 29, 2020.
[123] T. Romm, «State Department blames 'swarms of online, false personas' from Russia for wave of coronavirus misinformation online», *Washington Post*, mar. 05, 2020.
[124] R. Heilweil, «Facebook and Twitter are struggling to get coronavirus disinformation details from the government», *Vox*, mar. 06, 2020. https://www.vox.com/recode/2020/3/6/21166982/coronavirus-conspiracy-theories-state-department-social-media-russia (åpnet mar. 24, 2020).
[125] L. H. Newman, «Russia Is Learning How to Bypass Facebook's Disinfo Defenses», *Wired*, mai 03, 2020. https://www.wired.com/story/russia-ira-bypass-facebook-disinfo-defenses/ (åpnet apr. 07, 2020).
[126] R. Fredheim, «Robotrolling 2019/2», NATO Strategic Communications Centre of Excellence, Riga, 2019.
[127] European External Action Service (EEAS), «"Finland puts Russian kids in prison" – Disinformation that Shaped the Minds of Millions», *EU vs DISINFORMATION*, aug. 06, 2018. https://euvsdisinfo.eu/finland-puts-russian-kids-in-prison-disinformation-that-shaped-the-minds-of-millions/ (åpnet nov. 11, 2019).
[128] O. Solon, «How Syria's White Helmets became victims of an online propaganda machine», *The Guardian*, des. 18, 2017.
[129] R. Zhong, S. L. Myers, og J. Wu, «How China Unleashed Twitter Trolls to Discredit Hong Kong's Protesters», *The New York Times*, sep. 18, 2019.
[130] J. Alexander, «YouTube pressured to ban Chinese state media ads that spread misinformation about protesters», *The Verge*, aug. 21, 2019. https://www.theverge.com/2019/8/21/20826568/youtube-cctv-hong-kong-china-ads-state-media-twitter-facebook (åpnet aug. 22, 2019).
[131] Facebook, «Removing Coordinated Inauthentic Behavior From Russia, Iran, Vietnam and Myanmar», *About Facebook*, feb. 12, 2020. https://about.fb.com/news/2020/02/removing-coordinated-inauthentic-behavior/ (åpnet apr. 02, 2020).
[132] Facebook, «February 2020 Coordinated Inauthentic Behavior Report», *About Facebook*, mar. 02, 2020. https://about.fb.com/news/2020/03/february-cib-report/ (åpnet apr. 02, 2020).
[133] A. Kasprak og J. Liles, «How a Pro-Trump Network Is Building a Fake Empire on Facebook and Getting Away with It», *Snopes.com*, nov. 12, 2019. https://www.snopes.com/news/2019/11/12/bl-fake-profiles/ (åpnet nov. 27, 2019).
[134] B. Nimmo *mfl.*, «Operation #FFS: Fake Face Swarm», Graphika & DFRLab, USA, des. 2009. Åpnet: feb. 06, 2020. [Online]. Tilgjengelig på: https://graphika.com/uploads/Graphika%20Report%20-%20OperationFFS_Fake_Face_Storm.pdf.

