Fagfellevurdert

Internasjonal POLITIKK
Skandinavisk tidsskrift for Internasjonale Studier

Årgang 79, Nummer 1, side 90–113, 2021, ISSN 1891-1757, www.tidsskriftet-ip.no, Publisert mars 2021

Hvordan kan vi beskytte valg mot fremmed påvirkning?

Geir Hågen Karlsen
Forsvarets høgskole, Norge

Sammendrag

Russisk påvirkning av presidentvalget i 2016 har skapt frykt for manipulasjon av valg i Vesten. Både EU og USA forventer at trusselen vedvarer, og at nye metoder og kapasiteter utvikles. Artikkelen beskriver hva valgpåvirkning er, og hvordan slik påvirkning gjennomføres. Den gjør en systematisk gjennomgang av litteratur om beskyttelse av valg, og funnene sammenfattes i seks temaer med til sammen 38 mulige tiltak for å hindre valgpåvirkning: 1) bevisstgjøring; 2) forebygging; 3) samarbeide og koordinering; 4) beskyttende tiltak; 5) aktive mottiltak og avskrekking; 6) forskning, læring og kompetansebygging. Alle tiltak krever nøye vurdering av økonomiske, politiske, juridiske, praktiske og andre implikasjoner, samt særlig forholdet til demokrati og ytringsfrihet. Avslutningsvis påpekes fire problemstillinger som særlig aktuelle for videre vurdering: 1) bevisstgjøring via medier, samt målrettet mot partier og valgorganisasjon; 2) en helhetlig gjennomgang av trusler, sårbarhet og beskyttelsestiltak, særlig datasikkerhet; 3) forskning og utvikling; 4) avskrekking og eksponering av påvirkning. Mange tiltak er inngripende, særlig i forhold til demokrati, ytringsfrihet, sensur og selvsensur, og de viktigste utfordringer, begrensninger og kritikk mot restriktive tiltak gjennomgås. Vi må unngå at tiltak for å beskytte demokratiet i seg selv undergraver demokratiet.

Nøkkelord: Russland • informasjonspåvirkning • sosiale medier • propaganda • manipulasjon

*Kontaktinformation: Geir Hågen Karlsen, e-post: ghkarlsen@hotmail.com

Citation: Karlsen, G. H. (2021). Hvordan kan vi beskytte valg mot fremmed påvirkning? Internasjonal Politikk, 79(1), 90–113. http://dx.doi.org/10.23865/intpol.v79.2309

Bakgrunn

Etter den russiske innblandingen i det amerikanske presidentvalget i 2016 er det i vestlige land en utbredt frykt for påvirkning og manipulasjon av demokratiske valg. Det finnes en mengde litteratur, studier, rapporter og utredninger om hvordan man kan beskytte valg mot fremmed påvirkning, og hensikten med denne artikkelen er å gi en oversikt over foreslåtte eller gjennomførte tiltak for å beskytte valg. Artikkelen vil også se på utfordringene med og kritikken mot slike tiltak og til slutt peke ut noen problemstillinger som umiddelbart fremstår som aktuelle for nærmere vurdering i Norge.

Den russiske påvirkningen av presidentvalget er godt dokumentert i den såkalte Mueller-rapporten (2019), to detaljerte rapporter til Kongressen basert på omfattende datamateriale fra de store datafirmaene (DiRiesta et al., 2018; Howard et al., 2018) samt en rekke tiltaler mot russiske aktører. Senatet har utgitt totalt fem rapporter om russisk innblanding i valget og amerikanske myndigheters håndtering av innblandingen (U.S. Senate, 2019a–b, 2020 a–c). Påvirkningsaktivitetene er en kontinuerlig prosess med videreføring og utvikling av eksisterende teknikker (Francois et al., 2019), og amerikansk etterretning vurderte at både Russland, Kina og Iran var involvert i påvirkning av amerikansk politikk før presidentvalget (Director National Intelligence [DNI], 2020).

Oxford Internet Institute kartla i 2017 det de beskriver som «computational propaganda» med bruk av algoritmer, automatisering og reelle nettprofiler i Brasil, Canada, Kina, Tyskland, Polen, Taiwan, Russland, Ukraina og USA (Woolley & Howard, 2017). I en nyere rapport (Bradshaw & Howard, 2019) dokumenterte de manipulasjon av sosiale medier i hele 70 land, og de identifiserte syv land som drev manipulasjon av sosiale medier i utlandet, nemlig India, Iran, Kina, Pakistan, Russland, Saudi-Arabia og Venezuela. En trusselvurdering fra amerikansk etterretning til Senatet fremhevet Russland, Kina og Iran som aktører i forbindelse med valgpåvirkning (DNI, 2019). Av statlige aktører har vestlige sikkerhetstjenester identifisert Russland som den mest aktive aktøren for politisk påvirkning generelt (Karlsen, 2019). Kina driver også betydelig politisk påvirkning, og det er en rekke andre mindre aktører, hvor særlig Iran fremheves. Kina har vært involvert i omfattende politisk påvirkning i land som Australia (Hamilton, 2018) og New Zealand (Brady, 2017) og innblanding i det nylig avholdte valget på Taiwan (Cole, 2019), men det er så langt lite som tilsier innblanding i valg i Europa.

Det er viktig å merke seg forskjellen på illegitim informasjonspåvirkning og legitim kommunikasjonsvirksomhet. Det første vil typisk involvere villedning eller forfalskning, utnytte våre svakheter til fordel for en fremmed stat, forstyrre konstruktiv debatt eller blande seg inn i saker hvor utenlandske aktører ikke har en legitim rolle. En definisjon er at informasjonspåvirkning er påvirkningsaktiviteter gjennomført av fremmede makter eller ikke-statlige aktører for å påvirke målgruppers oppfatninger, adferd og beslutninger til fordel for den fremmede aktøren (Pamment et al., 2018). Generell påvirkning eller kommunikasjonsvirksomhet drives av mange, og er i de

fleste tilfeller normalt og legitimt. For enkelhets skyld vil denne artikkelen bruke begrepet «påvirkning», og det dreier seg da om illegitim, uønsket eller fremmedstatlig påvirkning i tilknytning til valg, som beskrevet over.

Når det gjelder påvirkning av demokratiske valg over internett og gjennom sosiale medier spesielt, er Russland klart mest aktiv. Det er imidlertid verdt å merke seg at det ikke ble dokumentert påvirkning i Sverige i 2018 eller i Tyskland i 2017. Til tross for omfattende påvirkning og hacking fra russisk side i forkant fant den tyske sikkerhetstjenesten ingen påvirkning av selve forbundsdagsvalget i 2017 (BfV, 2018, s. 270–271, 276). De tilskriver dette omfattende forebyggende tiltak og advarsler mot innblanding.

Det har vært gjentatte påstander om innblanding i valg i Storbritannia, både i forbindelse med avstemningen om uavhengighet i Skottland i 2014, EU-valget i 2016 og parlamentsvalget i 2019. Parlamentets etterretnings- og sikkerhetskomite gjennomførte en omfattende granskning av russisk påvirkning og innblanding i britisk politikk, men gav ingen klare svar på om valgene hadde blitt påvirket. Dog er det viktig å påpeke at betydelige deler av rapporten ikke ble offentliggjort (Intelligence and Security Committee of Parliament, 2020, s. 12–14).

SINTEF undersøkte kommunevalget i Norge i 2019, men fant ingen indikasjoner på fremmed påvirkning (Grøtan et al., 2019). Trusselen blir imidlertid ansett som alvorlig, og både Tyskland og Sverige iverksatte omfattende tiltak for å sikre sine valg. I Norge lanserte regjeringen i juni 2019 sin tiltaksplan (SMK, 2019) for å hindre uønsket påvirkning og hybride trusler i valggjennomføringen av kommunestyre og fylkestingsvalget.

Metode og tilnærming

Hensikten med artikkelen er å gi oversikt over aktuelle tiltak for å beskytte valg mot fremmed påvirkning. Den gjør en systematisk gjennomgang av forskning, studier, utredninger og policydokumenter som omhandler beskyttelse av valg. Dette brukes så til å identifisere 38 aktuelle tiltak gruppert i seks temaer.

Innsamlingen av materialet har vært rettet mot flere kilder. Det omfatter organisasjoner som arbeider særskilt med problematikken, som EU, NATO Centre of Excellence for Strategic Communication, Myndigheten för samhällsskydd och beredskap (MSB), Oxford Internet Institute, Oxford Technology and Elections Commission, svenske og norske kilder i forbindelse med valgene i 2018 og 2019 samt amerikanske myndigheter i forbindelse med oppfølgingen og etterforskningen av påvirkningen av presidentvalget i 2016. Videre er det gjennomført søk primært på «election» og «political», kombinert med «protection», «protecting», «influence», «interference», «intervention», «threat», «disinformation» og «manipulation». Den viktigste kilden for søk har vært Google Schoolar. Innsamlingen har vært rettet mot Europa og Nord-Amerika siden 2016. Påvirkningen av valget i 2016 var et vannskille med tanke på interesse for beskyttelse av valg. Dette er nært i tid, og gjør at deler av materialet muligens ikke har den nødvendige kritiske distanse og modenhet man kan

påregne etter hvert. Senere i artikkelen påpekes derfor behovet for en nøye vurdering av hvert enkelt tiltak i norsk sammenheng.

Det empiriske materialet gir en betydelig mengde råd om tiltak som dekker en rekke utfordringer, har varierende oppløsning, og i noen tilfeller er svært detaljerte. Kildene har også varierende tilnærminger og prioriteringer. Totalt omtaler materialet flere hundre mulige tiltak og opererer med en lang rekke kategoriseringer, grupper, områder eller temaer.