[135] I. Soares og F. Davey-Attlee, «The fake news machine: Inside a town gearing up for 2020», sep. 13, 2017. https://money.cnn.com/interactive/media/the-macedonia-story/ (åpnet feb. 06, 2020).
[136] A. Kantrowitz, «Social Media Platforms Make Their Liabilities Clear In First Russia Hearing», *BuzzFeed News*, okt. 31, 2017. https://www.buzzfeednews.com/article/alexkantrowitz/social-media-platforms-make-their-liabilities-clear-in (åpnet des. 04, 2019).
[137] E. Culliford, «Facebook announces steps to clamp down on misinformation ahead of 2020 election», *Reuters*, okt. 22, 2019. https://reuters.com/article/us-usa-election-facebook-idUSKBN1X022S (åpnet jan. 31, 2020).
[138] A. Webb, «Zuckerberg's Just Doing What He'd Have Been Forced to Do», *Bloomberg.com*, mar. 28, 2018. https://www.bloomberg.com/opinion/articles/2018-03-28/zuckerberg-s-just-doing-what-he-d-have-been-forced-to-do (åpnet des. 08, 2019).
[139] N. Tiku, «Facebook Is Steering Users Away From Privacy Protections», *Wired*.
[140] J. Constine, «A flaw-by-flaw guide to Facebook's new GDPR privacy changes», *TechCrunch*, apr. 18, 2018. http://social.techcrunch.com/2018/04/17/facebook-gdpr-changes/ (åpnet des. 08, 2019).
[141] E. Stewart, «Why #NeverWarren should make you nervous about 2020», *Vox*, jan. 15, 2020. https://www.vox.com/recode/2020/1/15/20829646/neverwarren-bernie-sanders-warren-twitter-hashtag-bots-democratic-debate (åpnet jan. 16, 2020).
[142] W. Oremus, «Facebook May Face Another Fake News Crisis in 2020», *Medium*, des. 04, 2019. https://onezero.medium.com/how-fake-news-is-still-fooling-facebooks-fact-checking-systems-fa8b0e0255b8 (åpnet des. 05, 2019).
[143] T. Davis, M. Hindman, og S. Livingston, «Facebook isn't ready for 2020», *Washington Post*. https://www.washingtonpost.com/opinions/2019/08/14/facebook-says-election-meddling-wont-happen-again-it-just-did/ (åpnet nov. 27, 2019).
[144] F. Gallagher, «Are Google, Twitter and Facebook doing enough to protect the 2020 election in the age of 'information disorder'?», *ABC News*, nov. 15, 2019.
[145] D. Alba, «How Russia's Troll Farm Is Changing Tactics Before the Fall Election», *The New York Times*, mar. 29, 2020.
[146] K. Roose, S. Frenkel, og N. Perlroth, «Tech Giants Prepared for 2016-Style Meddling. But the Threat Has Changed.», *The New York Times*, mar. 29, 2020.
[147] S. Bay og R. Fredheim, «How Social Media Companies are Failing to Combat Inauthentic Behaviour Online», NATO Strategic Communications Centre of Excellence, 2019.
[148] L. Feiner, «Twitter bans political ads after Facebook refused to do so», *CNBC*, okt. 30, 2019. https://www.cnbc.com/2019/10/30/twitter-bans-political-ads-after-facebook-refused-to-do-so.html (åpnet apr. 07, 2020).
[149] M. Kelly, «Google issues harsh new restrictions on political ad targeting», *The Verge*, nov. 20, 2019. https://www.theverge.com/2019/11/20/20975054/google-advertising-political-rules-twitter-ban-election-uk-general-2020 (åpnet nov. 21, 2019).
[150] J. Legum, «Facebook says Trump can lie in his Facebook ads», *Popular Information*, okt. 03, 2019. https://popular.info/p/facebook-says-trump-can-lie-in-his (åpnet okt. 04, 2019).
[151] C. Timberg, T. Romm, og D. Harwell, «A Facebook policy lets politicians lie in ads, leaving Democrats fearing what Trump will do», *Washington Post*, okt. 10, 2019. https://www.washingtonpost.com/technology/2019/10/10/facebook-policy-political-speech-lets-politicians-lie-ads/ (åpnet apr. 07, 2020).

[152] R. Manthorpe, «On Facebook, even tiny mistakes can have big consequences», *Sky News*, nov. 21, 2019. https://news.sky.com/story/sky-views-on-facebook-even-tiny-mistakes-can-have-big-consequences-11866011 (åpnet nov. 21, 2019).
[153] R. Cellan-Jones, «Facebook's News Feed experiment panics publishers», *BBC News*, okt. 24, 2017. https://www.bbc.com/news/technology-41733119 (åpnet des. 04, 2019).
[154] B. Paviour, «What a Facebook experiment did to news in Cambodia», *BBC News*, okt. 31, 2017.
[155] S. Dojcinovic, «Hey, Mark Zuckerberg: My Democracy Isn't Your Laboratory», *The New York Times*, nov. 15, 2017.
[156] J. Lytvynenko, «How A False Conspiracy Theory About The Texas Shooter Being An 'Antifa' Member Went Viral», *BuzzFeed News*, nov. 06, 2017. https://www.buzzfeednews.com/article/janelytvynenko/how-a-false-conspiracy-theory-about-the-texas-shooter-being (åpnet des. 05, 2019).
[157] S. Fiegerman, «In the wake of the Florida shooting, Facebook and Google spread conspiracy theories. Again.», *CNNMoney*, feb. 21, 2018. http://money.cnn.com/2018/02/21/technology/facebook-youtube-parkland-conspiracy-theories/index.html (åpnet mar. 07, 2018).
[158] S. Levin, «Las Vegas survivors furious as YouTube promotes clips calling shooting a hoax», *the Guardian*, okt. 04, 2017.
[159] T. McKay, «Once Again, Google Promoted Disinformation and Propaganda After a Mass Shooting [Updated]», *Gizmodo*, mai 11, 2017. https://gizmodo.com/once-again-google-promoted-disinformation-and-propagan-1820166979/amp (åpnet mar. 07, 2018).
[160] G. Mezzofiore, «Russian bots promote guns after Florida shooting», *CNN*, feb. 16, 2018. https://www.cnn.com/2018/02/16/us/russian-bots-florida-shooting-intl/index.html (åpnet mar. 07, 2018).
[161] T. Davidson, D. Bhattacharya, og I. Weber, «Racial Bias in Hate Speech and Abusive Language Detection Datasets», *arXiv:1905.12516 [cs]*, mai 2019, Åpnet: nov. 27, 2019. [Online]. Tilgjengelig på: http://arxiv.org/abs/1905.12516.
[162] M. Sap, D. Card, S. Gabriel, Y. Choi, og N. A. Smith, «The Risk of Racial Bias in Hate Speech Detection», i *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics*, Florence, Italy, 2019, s. 1668–1678, doi: 10/gf9wr8.
[163] L. Vaas, «Facebook Messenger may ban mass-forwarding of messages», *Naked Security*, mar. 24, 2020. https://nakedsecurity.sophos.com/2020/03/24/facebook-messenger-may-ban-mass-forwarding-of-messages/ (åpnet mar. 25, 2020).
[164] D. L. Cellan-Jones Rory, «WhatsApp restricts message-sharing», jan. 21, 2019. https://www.bbc.com/news/technology-46945642 (åpnet jan. 25, 2019).
[165] H. Walk, «Internet Content Moderation 101», *Hunter Walk*, des. 05, 2017. https://hunterwalk.com/2017/12/05/internet-content-moderation-101/ (åpnet des. 05, 2019).
[166] C. Newton, «The secret lives of Facebook moderators in America», *The Verge*, feb. 25, 2019. https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona (åpnet nov. 26, 2019).
[167] S. Levy, *Facebook: The Inside Story*. New York: Blue Rider Press, 2020.
[168] E. Dwoskin og N. Tiku, «Facebook sent home thousands of human moderators due to the coronavirus. Now the algorithms are in charge», *Washington Post*, mar. 23, 2020. https://www.washingtonpost.com/technology/2020/03/23/facebook-moderators-coronavirus/ (åpnet mar. 25, 2020).

[169] M. Vengattil og P. Dave, «Facebook contractor hikes pay for Indian content reviewers», *Reuters*, aug. 19, 2019. https://www.reuters.com/article/us-facebook-reviewers-wages-idUSKCN1V91FK (åpnet des. 09, 2019).
[170] S. Emerson, «A Former Twitter Employee Told Us How a Contractor Could Take Down Trump's Account», *Vice*, nov. 03, 2017. https://www.vice.com/en_us/article/gyjdm4/how-twitter-could-take-down-trump-account (åpnet des. 05, 2019).
[171] A. Jeffries, «Going rogue in Silicon Valley», *The Outline*. https://theoutline.com/post/2444/going-rogue-in-silicon-valley (åpnet des. 05, 2019).
[172] C. Newton, «Trump's account was deactivated after years of employees warning Twitter», *The Verge*, nov. 03, 2017. https://www.theverge.com/2017/11/3/16603620/rogue-twitter-employees-trump-account-deletion (åpnet des. 05, 2019).
[173] M. V. Ariana Tobin, «Facebook's Uneven Enforcement of Hate Speech Rules Allows Vile Posts to Stay Up», *ProPublica*, des. 28, 2017. https://www.propublica.org/article/facebook-enforcement-hate-speech-rules-mistakes (åpnet des. 06, 2019).
[174] A. Sankin, «How activists of color lose battles against Facebook's moderator army», *Reveal*, aug. 17, 2017. https://www.revealnews.org/article/how-activists-of-color-lose-battles-against-facebooks-moderator-army/ (åpnet nov. 27, 2019).
[175] K. Roose og P. Mozur, «Zuckerberg Was Called Out Over Myanmar Violence. Here's His Apology.», *The New York Times*, apr. 09, 2018.
[176] P. Mozur, «Groups in Myanmar Fire Back at Zuckerberg», *The New York Times*, apr. 05, 2018.
[177] A. Glaser, «Facebook Is Amplifying Ethnic Violence in Myanmar. Should It Leave?», *Slate Magazine*, mar. 19, 2018. https://slate.com/technology/2018/03/facebook-is-amplifying-ethnic-violence-in-myanmar-should-it-leave.html (åpnet des. 08, 2019).
[178] M. Ingram, «Casey Newton on dismantling the platforms and taking Facebook's cash», *Columbia Journalism Review*, aug. 14, 2019. https://www.cjr.org/the_new_gatekeepers/casey-newton-interview.php (åpnet nov. 27, 2019).
[179] BBC News, «Bleach peddled as autism cure on YouTube», *BBC News*, mai 21, 2019. https://www.bbc.com/news/technology-48355681 (åpnet sep. 30, 2019).
[180] M. Mali, «Critics fear Facebook fact-checkers losing misinformation fight», *TheHill*, jan. 20, 2020. https://thehill.com/policy/technology/478896-critics-fear-facebook-fact-checkers-losing-misinformation-fight (åpnet mar. 25, 2020).
[181] G. Pennycook, A. Bear, E. T. Collins, og D. G. Rand, «The implied truth effect: Attaching warnings to a subset of fake news headlines increases perceived accuracy of headlines without warnings», *Management Science*, nr. Articles in Advance, s. 1–14, 2020, doi: https://doi.org/10.1287/mnsc.2019.3478.
[182] M. Nunez, «Facebook's Fight Against Fake News Was Undercut by Fear of Conservative Backlash», *Gizmodo*, nov. 14, 2016. https://gizmodo.com/facebooks-fight-against-fake-news-was-undercut-by-fear-1788808204 (åpnet mar. 07, 2018).
[183] M. M. Grynbaum og J. Herrman, «New Foils for the Right: Google and Facebook», *The New York Times*, mar. 06, 2018.
[184] S. Frier, «He Got Rich by Sparking the Fake News Boom. Then Facebook Broke His Business», *Bloomberg.com*, des. 12, 2017. https://www.bloomberg.com/news/articles/2017-12-12/business-takes-a-hit-when-fake-news-baron-tries-to-play-it-straight (åpnet des. 05, 2019).