Det ble gjort en kvalitativ analyse av materialet, og innledningsvis ble det sammenfattet i 38 mulige tiltak. På grunn av det store spriket i oppløsning og tilnærming i materialet ble det gjort en vurdering for å finne hensiktsmessige formuleringer og detaljeringer av tiltakene. I praksis er det i de fleste tilfellene en aggregering av råd om tiltak med forskjellige vinklinger, prioriteringer eller oppløsning. For å få bedre oversikt ble tiltakene systematisert i seks temaer med utgangspunkt i de inndelingene som ble brukt i materialet. Vurderingen er at disse seks temaene var rimelig representative og et hensiktsmessig antall for å gi en lettfattelig oversikt.

Artikkelen beskriver først hva valgpåvirkning er, og bruker særlig valget i USA i 2016 for å illustrere hvordan slik påvirkning kan gjennomføres. Deretter går den gjennom litteratur og dokumenter som omhandler beskyttelse av valg mot fremmed påvirkning. Så sammenfattes dette i en oversikt over hva vi kan gjøre for å hindre valgpåvirkning. Det er et stort antall mulige tiltak, og for å gjøre materialet håndterlig er disse delt i seks temaer: (1) bevisstgjøring; (2) forebygging; (3) samarbeid og koordinering; (4) beskyttende tiltak; (5) aktive mottiltak og avskrekking; (6) forskning, læring og kompetansebygging. En rekke av tiltakene er inngripende og utfordrende, særlig for demokratiet og ytringsfriheten, og det tas derfor en gjennomgang av de viktigste utfordringene, begrensningene og kritikken mot slike tiltak. Avslutningsvis er det en vurdering av hvilke tiltak som kan være mest aktuelle for norske forhold, og det identifiseres fire problemstillinger som særlig peker seg ut for videre vurdering. Flere av tiltakene kan ha mange og omfattende implikasjoner, og det må tas betydelig forbehold. Det påpekes at hvert enkelt tiltak må vurderes grundig før beslutning.

Påvirkning av valg

Hva er valgpåvirkning?

Et valg er en langvarig og komplisert aktivitet, som involverer de fleste deler av samfunnet. Selve valget går i Norge over to dager, med mulighet for forhåndsstemming noen uker før. Valget er også avhengig av en del systemer for stemmegiving, telling og kommunikasjon av resultat. Det som omtales som «valgkampen» pågår fra begynnelsen av august til valget i september, mens valgkamp og påvirkning av velgernes preferanser er en kontinuerlig prosess (Karlsen, 2015). Hovedaktørene er partiene, med velgerne som målet. Kanalene partiene bruker, er medier, sosiale medier, reklame, markedsføring og direkte velgerkontakt som stander og hjemmebesøk. I tillegg til å være en kanal er mediene også selvstendige aktører, og vi har en rekke andre aktører,

som alle typer organisasjoner og bedrifter. Totalt gir dette et komplisert bilde med svært mange muligheter for påvirkning gjennom både aktører, kanaler, prosesser, temaer og valgsystemer (Burton & Shea, 2015; Ihlen et al., 2015).

Bay og Snore (2019) mener at innblanding i valg kan ha som hensikt å påvirke valgresultatet, undergrave tilliten til valget, undergrave demokratiet og det interne samholdet eller påvirke oppfatningen av et land internasjonalt. De hevder dette kan gjøres på tre måter. For det første ved å påvirke valget som en administrativ prosess, gjennom hacking av valgsystemer eller spredning av desinformasjon som undergraver tilliten til valget. For det andre ved å påvirke deltakelsen i valget, enten ved å spre desinformasjon om hvor, når og hvordan man stemmer, eller ved å undergrave viljen til å delta i valget. For det tredje ved å påvirke valget som en politisk prosess, ved cyberangrep, trolling og påvirkning i sosiale medier, lekkasjer og undergraving av politiske kandidater.

Brattberg og Maurer (2018) har en noe annen inndeling, og de mener valginnblanding kan rettes mot velgernes preferanser, deltakelsen i valget, eller valgprosessen. Dette kan skje på tre måter: gjennom informasjonsoperasjoner, eksempelvis i sosiale medier, gjennom cyberoperasjoner, eksempelvis hacking av datasystemer tilknyttet valget, eller gjennom såkalte blandede operasjoner, som inkluderer både informasjonsoperasjoner og cyberoperasjoner.

Basert på et omfattende forskningsarbeid (Pamment et al., 2018) har den svenske Myndigheten för samhällsskydd och beredskap (MSB, 2019) utviklet en håndbok for å motvirke uønsket informasjonspåvirkning. De har beskrevet seks ulike strategier som ofte benyttes i kampanjer for påvirkning:

- sosial og kognitiv hacking, som utnytter sosiale relasjoner og tankeprosesser
- falske identiteter, som skjuler den egentlige kilden til informasjonen
- teknisk utnyttelse, som bruk av falske automatiserte kontoer på sosiale medier (bots), falske videoer (deepfakes), kunstig intelligens og liknende
- desinformasjon, altså bruk av feilaktig eller manipulert informasjon
- ondsinnet retorikk, som skal villede, fordekke eller skremme andre fra å delta i debatten
- symbolske handlinger, som lekkasjer, hacking eller demonstrasjoner for å forsterke et budskap

Hvordan har valgpåvirkning vært gjennomført?

Som vist foran er det en rekke påstander om innblanding i valg, og en studie hevder endog at så mye som hvert niende valg i perioden 1946–2000 ble forsøkt påvirket av USA eller Sovjet og senere Russland (Levin, 2006). Påvirkningen av det amerikanske valget i 2016 er imidlertid unik i den forstand at det er særdeles godt dokumentert og analysert, og teknikkene og metodene illustrerer godt hvordan valgpåvirkning kan gjennomføres. Hovedaktøren var Internet Research Agency (IRA), beskrevet som en trollfabrikk i St. Petersburg. Den omtales som et sofistikert markedsføringsfirma (DiRiesta et al., 2018, s. 5) som anvender avanserte teknikker for digital påvirkning

(Howard et al., 2018, s. 6). Hovedaktiviteten til IRA er å benytte sosiale medier for påvirkning, og i begrenset grad bruker de digital annonsering. I tillegg ble det ved enkelte tilfeller gjennomført politiske markeringer og aksjoner organisert av rekrutterte amerikanske borgere. På sosiale medier opptrådte de som amerikanere, enten med falske profiler eller med stjålne identiteter. Operatørene ble instruert til å skape konflikt og støtte misfornøyde og radikale grupper. Ifølge tiltaledokumenter mener amerikanske myndigheter at det strategiske målet var, og fortsatt er, å så splid og misnøye i det politiske systemet, skape sosial og politisk polarisering, undergrave tillit til demokratiske institusjoner og påvirke amerikanske valg (U.S. District Court for the Eastern District of Virginia, 2018, s. 6).

I tillegg til IRAs informasjonspåvirkning foregikk to andre parallelle aktiviteter for påvirkning av valget i 2016. For det første omfattende kartlegging av og forsøk på inntrengning i digital valginfrastruktur og velgerdatabaser for å undergrave tilliten til valgprosessen. Ifølge etterforskningen var dette imidlertid mislykket (U.S. Senate, 2018). Den andre og mye mer alvorlige aktiviteten var hacking og lekkasje av kompromitterende e-poster og dokumenter. Clintons valgkamporganisasjon og Det demokratiske partiets systemer ble angrepet og materialet ble lekket via falske profiler som DCLeaks og Guccifer 2.0. Materialet ble så distribuert via andre profiler, mobilisering av aksjoner og velgergrupper, og spredning til mediene. Denne spredningen av kompromitterende materiale hang sammen med IRAs aktiviteter, og de forsterket hverandre (U.S. District Court for the District of Columbia, 2018).

IRAs kampanje var målrettet for å påvirke misfornøyde og radikale grupper og utnyttet derfor allerede kontroversielle og polariserte temaer som våpenlover, LHBT-relaterte saker, innvandring, bruk av sørstatsflagget og minoritetsspørsmål. En slik strategi gjorde at IRA eskalerte polariseringen. De utnyttet også situasjoner som dukket opp underveis i valgkampen, som påstander om politivold eller voldelige demonstrasjoner. Disse temaene ble utnyttet for å polarisere, for å demonisere motstandere og skape og forsterke samhold innad i tre spesifikke grupper: svarte, den politiske venstresiden og den politiske høyresiden (DiRiesta et al., 2018).

IRAs informasjonspåvirkning foregikk på et overraskende stort antall sosiale medier. Før 2016 var russisk informasjonspåvirkning i all hovedsak forbundet med Twitter, mens de under valget i USA benyttet Facebook, Instagram, Twitter, YouTube, Reddit, Tumblr, Pinterest, Vine, Grab, Meetup, VKontakte, LiveJournal, spill som Pokemon Go og musikkapper.

Det anslås at IRA nådde ut til 126 millioner brukere på Facebook, 20 millioner brukere på Instagram og 1,4 millioner brukere på Twitter, og at de lastet opp 1100 videoer på YouTube. Videre antas det at falske IRA-profiler på Instagram fikk hele 187 millioner engasjement, mot 77 millioner engasjement på Facebook. Målingen av engasjement i sosiale medier, som likerklikk og kommentarer for Instagram, kan være blåst opp med betalt aktivitet (DiRiesta et al., 2018). Enkelte av de falske IRA-profilene på Facebook og Instagram hadde over 100 000 følgere. De mest

fulgte profilene ble styrt av aktive personer som deltok i samtaler, engasjerte målgruppene og besvarte både påvirkere og medier. Automatiske profiler, såkalte bots, ble i hovedsak brukt på Twitter. Bots sørger for automatisk å tvitre overskrifter og retvitre fra andre Twitter-kontoer.