[185] T. Ong, «YouTube will start labeling videos from state-funded broadcasters», *The Verge*, feb. 02, 2018. https://www.theverge.com/2018/2/2/16964190/youtube-state-funded-broadcasters (åpnet des. 06, 2019).
[186] J. Valentino-DeVries, «I Approved This Facebook Message — But You Don't Know That», *ProPublica*, feb. 13, 2018. https://www.propublica.org/article/i-approved-this-facebook-message-but-you-dont-know-that (åpnet des. 06, 2019).
[187] N. Confessore og G. J. X. Dance, «On Social Media, Lax Enforcement Lets Impostor Accounts Thrive», *The New York Times*, feb. 20, 2018.
[188] Facebook Inc., «Transparency», 2019. https://transparency.facebook.com/ (åpnet mar. 25, 2020).
[189] M. Kelly, «Politicians aren't 'entirely' above the rules, Twitter says», *The Verge*, okt. 15, 2019. https://www.theverge.com/2019/10/15/20916264/twitter-trump-policies-public-figures-interest-moderation-speech (åpnet nov. 27, 2019).
[190] C. Newton, «Facebook announces new advertising disclosures days before Congressional hearings», *The Verge*, okt. 27, 2017. https://www.theverge.com/2017/10/27/16560792/facebook-ad-disclosures-political-advertising-russia (åpnet des. 04, 2019).
[191] K. Wagner, «Twitter is changing its advertising policies following Russia's election interference», *Vox*, okt. 24, 2017. https://www.vox.com/2017/10/24/16536934/twitter-change-policy-see-new-advertisements-russia-presidential-election (åpnet des. 04, 2019).
[192] Facebook Inc., «Ad Library», 2020. https://www.facebook.com/ads/library/?active_status=all&ad_type=all&country=NO&impression_search_field=has_impressions_lifetime (åpnet mar. 25, 2020).
[193] M. O. Jones, «Twitter have quietly suspended a network of between 1000-2000 troll [...]», *@marcowenjones*, des. 16, 2019. https://twitter.com/marcowenjones/status/1206672083889147904 (åpnet des. 17, 2019).
[194] I. Burrell, «BuzzFeed's 'fake news guy' Craig Silverman on digital advertising's 'tons' of bad actors», *The Drum*, feb. 20, 2020. https://www.thedrum.com/opinion/2020/02/20/buzzfeeds-fake-news-guy-craig-silverman-digital-advertisings-tons-bad-actors (åpnet apr. 01, 2020).
[195] R. Mac og Z. Hirji, «Facebook Said Politicians Can Lie In Ads. It's Taking Down Ads From Warren, Biden, And Trump For Other Reasons.», *BuzzFeed News*, okt. 15, 2019. https://www.buzzfeednews.com/article/ryanmac/facebook-warren-biden-trump-ads-take-down-profanity (åpnet nov. 27, 2019).
[196] E. Goodman og K. Kornbluh, «How Facebook shot themselves in the foot in their Elizabeth Warren spat», *The Guardian*, okt. 15, 2019.
[197] J. Kastrenakes, «Facebook will reduce reach of 'sensationalist and provocative' content», *The Verge*, nov. 15, 2018. https://www.theverge.com/2018/11/15/18097402/facebook-borderline-sensationalist-provocative-content-algorithm-changes (åpnet nov. 27, 2019).
[198] C. Newton, «YouTube just banned supremacist content, and thousands of channels are about to be removed», *The Verge*, jun. 05, 2019. https://www.theverge.com/2019/6/5/18652576/youtube-supremacist-content-ban-borderline-extremist-terms-of-service (åpnet nov. 27, 2019).
[199] K. Wagner, «Twitter changed its mind and will let Marsha Blackburn promote her 'inflammatory' campaign ad after all», *Vox*, okt. 10, 2017. https://www.vox.com/2017/10/10/16455902/twitter-marsha-blackburn-video-ad-reversal-allowed (åpnet nov. 27, 2019).