Det var utstrakt samarbeid, koordinering og deling av materiale på tvers av ulike sosiale medier, og kampanjen styrte også blogger, nettsteder og tenketanker som produserte mer nyanserte og akademiske artikler og innhold. I tillegg kjøpte de annonser på sosiale medier og nettsteder, men omfanget av dette var lite. Det ble ikke identifisert direkte forsøk på å få dekning i etablerte medier, og de analysene som til nå foreligger, har heller ikke omfattet slike medier. Likevel skal vi være klar over at etablerte medier kan plukke opp saker, desinformasjon eller påvirkningsforsøk fra sosiale medier eller nettsteder, og videreformidle dette til lesere.

Påvirkningskampanjen hadde en egen analyseavdeling som studerte den amerikanske samfunnsdebatten og aktivitet på sosiale medier, målte forskjellige parametere og drev søkemotoroptimalisering for best mulig målretting av sin kommunikasjon i forbindelse med påvirkningen av valget. De sendte også et analyseteam til USA for innhenting av informasjon tidlig i valgkampen (Mueller, 2019). Det syntes som de etter hvert opparbeidet stor forståelse av medielandskapet, aktørene og den politiske debatten, og de gav sine operatører detaljerte anvisninger for hvordan de skulle påvirke forskjellige målgrupper i den amerikanske befolkningen. I tilfelle et mer omfattende forsøk på å påvirke valg i Norge må det derfor antas at både statlige og ikke-statlige påvirkningsaktører vil ha god forståelse for konflikttemaer, kanaler og målgrupper også her hos oss.

Svenske myndigheter gjennomførte i forbindelse med Riksdagsvalget i 2018 flere undersøkelser for å avdekke mulig fremmed påvirkning. Institute for Strategic Dialogue (ISD) forsøkte å identifisere utenlandsk påvirkning av valget via internett (Colliver et al., 2018). De vurderte om russiske statsstøttede medier og automatiserte kontoer (bots) spredde desinformasjon til støtte for Sverigedemokratene eller Alternativ for Sverige. De analyserte også kampanjer fra høyreorienterte ikke-statlige aktører og undersøkte om russiske aktører deltok i internasjonale kampanjer på nettet for å sverte Sverige.

ISD fant at aktørene er involvert i sverting av Sveriges omdømme, men at målet var å påvirke internasjonale målgrupper, og ikke valget i Sverige. Det ble ikke registrert bruk av bots eller forsterkning av andres budskap fra russiske aktører. Den mest omfattende aktiviteten omhandlet undergraving av tilliten til valget gjennom påstander om valgfusk. Studien registrerte også at islamistgruppen Hizb-ut-Tahrir forsøkte å påvirke valgdeltakelsen i svenske muslimske miljøer.

I tillegg gjennomførte Myndigheten för samhällsskydd och beredskap (MSB) en analyse (Fernquist et al., 2018a) av bruken av bots på Twitter i forbindelse med valget, og en analyse (Fernquist et al., 2018b) av digitale diskusjoner i forbindelse med valget, uten at noen av disse indikerte utenlandsk påvirkning.

Oppsummert virker det som om det meste av utenlandsk valgpåvirkning har skjedd via sosiale medier. Det trenger ikke være veldig ressurskrevende, og er derfor mulig å få til for et bredt spekter av aktører. Samtidig ser vi at en stor aktør som Russland kan gjennomføre svært komplekse operasjoner med dataangrep og distribusjon av kompromitterende opplysninger, muligens også koordinert med gjennomføring av cybersabotasje mot valgsystemene.

Hva vet vi om beskyttelse av valg mot fremmed påvirkning?

Etter hvert som trusselen har blitt åpenbar, særlig etter valget i USA i 2016, har beskyttelse av demokratiske valg blitt et aktuelt tema. Denne artikkelen vil gi oversikt over internasjonal og norsk forskning, studier og utredninger som er mest relevant for beskyttelse av valg. Videre omtales et betydelig antall planer og policydokumenter, særlig fra EU, som er relevante for temaet. I denne sammenheng er det viktig å være oppmerksom på at planer og policydokumenter i tillegg til å være basert på forskning også er påvirket av forskjellige politiske føringer.

Det finnes også omfattende forskning som er relevant for en bredere forståelse, men som ikke vil dekkes i denne artikkel. Det gjelder særlig forskning om sosiale medier og polarisering, fremmede staters påvirkning av vestlig politikk generelt, hvorav valgpåvirkning bare er en del av en rekke kanaler og metoder, samt litteratur om desinformasjon, som ofte overlapper med utfordringene knyttet til valgpåvirkning.

Forskning og studier om beskyttelse av valg

I håndboken *Countering information influence activities – a handbook for communicators* har den svenske Myndigheten för samhällsskydd och beredskap (MSB, 2019), gitt detaljerte råd for håndtering og imøtegåelse av informasjonspåvirkning generelt, og ikke bare i forbindelse med valg. Håndboken er delt i tre deler: bevissthet om, identifisering av og kontring av informasjonspåvirkning. I forbindelse med kontring av informasjonspåvirkning legger de særlig vekt på forberedelser, herunder bevisstgjøring, bygging av tillit gjennom kommunikasjon og grundige risiko- og sårbarhetsanalyser.

Brattberg og Maurer (2018) har i *Russian election interference – Europe's counter to fake news and cyber attacks* gjennomgått tiltak og erfaringer fra Nederland, Frankrike, Storbritannia, Tyskland og Sverige. De deler mottiltak inn i fem kategorier: juridiske, tekniske, policymessige, operasjonelle samt bevissthet og utdanning, og de påpeker samtidig at det er essensielt med en læringsprosess over tid. De gir 14 konkrete forslag til tiltak, uten å kategorisere disse, samt ytterligere 11 tiltak spesifikke for USA. De mest relevante er inkludert i den etterfølgende oversikten over mulige tiltak.

Natos Center of Excellence for Strategic Communications har i studien *Protecting elections: A strategic communications approach* (Bay & Snore, 2019) sett på tiltak for å beskytte valg i Sverige, Finland, Estland og Lativa. Deres tilnærming

er basert på MSBs (2019) og Brattberg og Maurers arbeid. Studien anbefaler å starte med en kartlegging av informasjonsmiljøet og deretter trusselvurdering, og så vurdere egne kapasiteter opp mot risikoen. Forfatterne påpeker at beskyttelse av valg med svært mange aktører er krevende, og det er behov for både forebyggende og skadebegrensende tiltak. Basert på erfaringene fra de fire landene oppsummerer de en rekke tiltak under seks hovedpunkter: kartlegging, koordinering, beskyttelse og motstandsdyktighet, samarbeid og partnerskap, deteksjon og overvåkning samt utdanning og bevissthet.

Kolga et al. (2019) går i *Russia-proofing your election* gjennom påvirkning av valg i Sverige, Estland, Latvia, Litauen, Frankrike, Tyskland og Canada og fremmer en rekke forslag for å beskytte valget i Canada i 2019. Disse omfatter samarbeid med sosiale medieselskaper, datasikkerhet, regulering av utenlandske medier, avskrekkende kommunikasjon mot potensielle motstandere, internasjonalt samarbeid og endring av sikkerhetslovgivning for å muliggjøre cyberangrep mot de som eventuelt angriper valget. Mange av forslagene er svært detaljerte og ofte betydelig mer restriktive eller inngripende enn det de foregående anbefaler.

Det amerikanske senatet har utgitt totalt fem rapporter om russisk innblanding i valget og amerikanske myndigheters håndtering av innblandingen. Rapportene omhandler russiske intervensjoner mot valginfrastruktur (U.S. Senate, 2019a), bruk av sosiale medier (U.S. Senate, 2019b), amerikanske myndigheters håndtering (U.S. Senate, 2020a), gjennomgang av etterretningsvurderinger (U.S. Senate, 2020b) og vurdering av trusler og sårbarheter (U.S. Senate, 2020c). Den første anbefaler en lang rekke tiltak for amerikanske forhold i fire kategorier: avskrekking, deling av informasjon om trusler, datasikkerhet i valgsystemene og sikring av stemmegivning og -telling. Den andre har en lang rekke tiltak rettet mot sosiale medier-selskapene, lovgivning, bevisstgjøring og koordinering. Den tredje anbefaler bedre nasjonal koordinering og internasjonalt samarbeid, og forberedelser for informasjonskrig med klargjorte offensive tiltakspakker. Den siste anbefaler forsterket overvåkning av fremmede aktører, bedre rådgivning til og beskyttelse av både kandidater og de som gjennomfører valget, og styrking av etterretnings- og sikkerhetstjenestene.

Andre har også gitt anbefalinger som overensstemmer med de foregående, som for eksempel undersøkelsen av det svenske valget (Colliver et al., 2018) og en komparativ analyse av russisk innblanding i valg (Lamond & Dessel, 2019).

Natos Center of Excellence har i *Government responses to malicious use of social media* (Bradshaw et al., 2018) gitt en oversikt over anbefalte eller gjennomførte tiltak mot manipulasjon av sosiale medier i 43 land. Disse er samlet i fire grupper: tiltak rettet mot sosiale medier-selskap, tiltak mot angripere, tiltak rettet mot innbyggere, sivilsamfunn og medier samt tiltak for å bygge statlige kapasiteter mot manipulasjon. De påpeker også at det ikke finnes noen enkle løsninger på utfordringene, og at mange av tiltakene er problematiske. De anbefaler en dreining fra kontroll og kriminalisering til mer fokus på personvern og åpenhet om algoritmer og annonsering.

Oxford Technology and Elections Commission har i *A report of anti-disinformation initiatives* (Robinson et al., 2019) gitt en oversikt over en lang rekke tiltak mot desinformasjon og manipulasjon globalt. Rapporten påpeker at tiltak mot desinformasjon ofte er kontroversielle eller krevende å innføre, og at de kan brukes for å få kontroll over medier og hindre fri debatt og ytringsfrihet. I en annen rapport, *Literature review on elections, political campaigning and democracy* (Thwaite, 2019), har OxTec gjennomgått litteratur om illegitim digital påvirkning av valg. Rapporten påpeker at vi fortsatt vet lite om effekten av slik påvirkning, og fremhever særlig behovet for å ivareta personvern.

Teknologirådet har i en kortrapport (Barland & Tennøe, 2019) foreslått spilleregler for åpenhet om mikromålretting og merking av politisk reklame, og de gir også en oversikt over tiltak mot manipulering internasjonalt. Datatilsynet har i en rapport (2019) undersøkt bruken av digital målretting av politiske budskap generelt og i Norge spesielt, og har utformet seks råd om forsvarlig bruk av digital målrettingsteknologi. Rådene fokuser på utvikling av felles normer og ivaretakelse av personvern. De påpeker særlig at mikromålretting kan gjøre det politiske systemet sårbart for manipulering, bidra til diskriminering og gå ut over legitimiteten og tilliten til den demokratiske prosessen.

Bente Kalsnes har i sin bok *Falske nyheter – løgn, desinformasjon og propaganda i den digitale offentlighet* (2019) gått grundig gjennom hva falske nyheter og desinformasjon er, og hvordan de skapes og deles. Hun gir også en del råd om håndtering av utfordringene. Hun gjennomgår aktuell litteratur, beskriver hvordan faktasjekker bør gjennomføres, og anbefaler tiltak innen fire områder: media, teknologi og plattformer, lovverk samt skolering i kritisk medie- og informasjonsforståelse og kildekritikk.

Konsulentselskapet Proactima (Valdal et al., 2019) har levert rapporten *Sikkerheten i demokratiske prosesser i Norge* til valglovutvalget. De foreslår ni regulatoriske tiltak, hovedsakelig opp mot hjemler og sikkerhetskrav, samt 20 andre mulige tiltak, og påpeker også utfordringer for åpenhet og ytringsfrihet.

Planer og policydokumenter

EU har utviklet en *Action plan against disinformation* (2018a) for å styrke arbeidet mot desinformasjon. Planen omfatter fire pilarer: for det første styrking av evnen til å oppdage, analysere og eksponere desinformasjon, for det andre styrket koordinering og felles respons, for det tredje mobilisering av privat sektor mot desinformasjon og for det fjerde styrket bevissthet og motstandsdyktighet. Tiltakene følges opp med jevnlig rapportering (European Commission, 2019).

EU har også foreslått tiltak innen fem områder for å sikre frie og rettferdige valg: bedre samarbeid, åpenhet om politisk annonsering, regler for beskyttelse av personlige data, datasikkerhet samt mulighet for bøtelegging av politiske partier for personvernbrudd (European Commission, 2018b). I samarbeid med sosiale medierfirmaer og markedsføringsbransjen har EU også laget en *Code of practice on disinformation* (European Commission, 2018c), hvor de har gitt detaljerte råd mot

desinformasjon innen fem områder. Disse er kontroll med annonsering, regler for politiske annonser, sikring av plattformenes integritet for å unngå misbruk, tiltak for å sikre brukernes forståelse og innflytelse, samt tiltak for å styrke forskning om desinformasjon og politisk annonsering. Planen omfatter også forslag til beste praksis for markedsføringsbransjen.

I etterkant av parlamentsgranskingen av russisk påvirkning har den britiske regjeringen etablert sitt *Defending Democracy*-program, styrket arbeidet mot desinformasjon og iverksatt tiltak for å kontre fremmedstatlig påvirkning og ivareta valgsikkerhet. Programmet har fire prioriteter: sikring av demokratiske prosesser, systemer og institusjoner; beskyttelse av valg; oppmuntre til demokratisk deltakelse; fremme faktabasert debatt. Programmet omfatter en rekke tiltak som er på linje med det som er anbefalt i litteraturen foran (The Prime Minister, 2020).

Regjeringen lanserte i juni 2019 sin tiltaksplan (SMK, 2019) for å hindre uønsket påvirkning og hybride trusler i valggjennomføringen av kommunestyre og fylkestingsvalget. Den omfattet ti tiltak, blant annet tverrsektorielt samarbeid om risikoanalyser, informasjon til kandidater, partier og mediene, beredskapsordning for hacking av sentrale myndigheters profiler på sosiale medier, sikring av valggjennomføring og manuell telling av stemmer, kartlegging av mulig påvirkning samt avdekking av falske nyheter.

Som en del av regjeringens tiltaksplan mot påvirkning av valg har Medietilsynet, Faktisk.no og Landslaget for lokalaviser (LLA) gått sammen om en kampanje (Medietilsynet, 2019a) for å øke bevissthet om falske nyheter og desinformasjon. Kampanjen omfatter filmer og annonser som spres via aviser og sosiale medier, samt en quiz og konkrete råd om hvordan falske nyheter kan avdekkes. Medietilsynet har påvist at eldre er dårligst til å gjenkjenne falske nyheter, og at unge ofte ser det de mener er falske nyheter, men sjelden sjekker sakene (Medietilsynet, 2020).

Hva kan vi gjøre for å beskytte valg mot fremmed påvirkning?

Litteraturen og dokumentene som er omtalt foran gir en lang rekke råd som dekker et bredt spekter av utfordringer, har varierende oppløsning og er til dels svært detaljerte. De ulike kildene har også ulike tilnærminger og prioriteringer, og det er derfor nødvendig å strukturere og systematisere for å få en håndterbar sammenfatning av hensiktsmessige tiltak for å beskytte våre demokratiske valg mot fremmed påvirkning. Rådene favner bredt, fra undervisning i medieforståelse i skolen til sikkerhetslovgivning som tillater cyberangrep mot land som blander seg inn i valg. En del av rådene er tilpasset behov, regelverk og utfordringer i spesifikke land og er således ikke relevante for Norge. Andre må justeres for å være relevante.

Denne oversikten over tiltak må sees som en sammenfatning av mulige tiltak, hentet fra en omfattende litteratur om temaet, og ikke som konkrete råd om hva som bør gjennomføres. Aktuelle tiltak må videre vurderes nøye for å avklare økonomiske, politiske, juridiske, praktiske, sikkerhetspolitiske og andre implikasjoner, samt ikke

minst forholdet til demokrati og ytringsfrihet. Det presiseres at den etterfølgende gjennomgangen omhandler anbefalinger fra litteraturen og dokumentene, og ikke er basert på forfatterens eget syn. I konklusjonen identifiseres fire problemstillinger som utpeker seg som særlig aktuelle for videre vurdering i Norge.

De mulige tiltakene er delt inn i seks delvis overlappende temaer:

- bevisstgjøring
- forebygging
- samarbeid og koordinering
- beskyttende tiltak
- aktive mottiltak og avskrekking
- forskning, læring og kompetansebygging

For oversiktens skyld er de viktigste tiltakene i disse seks temaene gjengitt i tabell 1.

Tabell 1. Oversikt over mulige tiltak for beskyttelse av valg

Tema	**Tiltak**
Bevisstgjøring	
	Informasjon via medier
	Omtale av trussel fra myndigheter og sikkerhetstjenester
	Forskningskommunikasjon
	Oppfordre og bidra til mediedekning og debatt
	Direkte informasjon til de som gjennomfører valg, kandidater og partier
	Bredt anlagt opplæring og kampanjer for økt kunnskap og bevissthet
	Opplæring i nettvett
	Holdningskampanjer mot netthets
Forebygging	
	Trusselvurderinger
	Risiko- og sårbarhetsanalyser
	Krav til valgsystemer og -infrastruktur
	System for overvåkning og analyse av digital informasjonspåvirkning
	Rapporteringsmekanismer og varslingssystem
	Kapasitet til analyse av påvirkningsforsøk
	Involvering av medier
Samarbeid og koordinering	
	Bygge videre på tiltak under bevisstgjøring
	Klare roller, ansvar, myndighet og samarbeidsrutiner mellom offentlige organer
	Mekanismer for støtte til lokale valgorganisasjoner
	Institusjonalisere samarbeid med medier og partier
	Samarbeid med de internasjonale sosiale mediebedriftene
	Åpenhet om algoritmer og tilgang til forskning på digitale plattformer
	Samarbeid med allierte land og internasjonale kompetansemiljøer

(*Fortsatt*)

Tabell 1. (*Fortsatt*)

Tema	Tiltak
Beskyttende tiltak	
	Opplæring i datasikkerhet
	Støtte til partier, kandidater og valgorganisasjoner
	Sikre dataløsninger med backup og alternative systemer
	Bedre personvern
	Mulighet for sanksjoner
	Normer for mikromålretting og arkivering av annonser
	Åpenhet om finansiering av valgkamp
	En rekke regulatoriske tiltak ifm. valggjennomføring
Aktive mottiltak og avskrekking	
	Advarsler om at påvirkning blir overvåket
	Eksponering av påvirkningsforsøk
	Etablere enheter for nasjonal beskyttelse mot påvirkning
	Lovgivning og kapasitet til cyberangrep mot aktører som påvirker valg
Forskning, læring og kompetansebygging	
	Forskning på valgpåvirkning, sosiale medier og trusler
	Forskning på teknologi og metoder
	Bidrag i overvåkning, analysearbeid og trusselvurderinger
	Utviklingsarbeid og kompetansebygging i offentlig sektor

Bevisstgjøring

Den grunnleggende tanken er å gjøre myndigheter, befolkning og medier oppmerksomme på utfordringene, og at kunnskap og informasjon bidrar til å redusere både spredningen og effekten av desinformasjon og påvirkning. Bevisstgjøring fremheves gjennomgående i litteraturen (se særlig Bay & Snore, 2019; Brattberg & Maurer, 2018; European Comission, 2018a; Medietilsynet, 2019a; MSB, 2019) og kan gjøres med informasjon via medier, omtale av trusselen fra offentlige myndigheter, sikkerhetstjenester, forskningsmiljø og andre som har relevant informasjon, og ved å oppfordre til debatt om temaet. Aktuelle temaer er klargjøring av de viktigste truslene, eksempler på innblanding i valg fra andre steder, hvilke tiltak som er planlagt, og hvordan velgerne kan ha et bevisst forhold til informasjon og selv identifisere mistenkelig informasjon. Bevissthet og omtale vil også kunne bidra til rapportering av påvirkningsforsøk. Slike informasjonstiltak og kommunikasjon via redaksjonell omtale er rimelige, kan nå mange og er i hovedsak ukontroversielle. Man bør imidlertid sørge for god dokumentasjon og begrunnelse av truslene, slik at man bevarer troverdighet over tid og ikke blåser trusselen ut av proporsjoner.