[200] C. Newton, «Twitter's CEO keeps substituting talking for doing», *The Verge*, jan. 24, 2019. https://www.theverge.com/2019/1/24/18195245/jack-dorsey-twitter-media-tour-2019 (åpnet nov. 27, 2019).
[201] W. Oremus, «The One Rule of Content Moderation That Every Platform Follows», *Medium*, jun. 11, 2019. https://onezero.medium.com/the-one-rule-of-content-moderation-that-every-platform-follows-ab6323e0e293 (åpnet des. 05, 2019).
[202] S. Jeong, «AI is an excuse for Facebook to keep messing up», *The Verge*, apr. 13, 2018. https://www.theverge.com/2018/4/13/17235042/facebook-mark-zuckerberg-ai-artificial-intelligence-excuse-congress-hearings (åpnet des. 08, 2019).
[203] C. Warzel, «Internal Emails Show Twitter Struggled To Interpret Its Own Verification Rules While Hunting Trolls», *BuzzFeed News*, des. 19, 2017. https://www.buzzfeednews.com/article/charliewarzel/internal-emails-show-twitter-struggled-to-interpret-its-own (åpnet des. 06, 2019).
[204] C. Newton, «Twitter says it will remove verification badges from accounts that violate its rules», *The Verge*, nov. 15, 2017. https://www.theverge.com/2017/11/15/16658600/twitter-verification-badge-rules-harassment (åpnet des. 05, 2019).
[205] C. Newton, «Twitter says it will judge verified users' offline behavior», *The Verge*, nov. 16, 2017. https://www.theverge.com/2017/11/16/16667668/twitter-verification-removal-judge-offline-behavior (åpnet des. 05, 2019).
[206] C. G. Weissman og C. G. Weissman, «Twitter has quietly started verifying users again», *Fast Company*, jan. 08, 2018. https://www.fastcompany.com/40514426/twitter-has-quietly-started-verifying-users-again (åpnet des. 06, 2019).
[207] C. Newton, «Twitter's verification program was a mess from the start», *The Verge*, nov. 10, 2017. https://www.theverge.com/2017/11/10/16631774/twitter-verification-kessler-milo-abuse (åpnet des. 05, 2019).
[208] N. Garun, «Twitter may eventually let anyone become verified», *The Verge*, mar. 08, 2018. https://www.theverge.com/2018/3/8/17098178/twitter-open-verification-all-users-jack-dorsey-livestream (åpnet des. 08, 2019).
[209] C. Warzel og R. Mac, «Twitter Is Still Allowing Scammers To Hijack Verified Accounts To Take People's Money», *BuzzFeed News*, feb. 23, 2018. https://www.buzzfeednews.com/article/charliewarzel/twitter-allowed-cryptocurrency-scammers-to-hijack-verified (åpnet des. 08, 2019).
[210] K. Lyons, «Twitter's messy verification process is making candidates wait», *The Verge*, feb. 21, 2020. https://www.theverge.com/2020/2/21/21147563/twitter-verified-candidates-super-tuesday-elections-2020 (åpnet feb. 27, 2020).
[211] D. O'Sullivan, «A high school student created a fake 2020 candidate. Twitter verified it», *CNN*, feb. 28, 2020. https://www.cnn.com/2020/02/28/tech/fake-twitter-candidate-2020/index.html (åpnet apr. 03, 2020).
[212] EUvsDisinfo, «"To Challenge Russia's Ongoing Disinformation Campaigns": The Story of EUvsDisinfo», *EU vs DISINFORMATION*, apr. 22, 2020. https://euvsdisinfo.eu/to-challenge-russias-ongoing-disinformation-campaigns-the-story-of-euvsdisinfo/ (åpnet apr. 23, 2020).
[213] Directorate-General for Communications Networks, Content and Technology (European Commission), *A multi-dimensional approach to disinformation: Report of the independent high level group on fake news and online disinformation*. Brussels: Publications Office of the European Union, 2018.