Bevisstgjøring av aktørene som er direkte involvert i valg, er trolig et kosteffektivt, målrettet og lite kontroversielt tiltak. Dette kan omfatte bevisstgjøring av

og informasjon til de som er engasjert i avvikling av valg, forebygging av påvirkning, samt informasjon til kandidater og partier. Flere fremhever at partiene har behov for data- og sikkerhetsrådgivning. Tiltakene vil også henge nøye sammen med tiltak for å bedre samarbeid og koordinering mellom de mange aktørene som er involvert i valgavvikling.

Et mer omfattende alternativ er bredt anlagte tiltak mot større målgrupper. Dette kan være tiltak, opplæring eller kampanjer for å øke kunnskap om demokratiske prosesser, bevissthet om falske nyheter, desinformasjon, kildekritikk og medieforståelse, opplæring i nettvett i bred forstand og holdningskampanjer mot netthets. Deler av disse tiltakene kan være aktuelle for langvarig satsing i skolen. Medietilsynets kartlegging viser at eldre er dårligst til å gjenkjenne falske nyheter, og bevisstgjøring av disse er et aktuelt tiltak. Disse tiltakene vil være svært ressurskrevende og kreve langvarig innsats. Det er også et spørsmål om hvor mye myndigheter skal påvirke før det er et problem for sensur og ytringsfrihet.

Forebygging

Forebygging starter naturlig nok med en kartlegging og utarbeidelse av trusselvurderinger og risiko- og sårbarhetsanalyser (Bay & Snore, 2019; MSB, 2019). Disse danner grunnlag når man skal utarbeide beredskapsplaner og kommunikasjonsplaner med forberedte budskap for håndtering av aktuelle utfordringer. Litteraturen vektlegger at man bør gå gjennom og øve på planene, og at man også gjennomfører øvelser i krisehåndtering.

Det anbefales også at valgsystem og infrastruktur anses som skjermingsverdige, det vil si at de ifølge sikkerhetsloven har avgjørende betydning for grunnleggende nasjonale funksjoner (Valdal et al., 2019). Dette innebærer at de er underlagt spesielle krav til testing og beskyttelse. I tillegg bør systemene stresstestes for å sikre at de tåler aktuelle belastninger. Man bør også kartlegge utfordringer og identifisere kosteffektiv forebygging.

Et system for og kompetanse til å overvåke og analysere ulike former for digital informasjonspåvirkning fremheves som helt avgjørende. Det bør etableres rapporteringsmekanismer og varslingssystem som involverer myndigheter, internasjonale datafirmaer, medier og sivilsamfunn, slik at påvirkningsforsøk kan identifiseres og følges opp. Videre bør det etableres tilstrekkelig kapasitet til å analysere påvirkningsforsøk og følge opp med mottiltak. Disse tiltakene vil trolig kreve bidrag fra et antall departementer, etater, hemmelige tjenester og forsknings- og utviklingsmiljøer, og de bør sees i sammenheng med tiltak under samarbeid og koordinering samt forskning, læring og kompetansebygging.

Mediene er viktige aktører som bør involveres og bevisstgjøres. Det kan bidra til både kritisk journalistikk og beredskap mot påvirkning. Som et eksempel samarbeidet mediene i Frankrike under presidentvalget om å ikke publisere materiale basert på hacking eller desinformasjon. Litteraturen anbefaler å legge til rette for bred, faktabasert kvalitetsjournalistikk. Enkelte påpeker behov for kompetansebygging og

verktøy, slik at journalister lettere kan drive faktasjekk. For å sikre tilliten til mediene er det ønskelig med åpenhet om journalistiske prosesser. Enkelte land regulerer eller stiller krav om registrering av utenlandske medier. Tiltak som har med mediene å gjøre, favner bredt og bør vurderes nøye opp mot kostnader, medieuavhengighet og mulig sensur.

Samarbeid og koordinering

Tiltak her bygger på det som er nevnt under bevisstgjøring. Valg involverer en lang rekke aktører og offentlige myndigheter på forskjellige nivåer. Det bør være klare roller, ansvar, myndighet og samarbeidsrutiner mellom alle involverte offentlige organer – nasjonalt og lokalt. Det bør også være mekanismer for å støtte lokale valgorganisasjoner fra et mer spesialisert og kompetent sentralt nivå. Man bør også institusjonalisere samarbeid mellom alle aktører som er involvert i valgavvikling, herunder partiene og mediene, som omtalt over (Bay & Snore, 2019; European Comission, 2018a; Valdal et al., 2019). Utfordringene med roller og ansvar ble tydelig adressert i den britiske parlamentsrapporten om russisk innblanding og påvirkning, hvor de uttrykte at «det har vært overraskende vanskelig å fastslå hvem som har ansvar for hva» (Intelligence and Security Comittee of Parliament, 2020, min oversettelse).

Videre bør det etableres hensiktsmessige samarbeidsformer med de store internasjonale sosiale mediene for å håndtere desinformasjon, målrettet annonsering, tyveri av kontoer og annen manipulasjon, samt rutiner for varsling og informasjonsutveksling. EU har utviklet sin Code of Practice (European Commission, 2018c), som kan danne standard for dette samarbeidet. Enkelte, som Kolga et al. (2018, s. 27–28), foreslår betydelig strengere krav til sosiale medier enn EU. Åpenhet om funksjoner og algoritmer, samt tilgang til digitale plattformer, er også ønskelig for forskning på og analyse av påvirkning i sosiale medier.

Det bør også etableres samarbeid med allierte land om trusler, varsling og mottiltak og med internasjonale kompetansemiljø som EUs European External Action Service/East StratCom, Natos Centre of Excellence for Strategic Communication og det europeiske Centre of Excellence on Countering Hybrid Threats i Finland. Dette vil kunne bidra sterkt til erfaringsutveksling, læring og kompetansebygging.

Beskyttende tiltak

Det er svært mange beskyttende tiltak som er mulige, og de vil utvilsomt kreve prioritering og nøye vurdering. Datasikkerhet fremheves gjennomgående som svært viktig, og en lang rekke tiltak er aktuelle (European Comission, 2018b; Kolga et al., 2019; US Senate, 2019a). Særlig nevnes opplæring i datasikkerhet for alle involverte aktører og støtte til partier, kandidater og valgorganisasjon mot dataangrep. Av tekniske tiltak fremheves etablering av sikre løsninger med backup og uavhengige alternative løsninger, særlig for systemene som brukes til avvikling av valget og stemmetelling. Det diskuteres også strengere regulatoriske tiltak og forbud, men man er samtidig klar over at disse ofte har problematiske sider.

Personvern er et annet viktig område, og data som er relevant for valgavvikling bør beskyttes bedre. Dette vil innebære regulering av sosiale mediers bruk av persondata, etablering av felles normer for mikromålretting og ivaretakelse av personvern samt mulighet for sanksjonering og bøtelegging av brudd. EU har også en lang rekke mer detaljerte tiltak i sin handlingsplan. Internasjonalt samarbeid kan være aktuelt gjennom EUs Network of Cybersecurity Competence Centres.

Mikromålretting betyr at budskap, oftest basert på data fra sosiale medier, er spesielt tilpasset små grupper eller endog enkeltpersoner. Temaet ble aktualisert etter den mye omtalte Cambridge Analytica-skandalen, hvor analysefirmaet skulle ha brukt store mengder persondata uten nødvendig tillatelse til mikromålretting før presidentvalget i 2016. Både EU og andre fremhever behov for åpenhet om mikromålretting av kommunikasjon og målgrupper, merking og arkivering av annonser og mer åpenhet om finansiering av mikromålretting og valgkamp generelt.

EU og andre har foreslått en lang rekke regulatoriske tiltak. I Norge har Proactimas rapport (Valdal et al., 2019) til valglovutvalget gått grundig gjennom temaet og fremmet en rekke tiltak. En del er tekniske og praktiske forhold, som regulering av valggjennomføring og mulighet for tilsyn, forslag om å legge valggjennomføring under sikkerhetsloven, krav om to uavhengige tellinger, rolleavklaring mellom lokale og sentrale aktører, obligatorisk bruk av valgadministrasjonssystemet, beredskapshjemmel i valglovgivningen, opplæring og bevisstgjøring av valgmedarbeidere samt kontroll med valgmedarbeidere for å unngå innsidetrussel. Andre tiltak er mer prinsipielt eller demokratisk utfordrende, som regler mot kjøp og salg av falske klikk, forbud mot utenlandsk finansiering av valgkamp, utvidelse av definisjonen av ulovlig materiale eller regler mot spredning av falsk informasjon.

Aktive mottiltak og avskrekking

Det er også aktuelt med aktive mottiltak for å avskrekke aktuelle aktører. Det mest aktuelle tiltaket er advarsler fra norske myndigheter om at påvirkning vil bli overvåket og eksponert. Dette innebærer at man offentlig går ut og informerer om at man analyserer og overvåker mulige påvirkningsforsøk, og at man vil eksponere eventuelle forsøk. Tiltaket er i seg selv relativt enkelt og billig, men krever aktiv involvering fra politisk ledelse for å være troverdig. For at dette skal fungere effektivt, vil det trolig være behov for konseptuell utvikling og forståelse av avskrekking som virkemiddel, særlig med tanke på håndtering i cyberdomenet (Kristiansen & Hoem, 2019). Tiltaket vil også ha stor medieinteresse, og kan dermed nå mange. God dokumentasjon av eventuelle forsøk vil være avgjørende for å bevare troverdighet. Det forutsetter også at man har en troverdig overvåkning, og at det er politisk vilje til å følge opp påvirkningsforsøk. Slik offentlig eksponering av desinformasjon og påvirkning kan bidra til både avskrekking og bevisstgjøring.

Ved siste valg i Sverige kritiserte statsminister Löfven russiske påvirkningsforsøk og uttalte tydelig at de ville overvåke og nådeløst eksponere videre forsøk

(Brattberg & Maurer, 2018, s. 22). Likeledes vurderte tysk sikkerhetstjeneste at forbundsdagsvalget i 2017 forløp uten nevneverdig innblanding, nettopp fordi de hadde kunnskap om utfordringene og iverksatte omfattende mottiltak (BfV, 2018, s. 270–271, 276). Den amerikanske justisministeren, sammen med en rekke etatssjefer, advarte offentlig mot innblanding i valget i 2020 (Cybersecurity and Infrastructure Security Agency, 2019), og den amerikanske cyberstrategien fastslår at de forbeholder seg retten til å bruke alle midler mot fremmed innblanding (The White House, 2018). Senatet har senere bekreftet og forsterket denne tilnærmingen (U.S. Senate, 2020a).

En rekke land, samt EU, har etablert egne enheter for å beskytte landets velgere mot påvirkning utenfra (Bradshaw et al., 2018). I Sverige anbefalte en offentlig utredning sommeren 2020 etablering av en ny myndighet som skal ha ansvaret for landets psykologiske forsvar, og saken er til behandling i regjeringen (Statens offentliga utredningar, 2020). Det kan derfor være aktuelt å vurdere nasjonale kapasiteter for beskyttelse mot fremmed påvirkning, enten som en egen enhet eller gjennom samarbeid mellom eksisterende etater. Enkelte anbefaler også nasjonale kapasiteter og lovgivning som tillater bruk av cyberangrep mot aktører som påvirker valg. Det britiske parlamentets etterretnings- og sikkerhetskomite omtaler i sin rapport i detalj hvordan Storbritannia vi gå offensivt til verks (Intelligence and Security Comittee of Parliament, 2020, s. 5–8). Disse tiltakene er potensielt kostbare og må avklares grundig mot eksisterende kapasiteter, ansvarsforhold og lovgivning, og de kan dessuten ha sikkerhetspolitiske implikasjoner. Avskrekking i det digitale rom er også komplekse og krevende operasjoner med viktige teknologiske og kulturelle aspekter (Gjesvik & Øverbø, 2019).

Forskning, læring og kompetansebygging

Sikring og beskyttelse av valg i et digitalt samfunn som Norge er komplekst og omfatter mange aktører, og i løpet av kort tid har det blitt aktualisert med en rekke nye teknologiske utfordringer og trusler. Forskning og utviklingsarbeid er nødvendig for å bygge tilstrekkelig kompetanse og forståelse for utfordringene. Det vil også være en forutsetning for og en integrert del av analysearbeidet som gjøres for å forstå og overvåke truslene (Bay & Snore, 2019; Bradshaw et al., 2018; Brattberg & Maurer, 2018; European Commission, 2018b). Utfordringene med digital påvirkning av valg er nye, og kompetansen på temaet er begrenset. Dette forsterkes av at valg omfatter svært mange aktører. De mest åpenbare temaene er forskning på valgpåvirkning generelt, påvirkning over nettet og i sosiale medier spesielt og den løpende endringen i trusler, teknologi og metoder. En ny studie fra FFI anbefaler forskning på mulige aktører, målgrupper og sosiale medier som kan bedre situasjonsforståelsen til beslutningstagere i en tverrsektoriell totalforsvarsramme (Bergh, 2020). Forskning og utviklingsarbeid vil også kunne bidra direkte til bevisstgjøring og dermed forebygging. Påvirkning av valg må sees som en kontinuerlig prosess hvor aktørene stadig bruker nye metoder. Forskning og utvikling bør derfor pågå kontinuerlig for å bygge

tilstrekkelig forståelse. Tiltakene er økonomisk skalerbare, trolig ikke veldig kostbare, og bør anses som ukontroversielle.

Utfordringer, begrensninger og kritikk

En rekke av tiltakene er inngripende, restriktive og utfordrende, særlig for demokratiet og ytringsfriheten, og de utgjør en risiko for sensur eller selvsensur. Litteraturen omtaler et stort antall mulige tiltak, og mange har direkte eller indirekte konsekvenser. Ofte er de negative eller utfordrende konsekvensene tydelige, mens effekten av tiltakene er usikre. Det er avgjørende å finne en balanse mellom trusler, tiltak og konsekvenser, og man bør i den sammenheng ha en edruelig tilnærming til hvor alvorlig trusselen egentlig er.

Europakommisjonens ekspertgruppe advarte på det sterkeste mot å forby falske nyheter (Kalsnes, 2019, s. 132). De er bekymret for at tiltakene for å bekjempe falske nyheter og desinformasjon i land som Tyskland, Frankrike, Italia og Irland skal begrense ytringsfriheten og føre til selvsensur. MSB har gjennomført en detaljert studie (Winther, 2016) om hvilke rammer den svenske ytringsfrihetsloven setter for tiltak mot påvirkningskampanjer fra fremmede makter.

European Parliamentary Research Service (2019) påpeker at det er en risiko for at kommunikasjonsteknologien blir mer og mer politisert, og at det blir iverksatt flere regulatoriske tiltak. Dette kan igjen lede til en nedkjølingseffekt på demokrati og ytringsfrihet, ved at folk endrer adferd fordi de frykter overvåkning (Lysne et al., 2016). De advarer derfor mot rask og lite gjennomtenkt regulering og anbefaler å jobbe med åpenhet og ansvar, bevissthet og større investering i digital infrastruktur.

Lysne-utvalget (Lysne et al., 2016) utredet konsekvensene av Etterretningstjenestens mulige tilgang til elektronisk kommunikasjon. De identifiserte en rekke faktorer som talte imot slik overvåkning, og disse er trolig relevante for regulatoriske tiltak som skal beskytte valgprosessen. De omtalte formålsglidning, hvor formålene med tiltakene utvides, og den nevnte nedkjølingseffekten. Videre påpekte de faren for inngrep i enkeltpersoners menneskerettigheter, inngrep i kommunikasjonsvernet og risiko for misbruk, for eksempel ved deling av overskuddsinformasjon.

Natos Center of Excellence har i *Government responses to malicious use of social media* (Bradshaw et al., 2018, s. 6, 12) påpekt at det ikke finnes noen enkle løsninger på utfordringene, og at mange av tiltakene er problematiske. De anbefaler en dreining fra kontroll og kriminalisering til mer jobbing med personvern og åpenhet om algoritmer og annonsering. Manglende åpenhet om moderering og blokkering kan også ha en såkalt nedkjølingseffekt. De fremhever at tiltak i demokratiske land kopieres av autoritære stater og brukes til å legitimere undertrykkelse, sensur og udemokratiske tiltak. Europakommisjonens ekspertgruppe advarer også mot enkle løsninger og sier at enhver form for sensur, privat eller offentlig, absolutt må unngås (European Commission, 2018d).

Oxford Technology and Elections Commission har påpekt at tiltak ofte er kontroversielle eller krevende å innføre, og at de kan brukes for å få kontroll over mediene og hindre fri debatt (Robinson et al., 2019). I en annen rapport har de påpekt at vi fortsatt vet lite om effekten av slik påvirkning, og de fremhever særlig behovet for å ivareta personvern (Thwaite, 2019).

Studien av det svenske valget (Colliver et al., 2018, s. 7, 34–35, 38) påpekte at de større mediene burde rapportere mer korrekt og forståelsesfullt om utfordringene med innvandring og integrering, og ikke feie utfordringene under teppet. Innflytelsen til sensasjonalistiske medier kunne dermed reduseres. En annen svensk studie for MSB fremhever at ytringsfriheten er en grunnleggende rettighet, og at ytringer skal møtes med åpen og fri debatt, og ikke forbud eller begrensninger (Pamment et al., 2018, s. 112–113). De påpeker også at påvirkning i de aller fleste tilfeller er fullt lovlig, også når det kan være til skade for andre, og at det er svært problematisk hvis demokratiske stater begrenser ytringsfriheten på noen måte.

Den samme studien for MSB fremhever også at faktasjekk er problematisk hvis den på noen måte kan sies å begrense retten til alternative meninger og synspunkter. Internasjonalt har offentlig drevet faktasjekking ofte møtt kritikk og beskyldning om sensur (Robinson et al., 2019, s. 17). Europarådets generalsekretær Torbjørn Jagland var tydelig skeptisk da Faktisk.no ble etablert (Kalsnes, 2019, s. 92), og fryktet at de kunne bli en domstol i saker der det ikke finnes en absolutt sannhet (ABC-nyheter, 2017). Nestleder i Senterpartiet Ola Borten Moe omtalte deres søknad om statsstøtte som «på grensen til autoritær» (Jacobsen & Eckblad, 2018). Faktisk.no eies av en rekke store medieaktører, har blitt anklaget for sensur en rekke ganger, og har blitt kritisert for samarbeidet med Facebook, som gjør at andre mediers saker kan få opptil 80 prosent mindre synlighet (Minerva, 2019).