[214] J. Bayer, N. Bitiukova, P. Bard, J. Szakács, A. Alemanno, og E. Uszkiewicz, «Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and its Member States», *SSRN Electronic Journal*, 2019, doi: 10/ggd352.
[215] Global Engagement Center, «Global Engagement Center», *United States Department of State*, des. 19, 2018. https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/ (åpnet mar. 26, 2020).
[216] BBC News, «Unit set up to counter false coronavirus claims», *BBC News*, mar. 09, 2020. https://www.bbc.com/news/uk-politics-51800216 (åpnet mar. 26, 2020).
[217] European Parliament, «Terrorist content online should be removed within one hour, says European Parliament», *European Parliament*, apr. 17, 2019. https://www.europarl.europa.eu/news/en/press-room/20190410IPR37571/terrorist-content-online-should-be-removed-within-one-hour-says-ep (åpnet des. 08, 2019).
[218] R. Cellan-Jones, «Germany to enforce hate speech law», *BBC News*, jan. 01, 2018. https://www.bbc.com/news/technology-42510868 (åpnet des. 06, 2019).
[219] M. Rosemain og E. Pineau, «French lawmakers vote to target online hate speech in draft bill», *Reuters*, jul. 05, 2019. https://www.reuters.com/article/us-france-tech-regulation-idUSKCN1U01UQ (åpnet mar. 26, 2020).
[220] Associated Press, «Joe Biden says he's open to breaking up Facebook», *New York Post*, mai 13, 2019.
[221] T. McKay, «Kamala Harris Says 'We Have to Seriously Take a Look At' Breaking Up Facebook», *Gizmodo*, des. 05, 2019. https://gizmodo.com/kamala-harris-says-we-need-to-seriously-take-a-look-at-1834706259 (åpnet mar. 26, 2020).
[222] M. Stevens, «Zuckerberg Hates Warren's Plan to Break Up Facebook. She Doesn't Care.», *The New York Times*, okt. 01, 2019.
[223] A. Perrin og M. Anderson, «Share of U.S. adults using social media, including Facebook, is mostly unchanged since 2018», *Pew Research Center*, apr. 10, 2019. https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/ (åpnet des. 04, 2019).
[224] R. Botsman, «Dawn of the techlash», *The Guardian*, feb. 11, 2018.
[225] C. Newton, «The leader of the Time Well Spent movement has a new crusade», *The Verge*, apr. 24, 2019. https://www.theverge.com/interface/2019/4/24/18513450/tristan-harris-downgrading-center-humane-tech (åpnet mar. 26, 2020).
[226] C. Khan og D. Ingram, «Americans less likely to trust Facebook than rivals on personal data: Reuters/Ipsos poll», *Reuters*, mar. 25, 2018. https://www.reuters.com/article/us-usa-facebook-poll-idUSKBN1H10K3 (åpnet des. 08, 2019).
[227] H. Weisbaum, «Trust in Facebook has dropped by 66 percent since the Cambridge Analytica scandal», apr. 18, 2018. https://www.nbcnews.com/business/consumer/trust-facebook-has-dropped-51-percent-cambridge-analytica-scandal-n867011?icid=related (åpnet des. 03, 2019).
[228] C. Newton, «This is how much Americans trust Facebook, Google, Apple, and other big tech companies», *The Verge*, mar. 02, 2020. https://www.theverge.com/2020/3/2/21144680/verge-tech-survey-2020-trust-privacy-security-facebook-amazon-google-apple (åpnet apr. 02, 2020).
[229] Ipsos, «Ipsos SOME Tracker», Ipsos, Oslo, Q4'19, jan. 2020. [Online]. Tilgjengelig på: https://www.ipsos.com/sites/default/files/ct/news/documents/2020-01/ipsos_some_4._kvartal_2019.pdf.
[230] «Has the Coronavirus Killed the Techlash?», *Wired*.
[231] y Weinberg, archive → P., og F. C. on Twitter, «What Techlash? Virus Could Remake Industry Giants' Image», *The Information*, mar. 23, 2020.