Oppsummert er det betydelig bekymring for at beskyttelse av valg skal føre til inngripende og restriktive tiltak med negative konsekvenser for demokrati og ytringsfrihet. Ytringsfriheten er en grunnleggende rettighet, og ytringer skal møtes med fri debatt, ikke begrensninger. Konkret er bekymringene knyttet til risiko for sensur, selvsensur og nedkjølingseffekt, og det advares på det sterkeste mot å forby falske nyheter. Faktasjekk er også problematisk hvis det begrenser alternative meninger og synspunkter. Det påpekes at restriktive tiltak kopieres av autoritære stater og legitimerer udemokratiske tiltak. Som et alternativ til restriktive tiltak anbefales en dreining fra kontroll og kriminalisering mot personvern, åpenhet og sikring av digital infrastruktur.

Konklusjon

Basert på gjennomgangen av litteratur og dokumenter, og den etterfølgende oversikten med en lang rekke mulige tiltak, er det noen tiltak som fremstår som mer aktuelle for norske forhold. Det er særlig lagt vekt på om tiltakene er anbefalt av mange kilder, om de antas å kunne bidra til beskyttelse valg i betydelig grad, om de er billige

eller relativt enkle å iverksette, og om de er mindre kontroversielle. Dette må sees som en første indikasjon, og ikke som en fullverdig vurdering. Som nevnt må det tas betydelig forbehold om at alle tiltakene har konsekvenser og implikasjoner som må vurderes nærmere. De etterfølgende fire problemstillingene fremstår imidlertid som klart relevante for videre vurdering under norske forhold.

Bevisstgjøring bidrar til at myndighetene, befolkningen og mediene er oppmerksomme på utfordringene, og til å redusere både spredningen og effekten av desinformasjon og påvirkning. Hvis mediene gir informasjon om og omtaler utfordringene, kan det nå mange og være kosteffektivt og normalt ukontroversielt. Videre er bevisstgjøring av partier, kandidater og aktører som er direkte involvert i valgavviklingen målrettet og kosteffektivt, og det bidrar til bedre koordinering og samarbeid.

Man bør ta en helhetlig gjennomgang av trusler, sårbarhet og beskyttelsestiltak for å tette eventuelle hull og identifisere kosteffektive forebyggings- og sikringstiltak. Som en del av en slik helhetlig gjennomgang bør det særlig identifiseres nødvendige tiltak innen datasikkerhet.

Forskning og utviklingsarbeid er nødvendig for å bygge tilstrekkelig kompetanse og forståelse for utfordringene og vil også være en integrert del av analysearbeid som gjøres for å forstå og overvåke truslene. Utfordringene med digital påvirkning av valg er nye, og kompetansen på temaet er begrenset. Forskning og utviklingsarbeid vil også kunne bidra direkte til bevisstgjøring og dermed forebygging. Påvirkning av valg må sees som en kontinuerlig prosess med stadig utvikling fra aktuelle aktører, og forskning og utvikling bør derfor pågå kontinuerlig for å bygge tilstrekkelig forståelse. Dette er trolig ikke veldig kostbart og bør også anses som ukontroversielt.

Aktive mottiltak og avskrekking fremheves av mange, og ble særlig påpekt som en avgjørende faktor for å unngå innblanding i valg i Sverige og Tyskland. Dette innebærer at man offentlig går ut og informerer om at man analyserer og overvåker mulige påvirkningsforsøk, og advarer om at man vil eksponere eventuelle forsøk. Tiltaket er i seg selv relativt enkelt og billig, men det krever aktiv involvering fra politisk ledelse for å være troverdig. I Sverige ble budskapet sendt av statsministeren. Det forutsetter også at man har en troverdig overvåkning og at det er politisk vilje til å følge opp ved påvirkningsforsøk.

Trusselen vil sannsynligvis vedvare. EU beskriver russisk desinformasjon som «systematisk, med store ressurser og med et helt annet omfang enn andre land», og de sier det er en «del av en hybrid trussel som anvender en rekke virkemidler, metoder, og også ikke-statlige aktører» (European Commission, 2018a, min oversettelse). Amerikansk etterretning forventer at aktørene vil «videreutvikle sine kapasiteter og finne nye metoder etter hvert som de lærer av hverandres erfaringer, slik at trusselbildet vil endres betydelig til 2020 og fremtidige valg» (DNI, 2019, min oversettelse).

Valg er en helt grunnleggende demokratisk aktivitet med avgjørende betydning for hvordan samfunn utvikles og styres. Det er derfor helt nødvendig med tiltak for å sikre at disse avvikles trygt og tillitvekkende. Samtidig utfordrer en rekke av de tiltakene artikkelen omtaler både demokratiet og ytringsfriheten, og de kan utilsiktet føre

til sensur. De ulike tiltakene kan ha direkte eller indirekte konsekvenser, og noen av dem er klart negative, mens de positive effektene kan være usikre. Vi må derfor sørge for en rimelig balanse mellom trusler, tiltak og konsekvenser, og unngå at tiltak for å beskytte demokratiet i seg selv undergraver demokratiet.

Denne artikkelen har gitt en oversikt over et betydelig antall aktuelle tiltak for å beskytte valg, og har pekt ut fire problemstillinger som umiddelbart virker aktuelle for vurdering. En åpenbar mulighet for videre forskning er en vurdering av hvilke utfordringer og svakheter Norge spesielt står overfor, og en nærmere gjennomgang av tiltakene, for å analysere hvilke som er relevante, og hvordan disse kan overføres og tas i bruk i Norge.

Om forfatteren

Geir Hågen Karlsen er oberstløytnant, hovedlærer strategisk kommunikasjon ved Forsvarets høgskole og sjef Forsvarets enhet for psykologiske operasjoner. Han er utdannet ved Krigsskolen og Forsvarets stabsskole, og har en master i PR-ledelse og strategisk kommunikasjon fra Handelshøyskolen BI.

Referanser

ABC-nyheter. (2017, 07. juli). Jagland med bredside mot Faktisk.no. *ABC-nyheter*. https://www.abcnyheter.no/nyheter/politikk/2017/07/07/195315932/jagland-med-bredside-mot-faktisk-no

Barland, M. & Tennøe, T. (2019). *Valg, teknologi og politisk påvirkning.* Teknologirådet.

Bay, S. & Snore, G. (2019). *Protecting elections: A strategic communications approach.* NATO Strategic Communications Centre of Excellence.

Bergh, A. (2020). *Påvirkningsoperasjoner i sosiale medier – oversikt og utfordringer* (FFI-rapport 20/01694). Forsvarets forskningsinstitutt.

Bradshaw, S., Neudert, L.-M. & Howard, P. N. (2018). *Government responses to malicious use of social media.* NATO Strategic Communications Centre of Excellence.

Bradshaw, S. & Howard, P. N. (2019). *The global disinformation order – 2019 global inventory of organised social media manipulation.* Oxford Internet Institute.

Brady, A.-M. (2017). *Magic weapons: China's political influence activities under Xi Jinping.* The Wilson Centre.

Brattberg, E. & Maurer, T. (2018). *Russian election interference – Europe's counter to fake news and cyber attacks*. Carnegie Endowment for International Peace.

Burton, M. J., Miller, W. J. & Shea, D. M. (2015). *Campaign craft. The strategies, tactics and art of political campaign management (5. utg.)*. Praeger.

Bundesamt für Verfassungsschutz (BfV). (2018). *Verfassungsschutzbericht 2017*. BfV.

Cole, J. M. (2019, 30. desember). Chinese disinformation in Taiwan. *Taiwan Sentinel.*

Colliver, C., Pomerantsev, P., Applebaum, A. & Birdwell, J. (2018). *Smearing Sweden – international influence campaigns in the 2018 Swedish election.* Institute for Strategic Dialogue.

Cybersecurity and Infrastructure Security Agency. (2019). *Joint statement from DOJ, DHS, DNI, FBI, NSA and CISA on ensuring security of 2020 elections*. https://www.cisa.gov/cisa/news/2019/11/05/joint-statement-doj-dod-dhs-dni-fbi-nsa-and-cisa-ensuring-security-2020

Datatilsynet. (2019). *På parti med teknologien – digital målretting av politiske budskap i Norge*. Datatilsynet.

Director National Intelligence (DNI). (2019). *Worldwide threat assessment of the US iIntelligence community. Statement for the record to the Senate Select Committee in Intelligence.* DNI.

Director National Intelligence (DNI). (2020). *Statement by NCSC Director William Evanina: Election threat update for the American public*. https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public

DiResta, R., Shaffer, K., Ruppel, B., Sullivan, D., Matney, R., Fox, R., Albright, J. & Johnson, B. (2018). *The tactics and tropes of the Internet Research Agency.* New Knowledge.

European Commission. (2018a). *Action plan against disinformation*. https://eeas.europa.eu/sites/eeas/files/action_plan_against_disinformation.pdf

European Commission. (2018b). *State of the union 2018 – free and fair European elections*. https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-free-fair-elections_en.pdf

European Commission. (2018c). *Code of practice on disinformation*. https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

European Commission. (2018d). *Final report of the High Level Expert Group on fake news and online disinformation*. https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation

European Commission. (2019). *Action plan against disinformation – Report on progress – June 2019*. https://ec.europa.eu/commission/sites/beta-political/files/factsheet_disinfo_elex_140619_final.pdf

European Parliamentary Research Service. (2019). *Polarization and the use of technology in political campaigns and communication*. https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2019)634414

Fernquist, J., Kaati, L., Akrami, N., Cohen, K. & Schroeder, R. (2018a). *Automatiserade konton – en studie av botar på Twitter i samband med det svenska riksdagsvalet 2018.* Myndigheten för samhällsskydd och beredskap.

Fernquist, J., Kaati, L., Akrami, N., Pelzer, B. & Cohen. K. (2018b). *Digitala diskussioner om genomförandet av riksdagsvalet 2018*. Myndigheten för samhällsskydd och beredskap.

Francois, C., Nimmo, B. & Shawn, E. (2019). *The IRACopyPasta campaign.* Graphika.

Gjesvik, L. & Øverbø, E. J. (2019). Avskrekke hvem? Betydningen av strategisk kultur for cybersikkerhet. *Internasjonal politikk*, *77*(3), 278–287. https://doi.org/10.23865/intpol.v77.1396

Grøtan, T. O., Fiskvik, J., Haro, P. H., Auran, P. G., Mathisen, B. M., Magin, M., Brandtzæg, P. B. & Karlsen, G. H. (2019). *På leting etter utenlandsk informasjonspåvirkning – En analyse av det norske kommunestyre- og fylkestingsvalget 2019* (SINTEF rapport 2019:01292). SINTEF.

Hamilton, C. (2018). *Silent invasion: China's influence in Australia.* Hardie Grant.

Howard, P. N., Ganesh, B. & Liotsiou, D. (2018). *The IRA, social media and political polarization in the United States, 2012–2018. Computational propaganda research project.* University of Oxford.

Ihlen, Ø. Allern, S. & Skogerbø, E. (2015). *Makt, medier og politikk. Norsk politisk kommunikasjon.* Universitetsforlaget.

Intelligence and Security Committee of Parliament. (2020). *Russia.* The Parliament.

Jacobsen, T. & Eckblad, B. (2018, 22. oktober). Sp-politiker Ola Borten Moe angriper Faktisk.no etter søknad om statsstøtte. *Dagens Næringsliv*. https://www.dn.no/medier/senterpartiet/ola-borten-moe/vg/sp-politiker-ola-borten-moe-angriper-faktiskno-etter-soknad-om-statsstotte/2-1-456355

Kalsnes, B. (2019). *Falske nyheter – løgn, desinformasjon og propaganda i den digitale offentlighet.* Cappelen Damm Akademisk.

Karlsen, G. H. (2019). *Divide and rule: Ten lessons about Russian political influence activities in Europe*. Palgrave Communications.

Karlsen, R. (2015). Valgkamp – kort, lang, permanent. I Ø. Ihlen, S. Allern & E. Skogerbø (Red.), *Makt, medier og politikk. Norsk politisk kommunikasjon.* Universitetsforlaget.

Kolga, M., Janda, J. & Vogel, N. (2019). *Russia-proofing your election – global lessons for protecting Canadian democracy against foreign interference*. Macdonald-Laurier Institute.

Kristiansen, M. & Hoem, N. (2019). Avskrekking som element i cybersikkerhetsstrategi fra et småstatsperspektiv. *Internasjonal politikk*, *77*(3), 252–265. https://doi.org/10.23865/intpol.v77.1385

Lamond, J. & Dessel, T. (2019). *Democratic resilience – a comparative review of Russian interference in democratic elections and lessons learned for securing future elections.* Centre for American Progress.

Levin, D. H. (2016). When the great power gets a vote: The effects of great power electoral interventions on election results. *International Studies Quarterly*, *60*(2), 189–202. https://doi.org/10.1093/isq/sqv016

Lysne, O., Grytting, T., Jarbekk, E., Lunde, E. & Reusch, C. (2016). *Digitalt grenseforsvar (DGF)*. [Lysne II-utvalget] Forsvarsdepartementet.

Medietilsynet. (2019a). *Til felles kamp mot falske nyheter*. https://medietilsynet.no/om/aktuelt/felles-kamp-mot-falske-nyheter/

Medietilsynet. (2019b). *Eldre er dårligst på å gjenkjenne falske nyheter*. https://medietilsynet.no/om/aktuelt/eldre-er-darligst-pa-a-gjenkjenne-falske-nyheter/

Medietilsynet. (2020). *Barn og medier 2020 – om falske nyheter, delrapport 2*. https://medietilsynet.no/globalassets/publikasjoner/barn-og-medier-undersokelser/2020/200226-barn-og-medier-2020-delrapport-2.pdf

Minerva. (2019, 13. mars). *Slik reduserer Faktisk.no andre mediers synlighet på Facebook*. https://www.minervanett.no/faktiskno-nettavisen/slik-reduserer-faktiskno-andre-mediers-synlighet-pa-facebook/188706

Mueller, R. S. (2019). *Report on the investigation into Russian interference in the 2016 presidential election.* U.S. Department of Justice.

Myndigheten för samhällsskydd och beredskap (MSB). (2019). *Countering information influence activities – a handbook for communicators*. MSB.

Pamment, J., Nothhaft, H. & Fjällhed, A. 2018). *Countering information influence activities – the state of the art.* MSB. https://www.msb.se/RibData/Filer/pdf/28697.pdf.

Regeringskansliet. (2018). *En ny myndighet för psykologiskt försvar*. https://www.regeringen.se/rattsliga-dokument/kommittedirektiv/2018/08/dir.-201880/

Robinson, O., Coleman, A. & Sardarizadeh, S. (2019). *A report of anti-disinformation initiatives.* Oxford Technology and Elections Commission.

Statens offentliga utredningar. (2020). *Betenkande av Psykforsvarsutredningen. SOU 2020:29.* SOU.

Statsministerens kontor. (2019). *Ti tiltak for å hindre uønsket påvirkning i valggjennomføringen*. https://www.regjeringen.no/no/aktuelt/ti-tiltak-for-hindre-uonsket-pavirkning-i-valggjennomforingen/id2661220/

The Prime Minister. (2020). *Government response to the intelligence and security committee of parliament report 'Russia'*. Prime Minister's Office.

The White House. (2018). *National cyber strategy of the United States of America*. The White House.

Thwaite, A. (2019). *Literature review on elections, political campaigning and democracy.* Oxford Technology and Elections Commission.

U.S. District Court for the District of Columbia. (2018). Case 1:18-CR-32-DLF, Indictment, document 1, filed 16 Feb 2018.

U.S. District Court for the District of Columbia. (2018). Case 1:18-CR-215-ABJ, Indictment, filed 13 July 2018.

U.S. District Court for the Eastern District of Virginia. (2018). Case 1:18-MJ-464, Criminal Complaint, filed 28 Sep 2018.

U.S District Court for Western District of Pennsylvania. (2018) Case 2:18-CR-263-MRH, Indictment, filed 3 Oct 2018.

U.S Senate Select Committee on Intelligence. (2018). *Russian targeting of election infrastructure during the 2016 election: Summary of initial findings and recommendations.* U.S. Senate.

U.S. Senate Select Committee on Intelligence. (2019a). *Report on Russian active measures campaigns and interference in the 2016 U.S. election. Volume I: Russian efforts against election infrastructure.* U.S. Senate: Washington D.C.

U.S. Senate Select Committee on Intelligence. (2019b). *Report on Russian active measures campaigns and interference in the 2016 U.S. election. Volume II: Russia's use of social media.* U.S. Senate.

U.S. Senate Select Committee on Intelligence. (2020a). *Report on Russian active measures campaigns and interference in the 2016 U.S. election. Volume III: U.S. government response to Russian activities.* U.S. Senate.

U.S. Senate Select Committee on Intelligence. (2020b). *Report on Russian active measures campaigns and interference in the 2016 U.S. election. Volume IV: Review of intelligence community assessment.* U.S. Senate.

U.S. Senate Select Committee on Intelligence. (2020c). *Report on Russian active measures campaigns and interference in the 2016 U.S. election. Volume V: Counterintelligence threats and vulnerabilities.* U.S. Senate.

Valdal, A.-K., Wiencke, H. S., Dale, C., Tuastad, S., Holo, T., Røed, W. & Sandal, B. (2019). *Sikkerheten i demokratiske prosesser i Norge*. Proactima & Sekretariatet for valglovutvalget.

Winther, P. (2016). *Yttrandefrihetsgrundlagen och möjligheterna att möta påverkanskampanjer från främmande makt: Delrapport 2 (2016) på uppdrag av Myndigheten för Samhällsskydd och Beredskap*. Försvarshögskolan.

Woolley, S. C. & Howard, P. N. (2017). *Computational propaganda worldwide: Executive summary.* Working paper No. 2017.11. Computational Propaganda Research Project – University of Oxford.

Abstract in English

How can elections be protected against foreign interference?

Russian interference in the 2016 US presidential election have caused fear for manipulation of elections in the West. Both the EU and the US see this as a persistent threat and expect new methods and capabilities to emerge. This article

describes election interference and how it has been conducted. It reviews literature about protection of elections, and summarises the findings in six themes with a total of 38 possible measures: 1) awareness, 2) prevention, 3) cooperation and coordination, 4) protective measures, 5) active countermeasures and deterrence, 6) research and competence building. All measures require careful consideration of economic, political, legal, practical and other implications, and especially consequences for democracy and freedom of speech. Finally, four issues are proposed as particularly relevant for further consideration: 1) awareness through media, and also especially targeted at political parties and the election organisation, 2) a comprehensive assessment of threats, vulnerabilities and protective measures, especially in terms of data protection, 3) research and development, 4) deterrence and exposure of interference. Many of the measures are far-reaching when it comes to democracy, freedom of speech, censorship and self-censorship, and the article reviews challenges, limitations and critique of such restrictive measures. It is essential that measures to protect democracy in themselves do not undermine democracy.

Keywords: Russia • information influence • social media • propaganda • manipulation