https://www.theinformation.com/articles/what-techlash-virus-could-remake-industry-giants-image (åpnet apr. 02, 2020).
[232] N. Weiss-Blatt, «Covid-19 & The Techlash», *Medium*, apr. 01, 2020. https://medium.com/@niritweissblatt/covid-19-the-techlash-90556400fe00 (åpnet apr. 02, 2020).
[233] S. Cleland, «Coronavirus Is No Cure for Techlash», *The Precursor Blog*, mar. 27, 2020. http://www.precursorblog.com/?q=content/coronavirus-no-cure-techlash (åpnet apr. 02, 2020).
[234] W. Carless og M. Corey, «Inside hate groups on Facebook, police officers trade racist memes, conspiracy theories and Islamophobia», *Reveal*, jun. 14, 2019. https://www.revealnews.org/article/inside-hate-groups-on-facebook-police-officers-trade-racist-memes-conspiracy-theories-and-islamophobia/ (åpnet jun. 19, 2019).
[235] B. Zadrozny, «In Facebook groups, coronavirus misinformation thrives despite broader crackdown», *NBC News*, mar. 06, 2020. https://www.nbcnews.com/tech/social-media/facebook-groups-coronavirus-misinformation-thrives-despite-broader-crackdown-n1151466 (åpnet apr. 02, 2020).
[236] D. Lee, «Facebook may be 'pivoting' to something worse», *BBC News*, jul. 02, 2019. https://www.bbc.com/news/technology-48835250 (åpnet okt. 04, 2019).
[237] L. Moses, «'We're marching in the same direction': Facebook is emphasizing Groups, and publishers are following suit», *Digiday*, jan. 10, 2018. https://digiday.com/media/marching-direction-facebook-emphasizing-groups-publishers-following-suit/ (åpnet des. 06, 2019).
[238] The World staff, «Russia is trying to spread a viral disinformation campaign», *Public Radio International*, mar. 19, 2020. https://www.pri.org/stories/2020-03-19/russia-trying-spread-viral-disinformation-campaign (åpnet apr. 03, 2020).
[239] AFP-JIJI, «Russia-linked disinformation campaign fueling coronavirus alarm, U.S. says», *The Japan Times Online*, Tokyo, feb. 23, 2020.
[240] L. Markay, «Twitter Says Beijing's Coronavirus Lies Are Just Fine», *The Daily Beast*, mar. 23, 2020. https://www.thedailybeast.com/twitter-says-beijings-coronavirus-lies-are-just-fine (åpnet apr. 02, 2020).
[241] J. D'Urso, «Facebook Is Clamping Down On Coronavirus Misinformation In English, But Hoaxes Are Going Viral In Other Languages», *BuzzFeed*. https://www.buzzfeed.com/joeydurso/facebook-coronavirus-misinformation-viral-hoxes (åpnet apr. 02, 2020).
[242] M. Scott, «Social media giants are fighting coronavirus fake news. It's still spreading like wildfire.», *POLITICO*. https://www.politico.com/news/2020/03/12/social-media-giants-are-fighting-coronavirus-fake-news-its-still-spreading-like-wildfire-127038 (åpnet apr. 02, 2020).
[243] M. Richtel, «W.H.O. Fights a Pandemic Besides Coronavirus: An 'Infodemic'», *The New York Times*, feb. 06, 2020.
[244] R. Broderick og P. Dixit, «The Most Popular YouTube Videos About The Coronavirus Are Being Made In India — And They're Full Of Hoaxes», *BuzzFeed News*. https://www.buzzfeednews.com/article/ryanhatesthis/the-most-popular-youtube-videos-about-the-coronavirus-are (åpnet apr. 02, 2020).
[245] B. Smith, «When Facebook Is More Trustworthy Than the President», *The New York Times*, mar. 15, 2020.
[246] T. O. Grøtan *mfl.*, «På leting etter utenlandsk informasjonspåvirkning», SINTEF Digital, Trondheim, nov. 2019. Åpnet: feb. 10, 2020. [Online]. Tilgjengelig på:

https://www.regjeringen.no/contentassets/4d850821991746ecbcd9477a475baf73/sintef-rapport_2019-01292_gradering_apen.pdf.
[247] M. Kelly og E. Samuels, «How Russia weaponized social media, got caught and escaped consequences», *Washington Post*. https://www.washingtonpost.com/politics/2019/11/18/how-russia-weaponized-social-media-got-caught-escaped-consequences/ (åpnet nov. 28, 2019).
[248] C. Enge, «De ble lurt av NRK. Nå har Lillestrøm-elevene laget sin egen løgnkampanje.», *Aftenposten*, feb. 12, 2020.
[249] C. Newton, «Read the full transcript of Mark Zuckerberg's leaked internal Facebook meetings», *The Verge*, okt. 01, 2019. https://www.theverge.com/2019/10/1/20892354/mark-zuckerberg-full-transcript-leaked-facebook-meetings (åpnet mar. 30, 2020).
[250] A. C. Madrigal, «The Education of Mark Zuckerberg», *The Atlantic*, nov. 20, 2017. https://www.theatlantic.com/technology/archive/2017/11/the-mark-zuckerberg-theory-of-community/546290/ (åpnet des. 05, 2019).
[251] M. Zuckerberg, «A lot of you have asked what we're doing about...», *Facebook*, nov. 19, 2016. https://www.facebook.com/zuck/posts/10103269806149061 (åpnet des. 03, 2019).
[252] B. Thompson, «The Super-Aggregators and the Russians», *Stratechery by Ben Thompson*, sep. 18, 2017. https://stratechery.com/2017/the-super-aggregators-and-the-russians/ (åpnet des. 05, 2019).
[253] M. Kranzberg, «Technology and History:" Kranzberg's Laws"», *Technology and culture*, bd. 27, nr. 3, s. 544–560, 1986.
[254] K. Toyama, «Technology as amplifier in international development», i *iConference '11: Proceedings of the 2011 iConference*, Seattle, Washington, 2011, s. 75–82, doi: 10/dtr4n8.
[255] J. Edelman, «Can software be good for us?», *Medium*, jan. 19, 2019. https://medium.com/what-to-build/dear-zuck-fd25ecb1aa5a (åpnet des. 06, 2019).
[256] C. Newton, «Fresh battles over borderline content», *The Interface*, okt. 15, 2019. https://www.getrevue.co/profile/caseynewton/issues/fresh-battles-over-borderline-content-204976 (åpnet okt. 17, 2019).
[257] R. Brooks, «This Russian Campaign Turned Against Trump In The Days After The Election», *BuzzFeed News*, okt. 26, 2017. https://www.buzzfeednews.com/article/ryancbrooks/this-russian-campaign-turned-against-trump-in-the-days (åpnet des. 04, 2019).
[258] M. Williams og P. Burnap, «Antisemitic Content on Twitter», Community Security Trust, London, 2018. Åpnet: jun. 13, 2018. [Online]. Tilgjengelig på: https://cst.org.uk/public/data/file/4/2/Antisemitic%20Content%20on%20Twitter.pdf.
[259] M. L. Richter, «The Kremlin's Platform for 'Useful Idiots' in the West: An Overview of RT's Editorial Strategy and Evidence of Impact», European Values, Praha, 2017.
[260] J. S, «Never in my life have I seen so little effort — and such an ineffective campaign — receive so much publicity», *Medium*, mar. 12, 2018. https://medium.com/@indivigital01/never-in-my-life-have-i-seen-so-little-effort-and-such-an-ineffective-campaign-receive-so-much-6e7e3e078545 (åpnet des. 04, 2019).
[261] B. Nyhan, «Fake News and Bots May Be Worrisome, but Their Political Power Is Overblown», *New York Times*, feb. 13, 2018. https://www.nytimes.com/2018/02/13/upshot/fake-news-and-bots-may-be-worrisome-but-their-political-power-is-overblown.html (åpnet mar. 07, 2018).

[262] M. Elder og C. Warzel, «Stop Blaming Russian Bots For Everything», *BuzzFeed News*, feb. 28, 2018. https://www.buzzfeednews.com/article/miriamelder/stop-blaming-russian-bots-for-everything (åpnet des. 06, 2019).

About FFI

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

FFI's MISSION

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

FFI's VISION

FFI turns knowledge and ideas into an efficient defence.

FFI's CHARACTERISTICS

Creative, daring, broad-minded and responsible.

Om FFI

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

FFIs FORMÅL

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

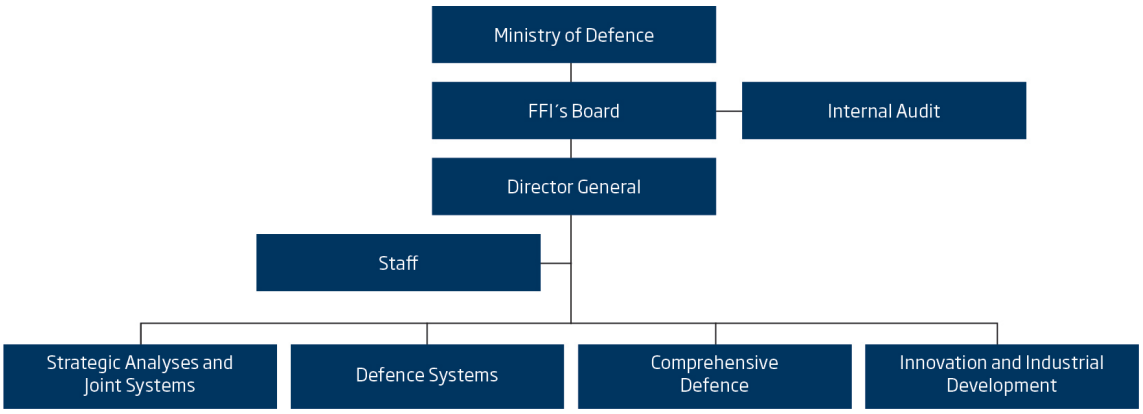
FFIs VISJON

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs VERDIER

Skapende, drivende, vidsynt og ansvarlig.

FFI's organisation



Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

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

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

Office address:
Instituttveien 20
N-2007 Kjeller

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

FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment