Proactima Stavanger
Postboks 8034
4068 Stavanger

Proactima Oslo
Møllergata 1-3
0179 Oslo

Proactima Bergen
Kong Christian Frederiks pl. 3
BI-bygget, 5006 Bergen

Proactima Trondheim
Innherredsveien 7
7014 Trondheim

T: 40 00 19 33 - org. nr. 915 641 938 - Post@proactima.com - www.proactima.com

RAPPORT Sekretariatet for valglovutvalget

Sikkerheten i demokratiske prosesser i Norge

Utredning - valgprosessen

Foto: Tore Fjeld for Kommunal- og moderniseringsdepartementet (CC BY-NC 2.0)

Kunde:	**Kontaktperson:**
Sekretariatet for valglovutvalget	Marie Svendsen Mjøsund

Oppsummering:

Regjeringen oppnevnte i juni 2017 et valglovutvalg som skal komme med forslag til ny valglov, og vurdere valgordningen. Utvalget har et bredt mandat, og skal se på alle sider av valggjennomføringen (Regjeringen, 2017). Mandatet beskriver at utvalgets arbeid skal tilrettelegge for «fortsatt høy tillit til valgordningen og gjennomføringen av valg i årene fremover».

Mandatet gir valglovutvalget mulighet til å «be om særskilte orienteringer og/eller utredninger på enkeltområder». Proactima AS, med støtte fra underleverandører Netsecurity AS og Aeger Group AS, har på oppdrag fra valglovutvalget gjennomført en utredning av sikkerheten i demokratiske prosesser i Norge.

Formålet med utredningen har vært å belyse sikkerhetsrelaterte spørsmål knyttet til valg, og som er relevante for de vurderinger valglovutvalget skal gjøre sitt arbeid, samt å bidra til å styrke arbeidet med å tilrettelegge for en valglov som også sikrer høy tillit i befolkningen.

Utredningen identifiserer og vurderer trusler, sårbarheter og risiko knyttet både til politiske påvirkningskampanjer og til den faktiske gjennomføringen av valget. Det gis videre innspill til regulatoriske tiltak og andre aktiviteter som kan bidra til å møte den identifiserte risikoen og sikre de demokratiske prosessene, også i et fremtidsperspektiv.

Nøkkelord	Sikkerhet, demokratiske prosesser, valg, trussel, påvirkning
Rapportnr.	1073276-RE-01
Forfatter(e)	Anne-Kari Valdal (Proactima AS), Hermann S. Wiencke (Proactima AS), Chris Dale (Netsecurity AS), Svein Tuastad (Proactima AS), Trine Holo (Aeger Group), Willy Røed (Proactima AS), Bjørg Sandal (Proactima AS)
Konfidensialitet	Intern
Revisjonsnr.	01
Revidert dato	24.05.2019
Antall sider	112

Rev.nr.	Dato	Årsak til revisjon
00		Første utkast
01	24.05.2019	Endelig rapport – etter behandling av innspill

Utarbeidet av	**Verifisert av**	**For Proactima AS**
Anne-Kari Valdal	Hermann S. Wiencke	Vibeke Langeland Pedersen

Innholdsfortegnelse

1 Sammendrag

Regjeringen oppnevnte i juni 2017 et valglovutvalg som skal komme med forslag til ny valglov, og vurdere valgordningen. For å styrke kunnskapsgrunnlaget om sikkerheten i de demokratiske prosessene i Norge, og styrke arbeidet med å tilrettelegge for en valglov som også sikrer høy tillit i befolkningen, har Proactima AS gjennomført en utredning på oppdrag fra valglovutvalget. Utredningen fokuserer på trusler mot demokratiske prosesser både knyttet til politiske påvirkningskampanjer og faktisk gjennomføring av valg, sårbarheter i den digitale verdikjeden, konsekvenser ved bruk av teknologi i valggjennomføringen, forholdet til regelverk og regulering, og på tiltak som kan bidra til å øke sikkerheten.

Utredningen har en systematisk tilnærming bygget på metodikk for risiko- og sårbarhetsanalyse på et overordnet nivå. I tillegg til erfaringsbaserte vurderinger har det blitt gjennomført gjennomgang av litteratur, artikler og nyheter, samt arbeidsmøter og intervjuer med Kommunal- og moderniseringsdepartementet, Valgdirektoratet, valglovutvalget, valgmedarbeidere i et utvalg kommuner og med Microsoft.

Det er gjort en overordnet vurdering av trusler og trusselaktører og valgt ut 20 fenomener/hendelser som grunnlag for å vurdere behov for sikkerhetstiltak av ulik form. For hver av disse er det sett på sannsynlighet for hendelsen gjennom vurderinger av trusler og virkemidler, og av barrierer og sårbarheter. Konsekvenser er vurdert opp imot 5 krav til demokratiske valg som er definert i utredningen:

- *Fri deltagelse* - At alle kandidater til valget, og velgere, har og får tilgang til å delta ved at det oppleves trygt og mulig - og at valget er hemmelig
- *Opplyst og informert* - At velgere får nok informasjon, riktig informasjon og balansert informasjon – til at de kan gjøre et «informert valg» (stemme)
- *Korrekt* - At de stemmer som er avgitt faktisk utgjør resultatet. Riktig manntall, riktig registrering, riktig antall stemmer
- *Gjennomført i tråd med plan* - At man faktisk får avholdt valget (og ikke hindres av sabotasje, naturhendelser, systemfeil eller organiseringsmangler)
- *Tillit* - At tilliten til den demokratiske valgprosessen opprettholdes i befolkningen (herunder at etterprøvbarhet og åpenhet er ivaretatt)

I tillegg har dimensjonene kunnskapsstyrke, det vil si kunnskap om fenomenet, og endringshastighet, i forhold til endringer i fremtiden, blitt vurdert med tanke på påvirkning på risiko.

Vurderingene viser at den største risikoen knyttet til den demokratiske valgprosessen, er relatert til påvirkning av kandidater og velgere i forkant av valggjennomføringen. Karakteristisk for mange av fenomenene innen disse områdene er at man har begrenset kunnskap om fenomen og effekter av disse. I tillegg er endringshastigheten er høy Dette er et uttrykk for rask teknologisk og kulturell utvikling, særlig innen dataanalyse og kommunikasjon, men også for et trusselbilde i stadig endring nasjonalt og internasjonalt.

Et fenomen som utmerker seg med stort risikobidrag er micromålretting av informasjon. Bruk av analyse ved algoritmer, maskinlæring og kunstig intelligens tilgjengeliggjør svært sensitiv informasjon om velgerne. Denne informasjonen kan brukes til å målrette informasjon i den hensikt å påvirke velgere i den retningen en (trussel)aktør ønsker, uten at velgeren selv er klar over det.

Hendelser av mer teknisk art og relatert til den digitale verdikjeden er gjennomgående vurdert å gi et mindre risikobidrag enn påvirkningshendelser. Til tross for omfattende og robust sikring av eksempelvis valgadministrasjonssystemet (EVA), foreligger det sårbarheter i den digitale verdikjeden knyttet til teknologiske endringer, kompleksitet, utfordringer med kompetanse og lange verdikjeder. Hovedårsaken til at risikoen samlet sett likevel vurderes som begrenset på dette området, er at det fortsatt er betydelige innslaget av manuelle prosesser i valggjennomføringen, som sikrer kontroll og redundans. Dette gjelder

for eksempel identifisering av velgeren og avlegging av stemme, og den pålagte manuelle tellingen av stemmer.

Utredningen viser også at redusert tillit til valg, myndigheter og demokrati er den dominerende konsekvensen av hendelsene. Nesten samtlige fenomener/hendelser vil påvirke tillitsdimensjonen negativt. Karakteristisk for tillit er også at en ikke nødvendigvis trenger å lykkes med et angrep for at den skal svekkes. Videre fremkommer at de økende truslene og risikoen knyttet til påvirkning, spesielt gjennom bruk av digitale verktøy og sosiale medier, kan gi store konsekvenser for hvor opplyst og informert velgerne er (grunnlaget for reelle valg) og den frie deltakelsen for både kandidater og velgere.

Minst påvirket i dag blir korrektheten i valget, igjen på grunn av de manuelle prosessene i valggjennomføringen. Dette er imidlertid et område som kan kreve innføring av betydelige sikkerhetstiltak i fremtiden, for å hindre økt risiko dersom også dagens manuelle prosesser digitaliseres.

For å ivareta sikkerheten i de demokratiske prosessene knyttet til valg, også i fremtiden, anbefales det at følgende regulatoriske tiltak vurderes:

- *Regulering av sikkerhetskrav til valggjennomføringen for regionale og lokale aktører*
- *Etablering av hjemmel for tilsyn med sikkerhetsreguleringen for valg.*
- *Vurdere sikkerhetslovens relevans for valgprosessen*
- *Vurdere og avklare endringer i roller og ansvar/myndighet mellom lokale og sentrale aktører i valggjennomføringen for å ivareta kravstilling og kontroll dersom sikkerhetskrav reguleres og det etableres hjemme for tilsyn*
- *Lovfeste krav om at myndigheter på alle nivåer i valggjennomføring skal benytte digital infrastruktur og programvare fra sentrale valgmyndigheter (EVA)*
- *Etablere en beredskapshjemmel i valglovgivningen*
- *Videreføre regulatorisk krav om to uavhengige tellinger av stemmene etter valg*
- *Utrede behov for regulering av bruk av mikromålretting som verktøy i valgkamp*
- *Etablere/tydeliggjøre hjemmel for å sanksjonere hacking, og forsøk på hacking, av valgsystemer*

I tillegg gir utredningen innspill til andre mulige tiltak, eksempelvis rettet mot videre utredninger, støtteordninger til partier og redaktørstyrte medier, teknologiske tiltak og barrierer, og bygging av kunnskap og robusthet i samfunnet.

2 Beskrivelse av oppdraget

2.1 Bakgrunn

Regjeringen oppnevnte i juni 2017 et valglovutvalg som skal komme med forslag til ny valglov, og vurdere valgordningen. Utvalget har et bredt mandat, og skal se på alle sider av valggjennomføringen (Regjeringen, 2017). Mandatet beskriver at utvalgets arbeid skal tilrettelegge for «fortsatt høy tillit tilvalgordningen og gjennomføringen av valg i årene fremover».

Mandatet understreker videre at «Utvalget skal basere arbeidet sitt på forskning og empirisk kunnskap, og bidra til økt forståelse av demokrati og valg.», og at «Utvalget kan be om særskilte orienteringer og/eller utredninger på enkeltområder».

Valglovutvalget ved sekretariatet valgte å be om en utredning av «sikkerheten i demokratiske prosesser i Norge» høsten 2018. Utredningen ble tildelt Proactima AS, med støtte fra underleverandører Netsecurity AS og Aeger Group AS.

Valglovutvalget har bedt om en rapport som utreder ulike trusler mot demokratiske prosesser i tilknytning til gjennomføring av valg i Norge. Cybersikkerhet og risikoer forbundet med økt bruk av teknologi i valggjennomføringen skal inngå som en sentral del av analysen. Valglovutvalget ba også om at utredningen skal beskrive hvilke konsekvenser truslene og risikoene kan få for tilliten til valgsystemet, og gi råd om hvordan sentrale og lokale valgmyndigheter best kan ivareta disse utfordringene på en forsvarlig måte.

Valglovutvalget understreker at det er avgjørende for legitimiteten til demokratiet at de som velges representerer folkets vilje, og at valget foregår korrekt og på en tillitsvekkende måte.

Som bakgrunn for oppdraget beskriver valglovutvalget blant annet:

«I dag benyttes teknologi i stor grad i valggjennomføringen. Det sikrer en effektiv gjennomføring, men har også konsekvenser for sikkerheten og kan påvirke tilliten til valget. Bruk av teknologi fører med seg risiko knyttet til de digitale verdikjedene. På noen området vil dette kunne være enkelt å håndtere og risikoen kan tolereres, på andre områder vil det måtte stilles høyere krav til sikkerhet. En særlig utfordring på området er at det ikke bare er et reelt brudd på sikkerheten som vil kunne føre til lavere tillit. Dersom noen klarer å sannsynliggjøre at de kan (eller har fått) tilgang til systemet på en uautorisert måte, kan det være nok for å ødelegge tilliten.

Bruk av digital teknologi i valggjennomføring varierer mellom ulike land. Mens mange land er svært konservative og bruker manuelle løsninger, finnes det andre land som har digitalisert mye av valgprosessen og gjennomfører valg over internett. Estland er eksempel på det siste. I Norge bruker vi et digitalt valgadministrasjonssystem, EVA, for å understøtte valg til kommunestyre, fylkesting og Storting, men stemmegivningen foregår fremdeles manuelt. Forsøk på e-valg ble gjennomført i 2011 og 2013, men ble ikke videreført som ordning etter at forsøket ble avsluttet.

Det har vært mye oppmerksomhet knyttet til cybersikkerhet og påvirkningsoperasjoner knyttet til valg de senere år, blant annet i USA, Frankrike og Sverige. Kombinert med private firmaers bidrag i påvirkningskampanjer, eksemplifisert ved Cambridge Analytica-skandalen og hacking av servere, viser dette at tillit til rettferdige og transparente demokratiske prosesser og valg i digitaliserte samfunn utfordres. Også her til lands er digitale sårbarheter og cyberangrep som politisk pressmiddel ansett som en reell trussel. Dette bekreftes av etterretningstjenesten som, i sin rapport Fokus 2018, beskriver en vedvarende etterretningsaktivitet mot Norge, opptrapping av russisk påvirkningsaktivitet mot demokratiske prosesser og offentlig opinion. De peker også på fortsatt utvikling av kapasiteter for digital sabotasje.

Åpenhet har vært en viktig bærebjelke i valggjennomføringen i Norge, og en viktig forutsetning for den høye tilliten. I Norge er mye av ansvaret for valggjennomføringen desentralisert. Kommunene har det største ansvaret for den praktiske gjennomføringen, ettersom mesteparten av dette gjøres av valgstyret i kommunen. Alle valgstyrets møter er åpne, også møter der opptellingen av stemmer skjer. Det legger til rette for god kontroll på lokalt nivå, fra både lokale medier og befolkningen. Det lokale ansvaret medfører også at digitale løsninger må tilpasses ulike lokale behov.»

2.2 Formål

Formålet med utredningen er å belyse sikkerhetsrelaterte spørsmål knyttet til valg, og som er relevante for de vurderinger valglovutvalget skal gjøre sitt arbeid. Videre beskriver valglovutvalget at:

«Et viktig formål med undersøkelsen er å styrke kunnskapsgrunnlaget om sikkerheten i de demokratiske prosessene i Norge. Både knyttet til politiske påvirkningskampanjer og til den faktiske gjennomføringen av valget. Dette vil kunne gi valglovutvalget nødvendig kunnskap og forståelse for dagens situasjon, og bidra til å styrke arbeidet med å legge til rette for en valglov som sikrer en demokratisk, sikker og etterrettelig valgordning nå og i fremtiden. Oppdraget skal også bidra til økt innsikt og forståelse for hvordan behovet for sikkerhets- og beredskapstiltak påvirker åpenheten, ansvarsdelingen og regelverksutformingen.»

Utredningen skal belyse aspekter ved sikkerheten i de demokratiske prosessene i Norge i tilknytning til gjennomføring av valg. Den skal bidra til å styrke arbeidet med å tilrettelegge for en valglov som også sikrer høy tillit i befolkningen.

I utredningen skal det identifiseres og vurderes trusler, sårbarheter og risiko knyttet til valggjennomføring, også i forkant av valg; og det skal anbefales tiltak og aktiviteter som kan møte den identifiserte risikoen og sikre de demokratiske prosessene.

Oppdragsbeskrivelsen summerer opp fire forskningsspørsmål som skal besvares gjennom utredningen:

«1. Hva er truslene mot demokratiske prosesser i tilknytning til gjennomføring av valg i Norge? Dette inkluderer politiske prosesser og opinionspåvirkning i forkant av valg, samt selve den praktiske gjennomføring av valget. Både mulighet for angrep av ulike art, og uintenderte hendelser som kan få betydning for gjennomføringen må belyses. Truslene må beskrives både opp mot sannsynlighet og opp mot konsekvens, og evt. virkning på tillit til demokratiet.

2. Hvordan fordeler sårbarheter seg langs den digitale verdikjeden i valggjennomføringen? Av hensyn til oppdragets omfang må denne delen av oppdraget begrenses til en mer overordnet oversikt. Det vil være hensiktsmessig å vise ulike aktørers ansvar for de ulike delene av kjeden, samt deres mulighet til å kontrollere om reglene følges og til å sikre overholdelse.

3. Hvilke samfunnsmessige konsekvenser har bruken av teknologi i valggjennomføringen? Tilbyder bes belyse og drøfte hvilke konsekvenser teknologi og sikring av de digitale verdikjedene har for ansvarsfordeling mellom ulike nivåer. Nå legger staten føringer i utformingen av systemet, men har i liten grad mulighet til å stille tekniske krav. Videre bes det om en vurdering av forholdet til regelverk og regulering. Til slutt bes det også om en vurdering rundt åpenhet og hvordan dette sikres på en god måte, samtidig som krav til sikkerhet ivaretas.

4. Hvilke skadeforebyggende og skadebøtende tiltak bør iverksettes for å beskytte demokratiske prosesser til tilknytning til gjennomføring av valg i Norge? Tilbyder bes om å gi innspill til mulige tiltak som kan bidra til å øke sikkerheten i den demokratiske prosessen i Norge.»

2.3 Avgrensninger

Utredningen er gjennomført i perioden november 2018 til mars 2019, og er en grovstudie som skal tjene som et underlag for valglovutvalgets arbeid knyttet til sikkerhet i demokratiske prosesser. Hensikten er å peke på områder som det er viktig at valglovutvalget tar i betraktning i det videre arbeidet. Utredningen fokuserer på sikkerhetselementer relevante for å ivareta demokratiske prosesserer, og dekker således ikke alle aspekter ved å ivareta demokratiske verdier og prinsipper i samfunnet, eller i tilknytning til valg.

I overenskomst med oppdragsgiver har utredningen avgrenset fokuset til aktiviteter knyttet til stortingsvalg. Dette valget anses å dekke mange av de mest relevante elementene, og vurderingen vil i all hovedsak også være gyldige for valgprosesser i Norge generelt. Videre ble det avtalt fokus på perioden i direkte tilknytning til gjennomføring av valg, og ikke på periodene mellom valg.

I utredningen er metodikk for risikovurdering benyttet for å sikre en systematisk og strukturert gjennomgang av relevante områder. Gjennom vurderingene fremkommer og belyses områder som vurderes å ha høy risiko og høy viktighet for sikker gjennomføring av valg i Norge. Det anbefales områder som bør tas i betraktning av valglovutvalget innenfor deres mandat, og også enkelte tiltak som bør gjennomføres og/eller vurderes av myndighetene i et videre perspektiv. Utredningen tar imidlertid ikke stilling til om risikoen kan aksepteres, og hvorvidt anbefalte tiltak eller regulering skal gjennomføres. Dette vil være myndighetenes ansvar å vurdere og beslutte.

Konklusjoner og anbefalinger vil innbefatte viktige elementer som Proactima mener bør ligge til grunn for og hensynstas ved regelverksutforming, regelverksendring og fordeling av roller og ansvar i prosessene. Utredningen vil imidlertid ikke gå inn på anbefalinger om konkrete regelverkskrav eller juridiske vurderinger rundt regelverksutviklingen.

Systembeskrivelser og beskrivelse av sårbarheter, spesielt i den digitale verdikjeden, er holdt på et overordnet nivå. Dette er både basert på en vurdering av hensiktsmessighet for valglovutvalgets arbeid, og begrensninger i utredningens tid og omfang; men også for å sikre forutsetningen om at utredningen skal kunne benyttes offentlig og ikke inneholde gradert eller skjermingsverdig informasjon.

3 Systemet som utredes

3.1 Demokrati og demokratiske verdier

Demokrati må skilles fra andre ønskverdige samfunnsmål som fred, menneskerettigheter, religionsfrihet, stabilitet og eiendomsrettigheter. Noen menneskerettigheter er nødvendige for å kunne ha demokrati, som ytringsfrihet og organisasjons- og forsamlingsfrihet, men de definerer ikke demokratiet (Berghagen, 2009). Andre samfunnsmål kan ofte følge av velordnede demokratier, som fred og likere fordeling, men det er likevel snakk om andre fenomener enn det vi strengt tatt definerer som demokrati.

En bredt forankret forståelse av hva demokrati som styreform er, er at demokratiet fastsetter regler for fordeling av byrder og goder i samfunnet, og at de som er satt til å fatte beslutningene er valgt ut av, kan regelmessig skiftes ut av og står ansvarlig ovenfor samfunnsmedlemmene (Rose, 2009). I en slik forståelse har valgene en helt essensiell rolle i å ivareta demokratiet.

En av de store, nyere demokratiteoretikerne, Robert A. Dahl, identifiserte fem nøkkelkriterier som standarder for et ideelt demokrati. I praksis vil det være vanskelig å leve opp til hvert av kriteriene fullt ut. Men de representerer ideelle fordringer, og i den grad de er mer eller mindre fraværende, vil demokratiet kunne sies å være mangelfullt:

1. Lik stemmevekt
2. Kontroll over dagsordenen
3. Opplyst forståelse
4. Reell mulighet for deltakelse og påvirkning
5. Alle medlemmer inkludert

Kriteriene 1 og 5 reflekterer krav om at alle kompetente medlemmer er potensielle deltakere hvor de står på lik fot. Ideelt sett har ingen person i kraft av nedarvet status, utdannelse eller inntekt krav på mer innflytelse enn den jevne mann og kvinne.

Kontrollen over dagsorden innebærer at det ikke er noen som står over den demokratiske forsamlingen og filtrerer hva som passer seg for demokratiet; også dette skal være en del av den demokratiske selvbestemmelsen – maktbinding skal være selvpålagt.

Det tredje og fjerde kriteriet innebærer i realiteten ganske strenge krav til samfunnsordenen når det gjelder å sette borgerne i stand til å være fullverdige medlemmer av demokratiet. Opplyst forståelse krever utdannelse og kompetanse til å forstå hva de ulike alternativene i et valg innebærer mens reell deltakelse på likefot forutsetter en samfunnsmessig infrastruktur der tilgang til felles kommunikasjonsplattformer er åpen, og der det er mulig å kommunisere ens meninger til de andre medlemmene i demokratiet. Den sterke formuleringen i Grunnlovens ytringsparagraf (§100, 6. ledd), «*Det påligger statens myndigheter å legge forholdene til rette for en åpen og opplyst offentlig samtale*», kan ses på bakgrunn av denne siste grunnleggende demokratiske forutsetningen.

Velfungerende samfunnssystemer, med relativt stor sosialøkonomisk likhet, høy institusjonell tillit og der borgerånden er høy, har klart bedre forutsetninger for å forsvare og videreutvikle en demokratisk samfunnsform (Kymlicka, 2001; Galston 1991; Pogge, 2008). På disse områdene ligger Norge sammen med de andre skandinaviske landene godt an. Tilliten til medborgerne og til de politiske institusjonene er komparativt svært høy (Den Europeiske Union, 2018; Wollebæk, 2011); det samme er den sosialøkonomiske likheten. Disse samfunnsforutsetningene er kanskje det viktigste vernet mot de identifiserte demokrati-truslene fordi de innebærer at anslag og forsøk på nedbrytende virksomhet ikke bare vil møte institusjonell motstand, men også en forventet, utstrakt borgermotstand. Den amerikanske historiekjenneren Timothy Snyder hevder det siste er den viktigste demokratiske beholdningen for å motvirke tyranni (Snyder, 2017).

Demokratiske modeller

Ut fra den utstrakte fellesforståelsen av hva demokrati består av, springer det ulike tradisjoner som vektlegger ulikt hvilke hensyn som de viktigste i demokratiet. Særlig er tre tradisjoner toneangivende i diskusjoner om hvordan demokratiet best bevares, styrkes og videreutvikles: a) Konkurransedemokratiet; b) deltakerdemokratiet og c) det deliberative demokratiet (Shorten, 2015; Rasch, 2007).

a) Konkurransedemokratiet, som også betegnes som den aggregative eller liberale demokratimodellen, ser for seg samfunnet som bestående av konkurrerende eliter som mer eller mindre holder hverandre i sjakk (Schumpeter, 1952). Demokratiet handler i grunnen om å skifte ut en elitegruppering når de ikke lenger har vist seg tilliten verdig. I denne tradisjonen er kunnskap en viktig forutsetning for velfungerende demokrati, og fordi man observerer at vanlig folk ofte mangler oppdatert kunnskap om mange samfunnsspørsmål, er ikke denne tradisjonen like opptatt av å øke deltakelsen til velgerne i høy grad i mellom valgene sammenlignet med de andre tradisjonene. Mange spørsmål er det i grunnen best at blir overlatt til de som kan mest om det, er tankegangen (jf. Brennan, 2016). Man har historisk innenfor denne tradisjonen hatt et klart blikk på hvordan institusjonelle løsninger sikrer maktdeling, og det demokratiske elementet som altoverveiende gis prioritet, er å sikre selve valgene.

b) Deltakerdemokratiet, som også omtales som en republikansk demokratimodell, har et videre blikk på hva som er viktig i demokratiet (Pettit, 2014; Skinner, 1978; Pateman 1970). Demokrati innebærer langt mer enn selve valghandlingen; det handler om at borgerne bryr seg om og deltar i utformingen av samfunnet i sine daglige liv. Demokratiet får et innslag av livsstil, og det å kunne ha frihet i ens liv, forutsetter også – i dette perspektivet – at man bruker sin politiske frihet til å være med i utformingen av samfunnsbetingelsene. Hvis man ikke gjør det, vil det være andre som i praksis bestemmer over en, og ens frihet blir dermed innsnevret (Taylor, 1991). Fellesskap og kollektiv orientering utgjør en premiss for denne tenkingen, men uten at det innebærer at man begrepsmessig innenfor tradisjonen hører til på høyre eller, kanskje særlig, på venstre side i politikken.

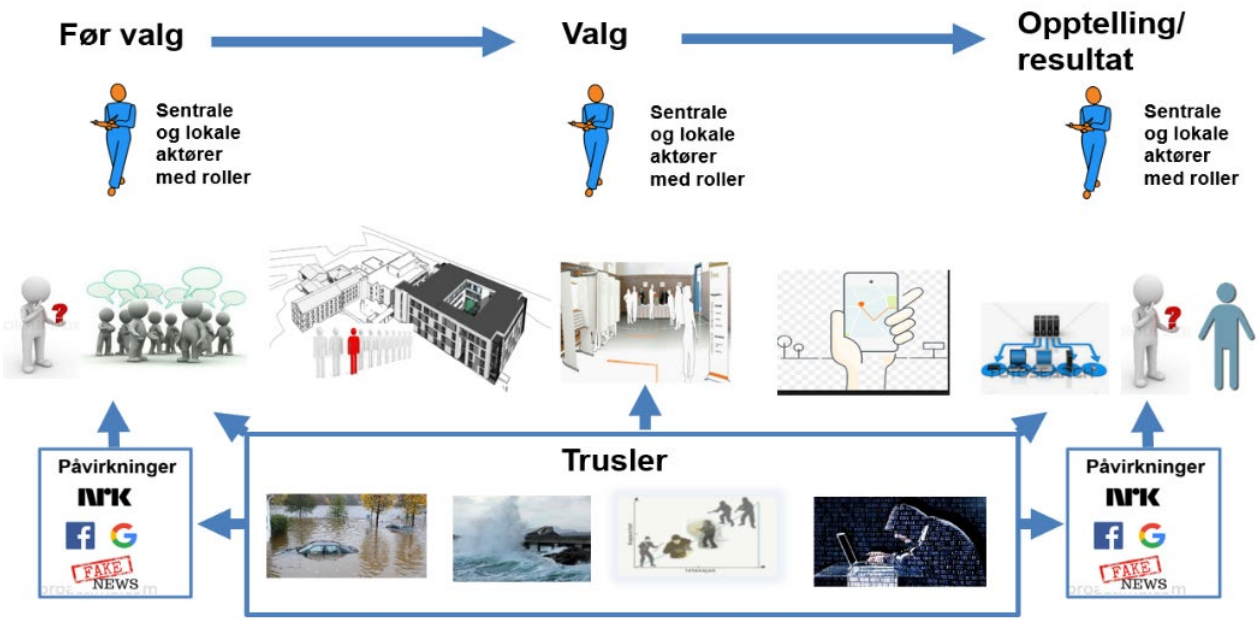
3) Det deliberative demokratiet konsentrerer seg om hvordan de demokratiske beslutningene fattes slik at de blir fornuftige og en følge av en argumenterende rådslaging hvor berørte parter har kommet til orde (Habermas, 1996; Gutmann and Thompson, 2004). I den tyske sosiologen og filosofen Jürgen Habermas sin pregende forståelse handler det om kraften i det beste argument (Habermas, 1996). Demokratiske beslutninger må i dette perspektivet ikke bare være uttrykk for en flertallsvilje, men for en flertallsvilje som så å si er kvalitetssikret gjennom en forutgående debatt. I debatten har de ulike meningsalternativene blitt prøvd ved at argumentene har måttet tåle et kritisk lys. Det følger av denne demokratiforståelsen at offentligheten, eller den offentlige sfære, spiller en viktig rolle ved at sentrale spørsmål kommer opp til debatt og at debatten påvirker beslutningstakerne. I offentligheten finner demokratiets felles samtale sted. Foraene hvor beslutninger fattes, viljesdannelsen i Habermas sin terminologi, må slik være koplet til denne felles samtalen. Med andre ord bør sfæren for viljesdannelse (beslutningsnivået) ha kanaler ikke bare til berørte parter, men også til miljøer som kan bringe til torgs vektige argument. Media får en nøkkelrolle som formidler mellom sfærene for menings- og viljesdannelse.

I praksis vil et hvert demokrati ha elementer av alle disse tre forståelsene eller modellene, og i grensesnittet mellom dem blir forberedelse, gjennomføring og oppfølging av valg en svært viktig del av å sikre de demokratiske verdiene. Valglovens formål er å legge til rette for «*frie, direkte og hemmelige valg*». I oppdraget til denne utredningen understreker også valglovutvalget at «*At de som velges representerer folkets vilje, og at valget foregår korrekt og på en tillitsvekkende måte, er avgjørende for legitimiteten til demokratiet*». Sikkerheten i valggjennomføringen er viktig for å ivareta flere av de demokratiske prinsippene (men ikke alle). I utredningen er det valgt å fokusere på 5 kvaliteter ved valggjennomføringen som er viktige å for å ivareta demokratiske prinsippene – og som kan rammes av trusler dersom sikkerheten ved valget ikke er tilstrekkelig.

- *Fri deltagelse* - At alle kandidater til valget, og velgere, har og får tilgang til å delta ved at det oppleves trygt og mulig - og at valget er hemmelig
- *Opplyst og informert* - At velgere får nok informasjon, riktig informasjon og balansert informasjon – til at de kan gjøre et «informert valg» (stemme)
- *Korrekt* - At de stemmer som er avgitt faktisk utgjør resultatet. Riktig manntall, riktig registrering, riktig antall stemmer
- *Gjennomført i tråd med plan* - At man faktisk får avholdt valget (og ikke hindres av sabotasje, naturhendelser, systemfeil eller organiseringsmangler)
- *Tillit* - At tilliten til den demokratiske valgprosessen opprettholdes i befolkningen (herunder at etterprøvbarhet og åpenhet er ivaretatt)

3.2 Overordnet systembeskrivelse – valg

Figur 1 viser en forenklet fremstilling av systemet som vurderes i denne utredningen. Hensikten er å gi en prinsipiell fremstilling av relevante faser, trusler, aktører og systemer/elementer i valggjennomføringen, og som er betraktet og vurdert i dette arbeidet. Prinsippskissen er overordnet lagt til grunn for betraktningene i utredningen, og har dannet grunnlag for å kartlegge og vurdere risiko.



Figur 1 Overordnet prinsippskisse – system

Prinsippskissen er delt inn i tre hovedfaser; 1) før valget, 2) gjennomføringen av stemmegivingen, og 3) opptelling/valgoppgjør og publisering av resultatet. Hver av disse fasene inneholder flere aktører, elementer og aktiviteter, som for eksempel:

Før valget:

- Partiene og kandidatene stiller (lister)
- Velgerne bestemmer seg for hvem de skal stemme på
- Manntallet kontrolleres og hentes
- Systemer og materiell settes opp og forberedes

Under valget:

- Mottak av tidligstemmer og forhåndsstemmer

- Kontroll mot manntall
- Kontroll og stemmegiving i valglokaler på valgdagen(-e)
- Forberedelse til telling

Etter valget:

- Forhåndstelling, endelig telling og kontrolltelling av stemmer (manuelt og eventuelt elektronisk)
- Valgoppgjør
- Offentliggjøring av resultat
- Godkjenning av valg

De ulike elementene er beskrevet i større detalj gjennom utredningen.

For hver av fasene finnes det ulike trusler og trusselaktører. Enkelte trusler er tilsiktede, det vil si at det finnes en trusselaktør som prøver å «angripe» valget med vilje. Det kan for eksempel være ved å påvirke velgerne til å stemme annerledes enn de ellers ville gjort. Her kan en skille mellom legitim og ikke-legitim påvirkning: At et politisk parti prøver å overbevise velgerne om å stemme på deres parti gjennom åpen debatt, er et eksempel på legitim påvirkning. Dersom noen derimot i det skjulte prøver å påvirke velgerne for eksempel gjennom målrettede mer eller mindre sanne budskap, vil ikke påvirkningen ha en slik legitimitet. Å prøve å påvirke opptellingen slik at resultatet ikke blir korrekt, er utvilsomt illegitimt. Andre trusler mot valget er utilsiktede, altså ikke gjort med vilje. Eksempler er at en valgmedarbeider taster feil på datamaskinen eller at velgere ikke får delta i valget på grunn av værforhold eller brann.

De ulike truslene vil true ulike elementer og deler av systemet som er beskrevet i figuren. Elementene kan være prosesser og sentrale eller lokale aktører, det kan rette seg direkte mot kandidater eller velgere, eller fokusere på digitale systemer eller valglokaler.

Utredningen fokuserer på det som vurderes som de mest relevante truslene mot sikkerheten i valgprosessen, hvordan de kan true verdier som er viktige for å sikre valg, og på hvilken måte. Barrierer og sårbarheter relatert til disse verdiene, samt effekter på ulike områder dersom truslene realiseres blir vurdert. Slik fremkommer hvor kritisk (konsekvenser og tilhørende sannsynlighet) ulike fenomener og hendelser er for de demokratiske valgprosessene.

3.3 Valgprosessen

Den norske valgordningen er basert på prinsipper om direkte valg og forholdsvalg i flermannskretser, der både politiske partier og andre grupper kan stille liste ved valgene.

Ved stortingsvalg er landet delt inn i valgdistrikter som tilsvarer fylkene, inkludert Oslo kommune som er eget fylke. Representanter til kommunestyre og fylkesting velges ved kommune- og fylkestingsvalg, der hver av kommunene og hvert fylke utgjør en valgkrets. For alle disse valgene er valgperioden 4 år, der kommune- og fylkesvalg avholdes samtidig midt mellom to stortingsvalg. Valgdagen settes til en mandag i løpet av de to første ukene i september i valgåret.

Krav til gjennomføring av valg stilles i valgloven (Kommunal- og moderniseringsdepartementet, 2002), samt i ytterligere bestemmelser gitt gjennom forskrifter. Valglovens formål er å «*å legge forholdene til rette slik at borgerne ved frie, direkte og hemmelige valg skal kunne velge sine representanter til Stortinget, fylkesting og kommunestyrer*». En rekke andre lover og forskrifter gjelder også for valg herunder forvaltningsloven, offentleglova, straffeloven, alkoholloven og forskrift om offisielle flaggdager.

I Figur 2 summerer Valgdirektoratet opp hovedansvar og oppgaver i valggjennomføringen:

Figur 2: Roller i valggjennomføringen. *Kilde: Valgdirektoratet - gjengitt med tillatelse*

I tillegg har Stortinget en rolle både som lovgiver, og som godkjenner av valget.

Hovedansvaret for gjennomføring av valg ligger hos de enkelte kommunene. Valgdirektoratet gir veiledning og opplæring i valggjennomføring, bruk av valgsystemene (EVA) og til valgansvarlige i kommunene. Bruk av valgsystemene (EVA) er ikke lovpålagt. Kommunene og fylkeskommunene konfigurerer og sikrer datamiljøene de lokale systemene (EVA Skanning) kjører i, og kommunene er selv ansvarlige for opplæring av sine valgmedarbeidere.

Selve valggjennomføringen deles grovt inn i fire faser; forberedelse, stemmegivning, opptelling og valgoppgjør. Stemmegiving dekker tidligstemmeperioden 1. juli –09. august, forhåndsstemmeperioden 10. august –fredag før valgdagen (06. september i 2019) og valdagen(-e) i september.

Utleggingsmanntall i kommunene legges ut i papirform i løpet av juni i valgåret slik at egne opplysninger kan kontrolleres av borgerne selv.

Ved avstemming krysses den enkelte av i elektronisk manntall eller på papirmanntall – avhengig av hva kommunen benytter. Stemmer avlegges på papir og stemmene legges i urne i valglokalet.

Når valglokalet stenger kontrollerer stemmestyret at innholdet i urnene er riktig ved å kontrollere at antall stemmesedler stemmer med antall avkrysninger i manntallet, og ved å sortere mellom ordinære stemmesedler og de som må gjennom ekstra behandling senere.

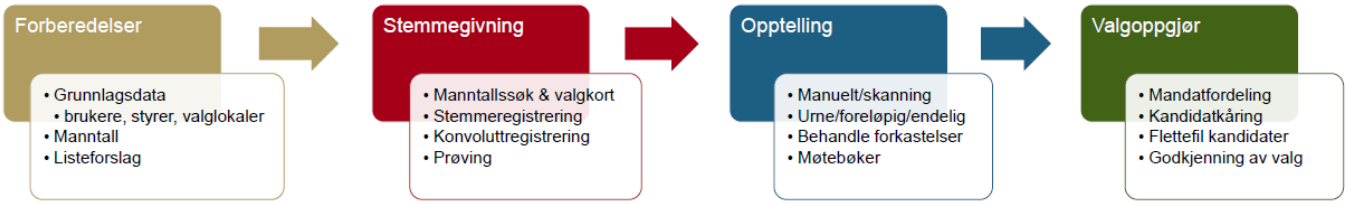
Valgstyret har ansvar for foreløpig og endelig telling i kommunene. Foreløpig telling gjennomføres manuelt i alle kommuner. Når foreløpig opptelling er godkjent, kan den endelige opptellingen gjennomføres. Valgstyret er også ansvarlige for denne. Endelig opptelling kan enten utføres manuelt, som for den foreløpige, eller maskinelt ved bruk av skannere.

Fylkesvalgstyret har ansvaret for å kontrollere alle stemmesedler og kontrollere møtebøker fra alle kommunene i fylkeskommunen. Fylkesvalgstyret kontrollteller alle stemmesedler på nytt og sammenligner resultatet med valgstyrenes resultater.

Ved stortingsvalg er det Stortingets fullmaktskomite som gjennomgår alle protokoller og møtebøker til slutt, og vurderer valgets gyldighet (godkjenner valget).

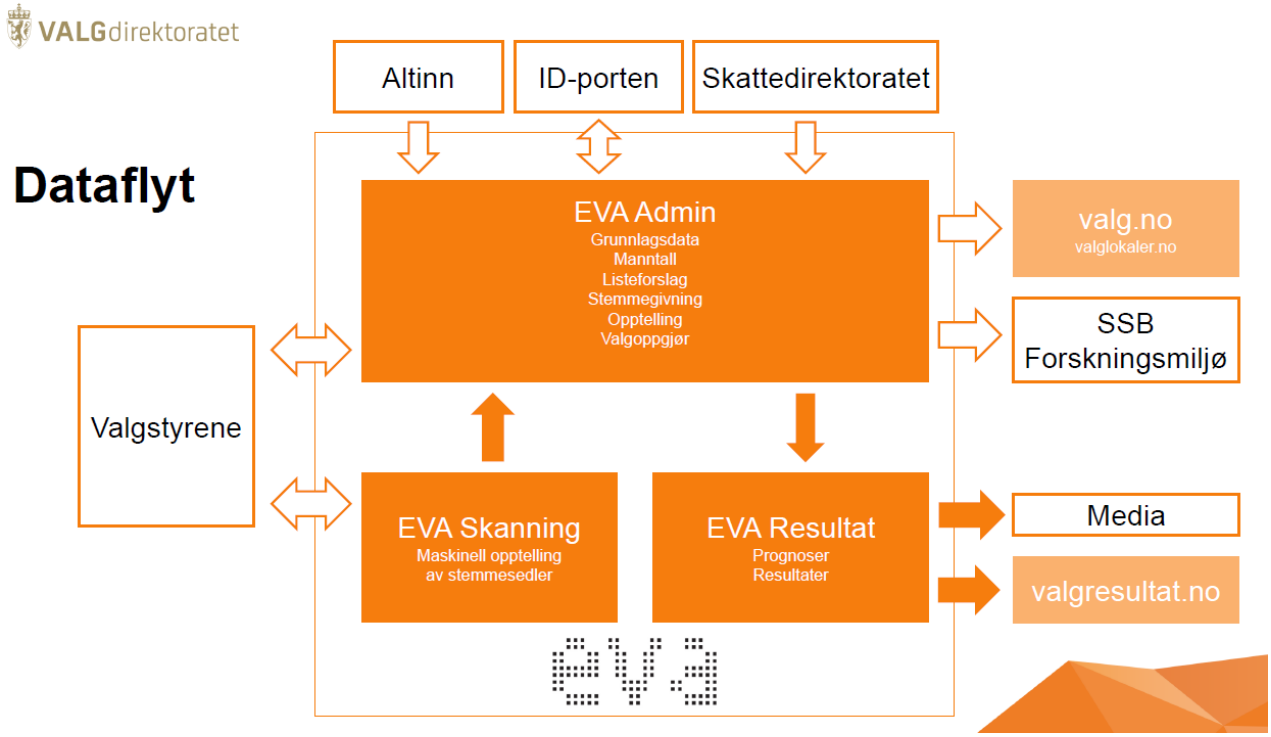
3.4 Den digitale verdikjeden

I Norge benyttes det digitale valgadministrasjonssystemet EVA, for å understøtte valg til kommunestyre, fylkesting og Storting, mens stemmegivningen fremdeles foregår manuelt. EVA utvikles, driftes og sikres av Valgdirektoratet, mens datamiljøene de lokale tilknyttede systemene kjører i, konfigureres og sikres av kommunene og fylkeskommunene. For gjennomføring av valg i kommuner og fylkeskommuner støtter EVA administrativt gjennom alle de fire nevnte fasene:



Figur 3: Valggjennomføring med EVA. *Kilde: Valgdirektoratet - gjengitt med tillatelse*

EVA består av tre hovedapplikasjoner; EVA admin, EVA skanning og EVA resultat. EVA Admin er en standard webapplikasjon som driftes og forvaltes sentralt av Valgdirektoratet, og gjøres tilgjengelig gjennom nettleser på kommuner eller fylkeskommuners PCer. EVA Skanning er en lokalt installert applikasjon som driftes av kommuner og fylkeskommuner. Applikasjonen er utviklet av Valgdirektoratet, og installasjonsfilene gjøres tilgjengelig for kommuner eller fylkeskommuner. EVA resultat er en intern applikasjon i Valgdirektoratet som sender tall mellom applikasjon og ut til andre interessenter som mediehus. I figuren fra Valgdirektoratet under skisseres flyt av data til og fra applikasjonene.



Figur 4: Dataflyt i, til og fra EVA. *Kilde: Valgdirektoratet - gjengitt med tillatelse*

Gjennom hele den digitale verdikjeden finnes det en rekke aktører og komponenter som både kan fungere som barrierer, og potensielt utgjøre sårbarheter i systemene. Manntallet overføres/innhentes fra

Skattedirektoratets baser, der både leverandører av utstyr og programvare, utviklere, driftere og ansatte brukere er en del av kjeden. Tilsvarende gjelder for utstyr og applikasjoner i Valgdirektoratet (EVA).

Kommunene og fylkeskommunene får tilgang til sentrale applikasjoner i EVA, og får lokal applikasjon og installasjonsfiler for EVA skanning fra Valgdirektoratet. Det er imidlertid kommuner og fylkeskommuner som selv står for utstyr, sikring, vedlikehold og bruk. Det foreligger veiledninger for bruk og sikring, samt rammeavtale for leverandører av støtte til EVA skanning. Det er imidlertid opp til kommuner og fylkeskommuner om og i hvilken grad de ønsker å følge anbefalingene eller benyttes leverandører med rammeavtale med Valgdirektoratet. Det kan derfor være grensesnitt mot ulike leverandører både av utstyr og programvare, og av støttetjenester, i tillegg til egne ansatte som kan sette opp, drifte og vedlikeholde.

4 Metodisk tilnærming

Systemet som skal utredes, og oppdragets innhold, er komplekst og krever tverrfaglig kompetanse og en systematisk tilnærming. Samtidig er oppdraget begrenset i tid og omfang, noe som gjør det nødvendig å holde fokus på de mest relevante problemstillingene med tanke på å understøtte arbeidet som skal utføres i valglovutvalget.

For å møte behovet for tverrfaglig kompetanse har arbeidet blitt utført av et sammensatt team som blant annet har dekket:
Valg og valggjennomføring – kunnskap om politikk og demokratiske prosesser, valglov og valgordninger, kunnskap om valgadministrasjonssystemet, erfaring og kunnskap og ulike måter og ordninger for valggjennomføring, aktører, roller og nivåer i valggjennomføring
Teknologikompetanse – Cybersikkerhet/IKT-sikkerhet, digitale verdikjeder, sårbarheter, digital sabotasje, teknologiske muligheter og risiko, digitale aktører og kapasiteter
Trusler – trusselvurderinger, identifisering av aktører og intensjoner, kapasiteter for trusselgjennomføring, angrepsvektorer, nasjonalt risikobilde
Hvordan påvirkes samfunn og velgere – nyheter og medier, kommunikasjon, menneskelige reaksjoner, bruk av digitale medier, påvirkningsvirksomhet, interesseparter
Risiko- og sårbarhetsvurderinger – metode og forskningstilnærming, utredningskompetanse, overordnet risikobilde, prosjektledelse og koordinering, tiltaksvurderinger og tiltakseffekter, regelverksforståelse og regelverksutvikling.

Metoder for kvalitativ risikoanalyse kjennetegnes ved å være prosessbaserte, tverrfaglige, systematiske og gi et godt grunnlag for å fokusere tid og ressurser mot de viktigste temaene og fenomenene. Det er derfor valgt å bygge arbeidet på metodikk for risiko- og sårbarhetsanalyse på et overordnet nivå. I store trekk har hovedtrinnene som for eksempel skisseres i den internasjonalt anerkjente standarden ISO 31000 (ISO, 2018) blitt brukt som støtte og hjelp i gjennomføring av utredningen, men tilpasset mål, behov, fokus fra oppdragsgiver og erfaringer i prosjektteamet. En slik systematisk tilnærming sikrer i stor grad at relevante og viktige elementer dekkes, diskuteres og vurderes i løpet av utredningen.

De tre hovedtrinnene som i tilpasset form er gjennomført som et underlag for denne utredningen er:

Omfang, kontekst og kriterier
Gjennom etablering av kontekst har informasjon blitt samlet inn og vurdert for å bygge en bred og felles forståelse av valgprosesser og utfordringer, samt identifisere viktige områder for videre analyse.
Etablering av kontekst har dekket:

- *Informasjonsinnhenting/erfaringer nasjonalt og internasjonalt*: I tillegg til den samlede erfaringen i det bredt sammensatte prosjektteamet har informasjon og erfaringer med valgsystemer, prosesser, trusler og sårbarheter internasjonalt og i Norge blitt innhentet. Internasjonale erfaringer har blitt høstet ved gjennomgang av litteratur, artikler og nyheter (se referanseliste). På nasjonalt nivå har det i tillegg blitt gjennomført en rekke arbeidsmøter og intervjuer med Kommunal- og moderniseringsdepartementet, Valgdirektoratet, valglovutvalget, Microsoft og med valgmedarbeidere i et utvalg kommuner av ulik størrelse og type.
- *Verdivurdering:* For å kunne gjøre en hensiktsmessig vurdering av risiko i valggjennomføring, er kriterier for demokrati, og kvaliteter som kreves av valggjennomføringen for å ivareta disse prinsippene identifisert. Gjennom utredningen fremkommer ulike verdier som må beskyttes i valggjennomføringen for at kravene skal sikres; eksempelvis i form av digitale systemer, informasjon, lokaler, velgere eller kandidater.

- *Trusselvurdering:* I tillegg til identifisering og vurdering av uintenderte hendelser som kan påvirke valgprosessene, beskrives aktører som kan ha ønske/intensjon om å påvirke/skade valgprosessen, hvilken kapasitet de har til å gjøre det, og på hvilken måte.

Risiko- og sårbarhetsvurdering
Risiko og sårbarhetsvurderingene er gjennomført ved å identifisere og vurdere potensielle hendelser og fenomener som kan forekomme før, under og etter valget. For å sikre en systematisk prosess der alle relevante forhold blir inkludert har denne blitt gjennomført med ulike innfallsvinkler. Det vil si med fokus på mulige fenomener/hendelser i selve valggjennomføringen, i den digitale verdikjeden, i forhold til de ulike kravene som må ivaretas i valget (i forhold til demokratiske prinsipper), og i et generelt faglig perspektiv. Fremgangsmåten som er benyttet for risiko- og sårbarhetsvurderingen tar utgangspunkt i internasjonale standarden ISO 31000 (ISO, 2018).

Eksisterende barrierer mot, og eventuelle sårbarheter i forhold til, de aktuelle hendelsene/fenomenene er vurdert og beskrevet. Konsekvenser som hendelsen eller fenomenet kan ha på de fem kravene til valg som beskrives i kapittel 3.1 (fri deltagelse, opplyst og informert, korrekt, gjennomført i tråd med plan og tillit) – er vurdert – sammen med hvor mye kunnskap vi har om fenomenet, hvor overførbart det er til ulike steder og områder og hvor raskt fenomenet endrer seg.

Til slutt er det gjort en oppsummering/samlet vurdering av hvor viktig/kritisk fenomenet er for sikkerhet i valgprosessen, og hvor stor mulighet samfunnet/myndighetene har til å endre eller påvirke negative konsekvenser.

Risikohåndtering
Risikohåndtering vil innbefatte både å identifisere hensiktsmessige tiltak, beslutte gjennomføring og følge opp gjennomføring og effekt. Denne utredningen fokuserer på å identifisere mulige tiltak knyttet til enkeltfenomener og hendelser (i hendelsesskjemaene vedlagt) – men først og fremst på å anbefale enkelte tiltak på et overordnet nivå som er relevant for valglovutvalgets fokus og arbeid.

Beslutninger om tiltak, gjennomføring og oppfølging ivaretas av norske myndigheter og er ikke en del av omfanget for denne utredningen.

Ytterligere detaljer om risikoanalysemetoden som er benyttet i utredningsarbeidet er vist i Vedlegg 1.

5 Trusler mot demokratiske prosesser i tilknytning til valg i Norge

5.1 Trusler mot demokratiet og mot valg?

Basert på de ulike demokratimodellene referert til innledningsvis i denne utredningen, kan demokratiet i det grunnleggende trues av ulike årsaker. Ut ifra perspektivet i konkurransedemokrati-modellen (Schumpeter, 1952), vil teoretisk sett trusler mot demokratiet lett oppstå når det over tid ikke skjer en noenlunde stabil eliteutskifting selv om valg avholdes regelmessig. Eksempler på det siste er de illiberale demokratiene som vi ser utspiller seg i Ungarn, Russland eller Tyrkia. En annen trussel er forstyrrelser i selve valgprosessen, som for eksempel hvis dataangrep fører til feilrapportering eller ødelegger for effektiv gjennomføring. Det siste er i prinsippet alvorlig ikke bare i kraft av selve hendelsene, men også som en trussel mot tillitskapitalen til demokratiet.

Sett fra den republikanske demokrati-modellen (Pettit, 2014; Skinner, 1978; Pateman 1970) vil den samlede demokratiske deltakelsen ikke bare under valgene, men også i periodene mellom valgene, være et essensielt hensyn. Særlig vil rekrutteringen til demokratiske verv og til partiene kunne være et kritisk punkt, og det samme gjelder i hvilken grad samfunnsmedlemmene kjenner og viser borgerånd.

Ut fra den deliberative demokratimodellen (Habermas, 1996; Gutmann and Thompson, 2004) spiller valgkampen og de politiske debattene en nøkkelrolle i demokratiet. Debatten må være opplysende og tendenser til en fragmentering av offentligheten kan virke nedbrytende på læringen i en felles offentlighet. Det samme gjelder en offentlig samtale pervertert av falske nyheter, ekkokammer eller avsondrete demokratiske samtaler i ulike grupperinger som mangler en felles argumentativ meningsbrytning.

Trusler mot de demokratiske prosessene, og trusselaktørene bak, vil altså kunne rette seg mot alle disse områdene for å svekke demokratiet – som oppsummert i systembeskrivelsene innledningsvis gjennom å svekke fri deltakelse, opplyst og informerte valg, korrekte valg, valg gjennomført etter plan og tillit til valg og prosess.

Angrep på, påvirkning av eller «juks» knyttet til valg er ikke noe nytt fenomen. I den vestlige verden er det imidlertid et område som ofte forbindes med ikke-demokratiske stater, og i mindre grad til de vestlige demokratiene. Samfunnet er i endring. Vi ser en økt politisk påvirkningsaktivitet i Europa. Valgprosesser er i økende grad utsatt for påvirkning fra en rekke aktører, også aktører utenfor statens grenser. De siste årene har fokus på trusler mot valg i demokratiene økt betydelig. De store og brede internasjonale diskusjonene og fokuset akselererte betydelig i forbindelse det amerikanske presidentvalget i 2016 og Brexit-avstemmingen i Storbritannia samme år. Det ble blant annet avdekket at detaljert informasjon om brukere av facebook ble samlet, analysert, solgt og brukt til å målrette budskap under den amerikanske valgkampen[1].

Det har over de siste årene blitt avdekket at statlige aktører, herunder Russland, aktivt har brukt produksjon og spredning av falske nyheter for å påvirke politiske prosesser og valgprosesser i en rekke land (USA, Frankrike, Nederland, Tyskland og Storbritannia). En rekke medier[2] referer i februar 2019 til meldinger om at USA blant annet sørget for å stenge nettilgangen for den den russiske trollfabrikken Internet Research Agency i St. Petersburg i forbindelse med mellomvalg i USA høsten 2018. Trollfabrikken skal også ha operert under det amerikanske valget i 2016.

Påstander om manipulering av stemmer via såkalte valgmaskiner (som benyttes til elektronisk stemmegivning), har vært et hett tema de siste årene. I 2018 demonstrerte en gruppe hackere i

[1] (https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html)
[2] https://www.nrk.no/urix/trump-blokkerte-russisk-trollfabrikk-1.14448589

samlingen DEF CON Voting Village blant annet at amerikanske valgmaskiner kunne hackes remote, og at hacking av maskinen lokalt kunne gjøres ved hjelp av en penn på to minutter (mens en gjennomsnittlig stemmeoperasjon tok 6 minutter)[3].

Mange faktorer påvirker hvem som blir utsatt for påvirkninger i valg, hvem aktørene er, – og hvilke metoder som benyttes. I dette ligger alt fra global politisk utvikling og maktbalanse, samfunnstrender og radikalisering; til lokale forhold og den teknologiske utviklingen.

5.2 Trusler mot Norge, trusselaktører og virkemidler

Vurderingen av aktører baserer seg på åpne etterretningskilder/trusselvurderinger fra eksempelvis PST og Etterretningstjenesten, og det refereres også fortløpende i teksten til andre informasjonskilder.

Av flere årsaker kan en se for seg at Norge ikke er spesielt attraktivt med tanke på å påvirke valgresultater og valg. Norge er et lite land, med begrenset innflytelse og makt på mange internasjonale felter. Utenrikspolitikken er preget av en høy grad av konsensus, slik at det er lite å vinne eller endre ved å endre sammensetningen på Stortinget. Det norske samfunnet er preget av en høy grad av tillit til demokratiet, til prosesser rundt valg, og til politikere – noe som gjør det mer krevende å påvirke gjennom eksempelvis falske nyheter. Det er begrenset tilstedeværelse av radikaliserte grupperinger, og det er også stor grad av åpenhet og gjennomsiktighet i et så lite samfunn – noe som også gjør påvirkningskampanjer vanskeligere å gjennomføre (PST, 2019).

Samtidig representerer Norge og Norden noen av spydspissene av liberaldemokratier. Flere stater med helt andre styresett kan ha interesse av å demonstrere hvor uegnet dette er som styreform. Norge er medlem av FN og NATO, og er slik del av et internasjonalt engasjement. Det norske engasjementet i Nordområdene og Arktis er av interesse for flere aktører, både av politiske og kommersielle årsaker.[4] Et langt på vei gjennomdigitalisert samfunn gir trusselaktører en stor angrepsflate på sosiale medier og i det digitale rom generelt. I kombinasjon med det som ofte beskrives som en lav årvåkenhet i sikkerhetsanliggender («naivitet») kan det gi et potensial for påvirkning som interesserer.

5.2.1 Trusselaktører

Trusselpotensialet mot demokratiske valgprosesser kan kategoriseres innenfor tre hovedaktørgrupper: Statlige, ikke-statlige og enkeltaktører.

Eksempler på **statlige aktører** er typisk Russland og Kina, men herunder kan også nære samarbeidspartnere som USA, Storbritannia og Sverige ligge. Det foregår kontinuerlig legitim (åpen) og fordekt (skjult) påvirkning fra andre stater for å få innflytelse og mulighet til å påvirke norsk standpunkt i store strategiske spørsmål. Russland er en dimensjonerende trusselaktører med tanke på kapasitet og utvist vilje til å angripe[5], og er beskrevet og vurdert i større detalj i vedlegg 4 til denne rapporten.

På tross av at kinesisk politikk har endret seg substansielt under nåværende leder Xi Jinping, har Kina tradisjonelt hatt en sterk føring på *ingen innblanding i andre staters indre anliggender*. Kina har økte interesser i Arktis og nordområdene i forbindelse med sitt *One-Belt Initiative*, hvor de ønsker å åpne en isfri sjøvei for handel via sjørutene gjennom Arktis. Kina ønsker også tilgang på muligheter for utvinning av naturressurser som mineraler og gass i Arktis. [6]

[3] https://defcon.org/images/defcon-26/DEF%20CON%2026%20voting%20village%20report.pdf
[4] Nordlys 2januar 2019, nyttårstale General Kjell Grandhagen https://fr-ca.facebook.com/pg/ndebatt/posts/

[5] https://www.nupi.no/Arrangementer/2017/Paavirkningsoperasjoner-og-desinformasjon-som-verdensfenomen

[6] https://www.vg.no/nyheter/utenriks/i/0EdWdG/kina-vil-bli-supermakt-i-norske-farvann

Norge-Kina-relasjonen har over lang tid vært på frysepunktet. Relasjonen er under oppmykning i forhold til økt handel og samarbeid innen forskning og næringsliv. Kina kan utgjøre en trussel for Norge innenfor cyberdomenet, gjennom cyberangrep og spionasje, innenfor flere sektorer av samfunnet. Det har vært gjennomført cyberangrep fra Kina mot Norge, så trusselen fra Kina kan på ingen måte utelukkes, men den vil først og fremst trolig rettes inn mot kritisk infrastruktur, forskning, finans- og næringsliv (Etterretningstjenesten, 2019). Det er lite sannsynlig at Kina vil ha interesse av å påvirke demokratiprosesser og valg i Norge, men heller konsentrere sin politiske påvirkning mot for eksempelvis Australia og Canada og andre land med store kinesiske eksilgrupperinger.

De mest fremtredende **ikke-statlige aktørene** er nettverk knyttet til ekstrem islamisme, og politiske miljøer på den ekstreme høyre- eller venstresiden.

Det har generelt vært få volds- og terrorhendelser mot valg eller valgprosesser fra slike miljøer. På tross av økende høyreekstremisme i Europa, vurderes ikke trusselen fra slike miljø å være spesielt stor i Norge. Det er flere grunner til det, men hovedårsaken er svak organisering og fravær av tydelige lederskikkelser (PST, 2019). Hvis det likevel skulle inntreffe voldelige demonstrasjoner eller annen voldsutøvelse mot valg eller valgprosessen vil den trolig være i begrenset omfang, dårlig organisert og inntreffe i regionalt geografiske områder i Norge hvor enklaver av miljøene allerede har tilhørighet, som for eksempel Trondheim, Kristiansand og enkelte submiljø på Østlandet. Trolig vil eventuell vold fra dette miljøet rettes inn mot sak og enkeltpersoner som de kan ha sterke antipatier mot og ikke nødvendigvis valget som sådan.

Enkeltaktører kan ha sympatier for de overnevnte aktørene, men kan også handle ut fra andre beveggrunner. Typiske eksempler på denne typen aktør er Anders Behring Breivik og radikaliserte islamister.

Det har vært enkelte angrep fra soloaktører mot parlament og politikere fra radikale islamistmiljøer i Nederland, Tyskland og Canada, men så langt ingen spektakulære angrep. Angrep fra islamistmiljøer i Norge mot valg anses som lite sannsynlig.

Andre enkeltaktører som vil kunne påvirke valg og demokratiske prosesser kan være større konsern, tenketanker og enkeltpersoner, som ved meningspåvirkning og/eller pengestøtte til partier eller enkeltpersoner, har som hensikt å påvirke utfall eller retning av valg eller prosess.

Hver av disse kan igjen knytte til seg en rekke underliggende aktører for å oppnå sine mål. De underliggende aktørene kan være rekrutterte, pressede, opportunistiske eller autonome, som illustrert i Figur 5. Rekrutterte aktører vil av egen vilje handle i henhold til hovedaktørens mål, direkte styrt av hovedaktøren. De pressede aktørene vil mot egen vilje handle i henhold til hovedaktørens mål, direkte styrt av hovedaktøren. De opportunistiske aktørene vil av egen vilje handle i henhold til hovedaktørens mål, men uten styring fra denne. De autonome aktørene vil handle i henhold til hovedaktørens mål uten at hovedaktøren styrer dette, og uten å selv ønske det (men gjennom sin egen agenda).

Figur 5: Underliggende aktører

5.2.2 Analyse av dimensjonerende aktør

Basert på kildene nevnt over og i teksten, er det gjort en mer omfattende analyse av Russland som trusselaktør i vedlegg 4 til rapporten. Russland er en dimensjonerende aktør for Norge både med tanke på vår geografiske beliggenhet, internasjonale interesser, og Russlands kapasitet. En analyse er derfor interessant for å forstå mulige intensjoner, virkemidler/metoder og kapasiteter. Analysen er basert på åpne etterretningskilder og kilder det ellers refereres til i teksten.

5.3 Påvirkning gjennom nett/sosiale medier

Påvirkninger av samfunn og velgere for å oppnå endring i holdninger eller atferd er, og har vært, en viktig del av samfunnsdebatten og av det å drive valgkamp. Påvirkning er målet med den politiske debatten – for å skaffe flere tilhengere for eget/partiets syn og vinne flertall for å prege samfunnsutviklingen. Det å jobbe for å endre en velgers syn og oppfatning av hva som er riktig og galt, best og dårligst i en slik åpen debatt, er legitimt – og nødvendig for at det politiske systemet skal virke. Intensjonen er kjent og klar.

Et stort fokus både nasjonalt og globalt har spesielt de siste årene imidlertid vært påvirkning, og forsøk på påvirkning, av valg på enn måte som ikke er legitim. Det er lett å se at påvirkning ved å bruke feilaktig/falsk informasjon ikke er ønsket. Når sannheter og usannheter blandes sammen, eller elementer tas ut av sammenheng eller bare deler av en problemstilling belyses, blir det vanskeligere å skille mellom hva som er en ønsket og legitim påvirkning, og hva som er en uønsket og illegitim påvirkning. En uønsket påvirkning kan sies å ha en dårlig intensjon, i motsetningen til den ønskede som har en god intensjon. Utfordringen er å definere hva som er godt, og hva som er dårlig. Ulike ståsteder gir gjerne ulike svar. I enkelte stater har en forsøkt å definere uønsket påvirkning av nasjonale valg som en påvirkning som kommer utenfra landets grenser. Erfaringer og saker som er avdekket de siste årene viser imidlertid at også statlige trusselaktører etablerer påvirkningsaktiviteter nasjonalt i den staten de ønsker å påvirke. En annen viktig karakteristikk ved uønsket påvirkning, er at den ofte er skjult. I det ligger at det ikke er kjent for den som blir forsøkt påvirket hvem som står bak og hva intensjonen med påvirkningen er (eller det at det faktisk søkes å påvirke.

Dersom nyheter eller påstander settes fram uten å stå i en sammenheng (kontekst) er det vanskeligere å vite om det som sies er rett eller feil. Korte meldinger på nettet er en god arena for nettopp å spre informasjon som tilsynelatende er rett, men som er tatt ut av kontekst. Dersom en nyhet inneholder deler som en velger kjenner seg igjen i og mener er korrekt, er det lett å feste lit til det som leses /høres.

Dersom deler av nyheten er feilaktig, gjør kombinasjonen av riktig og uriktig at det er vanskeligere å avsløre feilen eller usannheten. Det politiske uavhengige, amerikanske forskningssenteret Pew Research Centre[7] har forsket på folks medievaner og mener at personer under 50 år får halvparten av nyhetene sine gjennom digitale medier. De mener også at folk har lettere for å akseptere informasjon som bekrefter egen overbevisning og at en lettere avviser informasjon som ikke bekrefter eget syn. Stephen Lewandowsky jobber ved University of Bristol og er en av verdens ledende eksperter på det som kalles kontrafaktisk overbevisning. Han sier[8] at folk ofte starter med en forutinntatt overbevisning (kognitiv motivasjon) – for deretter å bruke all sin tenking på å støtte opp under oppfatningen.

Dagens digitalisering og omfattende bruk av sosiale plattformer gir trusselaktører en stor angrepsflate der mange velgere kan nås på kort tid. Den raske spredningen og delinger av nyheter setter også press på de redaktørstyrte mediene. Presset om å publisere raskt kan bidra til at det som betegnes som seriøse medier videreformidler uriktig innhold fordi kildene ikke blir sjekket godt nok – eller kanskje ikke i det hele tatt. På den måten bidrar de til å legitimere de uriktige nyhetene. Organisasjonen Freedom House (USA) undersøkte i 2017 ulike lands tilnærming til falske nyheter, og viser i sin rapport[9] til at minst 30 stater betaler kommentatorer for å lage og videreformidle falske nyheter. En forskningsrapport i Science fra 2018 (Soroush, Deb and Sinan, 2018) beskriver at falske nyheter sprer seg oftere enn ekte. Forskerne brukte seks ulike organisasjoner som jobber med å sjekke fakta – for å avklare om nyhetene var ekte. De mener at det er 70% prosent større sjanse for at falske nyheter blir retvitret framfor ekte.

Stadig mer informasjon om hver enkelt borger er tilgjengelig i det digitale rom i ulike deler og bruddstykker. Når dette kombineres med algoritmer som kan analysere store mengder data, gir det mulighet for å finne ut svært mye om den enkeltes preferanser, syn og interesser. Dette kan brukes til å tilrettelegge hverdagen for den enkelte, men åpner samtidig muligheten for å fore den enkelte med ensrettet informasjon som styrker forutinntatte meninger (motargumenter presenteres ikke). I verste fall kan en trusselaktør finne den enkelte velgers sårbarheter for påvirkning, og uten at velgeren er klar over det, tilpasse informasjon og budskap slik at meninger og oppfatning skyves i den retningen aktøren ønsker.

Når uønsket påvirkning er vanskelig å definere, blir den også vanskelig å hindre. Balansen mellom å fjerne illegitim påvirkning og det å drive sensur og hindre ytringsfriheten, er krevende.

5.3.1 Bruk av påvirkning mot valgprosesser

Påvirkning av politikere
Både nasjonalt og internasjonalt har det de siste årene vært fokus på forsøk på (og gjennomføring) av informasjonsinnhenting og påvirkning rettet mot politiske partier og kandidater som stiller til valg. En rekke hendelser og eksempler har kommet fram etter eksempelvis valget i USA i 2016, men også nasjonalt ble det i forkant av stortingsvalget i 2017 bekreftet[10] at det var gjennomført et hackerangrep som blant annet omfattet Arbeidspartiet og Forsvaret. Motivasjonen for slike angrep har flere utgangspunkt. Politikere, politiske og andre statlige organer sitter i beslutningsposisjoner og påvirker politisk retning nasjonalt og internasjonalt. Både det å skaffe seg informasjon om planer, strategier og retninger – og også påvirke disse, er av interesse for statlige og andre store interesseaktører. Både gjennom det at angrep

[7] https://www.pewresearch.org/
[8] https://journals.sagepub.com/doi/abs/10.1177/0963721416654436?journalCode=cdpa
[9] https://freedomhouse.org/article/new-report-freedom-net-2017-manipulating-social-media-undermine-democracy
[10] https://www.aftenposten.no/norge/i/A1OEz/Nasjonal-sikkerhetsmyndighet-Avansert-gruppe-sto-bak-hackerangrep-i-Norge

gjennomføres, og ved bruk av tilgang og informasjon som innhentes, kan aktøren påvirke og redusere tilliten til politikere, partier og demokratiske prosesser generelt. I tillegg kan bruk av informasjon gi aktøren mulighet til å både presse og påvirke enkeltindivider og organisasjoner til å skaffe mer informasjon eller bidra til beslutninger som gagner aktøren på noen måte.

En annen måte å ramme partier og kandidater på, er ved diskreditering av politikere. Dette kan direkte påvirke på hvem som får mulighet til å delta i det politiske arbeidet. Diskreditering kan medføre at en politiker mister verv og innflytelse over lang tid – og/eller for godt, og dermed potensielt forskyve balansen i det politiske landskapet. Diskreditering av spesielt profilerte politikere mer generelt kan også bidra til å svekke tilliten til systemet og demokratiet (det er ingen vits i å stemme, politikere er ikke til å tro på, det er bare rot osv.). Svertekampanjer eller såkalte «drittpakker» har blitt kjente begreper i det politiske medielandskapet. Vanligvis forstås med dette at det spres informasjon mer eller mindre koordinert i flere ulike kanaler, med det formål å påvirke omdømmet til aktuell politiker, organisasjon eller parti negativt. Karakteristisk er at informasjonen har sannhetselementer i seg – men ofte er tatt ut av sammenheng, eller bare viser deler av sannheten. Informasjonen er gjerne på områder/felter der aktuell politiker må gå ut for å tilbakevise denne eller forsvare seg. I veldig mange tilfeller ender diskrediteringen med at politikerne «fjernes» fra det politiske landskapet, da det de har gjort ikke anses som forenelig med rollen.

Netthets og ytringsklimaet generelt på nett, oppleves av mange som et økende problem. Til forskjell fra temaet «diskreditering» vil netthets typisk forhindre politikere eller andre fra å delta i debatten fordi de selv ikke ønsker å ta belastningen det medfører – ikke fordi de mister eller ikke får lov til å ta en posisjon. Netthets handler ofte om negative ytringer og meninger, ikke nødvendigvis om forhold som er sanne eller usanne. Det beskrives stadig i media at ordbruken i det offentlige ordskiftet har hardnet til – og at grensene for det som er «innenfor» stadig blir skjøvet på. Den offentlige samtalen – med respekt for andres synspunkt – presses stadig, og oftere enn tidligere blir ytterliggående synspunkt bifalt. Netthets kan bidra til at enkelte grupper avstår fra å delta i demokratiet og i valg.

Påvirkning av velgere

Falske nyheter har alltid eksistert, men har fått et tiltagende fokus i den offentlige debatten, spesielt etter presidentvalget i USA i 2016. Diskusjoner rundt hvorvidt og hvor mye usannheter, misvisende og feilaktig informasjon og falske nyheter påvirker valg – og hvordan slik påvirkning kan stoppes/reduseres – er utbredt. Å klare å skille fakta og falske nyheter fra meninger og ulike sider av en sak, er en stor utfordring med tanke på å fjerne dette fenomenet fra valgdebatten, uten at det blir stilt spørsmål vedrørende sensur og redusert ytringsfrihet. I mange tilfeller startes falske nyheter på plattformer for sosiale medier, og spres videre til mer tradisjonelle medier. Ofte legitimeres de ved å utnytte andre verktøy og fenomener som ekkokamre og avatarnettverk. Falske nyheter knyttet til politikere og valg kan fort få store konsekvenser. Informasjon, kommunikasjon og konsekvenser forløper raskt – og selv om en falsk nyhet avdekkes på et senere tidspunkt, kan skaden og konsekvensen være irreversibel.

Fenomenet «deep fake» er også økende i digitale medier. I dette ligger at AI-teknologi benyttes til å produsere og/eller endre lyd og bilde slik at det presenteres noe som faktisk ikke har skjedd. Utviklingen i teknologi på dette feltet skaper en økende utfordring med å avsløre at slike lyd-/bildemontasjer faktisk er falske. «Deep fake» endrer synet vårt på hva som er et bevis. Nå kan heller ikke levende bilder anses som en sannhet. Å produsere «deep fakes» krever ikke spesiell kunnskap, og kan i stor grad gjøres av hvem som helst.

En voksende industri gjennom flere år har vært muligheten for å, i digitale kanaler, påvirke menneskers oppfatning av hva som er populært, vanlige/riktige meninger og «trendy». Dette gjøres gjennom at både falske profiler (profiler for ikke-eksisterende brukere) og faktiske profiler, benyttes til å følge, like og mislike firmaer, nettsteder, innlegg og personer. Den faktiske «klikkingen» kan utføres både av algoritmer som autogenererer for eksempel likes, og av arbeidere ansatt i såkalte «klikkfarmer» der de betales for å

klikke på spesifikke nettsteder, innlegg osv. Disse arbeiderne kan også ha opprettet og administrerer et stort antall falske profiler. Bruk av falske profiler er brudd på «terms and services» for eksempel hos Facebook. Falske klikk er ikke regulert, det vil si at en kan reklamere for denne tjenesten på Finn.no. Kjøp av falske klikk og falske følgere brukes i dag av seriøse nettsteder. Dermed er falske klikk et middel i «vanlig» påvirkningsarbeid. Et økende fenomen har også vært store såkalte «avatarnettverk» som er falske profiler (eksisterer kun på nett) som kan benyttes til massiv påvirkning på saker og områder. Slike avatarer kontrolleres av en påvirkningsoperatør og har stor grad av sikkerhet innebygget i seg. For eksempel vil systemet beskytte operatøren mot å bruke IP adresser utenfor den geografiske regionen der den aktuelle avataren befinner seg, eller mot å legge ut informasjon som er på et annet språk enn det avataren er oppført med.

I Skandinavia er tilliten til myndigheter og systemer høy, og vi tar som en selvfølge at valgresultatet er korrekt. Imidlertid viser siste valg i Sverige at det ble sådd tvil om også dette[11]. Nettforbindelsen falt ned en periode under opptellingen. Da nettet kom opp igjen var «stillingen» mellom partiene betydelig endret. Dette førte til mistanker om at resultatene var endret/manipulert, og mistankene spredde seg raskt i ulike medier. Dette kan ha en direkte politisk hensikt, for eksempel for å fremme eget syn eller skape tvil om andres interesser og intensjoner. Imidlertid er dette ikke minst egnet til å svekke tilliten til myndigheter, systemer og demokratiske prosesser, og etablere mistro.

I dagens digitale samfunn er det en økende forretning knyttet til innhenting, analyse og salg av informasjon om brukerne. Algoritmer, maskinlæring og kunstig intelligens benyttes til innsamling av data, og analyse av informasjon med en effektivitet vi ikke tidligere har vært i nærheten av. Resultatet blir tilgang til svært detaljert informasjon om nettbrukerne, som i dag langt på vei er de aller fleste av oss. I sin enkleste form kan det dreie seg om isolerte opplysninger om interesser og preferanser for produkter. Ved bruk av algoritmer og kunstig intelligens har det imidlertid vist seg at det er mulig å analysere og identifisere, med forbløffende treffsikkerhet, preferanser og syn politisk og religiøst, etnisk tilhørighet, seksuell legning og andre dype personlighetstrekk hos brukerne. Resultatet blir tilgang til svært sensitiv informasjon som kan benyttes både til helt uskyldige formål og til mer diskutable formål – bevisst eller ubevisst. Ved å bruke den mest detaljerte og sensitive informasjonen som genereres om brukere av nettet, kan informasjon og budskap mikromålrettes mot hver enkelt bruker for å påvirke i den retningen aktøren ønsker. Slik påvirkning kan være rettet direkte mot beslutninger og valg av politisk retning, men også benyttes mer generelt for å polarisere, skape uro, forsterke fordommer og etablere mistillit (og gjerne i kombinasjon med andre fenomener som fake news). Saker som Cambridge Analytica og bruk av sensitiv brukerinformasjon i den amerikanske valgkampen i 2016 har aktualisert temaet[12].

5.4 Cyberangrep

I et cyberangrep er noen ute etter å avsløre, ødelegge, skade/endre eller utilgjengeliggjøre digitale data og/eller systemer. I en tid med stort fokus på digitalisering har cybersikkerhet blitt et tema som nærmest daglig er representert i nyheter landet rundt. Det pekes stadig på innbrudd i bedrifter, manglende sikkerhet i systemer, og bekymringer rundt kunstig intelligens og maskinlæring. Cybersikkerhet har allerede stort fokus knyttet til valgprosesser, selv om elektroniske valg ikke er realisert i Norge per i dag.

Cybersikkerhet preger den Norske mediedekningen, og borgernes bevissthet rundt trusler har blitt en daglig debatt. Personer, og en rekke bedrifter, har selv erfart å få hemmeligheter blottlagt, verdier kryptert og holdt til gissel, eller identitet misbrukt. Vi ser politiske partier sine epostkonti brutt inn i, og sensitiv informasjon kommer på avveie[13]. Bedrifter i Norge har vært på randen av konkurs fordi angripere

[11] https://www.isdglobal.org/isd-publications/smearing-sweden-international-influence-campaigns-in-the-2018-swedish-election/
[12] https://www.nrk.no/nyheter/cambridge-analytica-1.13973142
[13] https://www.aftenposten.no/norge/politikk/i/RAVQW/Arbeiderpartiet-utsatt-for-hacker-angrep

med liten kompetanse har klart å bryte seg inn i infrastrukturen og deretter kryptere alle servere mot løsepenger. Visma gikk ut offentlig med sitt innbrudd i 2019, der de mener at statlig tilknyttede aktører har klart å bryte seg inn i informasjonssystemene for å stele bedriftssensitiv informasjon[14].

Cybertrusselen er reel; den er progressiv og i rask utvikling. Det eksisterer sårbarheter i de fleste produkter, og selv velbrukte og kjente produkter som Microsoft Windows får månedlig kritiske sikkerhetsoppdateringer. En kritisk sikkerhetsoppdatering er en endring i programvaren som er ment å hindre trusler enkel tilgang til datamaskinen, for eksempel virus som klarer å spre seg på nettverk, uten at brukerne kan noe for det. Dette er helt normalt, og er typisk for komplisert og omfattende programkode slik som et operativsystem har. Til tross for dette klarer samfunnet likevel å fortsette mer eller mindre som før. Mye av grunnen ligger i at sikkerheten er bygget i flere lag, gjennom tiltak som brannmurer, antivirus og annen sikkerhetsteknologi. Det er likevel ingen tvil om at programvaren har sårbarheter til enhver tid, og noen ganger klarer ikke teknologien å beskytte oss.

Cyber kriminalitet har blitt «big business». Terrorist/hacking organisasjoner som The Dark Overlords annonserer at de leter etter nye medarbeidere, og tilbyr startlønninger opp i svimlende 500.000 kr i måneden[15]. Kostnadene som resultat av cyberkriminalitet utgjør milliarder på verdens basis, og i Storbritannia, er det estimert årlige kostnadstap på nærmere 320 milliarder norske kroner[16]. Så tidlig som i 2009 var Symantec ute med en rapport som pekte på at inntektene fra cyberkriminalitet hadde oversteget inntekter fra dopsalg[17].

Det er viktig å ikke underkjenne angriperne sine kapasiteter og motivasjon. I 2010 ble det avslørt et virus som klarte å hemme Iran sine uranutvinningsfasiliteter i flere år. Viruset ble blant annet distribuert via USB-brikker på konferanser som omhandlet utvinning av uran. Videre ville forfatterne av viruset at det kun skulle infisere og spre seg til datamaskiner som var av Iransk opprinnelse. Viruset var designet til å ta over datasystemer var tilkoblet industrikontrollsystemer, men kun av en spesifikk type, den som er i bruk for å styre anlegg for utvinning av uran. Viruset ble deretter brukt til å kamuflere seg i kontrollsystemene, for å gradvis, men målrettet hindre effektiv utvinning av uran[18].

Cyberdomenet har blitt et kritisk område også for Norge. Teknologien beveger seg så raskt at vanlige mennesker sliter med å henge med. Det blir også en utfordring at teknologien utvikler seg så raskt at politikere som blant annet skal beslutte rundt forsvarsmekanismer som digitalt grenseforsvar, ikke klarer å følge med på utviklingen.

5.4.1 Cyberangrep og valg

Den kanskje viktigste utfordringen med cyberdomenet i tilknytning til valg, er at det benyttes som en plattform og et verktøy for å drive påvirkning av ulike samfunnsgrupper. Noen av de mest relevante fenomenene av denne typen er beskrevet grundigere ovenfor.

Sveits hadde i 2018 utviklet og ønsket å rulle ut et trygt og sikkert internettbasert system for elektronisk stemmegiving, planlagt lansert i 2019. I starten av 2019 ble det imidlertid identifisert svakheter i systemet, noe som ville tillatt ett enkelt individ å påvirke valget i en hvilken som helst retning som man måtte ønske[19]. Det sveitsiske systemet ble hacket, men det var enda ikke satt i produksjon. Myndighetene testet ut programvaren online, slik at alle som ville kunne prøve å se om de kunne finne feil og sårbarheter, ofte kalt et «bug bounty»-program. Et slikt program lar eksperter og vanlige

[14] https://www.recordedfuture.com/apt10-cyberespionage-campaign/
[15] https://thehustle.co/dark-overlord-hacker-cybercrime-software-engineer-hiring/
[16] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
[17] https://www.symantec.com/content/en/us/home_homeoffice/media/pdf/norton_cybercrime_exposed_booklet.pdf
[18] https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html
[19] https://motherboard.vice.com/en_us/article/zmakk3/researchers-find-critical-backdoor-in-swiss-online-voting-system).

mennesker prøve å avdekke sårbarheter, i bytte mot en betaling dersom de rapporterer sårbarhetene. I det sveitsiske tilfellet Sveits, tilbød staten opp til 50 000 sveitsiske franc som betaling dersom sårbarheten lar en bruker manipulere valget uten å bli detektert.

Til tross for betydelige tiltak med innebygd sikkerhet, rutiner, beskyttelse og testing, vil innbrudd i kritisk infrastruktur som valgsystemer, ikke kunne utelukke/forhindres fullstendig. Det må antas at infrastruktur er eller kan bli, kompromittert, og at det i tillegg til å forsøke å hindre inntrenging, må etableres verktøy og prosesser som kan oppdage, detektere og hindre skade. Paradigmet har tidligere vært å investere i maksimal beskyttelse, og forsøke å tette alle skott. I dag finnes en anerkjennelse av at selv det beste forsvar kan feile. Paradigmet skifter mot et mer deteksjonsorientert IT-miljø som også fokuserer på deteksjon og håndtering for å hindre skade dersom forsvaret penetreres.

Selv om valgsystemer er blitt kompromittert, for eksempel i form av hacking, så betyr dette ikke at man har tapt «kampen». Trusselaktørene er ute etter å sikre sine mål, som for eksempel å påvirke valget. Dette er ikke gjort uten videre, og dersom de kan detekteres og «kastes ut» igjen før de når sine mål, er faktisk skade forhindret. Samtidig vil også slike angrep, dersom de blir kjent for allmenheten, bidra til å skape uro og redusere tilliten til system og prosesser.

Det er mange muligheter for å angripe IT-miljøer som underbygger valginfrastruktur som Norge innehar i dag. Det kan gjøres via menneskene som opererer infrastrukturen, hos eller via tjenesteleverandører, gjennom feil og sårbarheter i programvare eller i den underliggende maskinvaren som er i bruk.

I Norge har vi (i 2019) 356 kommuner. Den minste kommunen er Utsira med kun et par hundre innbyggere, mens kommuner som Oslo har flere hundre tusen innbyggere, nesten 700.000 per 1. Januar 2019[20].

Drift av IT-systemer er en komplisert oppgave, som de aller fleste private foretak sliter med i dag. Grunnleggende rutiner som programvareoppdateringer, sikkerhetskopiering og segmentering i nettverk blir ofte glemt eller ikke gjort regelmessig nok. Det er ingen grunn til å tro at norske kommuner er annerledes. Skanneutstyr og PCer som benyttes i kommunen er eksponert for hacking, eller kan være forhåndskonfigurert med virus fra leverandørene. En slik kommunal PC benyttes til å aksessere både EVA Scanning og EVA Admin, systemene for å håndtere skanning av stemmesedler og administrering av valgutførelse. Ved et slikt innbrudd vil et plantet virus kunne endre på informasjonen som blir tilført til EVA Admin, på samme måte som en banktrojaner kan få nettleseren din til å endre på beløpene og kontonummer som blir lagt inn i nettbanken. Manglende sikring og overvåking av IT-utstyret som benyttes gir mulighet for at virus introduseres. Et kamuflert virus vil være vanskelig å oppdage og stoppe.

Ved maskinell telling av stemmer skannes stemmesedlene med en skanner, og fortolkes av programvare som eies og utarbeides av Valgdirektoratet (EVA skann). Det er imidlertid kommunene som installerer EVA skann lokalt og som håndterer utstyr, programvare og bruk (med eller uten støtte fra leverandør). I dette systemet ligger flere muligheter for feil/manipulering av stemmeantall gjennom programvaren:

- Skannere kan vise feil «bilde» (for eksempel kryss flyttes til annet parti konsekvent)
- Fortolkningsprogrammet, EVA skann, kan lese noe annet enn det som det skannede bildet viser
- Feil/manipulering av overføringer mellom skanner og fortolker og mellom EVA skann og EVA admin.

Det elektroniske valgadministrasjonssystemet i Norge (EVA) utvikles og driftes av Valgdirektoratet (Vdir), og er også fysisk plassert hos Vdir. Som for utstyr og programvare som driftes av kommunene, vil det være muligheter for «innbrudd» også i EVA som driftes sentralt. Det kan for eksempel dreie seg om sårbarheter i programkode utviklet av Valgdirektoratet, sårbarheter introdusert i hardware, sårbarheter i

[20] https://www.ssb.no/befolkning/statistikker/folkemengde/aar-per-1-januar

tredje parts programvare eller at trusselaktørene får tilgang til nettverk der kritisk infrastruktur kjører via andre måter, for eksempel virus på en ansatt sin PC.

Manntallet ligger til grunn for hvem som får stemme i Norge – og overføres til valgadministrasjonssystemet fra Skattedirektoratet. En manipulering av manntallet kan gi «ikke-eksisterende» personer mulighet til å avgi stemmer som påvirker et valg, eller mulighet for å stemme mange ganger med samme identitet. Manntallet kan tenkes manipulert enten ved at Skattedirektoratet hackes fra utsiden, eller ved at selve registeret endres av noen med tilgang. Siden manntallet som legges i valgadministrasjonssystemet periodisk overskrives av oppdatert manntall fra Skattedirektoratet, er det manipulering av grunndata hos Skattedirektoratet som fremstår som mest hensiktsmessig for en trusselaktør. Generelt vil personlig oppmøte med sjekk av identifikasjon være nødvendig for å avlegge stemme i Norge. Dette gjør det svært utfordrende, og ikke minst kapasitetskrevende å benytte flere manipulerte stemmer. Ved stemmegiving fra utlandet er det imidlertid mulig å sende poststemmer uten å identifisere seg ved personlig oppmøte.

For det meste av aktuelle cyberangrep mot valg i Norge i dag (foruten det som er knyttet direkte til påvirkning og påvirkningsoperasjoner), vil det største skadepotensialet ligge i tap av tillit befolkningen og muligheten for at systemer og valggjennomføring saboteres. Siden stemmeavgivningen ikke er digitalisert, og tellingen foregår manuelt parallelt med maskinelt, vil manipulering av valgresultater være vanskelig å oppnå. Ved en overgang til eksempelvis elektronisk stemmegivning og/eller utelukkende maskinell telling, vil sårbarheter på dette området kunne endre seg betydelig.

5.5 Utilsiktede hendelser

Sikkerheten til valget kan også trues av utilsiktede hendelser. Eksempler på slike utilsiktede hendelser er:

Naturhendelser, for eksempel ekstremvær, flom, skred, pandemi eller andre spesielle naturhendelser som gjør det vanskelig eller ikke mulig å nå valglokalene.

Ulykkeshendelser, for eksempel brann i valglokale, ødeleggelse av valgmateriell, vannskade i serverrom som gjør at dataservere settes ut av spill og brudd på samfunnskritisk infrastruktur (veier, strømforsyning, internett).

Ufrivillige feil ved valggjennomføringen, for eksempel feiltasting på en datamaskin, feiltelling i forbindelse med manuell telling, feil bruk av skanner og ulike former for misforståelser eller forvekslinger som påvirker valggjennomføringen.

Andre utilsiktede hendelser eller fenomener, for eksempel at algoritmene for nettsøk er utformet slik at en får treff på nettsteder med informasjon som algoritmen «tror» at velgeren er interessert i. Sett i valgsammenheng vil det lett kunne oppstå ekkokamre, der velgere ikke får balansert informasjon før de foretar sine valg, men bare mer informasjon som styrker forutinntatte meninger og oppfatninger.

Utilsiktede hendelser er i større grad en tilsiktede, kartlagt, vurdert og håndtert for dagens valggjennomføring; eksempelvis gjennom beredskapsplaner i kommuner og sentralt – og gjennom Valgdirektoratets prosedyrer og rutiner. I denne utredningen har det derfor ikke blitt lagt betydelig vekt på å identifisere alle tenkelige utilsiktede hendelser som kan tenkes å få betydning for valggjennomføringen.

I tillegg er utilsiktede hendelser i mange tilfeller implisitt tatt med i utredningen selv om slike hendelser ikke eksplisitt er vurdert. Utilsiktede hendelser er i mange tilfeller medvirkende årsaker til andre uønskede hendelser, som er inkludert i analysen. For eksempel kan feil i stemmetelling skyldes både (utilsiktet) uoppmerksomhet og (tilsiktet) manipulering av skannere. Tilsvarende kan mangelfull tilgang til systemer og lokaler skyldes både (utilsiktet) ekstremvær og (tilsiktet) bombetrussel. I mange tilfeller vil det

imidlertid være snakk om ulike mekanismer som iverksettes for å håndtere tilsiktede og utilsiktede hendelser, og det vil også i mange tilfeller være forskjeller på sårbarheter relatert til tilsiktede og utilsiktede hendelser. For å ivareta dette er sårbarheter og risikoreduserende tiltak vurdert og foreslått både for utilsiktede og tilsiktede årsaker i tilfeller der begge årsakskategoriene har vært relevante.

6 Vurdering av sårbarheter og risiko knyttet til viktige hendelser og fenomener

For å gi bedre grunnlag for å vurdere behov for sikkerhetstiltak av ulik form, er det i utredningen gjennomført en prosess for å identifisere, og velge ut, aktuelle hendelser og fenomener som kan påvirke de fem kravene til valggjennomføring som defineres innledningsvis i kapittel 3.1:

- *Fri deltagelse* - At alle kandidater til valget, og velgere, har og får tilgang til å delta ved at det oppleves trygt og mulig - og at valget er hemmelig
- *Opplyst og informert* - At velgere får nok informasjon, riktig informasjon og balansert informasjon – til at de kan gjøre et «informert valg» (stemme)
- *Korrekt* - At de stemmer som er avgitt faktisk utgjør resultatet. Riktig manntall, riktig registrering, riktig antall stemmer
- *Gjennomført i tråd med plan* - At man faktisk får avholdt valget (og ikke hindres av sabotasje, naturhendelser, systemfeil eller organiseringsmangler)
- *Tillit* - At tilliten til den demokratiske valgprosessen opprettholdes i befolkningen (herunder at etterprøvbarhet og åpenhet er ivaretatt)

I vedlegg 2 til rapporten her finnes til dels detaljerte beskrivelser, refleksjoner og vurderinger knyttet til de utvalgte fenomenene/hendelsene. Det er viktig å understreke at utstrekning og form for det enkelte fenomen ikke er standardisert, og at et fenomen sjelden vil opptre alene eller uavhengig av de andre. Oppdelingen er således gjort for å kunne belyse farer, sårbarheter og relevante sikkerhetstiltak på en best mulig måte i forhold til målet med utredningen. Sikkerhetstiltak som skal innføres må derfor vurderes opp mot effekt på flere ulike områder – også utover fenomenene beskrevet i vedlegg 2. Dette er vektlagt i anbefalingene som gis i kapittel 8.

Identifisering av relevante fenomener/hendelser er gjort med tanke på å finne sikkerhetsmessige utfordringer ved valggjennomføringen, og ikke alle utfordringer knyttet til å ivareta demokratiske prinsipper (som for eksempel definert av Robert A. Dahl, se kapittel 3.1). Det er valgt å fokusere mer på intenderte handlinger enn på naturhendelser og uintenderte feil og hendelser i valggjennomføringen. Risiko knyttet til naturhendelser og uintenderte feil er i stor grad allerede detaljert adressert i risikovurderinger hos kommunal- og moderniseringsdepartementet, Valgdirektoratet og kommunene.

20 fenomener/hendelser er valgt ut, basert på relevans med tanke på de fem kravene over – og på trusselvurderingen i kapittel 5. I skjemaene, presentert i vedlegg 2, belyses og vurderes trusselaktørers intensjoner og kapasitet i forhold det konkrete fenomenet, samt barrierer og sårbarheter knyttet til dagens gjennomføring av valg i Norge. Til sammen utgjør disse vurderingene en betraktning av sannsynlighetsaspektet.

For hvert fenomen er det deretter gjort en vurdering av eventuell negativ effekt fenomenet kan ha på de fem kravene til valggjennomføring. Dette ivaretar konsekvensaspektet.

I tillegg er det gjort en vurdering av andre dimensjoner som påvirker risikoen og som er viktige å ta i betraktning når risikoen skal håndteres:

- Hvor mye kunnskap man har om fenomenet (motsats til usikkerhet - kunnskapsstyrke)
- Hvor raskt fenomenet endrer seg over tid (eksempelvis i teknologisk utvikling eller samfunnstrender – endringshastighet)
- Hvor styrbar risikoen relatert til fenomenet er (om det f.eks. kan adresseres med regulatoriske krav - styrbarhet)

I tabell 1 nedenfor oppsummeres kort hvilke fenomener/hendelser som er vurdert (skjemaene for det enkelte fenomen finnes i vedlegg 2). Fenomenene er ikke listet opp i prioritert rekkefølge etter risiko, men er til en viss grad sortert etter type fenomen. Som nevnt er det ikke klare skillelinjer mellom fenomenene men overordnet er «type fenomen» indikert i siste kolonne i tabellen.

Tabell 1: Oversikt over fenomener/hendelser som er vurdert spesielt

ID	Hendelse/fenomen	Kort beskrivelse av tema utgangspunkt for tema som diskuteres	Hovedtype
1	Lokal eller sentral politisk innflytelse på valget	I den norske valgprosessen er de folkevalgtes involvering i gjennomføring av valget relativt stor. Det er også valgstyrene på ulike nivåer – og i siste instans det folkevalgte Stortinget – som godkjenner valget og slik legitimiteten av gjennomføringen. Dette kan reise et spørsmål om politikeres innflytelse på valget. Domstolene har ikke en rolle som klageinstans i den norske ordningen - noe som har høstet kritikk fra blant annet OSSE.	Godkjenning av valg/ klage
2	Ulik mulighet til å delta i valgkampen	Politikken kan påvirkes ved at enkelte partier og organisasjoner får bedre mulighet til å delta i valgkamp gjennom tilføring av eksempelvis økonomisk kapasitet og tilgang i store medier. Videre kan partier som har fått støtte enten bevisst eller ubevisst oppleve at det knytter seg forventninger til fokus og syn på ulike saker når støtte gis.	Påvirkning av kandidater og partier
3	Overvåking/påvirkning av valgkandidater og politiske partier	Både nasjonalt og internasjonalt har det de siste årene vært mye oppmerksomhet rundt forsøk på (og gjennomføring) av informasjonsinnhenting og påvirkning rettet mot politiske partier og kandidater som stiller til valg. En rekke hendelser og eksempler har kommet fram etter eksempelvis valget i USA i 2016, men også nasjonalt ble det i forkant av stortingsvalget i 2017 blant annet bekreftet at det var gjennomført et hackerangrep som blant annet omfattet Arbeidspartiet og Forsvaret.	Påvirkning av kandidater og partier
4	Diskreditering av politikere	En bevisst diskreditering av politikere kan være rettet mot enkeltpolitikere og spesifikke partier, og slik ha en direkte påvirkning på hvem som får mulighet til å delta i det politiske arbeidet. Diskreditering kan ofte medføre at en politiker mister verv og innflytelse over lang tid – og/eller for godt; og dermed potensielt forskyve balansen i det politiske landskapet. Diskreditering av spesielt profilerte politikere mer generelt kan også bidra til å svekke tilliten til systemet og demokratiet.	Påvirkning av kandidater og partier
5	Netthets av politikere	Netthets og ytringsklimaet generelt på nett – oppleves av mange som et økende problem. Til forskjell fra temaet «diskreditering» vil netthets typisk forhindre politikere eller andre fra å delta i debatten fordi de selv ikke ønsker å ta belastningen det medfører – ikke fordi de mister eller ikke får lov til å ta en posisjon.	Påvirkning av kandidater og partier
6	Falske nyheter påvirker valget	Falske nyheter har alltid eksistert, men har fått økt oppmerksomhet i den offentlige debatten, spesielt etter presidentvalget i USA i 2016. Diskusjoner rundt hvorvidt og hvor mye usannheter, misvisende og feilaktig informasjon og falske nyheter påvirker valg – og hvordan slik påvirkning kan stoppes/reduseres – er utbredt.	Påvirkning av velgere
7	Klikkfarmer, falske følgere og avatarnettverk	En voksende industri gjennom flere år har vært muligheten for å, i digitale kanaler, påvirke menneskers oppfatning av hva som er populært, vanlige/riktige meninger og «trendy». Virkemidlene er spesielt egnet til å polarisere det politiske landskapet, ved å legitimere radikale synspunkter – og gi inntrykk av at smale strømninger er mer vanlige folkelige oppfatninger. De kan også gi «ekkokammereffekt» ved at personer med radikale synspunkter får bekreftelse i stedet for motstand når synet fremmes.	Påvirkning av velgere
8	Det skapes tvil om riktighet av valgresultatet	Grupper eller enkeltpersoner kan iverksette kampanjer for å så tvil om resultatet etter et valg, og indikere at dette er manipulert eller feil. Dette kan ha en direkte politisk hensikt, for eksempel for å fremme eget syn, eller skape tvil om andres interesser og intensjoner. Imidlertid er dette ikke minst egnet til å svekke tilliten til myndigheter, systemer og demokratiske prosesser, og etablere mistro.	Påvirkning av velgere
9	Trusler fører til at folk ikke våger å avlegge stemme	Trusselaktører kan fremme trusler som fører til at velgere ikke våger å møte opp i valglokalet, eksempelvis om at en bombe vil gå av. Bombetrusler kan ringes inn eller rykter om angrep kan spres i sosiale medier.	Påvirkning av velgere

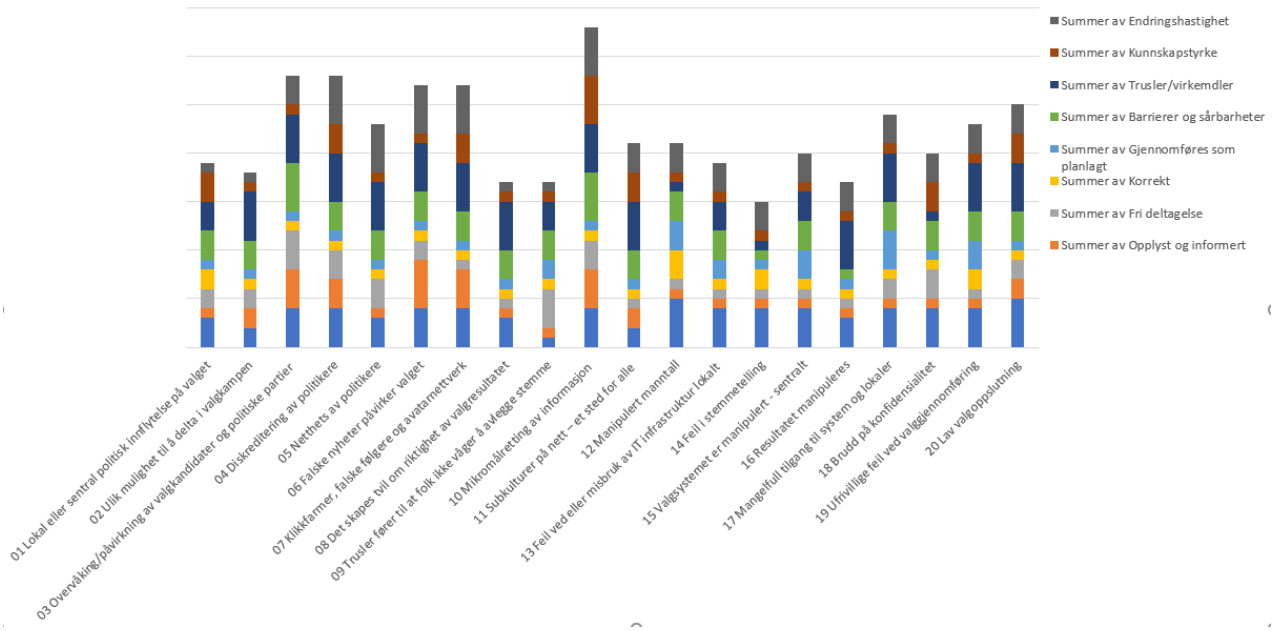
ID	Hendelse/fenomen	Kort beskrivelse av tema utgangspunkt for tema som diskuteres	Hovedtype
10	Mikromålretting av informasjon	I dagens digitale samfunn er det en økende forretning knyttet til innhenting, analyse og salg av informasjon om brukerne. Algoritmer, maskinlæring og kunstig intelligens benyttes til innsamling av data, og analyse av informasjon med høy effektivitet. Resultatet blir tilgang til svært detaljert informasjon om nettbrukerne. I sin enkleste form kan det dreie seg om isolerte opplysninger om interesser og preferanser for produkter. Ved bruk av algoritmer og kunstig intelligens har det imidlertid vist seg i nyere tid at det er mulig å analysere og identifisere, med forbløffende treffsikkerhet, preferanser og syn politisk og religiøst, etnisk tilhørighet, seksuell legning og andre dype personlighetstrekk hos brukerne. Resultatet blir tilgang til svært sensitiv informasjon som kan benyttes både til helt uskyldige formål og til å påvirke velgere i en valgsituasjon.	Påvirkning av velgere
11	Subkulturer på nett – et sted for alle	Ved økende bruk av digitale plattformer for informasjon og kommunikasjon, har det oppstått en rekke mer eller mindre lukkede samfunn på nett der informasjon og meninger utveksles. Slike type fora har alltid eksistert, men internett legger til rette for en stor oppblomstring, med lett tilgjengelige grupper og meningsfeller for alle. Mange kommuniserer og henter mye informasjon fra slike grupper på internett, der i mange tilfeller personer med de samme grunnleggende syn på sak eller område er samlet. Her vil det lett kunne oppstå «ekkokamre», der velgeren ikke får balansert informasjon før han foretar sine valg, men bare får mer informasjon som styrker forutinntatte meninger og oppfatninger.	Påvirkning av velgere
12	Manipulert manntall	Manntallet ligger til grunn for hvem som får stemme i Norge – og overføres til valgadministrasjonssystemet fra Skattedirektoratet. En manipulering av manntallet kan gi «ikke-eksisterende» personer mulighet til å avgi stemmer som påvirker et valg, eller gi mulighet for å avlegge flere stemmer med samme identitet.	Teknisk påvirkning
13	Feil ved eller misbruk av IT infrastruktur lokalt	Drift av IT systemer er en komplisert oppgave, som de aller fleste private foretak sliter med i dag. Grunnleggende rutiner som programvareoppdateringer, sikkerhetskopiering og segmentering i nettverk blir ofte glemt eller ikke gjort regelmessig nok. Det kan forventes at mye av det samme er gjeldende i norske kommuner som lokalt skal håndtere utstyr og programvare i valggjennomføringen. Et angrep på og via lokal infrastruktur kan potensielt også påvirke sentrale systemer.	Teknisk påvirkning
14	Feil i stemmetelling	Telling av stemmer er en kritisk del av valgprosessen. Feil i antall stemmer kan forekomme ved at stemmer «forsvinner», legges til eller endres/plasseres feil/telles feil. Prosessen med telling foregår i dag både manuelt og maskinelt.	Teknisk påvirkning
15	Valgsystemet er manipulert - sentralt	Det elektroniske valgadministrasjonssystemet i Norge (EVA) utvikles og driftes av Valgdirektoratet (Vdir), og er også fysisk plassert hos Vdir. Som for utstyr og programvare som driftes av kommunene, vil det være muligheter for «innbrudd» også i EVA, som driftes sentralt. Det kan for eksempel dreie seg om sårbarheter i programkode utviklet av Valgdirektoratet, sårbarheter introdusert i hardware, sårbarheter i tredje parts programvare eller at trussel aktørene får tilgang til nettverk der kritisk infrastruktur kjører via andre måter, f.eks. virus på en ansatt sin PC. Valgadministrasjonssystemet inngår i lange digitale verdikjeder som gir nye sårbarhetsutfordringer	Teknisk påvirkning
16	Resultatet manipuleres	Som beskrevet under «valgsystemet er manipulert – sentralt», vil det alltid finnes muligheter for å «bryte seg inn» i også sentrale valgsystemer. Resultatene kan manipuleres i EVA admin, EVA resultat, i overføringen til media og valgresultat.no og også direkte på f.eks. valgresultat.no.	Teknisk påvirkning
17	Mangelfull tilgang til system og lokaler	Det at valglokaler eller kritiske valgsystemer blir utilgjengelige kan hindre at folket får avlagt sin stemme; at stemmene telles eller at resultater kan genereres og formidles.	Teknisk påvirkning
18	Brudd på konfidensialitet	Et viktig prinsipp ved gjennomføring av valg i Norge (ref. valgloven) er at valget skal være hemmelig. Det vil si at alle skal kunne avlegge sin stemme uten at noen vet hva du har stemt. Dette prinsippet håndheves strengt i valglokalene i dag ved at ingen har tilgang til stemmebåsen når velgeren foretar sin avstemming. Også konfidensialitet vedrørende resultater er viktig for gjennomføringen. Hvordan påvirkes konfidensialitet ved mulige fremtidige endringer i valgsystemet?	Teknisk påvirkning

ID	Hendelse/fenomen	Kort beskrivelse av tema utgangspunkt for tema som diskuteres	Hovedtype
19	Ufrivillige feil ved valggjennomføring	Det foreligger en rekke muligheter for å gjøre feil i forbindelse med gjennomføringen av valg. Dette kan dreie seg om prosessuelle feil knyttet til valglovverket, tekniske feil med en rekke ulike konsekvenser og tilsvarende for menneskelige feil i gjennomføringen. Ikke minst gir rask teknologisk utvikling, lang tid mellom valggjennomføring og varierende eierskap til oppgaver ved valg, utfordringer med tanke på kompetanse.	Andre
20	Lav valgoppslutning	Lav valgoppslutning er et demokratisk problem, i større grad enn en sikkerhetsutfordring. Lav valgoppslutning er derimot ofte en negativ konsekvens av sikkerhetsutfordringer, og et resultat av at tilliten til myndigheter, demokratiske prosesser og valgsystemer svekkes.	Andre

6.1 Risiko knyttet til hendelser og fenomener

For hver hendelse/fenomen, har sannsynlighetsaspektene, konsekvensaspektene og de øvrige nevnte dimensjonene som påvirker risiko blitt vurdert på en enkel skala. Høy verdi er et uttrykk for at dimensjonen gir et stort bidrag til risiko. De detaljerte vurderingen finnes i det enkelte skjema i vedlegg 2.

Ved å summere risikobidragene for alle dimensjonene for hver hendelse/fenomen gis en indikasjon på risikobidraget hver enkelt av disse vurderes å gi til sikkerheten i valgprosessen. Figur 6 visualiserer de faktorene som bidrar i den totale risikovurderingen for alle de 20 hendelsene/fenomenene.



Figur 6: Sammenstilling med summering av dimensjoner som påvirker risiko for alle vurderte fenomener/hendelser

Vurderingene viser at den største risikoen knyttet til den demokratiske valgprosessen, er relatert til påvirkning av kandidater og velgere i forkant av valggjennomføringen. Karakteristisk for mange av fenomenene innen disse områdene er at man har begrenset kunnskap om fenomen og effekter av disse. I tillegg er endringshastigheten høy. Høy endringshastighet er et uttrykk for rask teknologisk og kulturell utvikling, særlig innen dataanalyse og kommunikasjon, men også for et trusselbilde i stadig endring nasjonalt og internasjonalt.

Et fenomen som utmerker seg med stort risikobidrag er mikromålretting av informasjon. Samfunnet – og ikke minst det norske - preges av en rask digitalisering. Både i privat og profesjonell sammenheng er en svært stor andel av velgerne aktive brukere av internett og digitale verktøy som samler detaljer informasjon om hver enkelt av oss. Når dette informasjonstilfanget kombineres med bruk av algoritmer, maskinlæring og kunstig intelligens som analyserer informasjonen med stor effektivitet, blir resultatet at det finnes tilgjengelig svært sensitiv informasjon om velgerne knyttet til eksempelvis helse, legning, religiøs overbevisning, politisk syn og andre preferanser. Denne informasjonen kan brukes til å målrette informasjon i den hensikt å påvirke velgere i den retningen en (trussel)aktør ønsker, uten at personen selv er klar over det. Det demonstreres også stadig hvor effektiv slik mikromålretting av informasjon er. Dette fenomenet får en høy samlet risikovurdering, fordi mikromålretting er et effektivt og lett tilgjengelig virkemiddel og vanskelig å beskytte seg mot. Effekten er stor, og i tillegg er kunnskapen om fenomenet begrenset og endringshastigheten stor.

Hendelser av mer teknisk art og relatert til den digitale verdikjeden er gjennomgående vurdert å gi et mindre risikobidrag enn påvirkningshendelsene beskrevet over. Det er gjort og gjøres et omfattende arbeid med å sikre valgadministrasjonssystemet EVA og tilhørende utstyr og komponenter, og sikringen fremstår som robust i dag. Sårbarheter vil likevel foreligge i den digitale verdikjeden, eksempelvis på grunn av raske teknologiske endringer, kompleksitet og utfordringer med kompetanse. Ikke minst vil også valgprosessen og tilhørende systemer og komponenter preges av utfordringene knyttet til lange og komplekse digitale verdikjeder. I disse verdikjedene med tjenester, komponenter, sammenvevde systemer og avhengigheter, kan en hendelse eller utnyttelse av en sårbarhet «langt borte» gi omfattende konsekvenser i sentrale og lokale systemer og komponenter i valgprosessen. Hovedårsaken til at risikoen samlet sett likevel vurderes som begrenset på dette området, er det fortsatt betydelige innslaget av manuelle prosesser som sikrer kontroll og redundans. Dette gjelder for eksempel identifisering av velgeren og avlegging av stemme, og den pålagte manuelle tellingen av stemmer. Disse manuelle prosessene utgjør en betydelig barriere mot at systemutfall skal hindre valggjennomføringen, og mot at en trusselaktør skal kunne manipulere stemmer og resultater. Det vil være svært kapasitetskrevende å samtidig manipulere både elektroniske systemer og manuelle prosesser som utføres av valgmedarbeidere.

Et fenomen som har fått betydelig fokus i etterkant av valget i Sverige i 2018, er kampanjer for å så tvil om valgresultatet er korrekt og indikere at det er begått valgfusk. Å fremsette slike påstander krever liten innsats av en trusselaktør. Ved å utnytte sosiale medier for å spre falsk informasjon og halvsannheter som bygger opp under konspirasjonstanker og lignende, kan dette være et svært effektivt verktøy for å svekke tilliten til styresett, systemer og prosesser. I Norge ligger det en betydelig barriere i den i utgangspunktet høye tilliten til myndigheter og systemer, samtidig som det norske samfunnet i liten grad, også sammenlignet med Sverige, preges av polarisering og aktive radikaliserte grupperinger. Norge er imidlertid mindre modne enn Sverige med tanke på forebyggende tiltak ved informasjons- og medierobusthet, kunnskaps- og kompetansebygging i ulike grupperinger og i samfunnsdebatten rundt denne typen anslag mot demokratiet.

6.2 Type konsekvenser av hendelser og fenomener

Som tidligere beskrevet er hendelser og fenomener vurdert med tanke på hvor store, og hvilken type, konsekvenser det har for valget dersom de benyttes/realiseres. For hver av de 20 beskrevne fenomenene er det gjort en verdisetting av konsekvenser for de fem områdene fri deltakelse, opplyst og informert, korrekt, gjennomført i henhold til plan og tillit (se beskrivelse av disse innledningsvis i kapittel 6).

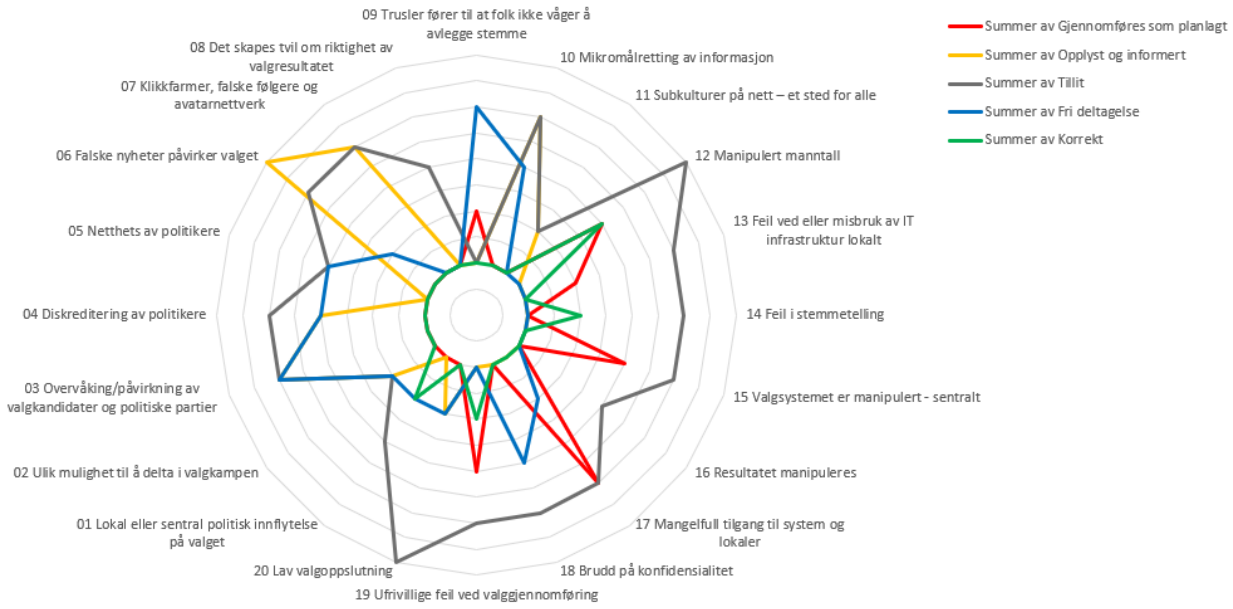
Figur 7 illustrerer hvordan de ulike konsekvensdimensjonene påvirkes av de fenomener og hendelser som er vurdert. Som det fremgår av figuren er redusert tillit til valg, myndigheter og demokrati den absolutt dominerende konsekvensen totalt sett. Realisering av nesten samtlige fenomener og hendelser vil påvirke tillitsdimensjonen negativt. Karakteristisk for denne dimensjonen er også at en ikke nødvendigvis trenger

å lykkes med å realisere angrepene/hendelsene. Bare det faktum at angrepet er gjennomført, og så en tvil om hvorvidt man lykkes – eller kunne ha lykkes – kan være nok til påvirke tilliten negativt. Tillit er helt grunnleggende for legitimiteten og funksjonen til den demokratiske styreformen. Når det fremkommer hvor sårbar denne dimensjonen er for dagens og fremtidens trusler, understrekes viktigheten av å jobbe for å opprettholde og styrke den høye tilliten til demokratiet som finnes i det norske samfunnet.

Videre fremkommer at de økende truslene og risikoen knyttet til påvirkning, spesielt gjennom bruk av digitale verktøy og sosiale medier, kan gi store konsekvenser for hvor opplyst og informert velgerne er (grunnlaget for reelle valg) og den frie deltakelsen for både kandidater og velgere.

Totalt sett fremstår konsekvenser, og dermed behovet for fokus og tiltak knyttet til de tre ovennevnte dimensjonene, (tillit, opplyst og informert, fri deltagelse) som betydelig mer fremtredende enn for konsekvenser for korrekte valg og evne til å gjennomføre valget. Hovedårsaken til dette er at identifisering av velgere, avstemming, telling og kontroll langt på vei gjennomføres i manuelle prosesser i stedet for, eller i tillegg til, elektroniske prosesser. Siden store deler av trusselbildet er knyttet til det digitale aspektet blir analoge/manuelle aktiviteter en kraftig barriere.

I Figur 7 synliggjøres både tyngden av ulike konsekvenser totalt – og hvordan ulike konsekvensområder er fordelt for de enkelte hendelsene.



Figur 7 Visualisering av hvilke typer konsekvenser som dominerer for den enkelte hendelse/fenomen, gitt at hendelsen skjer

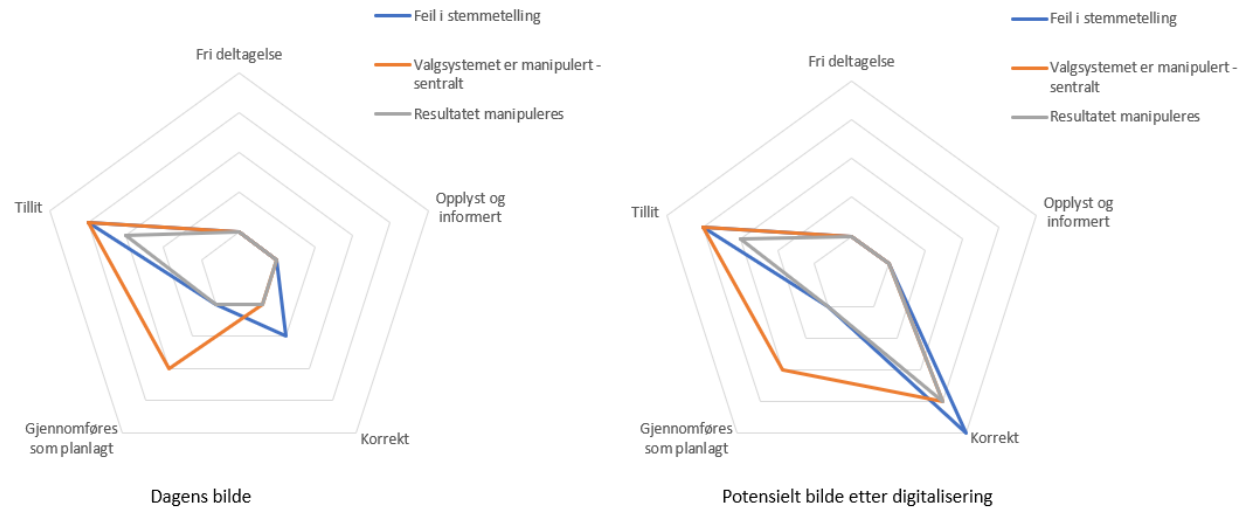
7 Risiko knyttet til fremtidige endringer

Oppdraget i denne utredningen har vært å fokusere på risiko forbundet med dagens valggjennomføring og dagens forutsetninger i omgivelsene. Valglovutvalgets – og myndighetenes – fokus, vil imidlertid naturlig nok være på å legge til rette for en valggjennomføring som også er sikker i fremtiden. En endring i forutsetningene som ligger til grunn i vurderingene i denne utredningen og analysen, vil også kunne endre risikoen knyttet til valg i betydelig grad.

Noen av disse endringene er det bare mulig å se konturene av, mens andre kan vi med stor sikkerhet si vil komme. De anbefalte tiltakene søker derfor å også ivareta de mest relevante endringer i forutsetninger. Eksempel på slike er:

- Politiske endringer, internasjonalt og nasjonalt. Endringer i det internasjonale politiske klima som involverer eksempelvis FN, NATO og Russland, vil kunne gjøre Norge til et mer attraktivt mål og øke trusselen mot demokratiske prosesser.
- Redusert tillit i befolkningen til politikere og systemer vil kunne øke sårbarheten for påvirkningsoperasjoner, og generelt medføre mindre stabilitet
- Digitalisering av valgrelevante systemer (folkeregisteret, stemmegiving og telling) uten manuelle paralleller vil åpne sårbarheter i forhold til å manipulere resultater av et valg, og kreve mer tekniske sikkerhetsbarrierer
- Rask digitalisering av samfunnet generelt åpner opp for falske nyheter og mikromålretting av informasjon og kan derigjennom true et opplyst og informert samfunn

Figur 8 er en illustrasjon og eksempel på hvordan konsekvensbildet kan endre seg for noen utvalgte fenomener/hendelser (feil i stemmetelling, valgsystemet er manipulert – sentralt og resultatet manipuleres) i en tenkt utvikling der manuell telling ikke er påkrevd – samtidig som andre uavhengige tellemetoder ikke er implementert.



Figur 8: Illustrasjon på hvordan konsekvensbildet kan endre seg ved en tenkt fremtidig overgang fra manuell og maskinell telling av stemmer, til heldigitalisering av valg

Et viktig element når det gjelder å sikre et fremtidig mer digitalisert valgsystem (som må forventes), er det paradigmeskiftet man ser innen IT-sikkerhet. Til tross for betydelige tiltak med innebygd sikkerhet, rutiner, beskyttelse og testing, vil man ikke fullt ut kunne beskytte seg mot innbrudd i kritisk infrastruktur som valgsystemer. Det må antas at infrastruktur er, eller vil bli, kompromittert men at det må etableres

verktøy og prosesser som kan oppdage, detektere og hindre skade. Paradigmet har tidligere vært å investere i maksimal beskyttelse, og forsøke å tette alle skott. I dag finnes en anerkjennelse av at selv det beste forsvar trolig vil kunne feile på et eller annet punkt. Paradigmet skifter mot et mer deteksjonsorientert IT-miljø som også fokuserer på deteksjon og håndtering for å hindre skade dersom forsvaret penetreres.

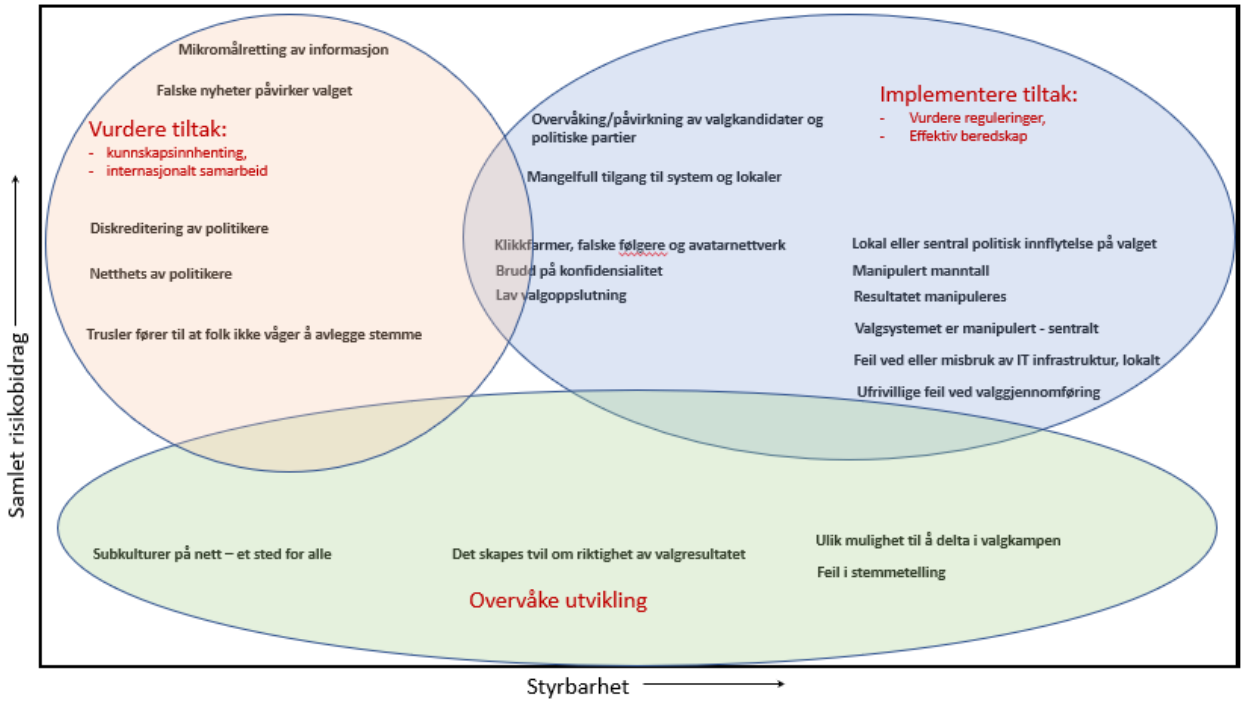
Som påpekt i kapittel 6, vil det imidlertid i dag kunne få store konsekvenser for tilliten til de demokratiske prosessene bare det at et angrep er gjennomført, og at det sås tvil om effekten. Dette understreker viktigheten av at befolkningen også har kunnskap om faktisk risiko knyttet til hendelsen. Når det forventes at systemet kan bli hacket, men det er stor sikkerhet for at ikke at valget påvirkes likevel, er det avgjørende at befolkningen også forstår dette om ikke mistillit skal oppstå. Vi har i 2018 og 2019 sett flere eksempler på at store virksomheter har gått ut med informasjon om at de har blitt angrepet og hacket, men at de har klart å beholde tillit i stor grad ved å vise at de har håndtert hendelsen og vært åpne og transparente om hva som har skjedd. Åpenhet, informasjon, kommunikasjon og bygging av kompetanse hos velgerne og i samfunnet blir derfor svært viktig for sikkerheten i demokratiske prosesser.

8 Innspill til mulige tiltak som kan bidra til å øke sikkerheten

Med bakgrunn i vurderinger gjort og beskrevet i utredningen, gis det her innspill til mulige tiltak som kan bidra til å øke sikkerheten. Rasjonale for innspillene ligger i hovedsak i risiko- og sårbarhetsvurderingen i vedlegg 2, og oppsummeres bare kort under. Det understrekes at innspillene er av overordnet art, og begrenset til området som defineres som sikkerhet i valgprosesser.

Risiko knyttet til hendelsene/fenomenene som er vurdert vil i varierende grad være styrbar. I denne rapporten har man brukt styrbarhet som et begrep for å beskrive i hvilken grad man kan implementere tiltak som effektivt forebygger eller håndterer en uønsket hendelse. Høy styrbarhet brukes typisk der det kan besluttes effektive tiltak (som reguleringer og beredskap) på et nasjonalt nivå. Lav styrbarhet brukes om fenomener som har internasjonale dimensjoner eller som eksempelvis krever langsiktige kunnskapsbyggende tiltak.

Figur 9 skisserer grovt hvordan de ulike hendelsene plasserer seg med hensyn på risiko (samlet risikobidrag), og mulighet for å gjennomføre effektive tiltak for å redusere risikoen (styrbarhet). Plassering på aksen «samlet risikobidrag» vil tilsvare stolpehøyde/summering av risikobidrag som er visualisert i Figur 6, og inkludere bidrag både fra sannsynlighetsvurderinger, konsekvensvurderinger og de øvrige definerte dimensjonene som påvirker risiko. En plassering høyt på aksen viser høy risiko. For styrbarhet vil plassering langt til høyre indikere høy styrbarhet for håndtering av risiko. For noen hendelser vil konkrete tiltak og regulatoriske krav være egnet for å redusere risiko. For andre hendelser er mer langsiktige tiltak med fokus på kunnskapsbygging og internasjonalt samarbeid mest hensiktsmessig. Mange av hendelsene vil befinnes seg i grenselandet mellom disse, eller kan håndteres gjennom en sum av ulike tiltakstyper. Det er viktig å påpeke at selv om det kan være vanskelig å beskytte seg fullstendig mot enkelte uønskede hendelser, kan risikoen langt på vei reduseres ved å ha gode planer og effektiv beredskap på plass når en hendelse inntrer. Figur 9 er en grov illustrasjon for strukturering av tiltaksvurderingene, og ikke en eksakt/korrekt oversikt.



Figur 9: Illustrasjon - tiltakstyper egnet for å håndtere ulike typer hendelser/risikoer

8.1 Innspill til mulige tiltak - regulatoriske

Regulering av valggjennomføring og hjemmel for tilsyn
Verdier og prosesser som er viktige for samfunnet er i Norge i stor grad underlagt sikkerhetskrav og -reguleringer fra myndighetene. Dette kan for eksempel være for å beskytte liv og helse for ansatte, eller i samfunn/omgivelser. Det kan være for å beskytte funksjoner som er kritiske for samfunnet som tilførsel av vann og kraft, eller for å beskytte andre verdier vi setter høyt. Ikke minst har det de siste årene vært et økende fokus på – og grad av regulering som er fokusert på beskyttelse mot intenderte trusler (der noen bevisst ønsker å skade).

Gjennomføring av valg er en viktig demokratisk prosess; og et område som både nasjonalt og internasjonalt får mye fokus fordi det oppleves som truet med dagens trusselbilde. Krav til sikkerhet i valggjennomføring er imidlertid i svært begrenset grad regulert i valglov og valgforskrift i dag. Valgdirektoratet har utarbeidet til dels omfattende veiledningsmateriale med anbefalte sikkerhetstiltak fysisk, teknisk og prosessuelt/organisatorisk. Det er imidlertid frivillig for kommuner og fylkeskommuner om de velger å følge anbefalingene, og det foreligger heller ingen hjemmel for å kunne pålegge kommuner og fylkeskommuner å følge dem.

Valgdirektoratet har utarbeidet opplæringsmateriell og tilbyr opplæring til valgansvarlige i kommuner og fylkeskommuner. Å følge opplæringen er imidlertid frivillig; og de lokale aktørene er selv ansvarlige for å vurdere behov og gjennomføre opplæring av øvrige valgmedarbeidere. Det foreligger ikke hjemmel for å pålegge de lokale aktørene opplæringstiltak.

Innspill til mulige tiltak:

- *Regulering av sikkerhetskrav til valggjennomføringen for regionale og lokale aktører*. Det foreslås et funksjonsbasert regelverk med fokus på en risikobasert tilnærming. I dette ligger at reguleringen stiller krav til hva som skal oppnås med tiltakene, mens lokale aktører gis handlefrihet med tanke på hvordan. Reguleringen bør dekke områder som teknisk sikkerhet for systemer og komponenter, fysisk sikring av lokaler og utstyr, personellsikring, kompetanse og organisering/rutiner. På flere av disse områdene vil det kunne være hensiktsmessig at spesifikasjoner i veileder fra Valgdirektoratet utgjør alternativ 1 for å oppfylle krav, mens alternativ 2 er at den lokale aktøren etter en risikovurdering finner andre tiltak som gir tilsvarende eller høyere sikkerhetsnivå. Det vil gjøre kravene håndterbare også for kommuner med begrenset kapasitet og kompetanse innen sikkerhet og risikostyring. Funksjonelle krav vil være robuste i forhold til endringer i teknologi og metoder i ulike fremtidsscenarioer (i motsetning til spesifikke krav).
- *Etablering av hjemmel for tilsyn med sikkerhetsreguleringen for valg*. Erfaringsmessig er bruk av tilsyn svært viktig for å sikre gjennomføringen av krav. Mulighet til å føre tilsyn med sikkerhetstiltak rundt valggjennomføringen vil være en viktig del både av å kartlegge og redusere risiko og sårbarhet i samfunnet. Hjemmel for tilsyn dekker både kontroll og mulighet for å gi pålegg i tråd med krav. Det understrekes at begrepet tilsyn dekker et spekter av metoder og verktøy for gjennomføring, ikke bare stedlig kontroll før, under og etter valggjennomføring. Det bør utredes hvor tilsynsfunksjonen mest hensiktsmessig bør ligge – og hvorvidt den bør legges på flere nivåer (sentralt – regionalt).

I 8.3 reflekteres det rundt problemstillingen regulering kontra lokalt selvstyre.

Forhold til sikkerhetsloven
Ny sikkerhetslov for Norge trådte i kraft 1. januar 2019 (Justis- og beredskapsdepartementet, 2019). Et overordnet formål med den nye loven er å bidra til å sikre Norges demokratiske styreform. Loven gjelder statlige, fylkeskommunale og kommunale organer, og skal adressere «*tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser*» herunder altså den

demokratiske styreformen. Det fremstår som naturlig å vurdere om valgprosessen faller inn under en slik definisjon og beskyttelsesbehov. KMD opplyser at en slik vurdering vil igangsettes for valgprosessen som en del av departementets arbeid med å identifisere grunnleggende nasjonale funksjoner. Det fremstår uansett som fornuftig å se på eventuelle overlappende eller tilstøtende områder for regulering for to så samfunnsovergripende lover som sikkerhetsloven og valgloven.

Innspill til mulige tiltak:

- *Vurdere sikkerhetslovens relevans for valgprosessen*. Dersom valgprosess, systemer, utstyr og så videre, faller innenfor sikkerhetslovens regulering; kan det potensielt også ivareta de innspilte tiltakene i 1) og 2) med tanke på sikkerhetskrav og tilsyn. At et slikt kontrollansvar tillegges sikkerhetsmyndigheten vil kunne gi en større uavhengighet, eller avstand, til politiske strukturer.

Sentrale og lokale aktørers roller og ansvar
Fordeling av roller og ansvar knyttet til valggjennomføring henger tett sammen med kravene som anbefales stilt i punktene over med tanke på regulering og tilsyn. Det ligger implisitt i anbefalingen om regulering og tilsyn at sentrale aktører da vil få større plikt og anledning til å stille krav, og kontrollere etterlevelse. Det kan vurderes å tillegge ansvar for kontroll og oppfølging også på regionalt/fylkesnivå (tilsyn med kommuner) og lokalt nivå (internkontroll). Det er imidlertid en utfordring, også på andre reguleringsområder, at det er krevende å følge opp sikkerhetstiltak, trusselbilde, risiko og sårbarhet og digitale systemer på grunn høye kompetansebehov. Det vil derfor kunne være utfordrende å etablere og ivareta gode kontrollfunksjoner på regionalt og lokalt nivå.

Innspill til mulige tiltak:

- *Vurdere og avklare endringer i roller og ansvar/myndighet mellom lokale og sentrale aktører i valggjennomføringen for å ivareta kravstilling og kontroll dersom 1) og 2) besluttes*.

Bruk av teknologi i valggjennomføring – obligatorisk bruk av sentralt system
Valgdirektoratet har i dag ansvar for å utvikle og drifte valgadministrasjonssystemet EVA, som tilbys alle fylker og kommuner i valggjennomføringen. Det foreligger ikke hjemmel for å pålegge de regionale og lokale myndighetene å benytte systemet. Med dagens samfunnsutvikling må det forventes økt digitalisering også på områder knyttet til valggjennomføring. Samtidig vil et trusselbilde i stadig endring og en rask teknologisk utvikling øke behovet for også teknisk kompetanse for å utvikle, drifte og sikre digitale plattformer og programvare.

Innspill til mulige tiltak:

- *Lovfeste krav om at myndigheter på alle nivåer i valggjennomføring skal benytte digital infrastruktur og programvare fra sentrale valgmyndigheter (EVA)*. Økt digitalisering vil stille stadig høyere krav til sikring av digitalt utstyr, programvare og infrastruktur – og til kompetanse for å ivareta sikringstiltak. Mulighet for å velge dette lokalt, kombinert med svært varierende kapasitet og kompetanse i de ulike kommunene, åpner for en stor fremtidig sårbarhet. Et obligatorisk sentralstyrt system reduserer denne sårbarheten ved å øke mulighet for styring og iverksettelse av økte sikringstiltak ved behov, samt lette kommunenes oppgaver.

Beredskapshjemmel i valglovgivningen
Med dagens valgordning og regulering finnes det ikke hjemmel for å eksempelvis utsette valget dersom det oppstår forhold som gjør det nødvendig. Valget må gjennomføres – og så eventuelt underkjennes og gjennomføres på nytt. En beredskapshjemmel som gir anledning til å utsette valggjennomføringen i kortere perioder lokalt, regionalt eller sentralt vil gi en økt robusthet for å håndtere uønskede hendelser. Dette kan for eksempel dreie seg om situasjoner der det fremsettes en trussel mot valglokaler i større eller mindre områder, som medfører at velgere ikke våger å ta seg frem for å stemme. Det kan være vær-

og klimarelaterte forhold som hindrer oppmøte, eller cyberangrep som setter hele eller deler av nødvendig infrastruktur ut av spill. Med klimatiske forhold som kan øke forekomsten av ekstremvær og mulighet for økt cybertrussel og angrep som saboterer infrastruktur bør det legges til rette for en sikrere og mer effektiv beredskap (mulighet for håndtering). Dette vil også kunne redusere risiko ved at en trusselaktør ikke ser det samme potensialet i å gjennomføre angrep. Konsekvensen blir mindre.

Innspill til mulige tiltak:

- *Etablere en beredskapshjemmel i valglovgivningen*. Det må nærmere utredes når hjemmelen skal kunne benyttes og av hvem (sentralt og eventuelt regionalt og lokalt), men hjemmelen må gi anledning til å utsette valggjennomføring i nærmere spesifiserte og begrensede perioder lokalt og/eller sentralt.

Krav om uavhengige tellinger av stemmer
Det foreligger en rekke større og mindre sårbarheter i den digitale verdikjeden for valggjennomføring, telling av stemmer og valgoppgjør. Per i dag er det imidlertid forskriftsfestet at minst én telling av stemmer avgitt ved valget (foreløpig telling) skal foregå manuelt; i tillegg til manuelle prosedyrer for verifiseringer og protokollføring. En slik manuell telling reduserer risikoen for å få manipulert resultater fra valget til et absolutt minimum fordi den er uavhengig av den maskinelle tellingen som ellers kan benyttes; og fravær av denne ville gitt betydelig større utfordringer og krav til tekniske sikkerhetstiltak både i dag og for fremtiden.

Innspill til mulige tiltak:

- *Videreføre regulatorisk krav om to uavhengige tellinger av stemmene etter valg.* Kravet om manuell telling utgjør i dag en svært sterk barriere mot manipulering av stemmetall og valgresultater. Det bør opprettholdes et krav om uavhengige tellinger også ved eventuell økt digitalisering av valgprosessen (som elektronisk stemmegiving). Det er viktig å sikre at det er reell uavhengighet mellom slike tellinger. For eksempel vil ikke to tellinger foretatt hos to ulike instanser, men i samme elektroniske system/programvare, ha den samme uavhengigheten som manuell og elektronisk telling.

Regulering av mikromålretting av informasjon under valgkamp
Kartlegging og analyse av store mengder data om velgere åpner muligheter for politiske partier, og andre, for å (mikro-)målrette informasjon og budskap for eksempel som en del av valgkampen. Det ligger et stort og til dels ukjent potensial i bruken av denne typen informasjon som verktøy i påvirkningsarbeid, og det kan også tenkes at økonomi vil skape et skille mellom politiske aktører som kan benytte verktøyet og de som ikke kan det.

Innspill til mulige tiltak:

- *Utrede behov for regulering av bruk av mikromålretting som verktøy i valgkamp*. Områder som for eksempel politisk reklame i tv, er allerede i dag regulert. Potensialet i mikromålretting er trolig mye større.

Sanksjoner ved cyberangrep
Hacking har blitt stor business og mange kriminelle aktører selger sine hacketjenester til store og små aktører om ønsker tilgang til informasjon, eller til å påvirke eller ødelegge. Cyberområdet er ennå ikke regulert som resten av samfunnet og det foreligger ikke alltid tydelige definisjoner på hva som er et lovbrudd og hvordan det eventuelt skal straffes. I EU pågår det våren 2019 arbeid med å etablere og tydeliggjøre regelverk med sanksjoner som kan benyttes mot de som hacker eller forsøker å hacke seg inn i for eksempel valgsystemer. Sanksjonene skal kunne anvendes både på individer, organisasjoner og

statlige aktører[21]. Straffelovens §§ 151-154 adresserer allerede påvirkning av stemmer og resultater i stor grad, mens andre former for eksempelvis sabotasje ikke fremkommer like tydelig.

Innspill til mulige tiltak:

- *Etablere/tydeliggjøre hjemmel for å sanksjonere hacking og forsøk på hacking av valgsystemer.* Kriterier, omfang, ansvar og myndighet bør utredes ytterligere for hensiktsmessig regulering.

8.2 Innspill til andre mulige tiltak

I det følgende listes det opp noen tiltak som kan vurderes for å møte sikkerhetsutfordringer knyttet til valg nå, og i fremtiden. Det vises til analysene som foreligger i vedlegg 2 for vurderinger som ligger til grunn for disse, samt for flere mulige tiltak.

a) Utredning av alternativ organisering av godkjenning av valg og klageorgan. Noen mulige alternativer er: Nasjonale valg: Ansvar for godkjenning av valget, og for klageordningen, ivaretas av domstol eller et eget dedikert organ. (Dette er vanlig i en rekke andre land, og Norge har blitt kritisert av valgobservatører for den ordningen vi har i dag). Vurdere om valgstyrene kunne vært ledet av representant for administrasjon, domstol eller andre dersom ordningen med «folkevalgte valgstyrer» videreføres. Vurdere å flytte godkjenning av valget bort fra folkevalgte organer.
b) Videreføre krav om åpenhet om økonomisk støtte til partier, og støtteordninger som sikrer «levemulighet» for en bredde av partier og organisasjoner.
c) Opprettholde og styrke støtteordninger til bred medieflora, inkludert meningsbærende aviser. Sikre bred informasjon i redaktørstyrte medier – journalistiske krav (motvekt, balanse) – eksempelvis gjennom subsidiering
d) Styrke krav til både sentrale og lokale aktører i valgprosessen om å vurdere og håndtere risiko for intenderte trusler.
e) Styrke/beskytte kandidater til valg gjennom informasjon og veiledning, etablere og videreføre offentlig-privat samarbeid for forskning, utvikling og implementering av teknologiske beskyttelsestiltak
f) Videreføre og utvikle faktasjekkfunksjoner som fakta.no, og informere om falske nyheter som avdekkes
g) Støtte og utvikle teknologiske tiltak for å avsløre og merke falske nyheter
    a. Avdekking av manipulerte bilder, lyd og film
    b. Identifisering og stenging av falske profiler og nettverk
    c. Identifisering og merking av pålitelige og ikke-pålitelige kilder til informasjon (direkte på nett)
h) Vurdere reguleringer for å kunne straffeforfølge spredning av falsk informasjon (men problematisk å skille bevisst/ubevisst og grad av «falskhet» uten å angripe ytringsfriheten)
i) Vurdere reguleringer som hindrer kjøp og salg av falske klikk som legalt påvirkningsverktøy
j) Informasjonstiltak for å øke kunnskap om demokratiske prosesser, påvirkning og sikkerhet rettet mot ulike befolkningsgrupper som barn/unge, eldre, innvandringsgrupper m.fl. (folkeopplysning - bygge robusthet)
k) Opplæring av kandidater, media og befolkning for å avdekke falske nyheter – spesielt barn/unge
l) Opplæring av rekrutteringsgrunnlaget til politiske partier og av kandidater til valg i håndtering av netthets – skape robusthet
m) Forberedelse i partiene – planer for håndtering av netthets, og støtteordninger for den som rammes

[21] https://www.politico.eu/article/europe-cyber-sanctions-hoped-to-fend-off-election-hackers/

n) Kombinere manuelle prosesser/kompetanse og teknologiske tiltak for å kvalitetssikre nyheter og informasjon
o) Fra myndighetssiden planlegge godt for scenarioer som kan komme. Fokus på informasjon og kunnskapsbygging i samfunnet.
    - Informere om at angrep eller påstander kan komme og øke kunnskap og bevissthet i ulike folkegrupperinger
    - Forsikre om rutiner og sikkerhet før valg gjennom transparent kommunikasjon
    - Ha klart materiale som kan publiseres dersom noe hender i valgprosessen (angrep)
    - Ha gode beredskapsplaner, med spesielt fokus på informasjon og kommunikasjon
p) Holdningskampanjer rettet mot netthets
q) Moderering av kommentarfelt o.l.- men med klare spilleregler for å unngå konflikt med ytringsfriheten. Rettslig forfølgelse av alvorlige tilfeller av netthets.
r) Sikre fokus på ivaretakelse av IKT-sikkerhet og relevans for valg i digitaliseringsprosess for folkeregisteret.
s) Styrke kontroll med medarbeidere i valgdirektoratet og valgmedarbeidere og leverandører på alle nivåer (hindre at innsidere oppstår/benyttes)
t) Online rådgivningsstøtte til valgmedarbeidere 24/7

8.3 Tiltakenes effekt på åpenhet, lokalt selvstyre og ytringsfrihet

Innføring av tiltak for å øke sikkerheten ved valg kan potensielt komme i konflikt med ivaretakelse av andre viktige verdier og prinsipper. Under er det kort gjort en betraktning i forhold til dette med utgangspunkt i tiltakene som er anbefalt i denne utredningen.

Sentralt og lokalt ansvar – regulering og lokalt selvstyre

I denne utredningen pekes det på muligheten for en større grad av regulering av valggjennomføringen, og også at sentrale aktører gis ansvar og myndighet for kontroll med lokale aktører. Dette kan sies å redusere det lokale selvstyret og den sterke tradisjonen med at det er kommunene som er ansvarlige for valggjennomføringen.

Grunnlovens §49 fikk i 2016 en tilføyelse som sier at «Innbyggjarane har rett til å styre lokale tilhøve gjennom lokale folkevalde organ».

Prinsipielt begrunnes kommunalt selvstyre med to sentrale verdier:

- lokal frihet / demokratisk selvbestemmelse
- effektivitet fordi en lokalt vet best hvor skoen trykker lokalt

Dette må balanseres mot to andre verdier:

- Likhet mellom kommunene i tjenester og kvalitet
- Effektivitet når saksområdet er slik at standardløsninger passer alle

En generell «formel» for bruk av skjønn kontra felles regulering (Rothstein, 1994) er:

- Hvis man skal håndheve forutsigbare utfordringer, er det lite behov for lokalt skjønn/autonomi
- Hvis det er ulike utfordringer i hvert enkelt tilfelle, er det behov for/noe å hente på å gi rom for utstrakt lokalt skjønn

Prinsipielt taler enkelte punkter mot en strengere nasjonal regulering av valgavvikling:

- Dersom inngrep i selvstyret virker unødvendig

- Dersom reguleringen truer viktige lokale verdier
- Dersom inngrepet er stort, men gir liten nytte
- Dersom det oppstår unødvendig omfattende byråkrati som det ikke er behov for
- Dersom det foreligger klare grunner til at kommuner kan ha ulike system eller liten sentral regulering
- Dersom man lokalt har god kompetanse som kjenner trusselbildet godt
- Dersom det i liten grad gir økt sikkerhet å gi overordnede pålegg/vurderinger
- Dersom lokal teknisk kompetanse er høy

Mens andre taler for en strengere nasjonal regulering av valgavvikling:

- Dersom det er behov for spesialisert kunnskap som ikke alle innehar
- Dersom det er lett å gjøre feil, og det kan få store konsekvenser
- Dersom selve «regulerings-intervensjonen» er liten fordi den er mer teknisk og ikke berører lokalpolitikk

På grunn av viktigheten av valgprosessen for å ivareta demokratiske verdier, er vurderingen i denne utredningen at en tydeligere regulering er hensiktsmessig for å sikre prosessen. Reguleringen som foreslås er på et funksjonelt nivå, og sikrer at det stilles krav til hva som må ivaretas i prosessen, samtidig som kommunene beholder stor grad av frihet i forhold til å velge hvordan. Dette vurderes derfor å gi minimal inngripen i lokalt selvstyre.

Ytringsfrihet

Tiltak for å håndtere uønsket påvirkning, herunder falske nyheter, netthets o.l., utløser ofte debatt rundt ytringsfrihet – og vil også kunne komme i en konflikt med denne. Et eksempel er krav om moderering av kommentarfelt, leserbrev og andre innlegg på nett – for å unngå hets, krenkelser og falske påstander. Det er selvsagt forskjell mellom moderering som er intern, og moderering som er pålagt. Den første trenger ikke være et problem med tanke på ytringsfrihet, mens det andre opplagt vil være det. Intern moderering av debatt kan nettopp styrke ytringsfrihet ved å forhindre bråk og usakligheter som avsporer debatten. Jamfør at også dagens leserbrevspalter er redigert, alt slipper ikke til. Det ville vært veldig annerledes om lovgiver sa hvordan leserbrevene skulle redigeres. Det same gjelder moderering av kommentarfelt i nettaviser. Redaksjonene bestemmer selv, men bør etablere felles retningslinjer for å følge allmenne saklighetsregler og slipper til gode innlegg uavhengig av om innholdet er kontroversielt, men tar ut trusler og sjikane.

Videre vil tiltak som handler om å avsløre informasjon som er direkte falsk i liten grad komme i konflikt med ytringsfriheten (forfalskede videoer, bilder og fakta), og bør styrkes. I mange tilfeller vil imidlertid situasjonen være at informasjon er delvis sann, eller utgjør bare en liten bit av bildet. I slike tilfeller vil både merking og fjerning av informasjonen, og ikke minst eventuell sanksjonering mot kilden, fort være grunnlag for diskusjon med tanke på ytringsfrihet.

Det finnes ikke et fasitsvar på hvordan teamet skal håndteres eller hva som er riktig eller galt, men det er viktig at teamet diskuteres og adresseres på kontinuerlig basis.

Åpenhet

Sikring mot tilsiktede handlinger har tradisjonelt ofte handlet om skjerming, hemmelighold og «låste dører». Når det gjelder demokratiske prosesser, og tiltak som anbefales i denne utredningen, er imidlertid åpenhet i seg selv i mange tilfeller en barriere og et effektivt tiltak. Ved å anbefale reguleringer som er funksjonelle og risikobaserte, gis det et godt utgangspunkt for å finne gode, hensiktsmessige og inkluderende tiltak lokalt. For tekniske systemer vil åpenhet i mange tilfeller gi bidrag til å avdekke sårbarheter (se for eksempel Sveits som åpent ba om hjelp hos alle for å finne feil og mangler i egne valgsystemer).

For å redusere sårbarhet knyttet til digitale valgsystemer legges det her stor vekt på barrieren som ligger i den parallelle manuelle tellingen og protokollføringen under valget. Den manuelle tellingen er gjennomsiktig og godt forståelig, og utfordrer ikke åpenhet. Det er imidlertid verdt å merke seg at en overgang til elektronisk stemmegiving mye lettere vil oppleves utfordrende i grensesnittet mellom teknologiske tiltak for å beskytte konfidensialiteten til stemmegiver og stemmer, og åpenhet og forståelse for hvordan prosessen foregår. Dette bør det tas høyde for, og adresseres i en digitaliseringsprosess.

Tiltak som er rettet mot å forstå og regulere eller håndtere påvirkning ved bruk av digitale plattformer vil bidra til større kunnskap og åpenhet – heller enn det motsatte.

Deler av sikkerhetsloven har stort fokus på å beskytte konfidensialiteten til informasjon og sårbarheter, dersom denne vil gjelde for valgsystemer og -prosesser i fremtiden. Her vil det viktigste for å sikre åpenhet være at tiltak implementeres etter gode vurderinger av hva som er nødvendig å skjerme – og hva som ikke er det.

9 Oppsummering av de fire forskningsspørsmålene

Under vises det kort til hvor i utredningen de ulike forskningsspørsmålene er tatt opp (for selve vurderingen vises det til aktuelt sted i utredningen):

1. Hva er truslene mot demokratiske prosesser i tilknytning til gjennomføring av valg i Norge? Dette inkluderer politiske prosesser og opinionspåvirkning i forkant av valg, samt selve den praktiske gjennomføring av valget. Både mulighet for angrep av ulike art, og uintenderte hendelser som kan få betydning for gjennomføringen må belyses. Truslene må beskrives både opp mot sannsynlighet og opp mot konsekvens, og evt. virkning på tillit til demokratiet.

- Utredningen tar opp 20 ulike uønskede fenomener/hendelser som kan påvirke de demokratiske prosessene i tilknytning til gjennomføring av valg i Norge. Detaljer knyttet til vurdering av trusler og risiko finnes i analyseskjemaene i vedlegg 2. Oppsummeringer finnes i utredningens kapittel 6. Utredningen viser at uønskede hendelser relatert til ulike former for påvirkning av kandidater/politikere og velgere, gir størst grunn til bekymring for sikkerheten i valgprosessene, og at dette i stor grad kan påvirke tillitten til valgprosessen, men også den frie deltagelse og om valget er opplyst og informert.

2. *Hvordan fordeler sårbarheter seg langs den digitale verdikjeden i valggjennomføringen? Av hensyn til oppdragets omfang må denne delen av oppdraget begrenses til en mer overordnet oversikt. Det vil være hensiktsmessig å vise ulike aktørers ansvar for de ulike delene av kjeden, samt deres mulighet til å kontrollere om reglene følges og til å sikre overholdelse.*

- Sårbarhetene i den digitale verdikjeden fremkommer på et overordnet nivå i analyseskjemaene i vedlegg 2 og i oppsummeringer i kapittel 6. Utredningen viser at den manuelle tellingen av stemmer som er forskriftsfestet i dag utgjør en svært viktig barriere mot manipulering av valgresultatet i den digitale verdikjeden. Ansvar for ulike aktører og muligheten til å kontrollere etterlevelse av krav belyses også videre i tiltak som anbefales i kapittel 8.1.

3. *Hvilke samfunnsmessige konsekvenser har bruken av teknologi i valggjennomføringen? Tilbyder bes belyse og drøfte hvilke konsekvenser teknologi og sikring av de digitale verdikjedene har for ansvarsfordeling mellom ulike nivåer. Nå legger staten føringer i utformingen av systemet, men har i liten grad mulighet til å stille tekniske krav. Videre bes det om en vurdering av forholdet til regelverk og regulering. Til slutt bes det også om en vurdering rundt åpenhet og hvordan dette sikres på en god måte, samtidig som krav til sikkerhet ivaretas.*

- Utredningen peker på valggjennomføringen som en samfunnskritisk funksjon for å ivareta demokratiske verdier i samfunnet og peker på hvordan reguleringer og tydeligere ansvarsfordeling på enkelte områder kan bidra til å gjøre valgprosessen mere robust også i en mer digital fremtid. Dette er ytterligere berørt i analyseskjemaer i vedlegg 2, og i betraktninger knyttet til anbefalte tiltak i kapittel 8.1. I tillegg er sikring av åpenhet diskutert i eget avsnitt i kapittel 8.3.

4. *Hvilke skadeforebyggende og skadebøtende tiltak bør iverksettes for å beskytte demokratiske prosesser til tilknytning til gjennomføring av valg i Norge? Tilbyder bes om å gi innspill til mulige tiltak som kan bidra til å øke sikkerheten i den demokratiske prosessen i Norge.*

- Utredningen oppsummerer forslag til mulige tiltak i kapittel 8 og diskuterer også dilemma knyttet til at enkelte tiltak også kan påvirke andre verdier, som lokalt selvstyre og ytringsfriheten.

10 Referanser

Bernhagen, Patrick (2009). "Measuring Democracy and Democratization", i Christian W. Haerpfer, Christian W. et al. (red.), Democratization. Oxford: Oxford University Press, pp. 24-40.

Brennan, Jason. (2016). Against democracy. Princeton University Press.

Dahl, Robert A. (1998). On Democracy. Yale University Press

Den Europeiske Union (2018). *Standard Eurobarometer 90*. *Public opinion in the European Union*. Nettsideressurs (10.04. 2019): http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/STANDARD/surveyKy/2215

Etterretningstjenesten (2019). FOKUS 2019 – Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer. https://forsvaret.no/fokus

Galston, William (1991). Liberal purposes. Goods, Virtues and Duties in the Liberal state. Cambridge University Press.

Gutmann, Amy og Dennis Thompson (2004). *Why Deliberative Democracy?* Princeton University Press.

Habermas, Jürgen (1996). Between Facts and Norms. Contributions to a Discourse Theory of Law and Democracy. MIT-press.

ISO (2018). ISO31000:2018 Risikostyring – Retningslinjer. April 2018.

Justis- og beredskapsdepartementet (2019). Lov om nasjonal sikkerhet (sikkerhetsloven). Kunngjort 01.06.2018. Ikrafttredelse 01.01.2019. https://lovdata.no/dokument/NL/lov/2018-06-01-24

Kommunal- og moderniseringsdepartementet. (2002). Lov om valg til Stortinget, fylkesting og kommunestyrer (valgloven).

Kymlicka, Will. (2001). Contemporary Political Philosophy: An Introduction, andre utgave. Oxford University Press.

Pateman, Carol. (1970). Participation and democratic theory. Cambridge University Press.

Pettit, Phillip. (2014). Just Freedom. A Moral Compass for a Complex World. W.W. Noryon & Company.

Pogge, Thomas W. (2008). *World Poverty and Human Rights.* Polity Press.

PST – Politiets Sikkerhetstjeneste. (2019). Trusselvurdering 2019. Publikasjon utgitt i 2019. https://www.pst.no/globalassets/artikler/trusselvurderinger/psts-trusselvurdering-2019.pdf

Rasch, Bjørn Erik. (2007). Demokrati. Fagbokforlaget.

Regjeringen (2017). Mandat for valglovutvalget. Tilgjengelig på https://www.regjeringen.no/no/dep/kmd/org/styrer-rad-og-utvalg/valglovutvalget/mandat-for-valglovutvalget/id2577295/

Rose, Richard. (2009). Democratic and undemocratic states', i Christian W. Haerpfer, Christian W. et al. (red.), Democratization. Oxford: Oxford University Press, ss. 41-53.

Rothstein, Bo. (1994). Vad bör staten göra? Om välfärdsstatens moraliska och politiska logik. SNS-Förlag.

Scumpeter, Joseph. (1952). Capitalism, socialism and democracy. Allan & Undwin.

Shorten, Andrew (2015). Contemporary Political Theory. Red Globe press.

Skinner, Quinton. (1978). The Foundations of Modern Political Thought. Cambridge University Press.

Snyder, Timothy. (2017). On Tyranny: Twenty Lessons from the Twentieth Century. Tim Duggan Books.

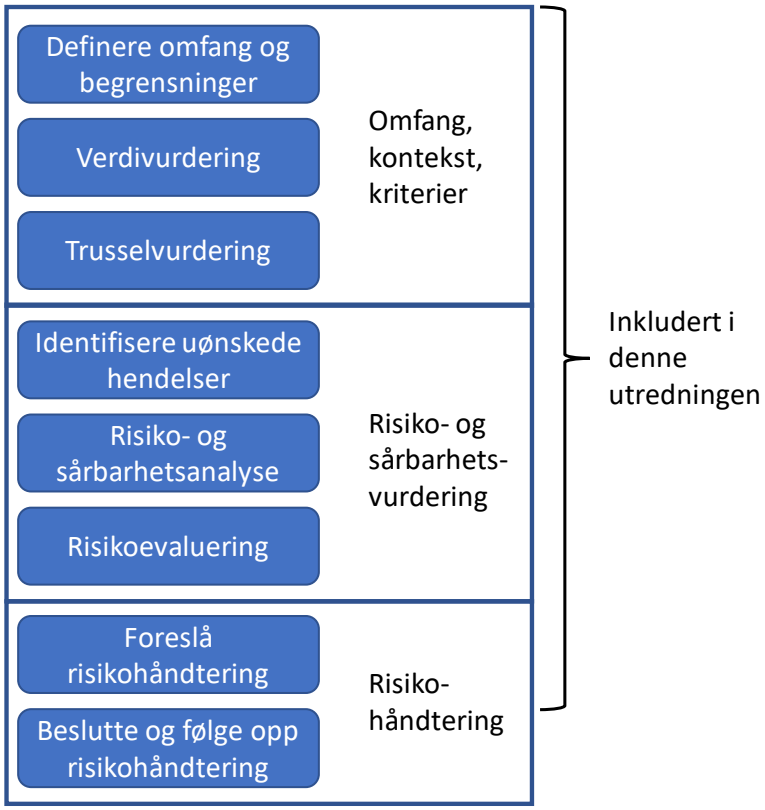
Soroush, Vosoughi, Deb, Roy and Sinan, Aral (2018), The spread of true and false news online. Science 09 Mar 2018: Vol. 359, Issue 6380, pp. 1146-1151

Taylor, Charles (1991). What is wrong with Negative Liberaty. I David Miller (red.), Liberty. Oxford University Press.

Wollebæk, Dag & Segaard, Signe Bock (2011). *Sosial kapital i Norge*. Cappelen Damm AS.

Vedlegg 1 Metodiske beskrivelser

Det finnes en rekke fremstillinger av trinnene som gjennomføres i en risikovurdering. Metoden som er benyttet i utredningsarbeidet tar utgangspunkt i en tilpasset versjon av den internasjonalt anerkjente standarden ISO31000:2018 "Risikostyring - Retningslinjer", Jf. Figur 10.



Figur 10 Trinnene i en risikovurdering. Basert på ISO31000:2018 Risikostyring - Retningslinjer.

Metoden består av tre trinn:

a) Omfang, kontekst og kriterier
b) Risiko- og sårbarhetsvurdering
c) Risikohåndtering

I det følgende gis en mer inngående beskrivelse av trinnene i Figur 10.

Omfang, kontekst, kriterier

Kontekst handler om å bygge et felles utgangspunkt for hva som skal vurderes og utredes, hva som skal fokuseres på og hva som er målet med utredningen. Følgende inngår i beskrivelsen av kontekst:

Definere omfang og begrensninger

Dette er beskrevet i oppdragsbeskrivelsen, jf. Kapittel 2 og i systembeskrivelsen i Kapittel 3.

For å møte behovet for tverrfaglig kompetanse er utredningen gjennomført av et tverrfaglig team som blant annet har dekket:

- *Valg og valggjennomføring* – kunnskap om politikk og demokratiske prosesser, valglov og valgordninger, kunnskap om valgadministrasjonssystemet, erfaring og kunnskap og ulike måter og ordninger for valggjennomføring, aktører, roller og nivåer i valggjennomføring
- *Teknologikompetanse* – Cybersikkerhet/IKT-sikkerhet, digitale verdikjeder, sårbarheter, digital sabotasje, teknologiske muligheter og risiko, digitale aktører og kapasiteter
- *Trusler* – trusselvurderinger, identifisering av aktører og intensjoner, kapasiteter for trusselgjennomføring, angrepsvektorer, nasjonalt risikobilde
- *Hvordan påvirkes samfunn og velgere* – nyheter og medier, kommunikasjon, menneskelige reaksjoner, bruk av digitale medier, påvirkningsvirksomhet, interesseparter
- *Risiko- og sårbarhetsvurderinger* – metode og forskningstilnærming, utredningskompetanse, overordnet risikobilde, prosjektledelse og koordinering, tiltaksvurderinger og tiltakseffekter, regelverksforståelse og regelverksutvikling.

Underveis i utredningsarbeidet har analysegruppen benyttet seg av informasjonsmateriell fra åpne kilder, både nasjonalt og internasjonalt. En oversikt over dette materiellet er dokumentert i Vedlegg 3. Kunnskapen som er oppnådd gjennom dette arbeidet er lagt til grunn for utredningen.

Hensikten med utredningen er å bidra til å ivareta de demokratiske verdiene som samfunnet ønsker å beskytte. Som en del av analysen er det gjort en vurdering av hva som må være ivaretatt i valg for at de demokratiske verdiene skal opprettholdes. Dette inkluderer forventninger i valgloven, der det står spesifikt at valg skal være frie, direkte og hemmelige. Videre er det gjort en avgrensning av fokus basert på oppdragsbeskrivelsen. Et eksempel i så måte at det kun er demokratiske verdier som er sikkerhetsrelatert som er vurdert nærmere. Ovennevnte er beskrevet nærmere i Kapittel 3.1, blant annet med basis i tenkningen til demokratiteoretikeren Robert A. Dahl. Resultatet av verdivurderingen er følgende fem krav/områder/forutsetninger:

- *Fri deltagelse* - At alle kandidater til valget, og velgere, har og får tilgang til å delta ved at det oppleves trygt og mulig - og at valget er hemmelig
- *Opplyst og informert* - At velgere får nok informasjon, riktig informasjon og balansert informasjon – til at de kan gjøre et «informert valg» (stemme)
- *Korrekt* - At de stemmer som er avgitt faktisk utgjør resultatet. Riktig manntall, riktig registrering, riktig antall stemmer
- *Gjennomført i tråd med plan* - At man faktisk får avholdt valget (og ikke hindres av sabotasje, naturhendelser, systemfeil eller organiseringsmangler)
- *Tillit* - At tilliten til den demokratiske valgprosessen opprettholdes i befolkningen (herunder at etterprøvbarhet og åpenhet er ivaretatt)

Verdivurdering

Verdivurdering handler om å identifisere sentrale innsatsfaktorer som er viktige i gjennomføringen av valget. Eksempler er fysisk infrastruktur som valglokaler og valgmateriell, samt teknisk infrastruktur som for eksempel skannere, manntall, EVA og teknisk utstyr hos valgdirektoratet. Disse verdiene/innsatsfaktorene er beskrevet på et overordnet nivå i systembeskrivelsen i Kapittel 3. Det presiseres at det ikke gjort en detaljert verdivurdering. Dette skyldes først og fremst at hensikten med utredningen er å gjøre vurderinger på et overordnet nivå. I tillegg kan det tenkes at en detaljert verdivurdering ville føre til at rapporten ikke kunne gjøres offentlig.

Trusselvurdering

Som tidligere nevnt kan verdiene trues både av hendelser som gjøres med vilje, slik som manipulering av valgresultatet, og av hendelser som ikke gjøres med vilje, som for eksempel spesielle værforhold som gjør at ikke alle får avgitt sin stemme eller at en valgmedarbeider taster feil på en datamaskin. For hendelser som ikke gjøres med vilje, er det ingen trusselaktør som aktivt 'styrer' truslene. Som følge av dette er trusselvurderingen gjort som en integrert del av risikoanalysen. For hendelser som gjøres med vilje er det snakk om trusselaktører som styrer eller bestemmer om de skal prøve å angripe noen av verdiene. Slike trusselaktører er tenkende individer som går målrettet til verks. På grunn av dette er det hensiktsmessig å beskrive de ulike relevante trusselaktørene og å gjøre en vurdering av i hvilken grad vi anser det som sannsynlig at de vil prøve å angripe verdiene. Sannsynligheten for angrep vurderes gjennom å vurdere hvor attraktive verdiene er, hvilken intensjon en trusselaktør har for å angripe disse verdiene og i hvilken grad trusselaktøren har kapasitet til å gjennomføre et slikt angrep. Dersom en trusselaktør både har intensjon om å angripe en verdi, og samtidig har kapasitet til å gjennomføre et slikt angrep, anses trusselen som høy. Trusselvurderingen for hendelser som er gjort med vilje er dokumentert i Kapittel 5 og i vedlegg 4. Denne trusselvurderingen identifiserer både aktører og deres aktuelle angrepsvektorer og metoder. Dette er et viktig underlag for senere vurderinger av sårbarhetene i systemene.

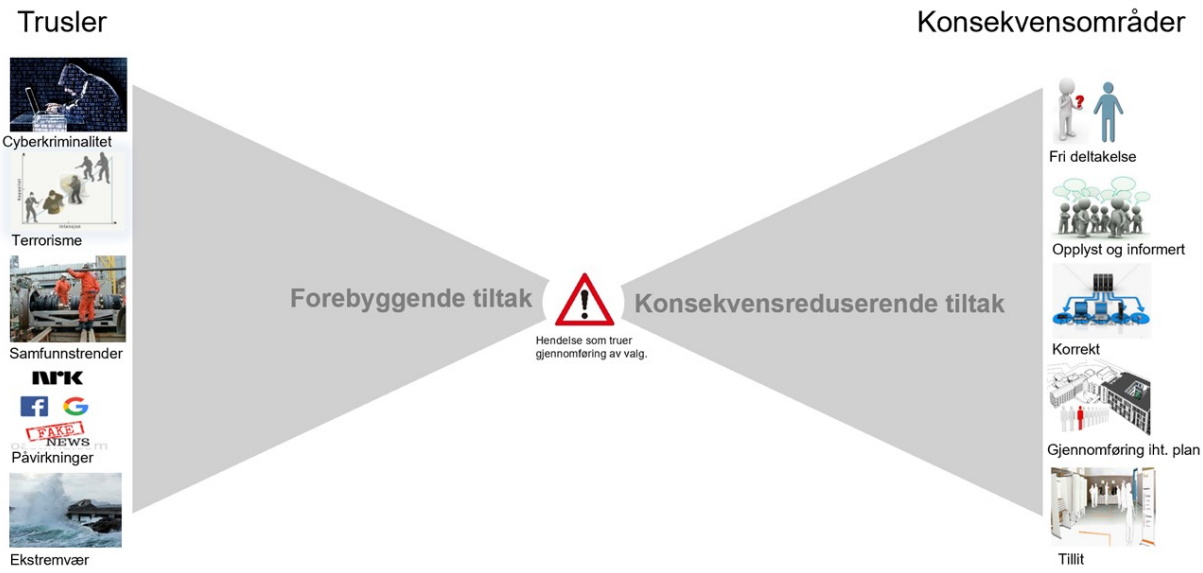
Risiko- og sårbarhetsvurdering

Identifisere uønskede hendelser

Med utgangspunkt i kunnskapen etablert gjennom kontekst, er uønskede hendelser identifisert. Dette er gjennomført som en idédugnad blant prosjektdeltakerne. Risiko- og sårbarhetsvurderingene er gjennomført ved å identifisere potensielle hendelser før, under og etter valget. For å sikre at en systematisk prosess der alle forhold blir inkludert, har prosessen blitt gjennomført med ulike innfallsvinkler. Dette inkluderer mulige hendelser i selve valggjennomføringen, i den digitale verdikjeden, med utgangspunkt i de ulike konsekvensdimensjonene og i et faglig perspektiv.

Figur 11 viser et såkalt sløyfediagram. I midten av figuren fremstilles en uønsket[22] hendelse, for eksempel at en skanner manipuleres eller at det brenner i et valglokale. Til venstre i diagrammet vises ulike trusler som kan føre til den uønskede hendelsen. I hvilken grad hver trussel skal ende opp med den uønskede hendelsen, kommer an på hvilke forebyggende barrierer som er etablert og sårbarheten til disse barrierene. Også til høyre for den uønskede hendelsen er det barrierer. Dette er barrierer som skal forebygge at konsekvensene blir alvorlige *selv om* den uønskede hendelsen inntrer. Dette er konsekvensreduserende barrierer, noen ganger omtalt som beredskapstiltak. Et eksempel er den manuelle tellingen av stemmesedler som gjennomføres for å avdekke om den elektroniske tellingen er blitt manipulert.

[22] Begrepet «uønsket» er sett fra samfunnets ståsted, ikke trusselaktørens ståsted.



Figur 11: Sløyfediagram for en uønsket hendelse.

Sløyfemodellen er en forenkling: I realiteten er det snakk om et stort antall mulige scenarioer eller hendelseskjeder fra venstre (årsaker) mot høyre (konsekvenser). Jo lengre mot høyre og venstre en prøver å beskrive disse potensielle årsakskjedene, jo flere muligheter finnes. Dette er begrunnelsen for at figuren ser ut som en sløyfe som utvider seg både mot høyre og venstre.

I enhver risikovurdering vil en måtte gjøre forenklinger. Dette betyr at man underveis i prosessen med risikovurderingen må ta velbegrunnede valg for å sikre at en belyser risikobildet på en relevant måte. Det er kun uønskede hendelser som anses som spesielt relevante med tanke på bakgrunn, formål og avgrensninger for denne utredningen, som er inkludert. Dette innebærer at listen over hendelser ikke inneholder alle tenkelige uønskede hendelser som kan tenkes å true valget. En slik fremgangsmåte ville imidlertid verken vært formålstjenlig eller gjennomførbar i praksis.

Risiko- og sårbarhetsanalyse

For hver av de uønskede hendelsene/scenarioene er risiko og sårbarhet analysert. Denne analysen er gjennomført av prosjektdeltakerne gjennom flere arbeidsmøter. Risiko- og sårbarhetsanalysen er dokumentert med ett skjema for hver uønsket hendelse som er vurdert. For hver uønsket hendelse er en rekke aspekter av risiko vurdert, jf. Tabell 2.

Tabell 2: Aspekter av risiko vurdert i risiko- og sårbarhetsanalysen

Aspekter av risiko	**Beskrivelse**
Beskrivelse	Beskrivelse og forklaring av hva hendelsen inkluderer
Trusler/virkemidler	Beskrivelse av hva og hvem som kan få hendelsen til å inntreffe (herunder trusselaktør)
Sårbarheter	En beskrivelse av identifiserte sårbarheter. Dette inkluderer sårbarheter relatert til både forebyggende tiltak og konsekvensreduserende tiltak

Konsekvenser	En vurdering av hvilke konsekvenser som kan bli resultatet av den uønskede hendelsen. Vurderingen er gjort for hver av de fem konsekvensdimensjonene
Kunnskapsstyrke	En beskrivelse av hvor god kunnskap risikoanalysen er basert på. Dette inkluderer forståelsen av fenomenet som vurderes, i hvilken grad det er tilgjengelig relevante data, hvor realistiske antagelsene er og i hvilken grad det er enighet blant eksperter på området
Overførbarhet	En vurdering av hvor 'overførbar' en uønsket hendelse er til andre situasjoner, andre lokasjoner etc.
Endringshastighet	En vurdering av i hvor stor grad/tempo kan vi forvente at forutsetningene i scenariet endrer seg over tid
Samlet vurdering	En samlet vurdering av risiko basert på en totalvurdering
Styrbarhet	I hvilken grad oppdragsgiver/samfunnet har anledning til å styre risikoen, for eksempel ved å innføre risikoreduserende tiltak
Foreslå tiltak	Forslag til tiltak for å håndtere risikoen, for eksempel tiltak for å forebygge en uønsket hendelse ved å redusere kjente sårbarheter, tiltak for å oppdage/ redusere konsekvensene dersom hendelsen skjer eller tiltak for å innhente mer kunnskap

Risikoevaluering

Basert på de identifiserte uønskede hendelsene, og analysen av risiko og sårbarheter, er et samlet risikobilde presentert. Dette er gjort på ulike måter og er forklart nærmere i kapittel 6.

Risikohåndtering

Risiko kan håndteres på flere måter[23], for eksempel ved å akseptere risikoen som den er eller ved å redusere risikoen ved hjelp av forebyggende eller konsekvensreduserende tiltak.

Foreslå risikohåndtering

For hver uønsket hendelse er det gjennomført en idédugnad om hvilke risikoreduserende tiltak som kan tenkes å være aktuelle. Resultatet fra denne idédugnaden er dokumentert i analyseskjemaene som er presentert i Vedlegg 2. Tiltakene er på ulike nivåer. For eksempel er enkelte tiltak relatert til regulering mens andre tiltak handler om å innhente kunnskap. Det er også foreslått tiltak for å redusere sårbarheter, herunder tekniske og operasjonelle tiltak for å redusere muligheten for at de uønskede hendelsene skal oppstå, for å oppdage at de faktisk har oppstått eller for å redusere konsekvensene, dvs. beredskapstiltak.

Som en del av risikoevalueringen har de ulike alternative tiltakene blitt vurdert samlet. Resultatet er en anbefaling om tiltak oppdragsgiver bør vurdere nærmere med tanke på implementering.

[23] Risiko kan (i prinsippet) håndteres ved å akseptere, redusere, øke/optimalisere, og overføre risiko (for eksempel med forsikring). De to siste fremgangsmåtene er lite aktuelle i denne utredningen.

Beslutte og følge opp risikohåndtering

Å beslutte hvilke tiltak som skal gjennomføres er et verdispørsmål der fordelene med å iverksette risikoreduserende tiltak må veies opp mot andre hensyn, slik som hensyn til den enkelte, kostnader og praktisk gjennomførbarhet. Dette er forhold som ligger på utsiden av utredningen. Det er således ikke opp til Proactima å beslutte hvilke risikoreduserende tiltak som skal iverksettes: Beslutning og oppfølging av tiltak er derfor ikke en del av denne utredningen.

Vedlegg 2 Risiko- og sårbarhetsvurdering

Forklaringer:

Beskrivelse – Beskrivelse og forklaring av hva hendelsen består av og dekker

Trusler/virkemidler – Beskrivelse av hvem som kan være aktuelle for å bruke dette for å påvirke valget, og hvordan de vil gjøre de

Barrierer og sårbarheter – Hva er det, med dagens forutsetninger, som hindrer at de lykkes – eller som gjør at de lykkes (sårbarheter)gjennomgang av hendelse/scenario – hvor har vi sett at sårbarhetene ligger i valgprosessen

Konsekvenser for krav til valgprosessen – Vi har definert 5 områder med krav som stilles til valgprosessen for å ivareta sikkerheten. Her vurderer vi hvor stor (negativ) påvirkning de ulike hendelsene kan ha på disse, basert på beskrivelsene over.

> *Fri deltagelse* - At alle kandidater til valget, og velgere, har og får tilgang til å delta ved at det oppleves trygt og mulig - og at valget er hemmelig
>
> *Opplyst og informert* - At velgere får nok informasjon, riktig informasjon og balansert informasjon – til at de kan gjøre et «informert valg» (stemme)
>
> *Korrekt*: At de stemmer som er avgitt faktisk utgjør resultatet. Riktig manntall, riktig registrering, riktig antall stemmer
>
> *Gjennomført i tråd med plan*: At man faktisk får avholdt valget (og ikke hindres av sabotasje, naturhendelser, systemfeil eller organiseringsmangler)
>
> *Tillit*: At tilliten til den demokratiske valgprosessen opprettholdes i befolkningen (herunder at etterprøvbarhet og åpenhet er ivaretatt)

Kunnskapsstyrke – hvor sikre/usikre er vurderingene. Hvor mye kunnskap har vi om fenomenet/hendelsen og forutsetningene vi legger til grunn.

Overførbarhet – hvor «overførbar» er hendelsen ifht andre situasjoner, andre lokasjoner etc. (vurderer om vi skal videreføre dette aspektet)

Endringshastighet – i hvor stor grad/tempo kan vi forvente at fenomenet og forutsetningene endrer seg?

Samlet vurdering – Hvor viktig/kritisk er hendelsen for sikkerhet i valgprosessen – og i hvor stor grad har vi mulighet til å endre/påvirke hendelsen

Aktuelle tiltak – adresserer aktuelle måter å motvirke hendelsen på (i hele spekteret fra opplæring av borgere, lovregulering og til fysiske og teknologiske sikringstiltak) Tiltakene bør adressere sårbarheter som påpekes

Innhold

1. Lokal eller sentral politisk innflytelse på valget

Hendelse/fenomen: Lokal eller sentral politisk innflytelse på valget

Beskrivelse

I den norske valgprosessen er de folkevalgtes involvering relativt stor. Hver kommune er ansvarlige for forberedelse og gjennomføring av valg i sin kommune. Det er også kommunenes ansvar å veilede velgeren ved spørsmål rundt valg. Valgstyret er et politisk organ, valgt av kommunestyret, og skal blant annet behandle listeforslag, rekruttere valgmedarbeidere, bestille utstyr, sørge for stemmelokaler, gjennomføre stemmegivning og telle opp avgitte stemmer (og foreta valgoppgjør ved kommunestyrevalg). Valglovgivningen stiller en rekke krav til gjennomføringen av valg; som skal hindre påvirkning av stemmegivning og resultat. Samtidig har kommunen stor grad av frihet i gjennomføringen av valg. Kommunestyret kan delegere beslutninger til valgstyret, og oppgaver til kommunens administrasjon. Grunnlovens §49 fikk i 2016 en tilføyelse som sier at «*Innbyggjarane har rett til å styre lokale tilhøve gjennom lokale folkevalde organ*».

Et fokusert tema i forbindelse med valg er stadig hvor stor valgdeltakelsen i befolkningen er. Stortingsmelding nr. 33 2007-2008 understreker at «Det representative demokratiet utgjør kjernen i det norske folkestyret. Derfor bør valgdeltakelsen generelt sett være høy, og velgergrupper i alle lag av befolkningen bør delta i størst mulig grad». Gjennom regjeringens nettsider fokuseres og oppfordres det til å arbeide med økt valgdeltakelse, og det er gjennomført forsøk under valgene i både 2015 og 2017 med utsendelse av personlig informasjon i form av brev og SMS til større og mindre grupper, for å se på effekt på valgdeltakelse. Gjennom kartleggingen i arbeidet med denne rapporten er det observert at kommunenes selvbestemmelse også gir utslag i hvordan og i hvilken grad ulike kommuner arbeider med å øke valgdeltakelse i befolkningen generelt, og i eventuelle underrepresenterte grupper spesielt. I enkelte kommuner er det valgt å gjennomføre målrettede tiltak, i andre ikke. I noen kommuner beslutter valgstyret eventuelle tiltak direkte, mens det i andre kommuner er et arbeid som på fast basis er delegert til kommunens administrasjon. Beslutninger om å gjennomføre eller ikke gjennomføre informasjons- og motivasjonskampanjer mot enkeltgrupperinger i regi av kommunen, vil klart kunne påvirke resultatene i et valg.

Også når det gjelder klage- og ankesaker (valgtvister) i forbindelse med stortingsvalg, er det valgorganene og Stortinget som har ansvar for å dømme, mens retten har en begrenset rolle (knyttet til myndighetsmisbruk eller alvorlige brudd på grunnleggende prosedyrer). Gjennom grunnloven og valgloven gis det nyvalgte Stortinget myndigheten til å godkjenne valget og valgbarheten til de nyvalgte representantene. De vurderer også ankesaker og ankeavgjørelser i tilknytning til dette. Stortingets avgjørelser kan ikke ankes til domstolene.

Trusler/virkemidler

I samtaler fremkommer at det i enkelte kommuner er en oppfatning av at det gjøres politisk motiverte beslutninger (i valgstyret) med tanke på å gjennomføre tiltak eller ikke for å øke valgdeltakelse, og i hvilke grupper det eventuelt gjennomføres tiltak. Om motivasjonen for slike beslutninger er politisk eller ikke, vil være vanskelig å bevise eller motbevise. Imidlertid vil det, til nærmere de folkevalgte organene slike beslutninger tas, være mulighet for å så tvil om motivasjonen og om integriteten til system og medarbeidere.

Både det faktum at personer som selv står på valglistene kan være med i lokale valgstyrer; og at det er Stortinget som godkjenner valget og selv er klageorgan for valget; er i flere omganger kritisert av Organisasjonen for sikkerhet og samarbeid i Europa (OSSE). Det at det i dag ikke er mulig å påklage en avgjørelse i klagesak knyttet til valget inn for domstolene, mener OSSE er et brudd med internasjonale konvensjoner; noe Veneziakonvensjonen har gitt dem medhold i.

Selv om en nasjonalt kan vurdere risikoen for valgpåvirkning gjennom folkevalgte organer som lav, vil internasjonal kritikk av valgordningen kunne bidra til redusert tillit til den demokratiske styreformen.

Vurdering: Middels trussel

Barrierer og sårbarheter

Den norske modellen er i stor grad tillitsbasert, og avhenger av tillit til politikerne. Man kan også hevde at dagens system skaper tillit til politikerne.

Betydelig involvering og deltakelse ansvarliggjør politikerne – og det at valget godkjennes av Stortinget kan redusere potensialet for at uttalelser om mistillit til resultatet benyttes politisk. Det kan også hevdes at misbruk av systemet raskt vil «alarmeres» av andre involverte, og at sårbarheten for misbruk slik reduseres.

Samtidig er trenden internasjonalt at tilliten til politikere og politiske prosesser går ned. Basert på dette kan dagens system være sårbart for en (eventuell) lavere tillit i fremtiden. Det kan hevdes etter valget at resultatet har blitt påvirket, med henvisning til at folkevalgte sitter i valgstyret. Dette er en sårbarhet som kan utnyttes strategisk.

Jyllands-Posten rapporterer i mai 2019 fra en undersøkelse som viser at andelen dansker som har stor tillit til politikerne, har falt fra 70 prosent i 2007, og til bare 29 % i 2019 (https://jyllands-posten.dk/politik/ECE11348846/tilliden-til-politikere-naar-historisk-lavpunkt-pia-kjaersgaard-har-tre-bud-paa-loesninger/).

Når de politiske partiene regulerer valgprosedyrer og valggjennomføring selv, er det et forskerfunn at egeninteressene til partiene teller med i vurderingene som gjøres (se eksempelvis Bernt Aardal (2019) *Styring eller representasjon. Et partisystem i endring* og Allern, Saglie og Østerud (red.) *Makt og opposisjon. De politiske partier som demokratiske paradoks. Oslo: Universitetsforlaget.* Dette er ikke det samme som korrupsjon eller urent politisk spill, men en konsekvens av at det i det store og hele er vanskelig å holde egeninteresser helt adskilt fra samfunnets interesser.

Fremtredende statsvitere har pekt på at det er grunn til å diskutere og spørre om hvor fornuftig det «relativt svake innslaget av formelle reguleringer av politisk virksomhet i Norge» er (ref. Allern, Saglie og Østerud (red.) *Makt og opposisjon. De politiske partier som demokratiske paradoks*. Oslo: Universitetsforlaget). Politikerne bestemmer selv sine egne vilkår, og det kan stilles spørsmål ved utfordringer knyttet til dette. «Partiene har selv makt til å bestemme hva slags rammer de skal operere innenfor, og dagens makthavere kan bestemme spillereglene for morgendagens opposisjon. Da er det desto viktigere at vi jevnlig har bred, grundig og åpen debatt om nettopp disse».

Representanter fra OSSE har fremholdt at nettopp den høye tilliten nordmenn har til systemet kan medføre at noen av sikkerhetsmekanismene og reglene som forventes og er etablert i andre land - ikke har blitt institusjonalisert i Norge.

Vurdering: Middels sårbarhet

Konsekvenser for krav til valgprosessen:

Fri deltagelse	*Opplyst og informert*	*Korrekt*	*Gjennomføres som planlagt*	*Tillit*
Fokus og aktiviteter som besluttes av valgstyrene kan påvirke grad av valgdeltakelse		Manglende uavhengig klageordning kan potensielt gi feil i valggjennomføringen		Har først og fremst betydning for tillit, siden det kan stilles spørsmål ved dagens ordning.
Liten konsekvens	Ingen/nesten ingen konsekvens	Liten konsekvens	Ingen/nesten ingen konsekvens	Noe konsekvens

Kunnskapsstyrke

Det foreligger informasjon om hvordan ordningene er etablert i andre land. OSSE har dokumentert vurderinger.	Middels

Overførbarhet

Gjelder alle valg, både lokale valg i alle kommuner og sentrale valg. Derfor høy overførbarhet.	Høy

Endringshastighet

En kan ikke se bort fra at tilliten til politikere og politiske prosesser vil falle i fremtiden. Endringene (i motsetning til innen del mer «teknologiske felter») er imidlertid ikke veldig raske.	Lav

Oppsummering	
Samlet vurdering – Vurderes ikke å være en stor utfordring i Norge i dag, men har fått kritikk internasjonalt ved flere anledninger og må derfor vurderes nøye.	*Styrbarhet* – Dette er områder som det er stor mulighet for å regulere gjennom lov og overenskomster
Middels	Høy

Aktuelle tiltak

- Gjøre en utredning av dagens og alternative systemer, der fordeler og ulemper ved ulike ordninger tas med i vurderingen. Herunder at den barrieren det tillitsbaserte systemet utgjør i dag også tas i betraktning

Noen mulige alternativer:

- Nasjonale valg: Ansvar for godkjenning av valget, og for klageordningen, ivaretas av domstol eller et eget dedikert organ. (Dette er vanlig i en rekke andre land, og Norge har blitt kritisert av valgobservatører for den ordningen vi har i dag).
- Vurdere om valgstyrene kunne vært ledet av representant for administrasjon, domstol eller andre dersom ordningen med «folkevalgte valgstyrer» videreføres.
- Vurdere å flytte godkjenning av valget bort fra folkevalgte organer også lokalt. Hevde prinsipp om at det ikke skal være de samme personene.

2. Ulik mulighet til å delta i valgkampen

Hendelse/fenomen: Ulik mulighet til å delta i valgkampen

Beskrivelse

I ulike lands styreform og valgsystemer, har partier og organisasjoner i ulik grad mulighet til å etablere seg og delta aktivt i valgkampen. I flere land, for eksempel USA, er kandidater og partier helt avhengige av donasjoner fra enkeltpersoner, selskaper og organisasjoner for å kunne hevde seg i valgkampen. Dersom utviklingen skulle gå i samme retning i Norge, vil det kunne føre til at ikke alle har lik mulighet til å delta i valgkampen.

Det kan også potensielt være vanskelig å se hvem som støtter hvem, og hvilke bindinger dette gir politisk.

I hvilken grad partier, kandidater og organisasjoner slipper til eksempelvis store riksdekkende medier; kan ha stor påvirkning på den reelle muligheten til å delta – bli hørt og bli valgt.

Trusler/virkemidler

Både statlige aktører, interesseorganisasjoner og kommersielle aktører vil kunne ha interesse av å styrke og fremme enkelte partier, saker og organisasjoner for å påvirke politikk og beslutninger lokalt og nasjonalt.

Politikken kan påvirkes ved at enkelte partier og organisasjoner får mulighet til å delta i valgkamp gjennom tilføring av økonomisk kapasitet; og andre ikke. Videre kan partier som har fått slik støtte enten bevisst eller ubevisst oppleve at det knytter seg forventninger til fokus og syn på ulike saker når støtte gis.

Trusselaktører kan også tenkes å påvirke hvem som høres (og synes) i store meningsbærende medier gjennom både kapital, støtte, fremheving av saker og påvirkning («god eller dårlig») av medieaktørene.

Vurdering: Høy trussel

Barrierer og sårbarheter

I Norge regulerer partiloven støtte til politiske partier. En stor del av finansieringen av partiene kommer gjennom offentlig støtte; i 2017 ca 67 % totalt (kilde: SSB). I hovedsak er denne støtten i form av grunnstøtte som tildeles alle partier med over 2,5 % av stemmene på landsbasis eller som fikk inn minst én representant ved siste stortingsvalg (1/10), og stemmestøtte, som gis som et likt beløp per stemme oppnådd ved siste stortingsvalg (9/10). Tilsvarende modeller for offentlig støtte finnes på fylkesnivå og kommunenivå. Dette gjør den norske modellen mer robust ifht truslene som beskrives. Samtidig ser vi at pengestøtte til partier blir mer vanlig, både fra organisasjoner og personer. I perioden fra 2006 til 2017 sank andelen offentlig støtte til partiene fra 75% til de nevnte 67 % (Kilde: SSB).

Partiloven stiller en rekke krav til bidrag også fra andre enn offentlige bidragsytere, blant annet at anonyme bidrag ikke kan mottas av politiske partier. Det er heller ikke tillatt å motta bidrag fra utenlandske givere. Åpenhet om støtte til politiske partier er et viktig prinsipp og krav i den norske modellen, og det kreves identifisering av både verdi og bidragsyter både for finansielle bidrag og andre ytelser til partiene. Dette utgjør en barriere mot skjult påvirkning.

Likevel påpekes i dag oftere at støtte fra private kan sees på som et problem; både «de rike onklene til høyre» og bindinger mellom fagbevegelsen og partier på venstresiden.

Det har flere ganger vært diskusjoner ifm. stortingsvalg der det hevdes at små partier får mindre taletid på TV enn de store partiene. Andre igjen hevder at flere av de små partiene får uforholdsmessig mye taletid i de store mediene. De store mediehusene har en langt på vei felles policy på dette området, for å sikre god tilgang til bredden av partier. Området er i seg selv vanskelig å både måle og regulere; men det fremstår ikke som et omfattende problem i den norske politiske debatten i dag.

Vurdering: Middels sårbarhet

Konsekvenser for krav til valgprosessen:				
Fri deltagelse	*Opplyst og informert*	*Korrekt*	*Gjennomføres som planlagt*	*Tillit*
Rekruttering til politisk aktivitet kan stoppe opp pga. ulike faktiske muligheter. Levekår for partier/organisasjoner uten privat støtte kan bli for dårlige	Grupper som er lite representert blir dårligere informert og kan ramle ut av debatt og valgkamp			I dag er, med eksisterende barrierer, tilliten til systemet fortsatt høy
Liten konsekvens	Liten konsekvens	Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Liten konsekvens

Kunnskapsstyrke	
Mekanismer og system er godt forstått	Høy

Overførbarhet	
Gjelder på alle nivåer, lokalt og sentralt	Høy

Endringshastighet	
Partifinansiering er økende, men ikke i stor hastighet	Lav

Oppsummering	
Samlet vurdering – Med dagens regulering og system i Norge vurderes ikke dette å ha høy Samlet vurdering	*Styrbarhet* – Forholdet kan langt på vei styres gjennom reguleringer
Lav	Høy

Aktuelle tiltak

- Videreføre regulering som krever åpenhet om økonomisk støtte til partier
- Videreføre og styrke støtteordninger som sikrer «levemulighet» for en bredde av partier og organisasjoner
- Sikre plass for «alle» i offentlige debatter i store medier
- Gjennomføre informasjonskampanjer mot utsatte grupper/organisasjoner
- Oppfordre til bred støtte der private går inn
- Inspirere barn og unge til å bli engasjerte og delta i debatter om viktige spørsmål i nærmiljøet
- Opprettholde og styrke støtteordninger til bred medieflora, inkludert meningsbærende aviser.

3. Overvåking/påvirkning av valgkandidater og politiske partier

Hendelse/fenomen: Overvåking/påvirkning av valgkandidater og politiske partier

Beskrivelse

Både nasjonalt og internasjonalt har det de siste årene vært satt stort fokus på forsøk på (og gjennomføring) av informasjonsinnhenting og påvirkning rettet mot politiske partier og kandidater som stiller til valg. En rekke hendelser og eksempler har kommet fram etter eksempelvis valget i USA i 2016, men også nasjonalt ble det i forkant av stortingsvalget i 2017 blant annet bekreftet at det var gjennomført et hackerangrep som omfattet Arbeidspartiet og Forsvaret.

Motivasjonen for slike angrep har flere utgangspunkt. Politikere, politiske og andre statlige organer sitter i beslutningsposisjoner og påvirker politisk retning nasjonalt og internasjonalt. Både det å skaffe seg informasjon om planer, strategier og retninger – og også påvirke disse, er av interesse for statlige og andre store interesseaktører. Både gjennom det at angrep gjennomføres, og ved bruk av tilgang og informasjon som innhentes, kan aktøren påvirke og redusere tilliten til politikere, partier og demokratiske prosesser generelt. I tillegg kan bruk av informasjon gi aktøren mulighet til å både presse og påvirke enkeltindivider og organisasjoner til å skaffe mer informasjon eller bidra til beslutninger som gagner aktøren på noen måte.

Trusler/virkemidler

I tilknytning til større etterretnings- og påvirkningsoperasjoner mot politiske miljøer, er statlige aktører den mest fremtredende interesseaktøren og trusselen. Dette er også aktører med svært stor evne og kapasitet, og flere er kjente for å jobbe med et bredt spekter av virkemidler for å oppnå målet om å innhente informasjon – og bruke den. I dette ligger både menneskelige metoder og interaksjoner, og teknologiske angrep som hacking.

Både omfattende angrep på amerikanske politikere og organisasjoner i 2016 og forsøkene på bruk av spear phising-angrep mot blant annet arbeiderpartiet i 2017, har blitt tillagt hackergruppen ÅPT 29 («Cozy bear») som knyttes til den russiske etterretningstjenesten FSB. https://www.tv2.no/a/8903847/

Vurdering: Høy trussel

Barrierer og sårbarheter

Trusler og metoder relatert til denne typen angrep har blitt mye fokusert de siste årene, og er derfor stadig mer kjent for kandidater og partier. I forkant av valget i Norge i 2017 utgav myndighetene en brosjyre utarbeidet av Etterretningstjenesten, Nasjonal sikkerhetsmyndighet og Politiets sikkerhetstjeneste; med råd til alle kandidater som stilte til valg om hvordan de kunne beskytte seg mot slik angrep. Undersøkelser og hendelser har visst at kunnskapsnivået både rundt trussel, angrepsmetoder og IT-sikkerhet blant kandidater til valg, ikke er gjennomgående høy. Tiltak som denne brosjyren er med på å heve bevisstheten hos de involverte og reduserer sårbarheten for at angrep skal lykkes. https://www.regjeringen.no/contentassets/e2d4d86919944a8586a0628ce5c63dca/pmvedlegg_sikkerhet-og-valg.pdf

Det norske samfunnet er karakterisert ved høy tillit og åpenhet, blant annet gjennom flere internasjonale undersøkelser. Høy tillit til mennesker og systemer er i mange tilfeller en barriere mot uønsket påvirkning fra trusselaktører, men kan også utgjøre en sårbarhet. Ikke minst gjelder dette ved bruk av såkalt «social engineering» der trusselaktøren etablerer og utnytter sosiale relasjoner med kandidater og andre som kan ha relevante tilganger eller informasjon.

Det foregår i dag en rekke nasjonale og internasjonale initiativer både fra offentlige og private aktører for å bevisstgjøre og beskytte kandidater og organisasjoner i forbindelse med valg – også teknologiske verktøy. Et eksempel, blant flere initiativer verden rundt, er Microsofts internasjonale initiativ «Defending Democray Program» og verktøyet «AccountGuard» som tilbys kandidater til valg. Dette er en kombinasjon av digitale verktøy, informasjon og support for å sikre kandidatene mot angrep fra trusselaktører. Programmet i eksempelet er ikke iverksatt i Norge i dag (https://www.microsoftaccountguard.com/en-gb/).

Vurdering: Høy sårbarhet

Konsekvenser for krav til valgprosessen:				
Fri deltagelse	*Opplyst og informert*	*Korrekt*	*Gjennomføres som planlagt*	*Tillit*
Angrep på kandidater kan brukes både til påvirkning, diskreditering, utpressing osv.	Informasjon om politiske prosesser og kandidater kan brukes til målretting av budskap, falske nyheter og påvirkning av opinion			Kjennskap til at trusselaktører har tilgang til og kan ha påvirket kandidater og partier vil kunne ha svært negativ effekt på tilliten i befolkningen
Stor konsekvens	Stor konsekvens	Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Stor konsekvens

Kunnskapsstyrke	
Både metoder og teknologi er godt kjent av faginstanser, men ikke nødvendigvis blant befolkningen og de politisk aktive generelt	Høy

Overførbarhet	
Kan treffe alle steder og nivåer	Høy

Endringshastighet	
Utvikling spesielt innen både digitale «våpen» og mottiltak	Høy

Oppsummering	
Samlet vurdering – Potensialet for påvirkning er stort fra tunge aktører og mot sentrale aktører som beslutter retning og valg. Viktig for tillit til demokratiske prosesser	*Styrbarhet* – Vanskelig å regulere bort, men mange mulige tiltak innen beskyttelse og kunnskap
Høy	Middels

Aktuelle tiltak

- Videreføre og videreutvikle informasjon og veiledning til kandidater, partier og borgere
- Forskning, utvikling og implementering av teknologiske beskyttelsestiltak
- Offentlig – privat samarbeid der det offentlige engasjerer seg aktivt for å stimulere og påvirke de store teknologiaktørene med tanke på bidrag og utvikling – og retningen på denne

4. Diskreditering av politikere

Hendelse/fenomen: Diskreditering av politikere

Beskrivelse

En bevisst diskreditering av politikere kan være rettet mot enkeltpolitikere og spesifikke partier, og slik ha en direkte påvirkning på hvem som får mulighet til å delta i det politiske arbeidet. Diskreditering kan ofte medføre at en politiker mister verv og innflytelse over lang tid – og/eller for godt; og dermed potensielt forskyve balansen i det politiske landskapet. Diskreditering av spesielt profilerte politikere mer generelt kan også bidra til å svekke tilliten til systemet og demokratiet (det er ingen vits i å stemme, politikere er ikke til å tro på, det er bare rot osv.).

Svertekampanjer eller såkalte «drittpakker» har blitt kjente begreper i det politiske medielandskapet. Vanligvis forstås med dette at det spres informasjon mer eller mindre koordinert i flere ulike kanaler, med det formål å påvirke omdømmet til aktuell politiker, organisasjon eller parti negativt. Karakteristisk er at informasjonen har sannhetselementer i seg – men ofte er tatt ut av sammenheng – eller bare viser deler av sannheten. Informasjonen er gjerne på områder/felter der aktuell politiker må gå ut for å tilbakevise denne eller forsvare seg. I veldig mange tilfeller ender diskrediteringen med at politikerne «fjernes» fra det politiske landskapet da det de har gjort, eller håndteringen av situasjonen, ikke anses som forenelig med rollen.

Det har blitt lettere de siste årene å etablere «drittpakker», i og med at informasjon om den enkelte er mer tilgjengelig nå enn før. For eksempel kan en kartlegge hver enkelt person langt tilbake i tid på sosiale medier. Det er også lettere å spre informasjon i dag enn tidligere. Hacking og andre måter å ulovlig innhente informasjon fra kandidater i valg, politiske partier o.l., har vært omtalt som verktøy og grunnlag for svertekampanjer, blant annet i det amerikanske valget i 2016. Totalt sett er derfor dette en betydelig større trussel enn før. Samtidig gir sosiale medier også muligheter for motstemmer, dvs. å hevde at det er snakk om svertekampanje. Totalt sett har vi altså en endret situasjon, men det er mer usikkert hvilken effekt den nye situasjonen har.

Media er en viktig samfunnsaktør som har som oppgave å «overvåke» makten. Dagens endrede kommunikasjonssituasjon der informasjon spres svært raskt i mange ulike kanaler; har satt media under et stadig sterkere press om å levere nyheter fort og først. Dette er utfordrende også med tanke på tid til å sjekke bakgrunn og kvalitet på informasjon og nyheter som videreformidles og fremlegges.

Det faktum at mye informasjon og nyheter også oppstår og kommuniseres i medier som ikke er underlagt en redaktør; gir også en større mulighet for trusselaktører som kan ha et ønske om å gjennomføre svertekampanjer enten for å forskyve makt – eller svekke tillit til styresettet i Norge.

En effekt av ovennevnte kan også være at politikere kvier seg for å uttale seg om særlig kontroversielle saker, for å unngå å «plante» muligheten for en fremtidig svertekampanje.

Trusler/virkemidler

Det er kjent at enkelte statlige aktører og også «hatgrupper» ønsker å svekke tilliten til system og politikere i såkalte vestlige stater. Dette inkluderer også målrettede angrep på enkeltpolitikere eller grupper av politikere som kvinner og innvandrere. I PSTs trusselvurdering 2019 beskrives at i enkelte vestlige land har utenlandske etterretningstjenester jobbet systematisk og langsiktig for å svekke innbyggernes tillit til sine egne demokratiske institusjoner og prosesser. Flere steder har etterretningstjenester vært involvert i å spre desinformasjon, initiere svertekampanjer gjennom sosiale medier, og i å spre rykter eller halvsannheter. Man ser at påvirkningsaktiviteten også kan rettes mot konkrete virksomheter eller personer for å påvirke utfallet av enkeltsaker. Også trusselen om å diskreditere, kan sette enkeltpolitikere og organisasjoner under press – og kan tenkes benyttet for å oppnå effekt på beslutninger og i viktige saker. I tillegg innebærer endringen fra papir til digitale medier at publiseringstakten øker, og at krav til vurderinger er under tidspress.

Dagens digitale mediestruktur åpner også for at svertekampanjer i praksis kan startes av «hvem som helst». Informasjon om enkeltpersoner og organisasjoner er lett tilgjengelig – ofte flere tiår tilbake i tid – og kan enkelt redigere og spres effektivt i flere kanaler. Redaktørstyrte medier kan også potensielt bli et verktøy for trusselaktører – gjennom det sterke trykket for å publisere først. Slik sett trengs det ingen statlig eller annen tung aktør for å benytte seg av diskreditering – spesielt for å påvirke prosesser, maktfordeling og beslutninger i lokale saker. Kombinasjonen med teknologisk mulighet

for å hente ut og/eller forfalske signaturer, uttalelser, bilder og også videoer, gjør diskreditering til et potent verktøy for mange aktører. På noen digitale arenaer er det vanskelig å spore hvor informasjon kommer fra, og risikoen for trusselaktøren som ønsker å diskreditere noen, er lav.

Vurdering: Høy trussel

Barrierer og sårbarheter

Det norske samfunnet er preget av høy tillit til politikere og til system – og oppfattes langt på veg som veldig «gjennomsiktig». Dette kan fungere som en barriere mot mange av metodene som beskrives over.

Imidlertid øker sårbarheten også i det norske samfunnet, ved at eksempelvis «svertekampanjer» er lettere å iverksette enn tidligere. Trender med fokus på «sensasjonelle nyheter», krav om å ta ansvar for handlinger ved å måtte forlate verv osv. – gjør også det politiske systemet sårbart for aktører som vil forskyve makt og svekke tilliten. Samtidig gir sosiale medier også muligheter for motstemmer, dvs. å hevde at det er snakk om svertekampanje.

Det foregår i dag mange både offentlige og private initiativer – herunder utvikling av teknologi – for å beskytte sin egen informasjon, og avdekke bruk av «uredelige midle» og usannheter.

Vurdering: Middels sårbarhet

Konsekvenser for krav til valgprosessen:

Fri deltagelse	*Opplyst og informert*	*Korrekt*	*Gjennomføres som planlagt*	*Tillit*
Sverting av enkeltpersoner og/eller organisasjoner kan påvirke reell deltakelsesmulighet	I den grad usannheter benyttes vil det påvirke hvorvidt informasjonen velgere får er riktig.			Innbyggerne kan miste tillit til en viktig eller meningsbærende politiker/organisasjon. Det kan tenkes at mistilliten sprer seg til å gjelde politikere generelt og at mangel på tillit til demokratiet kan være en sluttfølge.
Noe konsekvens	Noe konsekvens	Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Stor konsekvens

Kunnskapsstyrke

Endret situasjon med lett tilgang til både å finne informasjon, men også bekrefte og avkrefte den. Mye kunnskap om ulike fenomener, men usikker effekt på sikt.	Middels

Overførbarhet

Gjelder alle politikere	Høy

Endringshastighet

Rask utvikling	Høy

Oppsummering

Samlet vurdering– Kan få en betydelig påvirkning på politisk klima og landskap på sikt	*Styrbarhet* – Dette er et område som er vanskelig å regulere eller styre på annet vis
Middels	Lav

Aktuelle tiltak
• Videreføre arbeid med opplæring og støtte til politikere, partier og rekrutteringsgrunnlag for å beskytte egen informasjon og håndtere hendelser (herunder beskyttelse mot hacking og andre måter å stjele privat/hemmelig informasjon på) • Bygge robusthet i samfunnet/trene ifht pålitelige kilder osv. – herunder opplæring av barn • Opprettholde støtteordninger til redigerte medier

5. Netthets av politikere

Hendelse/fenomen: Netthets av politikere

Beskrivelse

Netthets og ytringsklimaet generelt på nett – oppleves av mange som et økende problem. Til forskjell fra temaet «diskreditering» vil netthets typisk forhindre politikere eller andre fra å delta i debatten fordi de selv ikke ønsker å ta belastningen det medfører – ikke fordi de mister eller ikke får lov til å ta en posisjon.

I en ny rapport fra Kommunenes Sentralforbund (KS) publisert i april 2019, (https://www.ks.no/contentassets/87402cb121fa4cf08a6bb0b466c03c43/FoU-hets-og-trusler.pdf) beskrives det at mer enn 4 av 10 av lokalpolitikere opplever hets eller trusler.

Rapporten sier videre at: «Blant de som har endret adferd sier nesten 6 av 10 at hendelsene har ført til begrenset talefrihet rundt politiske temaer (58 %) og at de har unnlatt å engasjere seg eller uttale seg i en spesifikk sak eller saksfelt (57 %). Litt over halvparten (52 %) har vurdert å slutte som politiker, mens 15 % har bestemt seg for å slutte. Omtrent 1 av 3 har også fått dårlig selvtillit som følge av hendelsene, samt har blitt bekymret for å være ute i offentlighet og for sikkerheten til de nærmeste. Rundt 1 av 10 har iverksatt ulike sikkerhetstiltak, både hjemme og på jobb, samtidig som de har endret daglige rutiner.»

Netthets handler ofte om negative ytringer og meninger – ikke nødvendigvis om forhold som er sanne eller usanne. Det beskrives stadig i media at ordbruken i det offentlige ordskiftet har hardnet til – og at grensene for det som er «innenfor» stadig blir skjøvet på. Den offentlige samtalen – med respekt for andres synspunkt – presses stadig, og oftere enn tidligere blir ytterliggående synspunkt bifalt.

Netthets kan bidra til at enkelte grupper avstår fra å delta i demokratiet og i valg.

Trusler/virkemidler

Fra England og Frankrike er det beskrevet tilfeller der statlige aktører målrettet prøver å påvirke ved hjelp av netthets i form av personangrep, eksempelvis basert på seksuell legning. Ved å systematisk hetse og angripe spesifikke grupper, ofte gjennom såkalte «trollfabrikker», søkes det både å påvirke politikk i ønsket retning fra trusselaktørens side, og å øke polarisering og mistillit mot styresettet i vestlige stater og mellom aktørene som deltar i valg. På overordnet og nasjonalt plan vil gjerne polarisering og mistillit generelt være mer fremtredende; samtidig som at høy belastning på spesifikke grupper over tid kan endre det politiske landskapet også her. På lengre sikt kan et hardere debattklima og hets av politikere svekke deltakelse og rekruttering til demokratiske prosesser – og utfordre synet på godheten i det demokratiske og vestlige styresettet.

Ulike former for netthets kan i lokalpolitikken direkte påvirke sammensetning av politiske organer, og beslutninger i saker dersom enkeltpersoner og/eller grupper velger å ikke delta i de demokratiske prosessene som resultat. Her kan både enkeltaktører, politiske grupperinger og andre interessegrupper være trusselaktører som benytter dette verktøyet.

Vurdering: Høy trussel

Barrierer og sårbarheter

En økende bevissthet rundt debattklima, og fokus på regulering av kommentar- og debattfelter på nettmedier bidrar til å beskytte samfunnet og enkeltpersoner mot netthets. Samtidig er moderering av debatt et område som raskt vil kunne utfordre ytringsfrihet og være vanskelig å finne en riktig balanse for.

Barn og unge i dag læres i mye større grad opp i god bruk av nett, og i håndtering av mobbing og hetsing på nett, enn dagens voksengenerasjon. Dette gir større robusthet mot fenomenet netthets.

Mange vil imidlertid hevede at økende aksept for hardere språkbruk og debattklima, vil kunne gjøre samfunnet sårbart for at enkeltindivider og ulike grupperinger faller ut av politisk debatt og valg.

Vurdering: Middels sårbarhet

Konsekvenser for krav til valgprosessen:				
Fri deltagelse	*Opplyst og informert*	*Korrekt*	*Gjennomføres som planlagt*	*Tillit*
Det kreves at politikere må være svær robuste for å «står i det». Det kan redusere den frie deltakelsen				Redusert respekt for debatt og kanskje for politikere generelt, kan på sikt utfordre tilliten til system og demokratiet
Noe konsekvens	Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Noe konsekvens

Kunnskapsstyrke	
Kunnskapen om fenomenet er høy, og etter hvert om effektene også (ref. rapport fra KS over)	Høy

Overførbarhet	
Treffer på alle «arenaer» og både lokalt og sentralt	Høy

Endringshastighet	
Bruken av sosiale medier og også debattklimaet oppleves av mange å endre seg raskt	Høy

Oppsummering	
Samlet vurdering – Fenomenet kan over tid betydelig påvirke hvem som deltar i den politiske debatten, og er derfor viktig å adressere	*Styrbarhet* – Svært begrenset mulighet til å regulere. Krever mer langsiktige tiltak.
Middels	Lav

Aktuelle tiltak

- Grunnleggende opplæring av barn og unge i «nettkutyme» - uten å redusere ytringsfriheten.
- Opplæring av rekrutteringsgrunnlaget til politiske partier og av kandidater til valg i håndtering av netthets – skape robusthet
- Forberedelse i partiene – planer for håndtering av netthets, og støtteordninger for den som rammes
- Moderering av kommentarfelt o.l.- men med klare spilleregler for å unngå konflikt med ytringsfriheten
- Rettslig forfølgelse av alvorlige tilfeller av netthets – også utfordrende med tanke på grensen mot ytringsfrihet

6. Falske nyheter påvirker valget

Hendelse/fenomen: Falske nyheter

Beskrivelse

På nettstedet « www.dubestemmer.no», som er et samarbeid mellom Utdanningsdirektoratet og Datatilsynet, beskrives falske nyheter slik: «Falske nyheter ser ofte ut som vanlige nyhetssaker og kan derfor være vanskelig å oppdage. Slike artikler kan inneholde både falsk og ekte informasjon. De som lager og sprer usannheter kan ha politiske motiver eller ha et ønske om å skape informasjonskaos, få oppmerksomhet eller oppnå økonomisk vinning eller svindel.»

Falske nyheter har alltid eksistert – men har fått et tiltagende fokus i den offentlige debatten, spesielt etter presidentvalget i USA i 2016. Diskusjoner rundt hvorvidt og hvor mye usannheter, misvisende og feilaktig informasjon og falske nyheter påvirker valg – og hvordan slik påvirkning kan stoppes/reduseres – er utbredt.

Å klare å skille fakta og falske nyheter fra meninger og ulike sider av en sak – er en stor utfordring med tanke på å fjerne dette fenomenet fra valgdebatten; uten at det blir stilt spørsmål vedrørende sensur og redusert ytringsfrihet. I mange tilfeller startes falske nyheter på plattformer for sosiale medier – og spres videre til mer tradisjonelle medier. Ofte legitimeres de ved å utnytte andre verktøy og fenomener som ekkokamre og avatarnettverk. Falske nyheter knyttet til politikere og valg kan fort få store konsekvenser. Informasjon, kommunikasjon og konsekvenser forløper raskt – og selv om en falsk nyhet avdekkes på et senere tidspunkt, kan skaden og konsekvensen ofte være irreversibel.

Fenomenet «deep fake» er også økende i digitale medier. I dette ligger at AI-teknologi benyttes til å produsere og/eller endre lyd og bilde slik at det presenteres noe som faktisk ikke har skjedd. Utviklingen i teknologi på dette feltet skaper en økende utfordring med å avsløre at slike lyd-/bildemontasjer faktisk er falske. «Deep fake» endrer synet vårt på hva som er et bevis. Nå kan heller ikke levende bilder anses som et «sannhetsvitne». Å produsere «deep fakes» krever ikke spesiell kunnskap, og kan i stor grad gjøres av hvem som helst.

Trusler/virkemidler

Ulike former for falske nyheter har blitt benyttet og benyttes av en rekke både legitime og illegitime aktører i tilknytning til valgprosesser. Blandingen av «ekte nyheter», «halvsannheter og falske nyheter; sammen med et økende antall digitale plattformer og verktøy, gir store muligheter – og lav risiko for aktører som vil benytte dette i påvirkningsøyemed.

Det har over de siste årene blitt avdekket at statlige aktører, herunder Russland, aktivt har brukt produksjon og spredning av falske nyheter for å påvirke politiske prosesser og valgprosesser i en rekke land (USA, Frankrike, Nederland, Tyskland og Storbritannia. Media referer i februar 2019 til meldinger om at USA blant annet sørget for å stenge nettilgangen for den den russiske trollfabrikken Internet Research Agency i St. Petersburg i forbindelse med mellomvalg i USA høsten 2018. Trollfabrikken skal også ha operert under det amerikanske valget i 2016.

Bruk av falske nyheter i aksjoner for å påvirke og polarisere er også avdekket brukt av ytterliggående grupper som venstreradikale og høyreradikale; og er enkelt tilgjengelig for de fleste aktører som ønsker å påvirke valgprosess, og ikke minst tillit til politikere og systemer. Det har blant annet dukket opp grupperinger der det går sport i å få falske nyheter til å «gå viralt» og spre seg lengst mulig. Bevisst eller ubevisst kan også slike aktiviteter bidra til å redusere hvor «opplyste» befolkningen er før valg – og til å polarisere det politiske landskapet.

Vurdering: Høy trussel

Barrierer og sårbarheter

Det norske samfunnet er lite, og relativt oversiktlig og transparent/åpent. Dette fungerer som en barriere ved at falske nyheter lettere kan avsløres enn i mange andre land. Norge er også et land med stor grad av politisk konsensus om utenrikspolitikk og grunnleggende verdier. Sammen med høy tillit til system og politikere gir dette mindre grobunn for polarisering og fronter ved bruk av falske nyheter.

Samtidig kan det hevdes at den store tilliten (av noen beskrevet som naiviteten) i samfunnet, også kan bidra til sårbarhet ved at mennesker i stor grad stoler på informasjon som gis, særlig dersom nyheten spres via anerkjente mediekanaler.

Befolkningen i Norge har høy teknologisk kompetanse, er høyt utdannet og opplyst, noe som gir grunnlag for å bruke hensiktsmessige verktøy, og også selv avdekke falske nyheter.

I forbindelse med at det skal gjennomføres valg til Parlamentet i EU våren 2019; har EU hatt et stort fokus på og vist bekymring for bruk av falske nyheter for å påvirke valget. Det har derfor blitt jobbet med en rekke initiativer og utvikling av ulike verktøy for å sikre valget i 2019. I dette ligger både informasjonskampanjer, reguleringer og utvikling av teknologi for å avdekke og merke falske nyheter – og i samarbeid med store private teknologiaktører.

Dette er tiltak som også vil komme Norge «til gode» og som kan benyttes for å styrke barrierene mot at valget i Norge skal påvirkes av falske nyheter også. Per i dag er det lite etablerte og formaliserte tiltak i Norge for å avdekke falske nyheter, noe som i seg selv gir en viss sårbarhet.

Vurdering: Middels sårbarhet

Konsekvenser for krav til valgprosessen:

Fri deltagelse	*Opplyst og informert*	*Korrekt*	*Gjennomføres som planlagt*	*Tillit*
Kan påvirke kandidater til ikke å stille eller at de mister posisjoner og muligheter	Forvirring og feilinformasjon av velgere			Velgerne mister tillit til informasjon og til kandidater. Vet ikke hva som er riktig lenger
Liten konsekvens	Svært stor konsekvens	Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Stor konsekvens

Kunnskapsstyrke

Fenomenet er etter hvert godt kjent og beskrevet	Høy

Overførbarhet

Kan forekomme både i digitale og analoge medier og kanaler, på ulike steder og nivåer.	Høy

Endringshastighet

Rask teknologisk utvikling og nye muligheter til forfalskning, parallelt med utvikling av mottiltak	Høy

Oppsummering

Samlet vurdering – Falske nyheter / manipulasjon påvirker både kunnskapen hos velgerne og tilliten til personer og politiske parti. Dette er alvorlig for demokratiet.	*Styrbarhet* –– Vanskelig å kontrollere da fenomenet forekommer i veldig mange ulike former og medier
Høy	Lav

Aktuelle tiltak

- Støtte og utvikle teknologiske tiltak for å avsløre og merke falske nyheter
  - Avdekking av manipulerte bilder, lyd og film
  - Identifisering og stenging av falske profiler og nettverk
  - Identifisering og merking av pålitelige og ikke-pålitelige kilder til informasjon (direkte på nett)
- Reguleringer for å kunne straffeforfølge spredning av falsk informasjon (men problematisk å skille bevisst/ubevisst og grad av «falskhet» uten å angripe ytringsfriheten)
- Opplæring av kandidater, media og befolkning for å avdekke falske nyheter – spesielt barn/unge
- Støtte til å etablere og drive uavhengige faktasjekkertiltak som www.faktasjekk.no
- Kombinere manuelle prosesser/kompetanse og teknologiske tiltak for å kvalitetssikre nyheter og informasjon
- Informere om avdekkede falske nyheter og gi generell folkeopplysning
- Pressestøtte for å sikre «seriøse» medier og god informasjon

7. Klikkfarmer, falske følgere og avatarnettverk

Hendelse/fenomen: Klikkfarmer, falske følgere og avatarnettverk

Beskrivelse

En voksende industri gjennom flere år har vært muligheten for å, i digitale kanaler, påvirke menneskers oppfatning av hva som er populært, vanlige/riktige meninger og «trendy». Dette gjøres gjennom at både falske profiler (profiler for ikke-eksisterende brukere) og faktiske profiler, benyttes til å følge, like og mislike firmaer, nettsteder, innlegg og personer.

Den faktiske «klikkingen» kan utføres både av algoritmer som autogenererer f.eks. likes; og av arbeidere ansatt i såkalte «klikkfarmer» der de betales for å klikke på spesifikke nettsteder, innlegg osv. Disse arbeiderne kan også ha opprettet og administrerer et stort antall falske profiler. Slik aktivitet har gitt grobunn for business i spesielt fattigere land med lave personellkostnader.

Bruk av falske profiler er brudd på «terms of services» på steder som for eksempel hos Facebook. Falske klikk er ikke regulert, dvs. at en kan reklamere for denne tjenesten på nettsider som Finn.no.

Kjøp av falske klikk og falske følgere brukes i dag av flere seriøse nettsteder. Dermed blir falske klikk et middel i «vanlig» påvirkningsarbeid.

Et økende fenomen har også vært store såkalte «avatarnettverk» som er nettverk av falske profiler (eksisterer kun på nett) som kan benyttes til massiv påvirkning på saker og områder. Slike avatarer kontrolleres av en påvirkningsoperatør. Nettverkene er svært avanserte og har stor grad av sikkerhet innebygget i seg. F.eks. vil systemet beskytte operatøren mot å bruke IP adresser utenfor den geografiske regionen den aktuelle avataren skal befinne seg i, eller mot å legge ut informasjon som er på et annet språk enn det avataren er oppført med. I motsetning til enklere mer tradisjonelle falske profiler blir dermed disse avatarnettverkene både et mye kraftigere verktøy i påvirkningsøyemed, og dessuten mye vanskeligere å avsløre og eventuelt fjerne.

Trusler/virkemidler

Som for bruk av falske nyheter er også denne typen virkemidler kjent brukt av statlige aktører, som Russland.

Virkemidlene er spesielt egnet til å polarisere det politiske landskapet, ved å legitimere radikale synspunkter – og gi inntrykk av at «smale strømninger» er mer vanlige folkelige oppfatninger. De kan også gi «ekkokammereffekt» ved at personer med radikale synspunkter får bekreftelse i stedet for motstand når synet fremmes.

Dette kan ha en direkte effekt på velgere som «sitter på gjerdet», og får bekreftet synspunkter de ellers ville være usikre på. Effekten blir litt som produktomtaler som påvirker oss til å velge en jakke fremfor en annen fordi så mange andre har positive erfaringer. Motsatt kan det også mobilisere velgere med motsatt standpunkt til å faktisk avlegge sin stemme for å motvirke det som fremstår som «main stream».

Vurdering: Høy trussel

Barrierer og sårbarheter

Enkle falske profiler, klikkfarmer osv. har blitt enklere å avdekke med teknologi. Samtidig utvikles stadig mer avanserte former for Avatarnettverk som er svært vanskelige å avsløre.

Gode falske profiler og avatarnettverk har blitt en populær handelsvare fordi potensiell verdi av bruk i markedet er så stor. De samme produktene kan benyttes også i forbindelse med valg og demokratiske prosesser generelt.

Vurdering: Middels sårbarhet

Konsekvenser for krav til valgprosessen:				
Fri deltagelse	*Opplyst og informert*	*Korrekt*	*Gjennomføres som planlagt*	*Tillit*
	Falske nyheter og ekstreme meninger får falsk kredibilitet når tilsynelatende mange støtter meningene			Er i seg selv egnet til å støtte opp under mistillit til styresett, politikere og demokrati. Legitimerer kritikk
Ingen/nesten ingen konsekvens	Stor konsekvens	Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Stor konsekvens

Kunnskapsstyrke	
Har god forståelse om fenomenet men lite bevissthet om omfanget.	Middels

Overførbarhet	
Kan i begrenset omfang treffe overalt, men for mer avanserte former trolig ikke «main stream».	Middels

Endringshastighet	
Rask endring i teknologi og muligheter (og tiltak)	Høy

Oppsummering	
Samlet vurdering – Rask utvikling kan gi nye og flere muligheter for påvirkning som må følges opp i fremtiden	*Styrbarhet* – Kan til en viss grad reguleres med straffelovgivning, men vanskelig å holde kontroll på.
Middels	Middels

Aktuelle tiltak

- Forskning, for å forstå teknologi og utvikle tiltak
- Offentlig-privat samarbeid for å utvikle gode mottiltak (falske profiler lar seg ofte avsløre av leverandørene ved å utvikle algoritmer og søk som avslører falske profiler. Dette er betydelig vanskeligere med «avatarnettverk» ettersom disse profilene blir forvaltet med mye større nøyaktighet og forsiktighet av trussel aktørene. (Referanse: https://2f8dep2znrkt2udzwp1pbyxd-wpengine.netdna-ssl.com/wp-content/uploads/2017/01/BRICProposalBaselineDocument27a-Oct-16.pdf)
- Kreve større verifikasjon og attribusjon av individer som skal kunngjøre meninger på Internett. For eksempel; NRK har i mange tilfeller i artikler publisert på nettsidene krevd at man må svare på en enkel spørreundersøkelse som beviser man har lest artikkelen, før man får lov å kommentere på den.
- Regulering som fjerner muligheten for å handle med «falske klikk» lovlig

8. Det skapes tvil om riktighet av valgresultatet

Hendelse/fenomen: Det skapes tvil om riktighet av valgresultatet

Beskrivelse

Grupper eller enkeltpersoner kan iverksette kampanjer for å så tvil om resultatet etter et valg, og indikere at dette er manipulert eller feil. Dette kan ha en direkte politisk hensikt, f.eks. for å fremme eget syn eller skape tvil om andres interesser og intensjoner. Imidlertid er dette ikke minst egnet til å svekke tilliten til myndigheter, systemer og demokratiske prosesser, og etablere mistro.

I Skandinavia har tilliten til myndigheter og systemer tradisjonelt vært høy, og vi tar som en selvfølge at valgresultatet er korrekt. Imidlertid viser siste valg i Sverige at det ble sådd tvil om også dette. I en rapport som tar for seg påvirkningskampanjer under valget i Sverige i 2018 (https://www.isdglobal.org/isd-publications/smearing-sweden-international-influence-campaigns-in-the-2018-swedish-election/), beskrives det hvordan anklager om valgfusk ble fremsatt av både svenske og internasjonale grupperinger fra ytterliggående høyre i perioden etter valget. Rapporten beskriver også hvordan det i stort omfang ble gjort forberedelser fra de samme grupperingene i forkant av valget, for at de skulle kunne «underbygge» anklager om at valget var rigget slik, at Sverigedemokraterna (SD) ikke skulle nå opp. Eksempler er at det ble satt opp egne nettsider der sympatisører ble oppfordret til å samle inn og rapportere hendelser og elementer som kunne være valgfusk. Denne samlingen av historier og påstander ble spredd i stort omfang etter valget for å underbygge teoriene om valgfusk. Nettforbindelsen falt også ned en periode under opptellingen av stemmer. Da nettet kom opp igjen var «stillingen» mellom partiene betydelig endret. Dette ble raskt utpekt som en del av et opplegg for å endre/manipulere stemmetallene, og mistankene spredde seg raskt i ulike medier.

Flere av virkemidlene som adresseres i andre vurderinger her, kan altså benyttes for å oppnå effekten med å så tvil om resultatet. Selv om eksempelvis Valgdirektoratet går ut i etterkant og avkrefter slike rykter, kan det ha oppstått en mistanke som kan skape usikkerhet som vedvarer over tid.

Trusler/virkemidler

Både statlige aktører og enkelte politiske og andre -interessegrupperinger vil kunne ha interesse av å så tvil om valgresultatet. Først og fremst vil nok motivasjonen ligge i å vise evne (skape uro, frykt og polarisering), og å skape mistillit til myndighetene og deres evne til å sikre prosessene rundt valg.

Som i eksempelet beskrevet fra det svenske valget i 2018, kan kampanjer av denne typen benyttes for å bygge opp under påstander om at enkelte politiske retninger motarbeides – og slik skape økt splittelse og polarisering i samfunnet. Samtidig kan det på sikt bidra til at de politiske retningene som fremstilles som «dårlig behandlet» sanker flere stemmer ved neste valg som en protest mot dette.

De skandinaviske landene, som både Sverige og Norge, regnes som «fyrtårn» med tanke på demokratisk og vestlig styreform. Slike land vil derfor kunne være interessante mål for internasjonale og statlige aktører som ønsker å vise at denne styreformen ikke fungerer, og at landene ikke har kontroll på valgprosessene sine.

Også trusselaktører som ikke nødvendigvis har en politisk intensjon kan tenkes å ha interesser av det oppstår tvil om valgresultatet, kun for å demonstrere at de klarer det (noe som kan gi status i enkelte miljøer).

Vurdering: Høy trussel

Barrierer og sårbarheter

En trusselaktør kan bruke denne angrepsmåten mot det norske demokratiet for å lamme norske beslutningstakere. Ved å så tvil om valgresultatet kan en avgjørelse om valgutfallet la vente på seg. I denne perioden vil riktignok sittende regjering fortsette inntil Stortinget klarer å enes om det nye parlamentariske grunnlaget, men den sittende regjerings oppmerksomhet vil med stor sannsynlighet være påvirket av prosessen. I ytterste konsekvens kan sittende regjering bli handlingslammet.

Sammenlignet med Sverige, kan Norge være mer sårbare for et slikt anslag, da Norge i mindre grad har fokusert på barrierer og forebyggende tiltak mot dette enn Sverige. I Sverige er lovverket tilrettelagt for å bekjempe slike angrep på demokratiet på en mer inngripende måte enn i Norge. I tillegg er det en større informasjons-/medierobusthet i Sverige der man tradisjonelt har sterke apparater for å forebygge mot et slikt anslag. Det har i Sverige blant annet blitt vektlagt å

gjennomføre en mengde forebyggende informasjonstiltak i forkant av valg, rettet mot grupper som media, skoler, ungdommer, eldre og innvandrergrupper; noe som på nasjonalt plan ikke har vært fremtredende i Norge. Den svenske samfunnsdebatten rundt påvirkninger også i tilknytning til valg, har også vært mer omfattende i Norge de siste årene. Dette er med på å øke robustheten i det svenske samfunnet.

Samtidig er den høye tilliten til myndigheter og prosesser i seg selv en barriere mot at de norske borgerne lett tror på slike påstander i Norge. Dersom tilliten reduseres vil sårbarheten for denne typen angrep øke betydelig. Jyllands-Posten rapporterer i mai 2019 fra en undersøkelse som viser at andelen dansker som har stor tillit til politikerne, har falt fra 70 prosent i 2007, og til bare 29 % i 2019 (https://jyllands-posten.dk/politik/ECE11348846/tilliden-til-politikere-naar-historisk-lavpunkt-pia-kjaersgaard-har-tre-bud-paa-loesninger/

Vurdering: Middels sårbarhet

Konsekvenser for krav til valgprosessen:

Fri deltagelse	*Opplyst og informert*	*Korrekt*	*Gjennomføres som planlagt*	*Tillit*
				Selv om «valgjuks» avkreftes vil tilliten kunne være svekket og mer «skjør». Mistanken sås.
Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Noe konsekvens

Kunnskapsstyrke

Kjente fenomener, uten at de nødvendigvis er håndtert i stor grad	Høy

Overførbarhet

Kan forekomme «over alt»	Høy

Endringshastighet

Fenomenet i seg selv endres i liten grad, men bruk og omfang kan endres	Lav

Oppsummering

Samlet vurdering – Åpenhet, sikring av prosesser og høy grad av tillit til systemer og prosesser medfører at dette normalt vil ha relativt liten effekt i dag.	*Styrbarhet* – Det kan ikke hindres at juks blir påstått, men det kan sikres mot juks og svares godt ut
Lav	Middels

Aktuelle tiltak

- Fra myndighetssiden planlegge godt for scenarioer som kan komme. Fokus på informasjon og kunnskapsbygging i samfunnet.
  - Informere om at beskyldninger kan komme og øke kunnskap og bevissthet i ulike grupperinger
  - Forsikre om rutiner og sikkerhet før valg, gjennom transparent kommunikasjon
  - Ha klart materiale som kan publiseres dersom noen problematiserer muligheten for å hacke skannere.
  - Være raskt ute med gode forklaringer og forklaringer dersom beskyldninger kommer

9. Trusler fører til at folk ikke våger å avlegge stemme

Hendelse/fenomen: Trusler fører til at folk ikke tør stemme

Beskrivelse

Trusselaktører kan fremme trusler som fører til at velgere ikke våger å møte opp i valglokalet, eksempelvis om at en bombe vil gå av. Bombetrusler kan «ringes» inn.

Sosiale medier kan være godt egnet for å oppnå et slikt mål. De kan brukes anonymt for å skape frykt og medføre uro og krisetilstander. En slik effekt kan også eskaleres ved at «copy cats» gjentar for å oppnå oppmerksomhet.

Trusler/virkemidler

Slike trusler kan være målrettede for å redusere valgdeltakelse i spesifikke områder, kommuner eller fylker. Da vil et valg kunne dreies i en politisk retning basert på kunnskap om hvilket flertall som normalt ligger hvor.

Effekten kan også være fokusert mer generelt på å skape uro og frykt, være mer uspesifikk og gi utslag generelt på valgdeltakelse.

Denne typen virkemidler er per i dag ikke kjent brukt i Norge eller land vi vanligvis sammenligner oss med.

Vurdering: Middels trussel

Barrierer og sårbarheter

Denne typen virkemiddel er ikke godt kjent i Norge – men er heller ikke så lett å sikre seg mot.

På mindre steder med få valglokaler, vil en slik hendelse kunne redusere valgdeltakelsen betydelig, og slik påvirke valget. Siden det i dag ikke finnes noen beredskapshjemmel som gir mulighet for å utsette valget i kort tid ved en slik type hendelse, vil valget måtte gjennomføres, eventuelt underkjennes for deretter å gjennomføre nytt valg.

På større steder vil det normalt være relativt enkelt å kunne avlegge stemme i et annet lokale dersom dette er utsatt for trusler eller hendelser. En trussel vil derfor måtte dekke betydelige områder for å sikre effekt.

Uspesifikke trusler mot mange valglokaler vil kunne ha en effekt som er vanskelig å måle, og det vil derfor være en utfordring å vurdere om valget skal godkjennes eller måtte gjennomføres på nytt (som beskrevet for mindre steder over).

Vurdering: Middels sårbarhet

Konsekvenser for krav til valgprosessen:

Fri deltagelse	*Opplyst og informert*	*Korrekt*	*Gjennomføres som planlagt*	*Tillit*
Å ikke tørre å komme til valglokalet vil i stor grad forhindre en fri valgdeltakelse for velgerne			Vil dersom stort omfang kunne påvirke muligheten til å gjennomføre valget som forutsatt	
Stor konsekvens	Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Liten konsekvens	Ingen/nesten ingen konsekvens

Kunnskapsstyrke

Vi forstår fenomenene	Høy

Overførbarhet

Kan skje i alle valglokaler i alle valg	Høy

Endringshastighet	
Ingen stor «utvikling» på området	Lav

Oppsummering	
Samlet vurdering – Lite kjent, men kan medføre betydelig frykt	*Styrbarhet* – vanskelig å sikre seg mot eller regulere på noe vis
Middels	Lav

Aktuelle tiltak

- Etablere gode beredskapsplaner, med spesielt fokus på informasjon og kommunikasjon
- Vurdere regulering som gir økt fleksibilitet med tanke på å flytte tid og sted for valggjennomføring (beredskapshjemmel)
- Vurdere valgordninger som ikke krever oppmøte i spesifikke lokaler

10. Mikromålretting av informasjon

Hendelse/fenomen: Mikromålretting av informasjon

Beskrivelse

I dagens digitale samfunn er det en økende forretning knyttet til innhenting, analyse og salg av informasjon om brukerne. Algoritmer, maskinlæring og kunstig intelligens benyttes til innsamling av data og analyse av informasjon med en effektivitet vi ikke tidligere har kunne komme i nærheten av. Resultatet blir tilgang til svært detaljert informasjon om nettbrukerne, som i dag langt på vei er de aller fleste av oss. I sin enkleste form kan det dreie seg om isolerte opplysninger om interesser og preferanser for produkter. Ved bruk av algoritmer og kunstig intelligens har det imidlertid vist seg i nyere tid at det er mulig å analysere og identifisere, med forbløffende treffsikkerhet, preferanser og syn politisk og religiøst, etnisk tilhørighet, seksuell legning og andre dype personlighetstrekk hos brukerne. Resultatet blir tilgang til svært sensitiv informasjon som kan benyttes både til helt uskyldige formål og til mer diskutable formål – bevisst eller ubevisst. Grovt sett kan eksempelvis 3 overordnede fenomener betraktes:

Målretting av salg – er den mest kjente og «tidligste» bruken av informasjon som ble og blir samlet inn via nettbruk. I enkel og mer avansert form analysers vi som brukere slik at markedsføring både på og utenfor nettet kan målrettes mot våre interesser. Denne bruken av informasjon er vel etablert, og for mange lett synlig gjennom typen annonser og produkter som dukker opp ved nettbruk. Dette fenomenet har i seg begrenset interesse og relevans når det gjelder sikkerheten ved valg

Målretting av informasjon (ekkokammer) - I store digitale medier som facebook, google, yahoo – men også i digitale aviser og nyhetsinnsamlere, er den feeden den enkelte mottar i stor grad styrt av algoritmer som sorterer og leter frem hva som er mest «relevant» for leseren. Relevans er ikke basert på hva den enkelte bestemmer den vil lese – men hva algoritmen analyserer at du vil ha basert på hva du har lest eller søkt på før.

Sett i valgsammenheng vil det lett kunne oppstå «ekkokamre», der velgere ikke får balansert informasjon før de foretar sine valg, men bare mer informasjon som styrker forutinntatte meninger og oppfatninger. Dette er en dreining fra en situasjon der velgere har forholdt seg hovedsakelig til redaktørstyrte medier som i større og mindre grad har underlagt seg journalistiske prinsipper som «vær varsom-plakaten».

Den amerikanske forfatteren Eli Pariser har blant annet skrevet boken «The filter bubble» (2011) og gitt en rekke forelesninger som beskriver og diskuterer dette fenomenet – og konsekvensen det har og kan ha i samfunnet og på demokratiet. Han er opptatt av at vi blir mindre «opplyste» og i større grad operer i vår egen «filterboble» der vi ikke blir motsagt eller våre syn utfordres av andre syn. Vi får bare bekreftet oppfatninger vi allerede har. Han understreker også at dette er mye av de samme diskusjonene som for 100 år siden presset frem nettopp de journalistiske prinsippene som de fleste medier tiltrer i dag. Se f.eks. artikkel hos Telenor: https://link.no/ekkokammer/

Dette fenomenet er i utgangspunktet ikke styrt av en aktør som vil skyve opinionen i en spesifikk retning, men kan likevel ha en rekke mer og mindre utilsiktede og kanskje også uønskede effekter som beskrevet.

Mikromålretting – De sensitive analysene og informasjonen om brukerne fra nettalgoritmer har imidlertid også et stort potensial for å kunne utnyttes målbevisst av aktører med ulike intensjoner. Ved å bruke den mest detaljerte og sensitive informasjonen som genereres om brukere av nettet, kan informasjon og budskap mikromålrettes mot hver enkelt bruker for å påvirke i den retningen aktøren ønsker. Slik påvirkning kan være direkte mot beslutninger og valg av politisk retning, men også benyttes mer generelt for å polarisere, skape uro, forsterke fordommer og etablere mistillit (og gjerne i kombinasjon med andre fenomener som fake news m.fl.). Saker som Cambridge Analytica og bruk av sensitiv brukerinformasjon i den amerikanske valgkampen i 2016 har aktualisert temaet.
https://www.nrk.no/nyheter/cambridge-analytica-1.13973142

Trusler/virkemidler

Ekkokammereffekten som beskrevet over, har i seg selv et potensial for å påvirke hvorvidt borgerne faktisk tar «opplyste» valg når det skal stemmes; også uten at aktører bruker effekten bevisst for å påvirke velgerne.

Når det gjelder mikromålretting og bruk av sensitive opplysninger om befolkingen, er det et potensielt verktøy for en rekke aktører fra fremmede makter til nasjonale politiske partier og enkeltpersoner. I saken knyttet til Cambridge Analytica (CA), benyttet CA informasjon hentet inn via Facebook til å utvikle programvare for å påvirke velgere, og tilbød dette på markedet. Flere politiske aktører i og utenfor USA har blitt knyttet til bruk av tjenesten.

https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html? Det har blitt beskrevet en mulig bruk der hvilket budskap som formidles – og på hvilken måte, tilpasses mottakergruppene for å oppnå polarisering og politisk påvirkning.

Datatilsynet i Norge uttrykte nylig bekymring formuligheten for bruk av mikromålretting av informasjon i forbindelse med valgkamp – og iverksetter undersøkelser i forbindelse med årets valgkamp. De ser som en stor utfordring at det er liten åpenhet både om hva slags informasjon som samles inn, hvordan den analyseres og hvordan den benyttes, og peker på utfordringer knyttet både til personvern, manipulasjon og eksklusjon. https://www.nrk.no/hordaland/mangler-regler-for-politisk-nettreklame-1.14474786#fact-1-14478415

Påvirkning av velgere har alltid vært en kjerne i det å drive valgkamp, men bruken av digitale analyser og plattformer gjør det vanskeligere for velgeren å skjønne hva og hvordan det skjer.

Den stadig mer utstrakte bruken av valgomater i norske medier kan potensielt utnyttes av ulike aktører. Det ligger en stor mulighet i det å påvirke hvordan valgomaten plasserer brukeren med tanke på partitilhørighet, da mange velgere faktisk stemmer på det partiet valgomaten konkluderer med. I tillegg kan informasjon fra valgomatene inneholde svært mye informasjon om bruker, synspunkter og med det etter hvert indikasjoner på valgresultater (og den enkeltes preferanser).

Vurdering: Høy trussel

Barrierer og sårbarheter

Når informasjon, nyheter, budskap og påstander er tilpasset meninger og oppfatninger vi allerede sitter med, blir terskelen for å tro og agere på det vi hører lavere. Psykologisk har vi lettere for å akseptere informasjon som støtter opp under det synet vi allerede har. Når informasjon målrettes (bevisst eller ubevisst) mot preferanser og «tilbøyeligheter» eller ting som berører oss spesielt – blir vi sårbare. Det at bruken, og ikke minst hvem som står bak målrettingen ikke er åpent tilgjengelig eller lett å forstå, gjør denne sårbarheten større i befolkningen.

Det at befolkningen i Norge er høyt utdannede og teknologisk langt fremme kan fungere som en barriere mot påvirkning og manipulasjon, men mangelen rundt forståelse av og åpenhet rundt at og hvordan manipulasjonen foregår svekker denne barrieren. Den store graden av digitalisering i samfunnet, der de aller fleste er aktive nettbrukere, gjør også at tilfanget av informasjon om den enkelte av oss er stort for en potensiell aktør som vil analyser og utnytte denne.

Vurdering: Høy sårbarhet

Konsekvenser for krav til valgprosessen:

Fri deltagelse	*Opplyst og informert*	*Korrekt*	*Gjennomføres som planlagt*	*Tillit*
Prinsipper rundt hemmelige valg utfordres ved at analyser definerer politisk tilhørighet	Opplever ikke en åpen og opplyst debatt. Kan få «sortert» informasjon			Ulike budskap, polarisering. Mulighet for kombinasjon med andre verktøy
Noe konsekvens	Stor konsekvens	Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Stor konsekvens

Kunnskapsstyrke

Området er fortsatt begrenset beskrevet og effektene ikke godt kjent	Lav

Overførbarhet

Kan forekomme globalt og lokalt	Høy

Endringshastighet

Teknologisk utvikling går raskt og er foreløpig lite styrt/regulert	Høy

Oppsummering

Samlet vurdering – Økende fokus og rask utvikling. Gir mulighet for stor påvirkning	*Styrbarhet* – Deler av fenomenet kan reguleres, men liten åpenhet gjør det utfordrende
Høy	Lav

Aktuelle tiltak

- Regulering og håndheving av krav knyttet til innhenting, analyse og bruk av informasjon
- Teknologisk tiltak for å hindre mikromålretting
- Krav til åpenhet rundt bruk av målretting etc. i valgkamp/politisk reklame osv. (tv-reklame er regulert, nettbruk i liten grad)
- Sikre bred informasjon i redaktørstyrte medier – journalistiske krav (motvekt, balanse) – eksempelvis gjennom subsidiering
- Forskning på bruk og effekt av mikromålretting
- Undersøke og styre bruk av valgomater og lignende kartleggingsverktøy

11. Subkulturer på nett – et sted for alle

Hendelse/fenomen: Subkulturer på nett – et sted for alle

Beskrivelse

Ved økende bruk av digitale plattformer for informasjon og kommunikasjon, har det oppstått en rekke mer eller mindre lukkede samfunn på nett der informasjon og meninger utveksles. Slike typer fora har alltid eksistert, men internett legger til rette for en stor oppblomstring, med lett tilgjengelig grupper og meningsfeller for alle. Mange kommuniserer og henter mye informasjon fra slike grupper på internett – der i mange tilfeller personer med de samme grunnleggende syn på sak eller område er samlet. Her vil det lett kunne oppstå «ekkokamre», der velgeren ikke får balansert informasjon før han foretar sine valg, men bare får mer informasjon som styrker forutinntatte meninger og oppfatninger.

I «Det norske akademis ordbok» defineres ekkokammer ved - det at informasjon, meninger blir gjentatt og forsterket innen en gruppe, et medium, uten diskusjon med dem som har andre synspunkter.

Utstrakt bruk av informasjonsinnhenting fra slike uregulerte grupper er en dreining fra en situasjon der velgere har forholdt seg hovedsakelig til redaktørstyrte medier som i større og mindre grad har underlagt seg journalistiske prinsipper som «vær varsom-plakaten».

Det at alle slags grupperinger finnes, gjør at også at individer med radikale syn og meninger raskt finner meningsfeller og slik «legitimerer» sin oppfatning av verden.

Trusler/virkemidler

Dersom store deler av informasjonen og nyheter enkelte forholder seg til hentes fra beskrevne interessegrupper, er det i seg selv en bekymring med tanke på balansert informasjon og informerte valg.

Dersom trusselaktører utnytter de samme plattformene til å plante informasjon, legge ut radikale og polariserende meninger og påstander, blir også samfunnseffekten større. Slike virkemidler er blant annet kjent å være en del av verktøykassen for enkelte statlige aktører.

Ved at nett og grupper er lett tilgjengelig og ikke krever tilstedeværelse fysisk, er dette også mulig å utnytte for aktører på alle nivåer for øvrig.

Reuters Institute utgir årlig sin «Digital News Report» som både kartlegger vaner og syn på nyheter, og analyserer effekten av endringer. Rapporten for 2018 (http://media.digitalnewsreport.org/wp-content/uploads/2018/06/digital-news-report-2018.pdf?x89475) viser blant annet en tendens til at mange – særlig unge – flytter sin nyhetsinnhenting og diskusjon av nyheter, fra store sosiale medieplattformer til mindre og mer lukkede og private sosiale medier, som Whats app og Snapchat ; der utsagn også i mindre grad utfordres. En av rapportens hovedforfattere Nic Newman uttrykker bekymring for denne nettopp tendensen, som han mener øker risikoen for også å spre falske nyheter. (https://www.aftenposten.no/kultur/i/jPJ8Wb/Medievaner-i-endring-Farre-bruker-Facebook-som-nyhetskilde)

Vurdering: Høy trussel

Barrierer og sårbarheter

Norge er et lite og oversiktlig samfunn med stor åpenhet, der de fleste i noen grad eksponeres for (og kjenner) de brede og redaktørstyrte mediene. Disse nyter også stor tillit i samfunnet. Det foregår betydelig offentlig debatt i disse og på åpne sosiale plattformer digitalt. Dette reduserer risikoen for at slike lukkede fora blir eneste kilde til informasjon, og at individer aldri hører innsigelser på påstander og diverse syn.

Samtidig er nordmenn i stor grad brukere av digitale plattformer og deltar i grupper og fora uavhengig av geografi. Slik sett har mange mulighet for å velge bort bredere medier som informasjonskilde.

Vurdering: Middels sårbarhet

Konsekvenser for krav til valgprosessen:				
Fri deltagelse	*Opplyst og informert*	*Korrekt*	*Gjennomføres som planlagt*	*Tillit*
	Objektiv informasjon og motargumenter når ikke velgerne			Gir eksempelvis grobunn og rom for å fokusere informasjon om at demokratiet ikke fungerer – uten at dette blir motsagt
Ingen/nesten ingen konsekvens	Liten konsekvens	Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Liten konsekvens

Kunnskapsstyrke	
Kjent fenomen, men ikke effektene av dagens omfang er mindre kjent	Middels

Overførbarhet	
Mest relevant i en nasjonale eller internasjonal kontekst	Middels

Endringshastighet	
Moderat utvikling	Middels

Oppsummering	
Samlet vurdering – Antas ikke å ha stor påvirkning på valg i Norge i dag	*Styrbarhet* – Vanskelig å regulere, men noe forebyggende tiltak kan gjennomføres
Lav	Lav

Aktuelle tiltak

- Forskning på effekten av denne typen «ekkokamre» og potensialet for misbruk av aktører som vil manipulere
- Sikre enkel tilgang til bred og kvalitetssikret informasjon – også fra staten
- Opplæringstiltak for unge – bruk av medier osv.
- Tiltak for å motarbeide «utenforskap», også på informasjons og mediesiden
- Støtteordninger for «brede» medier

12. Manipulert manntall

Hendelse/fenomen: Manipulert manntall

Beskrivelse

Manntallet ligger til grunn for hvem som får stemme i Norge – og overføres til valgadministrasjonssystemet (EVA) fra Skattedirektoratet.

En manipulering av manntallet kan gi «ikke-eksisterende» personer mulighet til å avgi stemmer som påvirker et valg. Manntallet kan tenkes manipulert enten ved at Skattedirektoratet hackes fra utsiden, eller ved at manntallet endres av noen med tilgang. Siden manntallet som legges i valgadministrasjonssystemet (EVA) periodisk overskrives av oppdatert manntall fra Skattedirektoratet, er det manipulering av grunndata i Skattedirektoratet som fremstår som mest hensiktsmessig for en trusselaktør. Det vil også være mulig å fjerne noen fra manntallet.

Man kan også se for seg at manntallet kan manipuleres under selve valggjennomføringen ved at f.eks. et virus introduseres i/til EVA, og at dette kan fjerne avkrysninger for avlagte stemmer slik at stemmegiveren kan møte opp og avlegge nye stemmer en rekke ganger.

Generelt vil personlig oppmøte med sjekk av identifikasjon være nødvendig for å avlegge stemme i Norge. Dette gjør det svært utfordrende, og ikke minst kapasitetskrevende å benytte flere manipulerte stemmer. Ved stemmegiving fra utlandet er det imidlertid mulig å sende poststemmer uten å identifisere seg ved personlig oppmøte.

Trusler/virkemidler

Manntallet er i utgangspunktet et attraktivt sted for manipulering med tanke på å påvirke valg. Det er ikke kjent at denne typen påvirkning har blitt forsøkt i Norge.

Med tanke på dagens systemer må det anses å være «overkommelig» å forfalske en identitet gjennom å manipulere folkeregisteret. En operasjon som skaper et stort antall stemmegivere, og å benytte disse til å avgi stemme, vil imidlertid kreve omfattende kapasitet hos trusselaktøren på grunn av kravet om å møte opp og identifisere seg for å avlegge stemme.

Selv ved bruk av falske velgere lokalisert i utlandet, vil det være krevende å sende et så stort antall brevstemmer at det gir nasjonale utslag.

Vurdering: Lav trussel

Barrierer og sårbarheter

På grunn av kravet om personlig oppmøte og identifisering ved stemmegiving innenlands, vil det være krevende både å få avlagt stemme flere ganger på samme identitet etter en eventuell manipulasjon av manntallet, og å benytte seg av mange falske velgeridentiteter for å kunne avlegge falske stemmer.

Norge er relativt lite og oversiktlig, og valgdistriktene likeså. Hvert valgdistrikt mottar i snitt svært få poststemmer fra utlandet, og vil reagere dersom antallet øker betydelig.

Det kan tenkes at et fåtall poststemmer kan endre en politisk sammensetning av styrende organer lokalt i mindre kommuner – og det er flere tilfeller av at et svært lavt antall stemmer er utslagsgivende også i større kommuner. For en trusselaktør som skal benytte «falske velgere» fra utlandet vil det imidlertid være knyttet betydelig usikkerhet til å manipulere et riktig antall, på riktig sted. Dette i tillegg til en arbeidskrevende prosess for å få avgitt stemmer.

På nasjonalt nivå vil det – med mindre man aksepterer svært stor usikkerhet for innsatsen, være svært vanskelig å gjøre utslag av betydning ved å benytte denne metoden i dag.

For en aktør som i større grad ønsker å påvirke tilliten til systemet kan det imidlertid være en mulighet å fjerne velgere fra manntallet. Et slikt tilfelle vil trolig ikke påvirke resultatet av et valg fordi manglende oppføring vil kunne avdekkes og rettes opp i og etter valggjennomføringen (velgeren får avlegges stemmen sin og feilen korrigeres i manntallet i ettertid), men vil kunne påvirke tilliten til manntall og valg negativt.

Det er imidlertid verdt å merke seg at omfattende digitalisering av folkeregisteret gir andre og kanskje større potensialer for å påvirke manntallet via cyberangrep. Samtidig gir det økt mulighet for kontroll og kvalitetssikring som kan redusere feil og manipulering. Imidlertid vil en samtidig digitalisering av valgprosessen, f.eks. der hjemmestemming innføres, kunne åpne sårbarheter og gi lettere adgang til å avgi falske stemmer.

Vurdering: Middels sårbarhet

Konsekvenser for krav til valgprosessen:

Fri deltagelse	*Opplyst og informert*	*Korrekt*	*Gjennomføres som planlagt*	*Tillit*
		Om manipulering av manntallet lykkes i kombinasjon med at en aktør får avlagt falske stemmer blir resultatet påvirket direkte (men trolig ikke mye)	Mangler ved manntallet (feil, utilgjengelig) kan forsinke valggjennomføringen betydelig	Om det ble avdekket manipulering av manntallet ville det påvirke tilliten til prosess og system betydelig
Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Noe konsekvens	Noe konsekvens	Svært stor konsekvens

Kunnskapsstyrke

Kjente mekanismer og prosesser	Høy

Overførbarhet

Sentralt manntall (kun ett)	Lav

Endringshastighet

Digitaliseringsprosjekter pågår	Middels

Oppsummering

Samlet vurdering – Antas å være lite sannsynlig sted for påvirkning i dag, men potensiale ved endring og digitalisering må følges opp	*Styrbarhet* – God mulighet for å sikre og regulere
Middels	Høy

Aktuelle tiltak

- Kvalitetssikringsrutiner i Skattedirektoratet – samt digital beskyttelse mot inntrenging på ulike måter
- Sikring av overføringsrutiner og oppdateringsrutiner/protokoll mot valgadministrasjonssystemet
- Kvalitetssikring/overvåking av brevstemmer
- Fokus på IKT-sikkerhet i digitaliseringsprosesser i Skattedirektoratet, og ikke minst ved eventuell videre digitalisering også av valgprosessen

13. Feil ved eller misbruk av IT infrastruktur, lokalt

Hendelse/fenomen: Feil ved eller misbruk av IT infrastruktur, lokalt

Beskrivelse

I Norge har vi (i 2019) 356 kommuner, både store og små. Den minste kommunen er Utsira med kun et par hundre innbyggere, mens kommuner som Oslo har flere hundre tusen innbyggere, nesten 700.000 per 1. Januar 2019. (Referanse: https://www.ssb.no/befolkning/statistikker/folkemengde/aar-per-1-januar).

Drift av IT systemer er en komplisert oppgave, som de aller fleste private foretak sliter med i dag. Grunnleggende rutiner som programvareoppdateringer, sikkerhetskopiering og segmentering i nettverk blir ofte glemt eller ikke gjort regelmessig nok. Det kan forventes at mye av det samme er gjeldende i norske kommuner.

I tillegg til systemet for skanning av stemmesedler (som omtales i egen hendelse/system), er også PCer som benyttes i kommunen eksponert for hacking, eller å være forhåndskonfigurert med virus fra leverandørene. En slik PC benyttes til å aksessere både EVA Scanning og EVA Admin, systemet for å håndtere skanning av stemmesedler og administrasjonssystemet for valgutførelse. Ved et slikt innbrudd vil da virus kunne endre på informasjonen som blir tilført til EVA Admin, på lik linje som en banktrojaner kan få nettleseren din til å endre på beløpene og kontonummer som blir lagt inn i nettbanken. Se også vurderinger rundt fenomenet «manipulasjon av manntallet».

Manglende sikring og overvåking av IT-utstyret som benyttes gir mulighet for at virus introduseres. Et kamuflert virus vil være vanskelig å oppdage og stoppe. Samtaler med kommunene viser at hvilket utstyr som benyttes, hvem det håndteres av og hvordan det oppbevares – varierer i ulike kommuner.

Trusler/virkemidler

Den største trusselen knyttet til feil med IT-utstyr som settes opp og opereres i den enkelte kommune, er trolig introduksjon av virus som kan virke lokalt, eller potensielt introduseres til valgadministrasjonssystemet sentralt via det lokale utstyret.

Med dagens valgordning og prosesser vil potensialet i virusintroduksjon først og fremst ligge i at utstyr og prosesser skades/ødelegges slik at gjennomføring av valget forsinkes/kompliseres/stoppes; eventuelt at viruset benyttes for å få tilgang til informasjon om og i systemet, eller hos personell som er koplet til systemet (kartlegging).

Statlige etterretningsorganisasjoner kan ha interesse av en slik mer langsiktig kartlegging av personer og informasjon; og kanskje også i tilfeller av å sabotere systemene for å redusere tilliten til prosessen. Samtidig kan mer enkeltindivider og grupperinger se det som en utfordring å klare å hacke og sabotere valgsystemer, og slik utgjøre en trussel.

Vurdering: Middels trussel

Barrierer og sårbarheter

Relativt detaljerte retningslinjer er utgitt fra Valgdirektoratet når det gjelder oppsett, håndtering og skjerming av utstyr som skal benyttes i valg. Det er ingen indikasjoner på at ikke kommunene ønsker å følge opp disse rutinene på best mulig måte men, som det beskrives innledningsvis, tilsier erfaring med varierende kompetanse og kapasitet at grad av implementering og oppfølging vil variere og skape sårbarheter. Retningslinjene er også nye for kommunene, og det må forventes at implementeringen og ikke minst forståelsen vil ta tid. Det foreligger videre i dag ikke noen hjemmel for å pålegge kommunene å følge veiledningene fra Valgdirektoratet, eller for å føre noen form for tilsyn med hvorvidt tilstrekkelig sikring gjennomføres. Dette øker sårbarheten ovenfor en angriper.

Varierende kompetanse i oppsett og bruk av utstyr og systemer i de ulike kommunene, kan medføre feil og utgjør slik en sårbarhet. Angrepsflaten for hacking er stor siden valgadministrasjonssystemet aksesseres fra valgmedarbeidere over hele landet. Kompetanse utfordres også lokalt ved at systemet er/tas i bruk kun i en begrenset periode hvert annet år.

I dagens prosess med en rekke manuelle prosesser (stemmetelling, protokollføring m.fl.) parallelt med de digitale, vil muligheten for å påvirke valgresultater gjennom den lokale infrastrukturen være liten. Mulighetene for å introdusere programvare som kan påvirke gjennomføring og eventuelt innhente informasjon fra systemene lokalt er reel og tilknyttet stor usikkerhet med tanke på variasjon i lokale løsninger og manglende tilsyn.

Variasjonen gjør det imidlertid samtidig mer utfordrende for en trusselaktør å enkelt nå alle kommuner i et angrep. Angrep på/mot sentral infrastruktur diskuteres i eget punkt.

Sårbarhet knyttet til denne typen hendelser vil kunne endres betydelig ved økt digitalisering og dersom dagens parallelle prosesser (manuelle) tas bort.

Vurdering: Middels sårbarhet

Konsekvenser for krav til valgprosessen:

Fri deltagelse	*Opplyst og informert*	*Korrekt*	*Gjennomføres som planlagt*	*Tillit*
			Mest sannsynlig påvirkning lokalt	Avdekking av at struktur har blitt hacket, sabotert eller overvåket vil påvirke tillit betydelig
Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Liten konsekvens	Stor konsekvens

Kunnskapsstyrke

Tekniske løsninger og komponenter er godt kjent – men ikke nødvendigvis i den enkelte kommune	Høy

Overførbarhet

Hendelser kan forekomme i alle kommuner	Høy

Endringshastighet

Teknologisk utvikling, men ikke noe spesielt for dette området	Middels

Oppsummering

Samlet vurdering – Relevans vil øke ved økt digitalisering	*Styrbarhet* – God mulighet for å adresse gjennom krav/regulering og oppfølging
Middels	Høy

Aktuelle tiltak

- Kravsetting til utstyr, oppsett og håndtering – regulering med adgang til tilsyn hos kommunene
- Opplæring og informasjon til valgmedarbeidere – både teknisk og vedrørende trusselforståelse
- Tekniske beskyttelsestiltak og overvåkingstiltak for systemene

14. Feil i stemmetelling

Hendelse/fenomen: Feil i stemmetelling

Beskrivelse

Telling av stemmer er en kritisk del av valgprosessen. Feil i antall stemmer kan forekomme ved at stemmer «forsvinner», legges til eller endres/plasseres feil/telles feil. Prosessen med telling kan i dag foregå manuelt eller maskinelt.

Manuell telling av stemmer:

Det kan forekomme feil i den manuelle tellingen av stemmer enten ved at det ubevisst gjøres feil, eller ved at valgmedarbeidere bevisst vil manipulere valget. I begge tilfeller vil konsekvensene normalt være veldig lokale; eller i det siste tilfellet – kreve mange «korrupte» valgmedarbeidere i mange kommuner.

Maskinell telling av stemmer:

Ved maskinell telling av stemmer skannes stemmesedlene med en skanner – og fortolkes av programvare som eies og utarbeides av Valgdirektoratet (EVA skann). Det er imidlertid kommunene som installerer EVA skann lokalt og som håndterer utstyr, programvare og bruk (med eller uten støtte fra leverandør). I dette systemet ligger flere muligheter for feil/manipulering av stemmeantall gjennom programvaren:

- Det gjøres manuelle feil av de som opererer skannere lokalt
- Skannere kan vise feil «bilde» (eks kryss flyttes til annet parti konsekvent)
- Fortolkningsprogrammet, EVA skann kan lese noe annet enn det som det skannede bildet viser
- Feil/manipulering av overføringer mellom skanner og fortolker og mellom EVA skann og EVA admin

Trusler/virkemidler

Endring og manipulering av stemmer og telling har tradisjonelt vært en «vanlig» metode for valgpåvirkning, men i større grad i stater med dårligere infrastruktur, mindre åpenhet og mindre gjennomarbeidede rutiner og systemer for valg (og med lavere tillit til systemene).

Spesielt statlige aktører vil kunne ha interesse av å manipulere valg sentralt både med tanke på å påvirke resultatet og for å ødelegge tilliten befolkningen har til system og prosesser. På mer lokalt nivå kan endring av stemmetall være av interesse ifht. enkeltsaker, og for flere aktører.

Digital manipulering vil trolig kunne utføres enklere og med mindre risiko enn manuell manipulering av stemmer. Det vil likevel kreve betydelig kompetanse og innsats å få tilgang til programvare og gjennomføre slik manipulering i stor skala. Kommunenes skannesystemer er ikke koplet sammen så et bredt nedslag vil trolig måtte lanseres via EVA admin sentral hos Valgdirektoratet. Disse sentrale systemene er satt opp med betydelig sikkerhet – og er overvåket.

Påstander om manipulering av stemmer via såkalte Valgmaskiner, har vært et hett tema de siste årene. I 2018 demonstrerte en gruppe hackere i samlingen DEF CON Voting Village blant annet at amerikanske valgmaskiner kunne hackes remote, og at hacking av maskinen lokalt kunne gjøres ved hjelp av en penn på 2 minutter (mens en gjennomsnittlig stemmeoperasjon tok 6 minutter). https://defcon.org/images/defcon-26/DEF%20CON%2026%20voting%20village%20report.pdf

Per i dag er ikke valgmaskiner i bruk i Norge, og scenarioet derfor ikke aktuelt før en form for slike eventuelt innføres.

Vurdering: Lav trussel

Barrierer og sårbarheter

Manuelle tellinger foregår i stor grad under oppsyn, og i utgangspunktet alltid med 2 valgmedarbeidere til stede, noe som må anses som en god barriere mot manipulering. Det vil kreve betydelig kapasitet å få flere valgmedarbeidere til å bevisst endre stemmetall, både på en enkelt lokasjon og ikke minst om dette skal foregå i flere distrikter og gi et utslag nasjonalt. Ved stortingsvalg kontrolltelles kommunenes opptellinger av fylkesvalgstyrene.

Valgdirektoratet har inhouse eierskap og utvikling av programvaren for skanning, og har solide og detaljerte veiledninger til kommunene som skal anskaffe utstyr, installere, vedlikeholde, oppbevare og håndtere utstyr og programvare.

Det foreligger imidlertid ingen hjemmel for å pålegge kommunene noe av dette, og de står i praksis fritt til å velge både hvem som håndterer utstyr og programvare, og hvordan. Det finnes en rammekontrakt med 3 forhåndsgodkjente leverandører (Valgdirektoratet) som kommunene kan benyttes/avrope om kommunene ønsker, men det er heller ikke noe krav om dette. Det finnes heller ikke noen hjemmel for å føre noen form for tilsyn eller oppfølging med hvorvidt kommunene håndterer dette i tråd med veiledning.

En skanner kan påvirkes tidlig i leverandørkjeden, hos kommunen eller hackes via nett (vedlikehold kan utføres online, og da kan systemet også aksesseres med andre formål). Som for resten av samfunnet må det påregnes at kommunene, med sin store variasjon i størrelse og form, og er svært varierte med tanke på kompetanse, utstyr og økonomi. I kombinasjon med at det ikke foreligger regulatoriske krav eller oppfølging fra sentrale myndigheter, utgjør dette en stor sårbarhet ifht. å påvirke stemmetall.

I valgprosessen foreligger det imidlertid i dag både kontrollrutiner/sjekkprøver ved telling maskinelt (disse er ikke pålagte), samt forskriftsfestet krav om manuell forhåndstelling. Så lenge 2 slike uavhengige tellemetoder opprettholdes er det en svært effektiv barriere med tanke på å avdekke forøk på manipulering av stemmetall, og sårbarheten for dette blir følgelig da veldig liten. Det er viktig at det er en reel uavhengighet i tellemetodene. To tellinger på to ulike maskiner gir ikke nødvendigvis tilstrekkelig uavhengighet på samme måte som en manuell telling gir. Fellesfeil (Common cause) er et velkjent fenomen innen storulykketeori, og erfaringer viser at man ofte feiler i å skape reelt uavhengige systemer og dermed har sårbarheter som man ikke er klar over.

Det er viktig å merke seg at en økt digitalisering uten mulighet for manuell «back up» vil stille betydelige krav til sikringstiltak for å opprettholde sikkerhetsnivået i valgprosessen og stemmetellingen.

Vurdering: Lav sårbarhet

Konsekvenser for krav til valgprosessen:

Fri deltagelse	*Opplyst og informert*	*Korrekt*	*Gjennomføres som planlagt*	*Tillit*
		Liten påvirkning på valgresultatet i dag pga. de uavhengige tellemetodene og kontrollrutinene som vil avsløre forsøk på manipulering.		Avdekking av forsøk på manipulering av stemmetall vil svekke tilliten, selv om konsekvensen ikke blir feil valgresultat
Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Liten konsekvens	Ingen/nesten ingen konsekvens	Stor konsekvens

Kunnskapsstyrke	
Trusler og sårbarheter er velkjente i dag, men økt digitalisering kan endre dette	Høy

Overførbarhet	
Kan forekomme i alle kommuner	Høy

Endringshastighet	
Dersom økt digitalisering velges øker endringshastigheten	Middels

Oppsummering

Samlet vurdering – Med dagens uavhengige metoder for telling er ikke denne hendelsen svært viktig, men ved endring i denne situasjonen vil viktigheten av denne typen hendelse kunne øke betydelig	*Styrbarhet* – Verktøy og metoder kan reguleres

Lav	Høy

Aktuelle tiltak

- Regulering og krav til utstyr, håndtering, oppbevaring osv. for elementer til skanning og telling av stemmer, samt etablere tilsynsordning med etterlevelse
- Vurdere om tekniske systemer og periferutrusting i større grad skal eies og driftes av sentrale myndigheter; eksempelvis at sentrale myndigheter eier og vedlikeholder valgutstyr og har ansvar for å distribuere og sette dette opp for bruk i valgperiodene
- Opprettholde krav om uavhengige tellemetoder og tydeliggjøre/definere hvilke krav som stilles til uavhengighet
- Videreføre/utvikle og stille krav til opplæring og kompetanse for involverte i valg
- Ytterligere regulere krav til gjennomføring av avstemming og telling (4 øyne, kontrolltellinger m.fl.)

15. Valgsystemet er manipulert - sentralt

Hendelse/fenomen: Valgsystemet er manipulert - sentralt

Beskrivelse

Det elektroniske valgadministrasjonssystemet i Norge (EVA) utvikles og driftes av Valgdirektoratet (Vdir), og er også fysisk plassert hos Vdir. Som for utstyr og programvare som driftes av kommunene, vil det være muligheter for «innbrudd» også i EVA som driftes sentralt. Det kan for eksempel dreie seg om sårbarheter i programkode utviklet av Valgdirektoratet, sårbarheter introdusert i hardware, sårbarheter i 3. parts programvare eller at trusselaktørene får tilgang til nettverk der kritisk infrastruktur kjører via andre måter, f.eks. virus på en ansatt sin PC.

Til tross for betydelige tiltak med innebygd sikkerhet, rutiner, beskyttelse og testing, vil man ikke fullt ut kunne beskytte seg mot innbrudd i kritisk infrastruktur som valgsystemer. Det må antas at infrastruktur er, eller kan bli, kompromittert men at det må etableres verktøy og prosesser som kan oppdage, detektere og hindre skade. Paradigme har tidligere vært å investere i maksimal beskyttelse, og forsøke å tette alle skott. I dag finnes en anerkjennelse av at selv det beste forsvar vil kunne feile på et eller annet punkt. Paradigmet skifter mot et mer deteksjonsorientert IT-miljø som også fokuserer på deteksjon og håndtering for å hindre skade dersom forsvaret penetreres.

Selv om valgsystemer har blitt kompromittert, f.eks. i form av hacking, så betyr dette ikke at man har tapt «kampen». Trusselaktørene er ute etter å sikre sine mål, som kan være å påvirke valget. Selv om aktøren kommer seg inn i systemet kreves det både kompetanse og tid for å klare å gjennomføre endringer av betydning. Dersom de da kan detekteres og «kastes ut» igjen før de når sine mål, er den faktiske skaden forhindret.

Samtidig vil slike angrep, dersom de blir kjent for allmenheten, likevel kunne bidra til å skape uro og redusere tilliten til system og prosesser; selv om de ikke nødvendigvis klarer å påføre en faktisk skade i systemet

Manipulering av resultater konkret, samt sabotasje og utfall av systemet, er diskutert i egne hendelsesbeskrivelser (hendelse 16 og 17), og adresseres ikke videre her.

Trusler/virkemidler

Angrep på EVA vil enten kommer fra utsiden, eller ved bruk av en innsider med tilgang til hele eller deler av systemet. Bruk av innsidere til å bryte seg inn i eller skade EVA vil trolig i hovedsak begrense seg til statlige aktører som har en kombinasjon av interesse og kapasitet til å gjennomføre slike operasjoner. Samtidig vil en innsider ha det absolutt største potensialet til å påføre omfattende skade når det kan opereres innenfor mange av de etablerte barrierene (og der gjerne øvrige sikkerhetstiltak, deteksjonsmuligheter og mottiltak er godt kjent.

Angrep ved hacking eller introduksjon av sårbarheter utenfra kan være aktuelt både for statlige aktører, kriminelle som selger digitale sårbarheter, og hacktivister/andre som ønsker å bryte seg inn først og fremst for å demonstrere og/eller skape mistillit.

Med dagens brede konsensus i det norsk politikk, eksisterende barrierer i valgprosessen; og den norske rollen i det internasjonale politiske bildet, er trolig både motivasjon og potensiell gevinst ved et større angrep fra en statlig aktør begrenset. Det er imidlertid anerkjent i åpne trusselvurderinger at aktører som eksempelvis Russland, og etter hvert Kina, benytter betydelig kapasitet til å legge til rette for og trene på et fremtidig angrep. I dette ligger både å øve på å gjennomføre angrepene, og kunne bryte seg inn i valgsystemer; men også etterretning og identifisering av sårbarheter til fremtidig bruk.

Det finnes i dag også mange eksempler på at PCer, servere og komponenter kommer forhåndskonfigurert med virus fra leverandørene; eller har blitt påført sårbarheter før mottak hos sluttbruker. Nettverksutstyr fra den velkjente produsenten Cisco, nettverksenheter brukt verden over, ble snappet opp i verdikjeden av NSA (National Security Agency, USA's Nasjonale Sikkerhetsmyndighet). Formålet med avskjæringen i bestillingene var for USA å bygge inn bakdører i enhetene, noe som tillater dem å detaljovervåke innkommende og utgående nettverkstrafikk i organisasjonene hvor enhetene blir rullet ut. https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/

Samtidig vil også angrep der faktisk skade ikke skjer, men der et «vellykket innbrudd» blir kjent for allmennheten bidra til å redusere tilliten til de demokratiske valgprosessene og -systemene. For enkelte trusselaktører vil dette kunne være et mål i seg selv.

Nettkriminelle som lever (godt) av å selge sårbarheter de finner, eller etablerer, i både statlige og private systemer, vil også ha interesse av valgsystemer. Interesserte kjøpere vil typisk være de samme statlige aktørene som nevnt over. For enkelte grupper hackere vil det også kunne gå sport i, og gi status, å bryte seg inn i kritiske systemer. Slike innbrudd vil trolig i liten grad påføre direkte skade, men vil kunne bidra til å redusere tillit til systemer og myndigheter.

Vurdering: Middels trussel

Barrierer og sårbarheter

Åpenhet og innsyn i kildekode og rutiner anses å være viktige tiltak for å sikre valgsystemer. Sveits er et av landene som i 2019 hadde planer om å rulle ut et trygt og sikkert elektronisk valgsystem med internettavstemming. Samme året som utrullingen ble det imidlertid avdekket svakheter i systemet, som ville tillatt ett enkelt individ å påvirke valget i den retningen vedkommende ønsket. (Referanse: https://motherboard.vice.com/en_us/article/zmakk3/researchers-find-critical-backdoor-in-swiss-online-voting-system). Sårbarheten ble avdekket nettopp ved åpenhet og innsyn. Myndighetene testet ut programvaren online, slik at alle som ønsket kunne prøve å se om de fant feil og sårbarheter, gjennom et såkalt «bug bounty» program. Dette er et program som lar eksperter og vanlige mennesker prøve å avdekke sårbarheter, og der de mottar «finnerlønn» om de avdekker noe. I Sveits sitt tilfelle tilbød myndighetene, dersom sårbarheten lot en bruker manipulere valget uten å bli detektert, opptil 50.000 Sveitsiske Franc som betaling, mot at de får rettet sårbarheten. I Sveits sitt tilfelle medfører trolig avdekkingen av kritiske sårbarheter at lanseringen av systemet utsettes på ubestemt tid.

Det norske Valgdirektorat fokuserer også på åpenhet og å gi mest mulig innsyn i systemer og rutiner. Dette bidrar til at systemer på sikt kan designes og bygges med større innebygd sikkerhet. https://valg.no/valg-i-norge/valggjennomforing-i-norge/elektronisk-valgadministrasjonssystem/systemdokumentasjon-og-kildekode-i-eva/. Det dokumenteres og publiseres også hvilke sikkerhetstester som er gjort, og kildekoden for noen av systemene er tilgjengelig online. Slik åpnes det for at dette blir gjennomgått, testet og kvalitetssikres av andre. For eksempel kan man se en liste over sikkerhetstester og mennesker som har pekt på svakheter her: https://valg.no/.well-known/acknowledgements.txt .

Åpenhet og publisering av kildekode, sikkerhetstester o.a. bidrar også til å redusere svakheten som ligger i at systemet kun benyttes i perioder hvert annet år. Når systemet ikke er i operasjon store deler av tiden vil ikke kildekoden bli kontinuerlig verifisert og testet under produksjon. Samtidig vil det at systemet ikke er kontinuerlig i drift ved at angrepsflaten trusselaktørene kan benytte seg av, kun er tilgjengelig en kort tid av gangen (i alle fall om angrepet kommer fra utsiden).

Åpenhet og innsyn er viktige verdier for å lage robuste systemer for valgsikkerhet, men like viktig er det med prosesser for ettersyn, deteksjon og overvåkning. Man må ta for gitt at digitale løsninger kan hackes og påvirkes, gjerne på måter som er vanskelig å fatte og forstå i dag. Det må forutsettes at trusselaktørene har kapasiteter til å gjøre det meste digitalt, slik at innsats også må legges i supplerende manuelle rutiner, deteksjon og ettersyn i valgprosessene.

Det er gjort et omfattende arbeid med sikring av system og informasjon som håndteres i EVA, og løsningen fremstår som robust. Som poengtert innledningsvis her i beskrivelsen vil imidlertid også et kontinuerlig arbeid med å utvikle og implementere verktøy og prosesser som kan oppdage, detektere og hindre skade være helt essensielt.

Per i dag er nok den mest effektive barrieren mot konsekvenser av manipulering av valgadministrasjonssystemet (EVA), de parallelle manuelle prosessene for telling og kontroll av stemmer og resultater.

Vurdering: Middels sårbarhet

Konsekvenser for krav til valgprosessen:				
Fri deltagelse	*Opplyst og informert*	*Korrekt*	*Gjennomføres som planlagt*	*Tillit*
		Med dagens parallelle manuelle prosesser vil forsøk på manipulering med stor grad av sikkerhet avdekkes og ikke påvirke valget direkte.	Selv om forøk på manipulering blir avdekket, vil det kunne sås tvil om riktighet i prosessen, og i verste fallmedføre at valget blir underkjent og må gjennomføres på nytt.	Vellykkede innbruddsforsøk, selv om de ikke påvirker valget direkte, vil i stor grad kunne bidra til svekkelse av tillit i befolkningen
Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Noe konsekvens	Stor konsekvens

Kunnskapsstyrke	
Fenomenet er godt kjent og stadige nye eksempler blir kjent	Høy

Overførbarhet	
Vil hovedsakelig rettes mot sentrale systemer, men mulig innfall via kommuner også	Middels

Endringshastighet	
Nye angrepsmetoder, men også nye tiltak, utvikles fortløpende	Middels

Oppsummering	
Samlet vurdering – Mest konsekvens i tillitsdimensjonen i dag. Ved økt digitalisering vil denne typen fenomen bli stadig viktigere å håndtere/styre	*Styrbarhet* – Gjennom regulering, gjennomføring av parallelle prosesser og tiltak for å sikre og detektere kan risiko styres langt på vei.
Middels	Høy

Aktuelle tiltak

- Opprettholde parallelle prosesser for kvalitetssikring (eksempelvis manuell telling, protokollføring, kontroller og godkjenning)
- Åpenhet om kildekoder mm
- Privat-offentlig samarbeid og tiltak for å beskytte, detektere og overvåke systemet
- Gode planer for å forberede og håndtere hendelser – herunder informasjons og kunnskapsbygging i befolkningen med tanke på at et innbrudd i et valgsystem ikke trenger å bety kritisk skade eller et kompromittert valg.
- Styrke personellsikring for medarbeidere i valgdirektoratet og valgmedarbeidere og leverandører på alle nivåer

16. Resultatet manipuleres

Hendelse/fenomen: Resultatet manipuleres

Beskrivelse

Som beskrevet under «valgsystemet er manipulert – sentralt», vil det alltid finnes muligheter for å «bryte seg inn», også i sentrale valgssystemer.

Resultatene kan potensielt manipuleres i EVA admin, EVA resultat, i overføringen til media og valgresultat.no og også direkte på f.eks. valgresultat.no.

Slike digitale manipuleringer vil i dag avdekkes og korrigeres gjennom manuelle tellinger, protokoller og godkjenninger.

Utfordringen blir hvorvidt en feil detekteres og korrigeres raskt nok til at publisering av feilaktige resultater unngås. Dersom feil resultater blir lagt ut og må korrigeres vil det kunne ha stor negativ effekt på tilliten til systemer og myndigheter, og gi grobunn for spekulasjoner. Dette kan i seg selv være motivasjon nok for enkelte aktører.

Forbudet mot publisering av valgdagsprognoser og resultater før stenging av valglokalene på valgdagen, bidrar til å hindre at eventuelle falske resultater påvirker stemmegivingen. Dersom publisering skulle forekomme før klokka 21 på valgdagen vil slik påvirkning være mulig – noe som diskuteres under hendelse/fenomen «Brudd på konfidensialitet».

Trusler/virkemidler

Både statlige aktører og politiske og andre sterke interessegrupper kan ha ønske om å påvirke og endre valgresultater lokalt og sentralt i Norge.

Endring av resultat for å så tvil om at systemer og myndigheter fungerer og er «sikre» vil imidlertid kunne være oppnåelig både for statlige og politiske aktører; og for andre grupperinger som bare ønsker å demonstrere egen evne og manglende sikkerhet.

Vurdering: Høy trussel

Barrierer og sårbarheter

Barrierer i det digitale systemer er adressert i andre hendelsesbeskrivelser for både lokale og sentrale systemer. Videre er barrierene mot at et faktisk feilaktig resultat skal bli stående som gyldig, sterke ved at det gjennomføres parallelle manuelle rutiner, tellinger og godkjenninger (og protokollføring) gjennom hele valgprosessen).

Med dagens redundante systemer for telling og kvalitetssikring av resultat er en manipulering av resultatet som faktisk «blir stående», vanskelig å forestille seg. Det kan tenkes at sårbarheten for at feilaktige resultater publiseres (men senere rettes opp), er større. Slik manipulering og feilrapportering kan forekomme både lokalt, sentral, manuelt og digitalt. Ved publisering først etter at valglokalene stenges vil dette imidlertid ikke påvirke avstemmingen i valget.

Norge er preget av høy tillit til myndigheter og system. Dette vil være en barriere mot å enkelt så tvil om myndighetenes intensjoner ved valg.

Å så tvil om systemers godhet og myndighetenes evne til å sikre systemene vil trolig være enklere for aktører som ønsker å skape mistro og uro.

Vurdering: Lav sårbarhet

Konsekvenser for krav til valgprosessen:				
Fri deltagelse	*Opplyst og informert*	*Korrekt*	*Gjennomføres som planlagt*	*Tillit*
		Med dagens redundante systemer vil det kreve svært mye å faktisk endre resultatet gjennom manipulasjon.		Kan raskt påvirke troen på hvor sikre systemene er og hvor gode myndighetene er til å sikre valget.
Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Noe konsekvens

Kunnskapsstyrke	
Velkjente sårbarheter og metoder	Høy

Overførbarhet	
Kan manipuleres lokalt og/eller sentralt	Høy

Endringshastighet	
Digitale angrepsmetoder og forsvar endres stadig. Grad av digitalisering medfører endring i risiko og tiltaksbehov.	Middels

Oppsummering	
Samlet vurdering – Muligheten for å varig endre resultatet av valget anses som lavt i dag, men en selv en «kortvarig» feil kan påvirke tilliten. Viktigheten øker om valget i større grad digitaliseres	*Styrbarhet* – Kan langt på vei styres gjennom tekniske tiltak og regulering vedrørende uavhengige parallelle rutiner og øvrige prosesser.
Middels	Høy

Aktuelle tiltak

- Opprettholde parallelle prosesser for kvalitetssikring (eksempelvis manuell telling, protokollføring, kontroller og godkjenning) – og informere om at denne redundansen finnes
- Privat-offentlig samarbeid og tiltak for å beskytte, detektere og overvåke systemet
- Videreføre kvalitetssikrings- og kontrollpunkter før resultater offentliggjøres, og krav om å avvente offentliggjøring til valglokaler er stengte
- Etablere gode planer for å kommunisere og håndtere en eventuell publisering av feilaktige resultater

17. Mangelfull tilgang til system og lokaler

Hendelse/fenomen: Mangelfull tilgang til system og lokaler

Beskrivelse

Det at valglokaler eller kritiske valgsystemer blir utilgjengelige kan hindre at folket får avlagt sin stemme; at stemmene telles eller at resultater kan genereres og formidles.

At valglokaler eller valgsystemer blir utilgjengeliggjort kan forårsakes av en rekke ulike hendelser. Enkeltlokaler kan utilgjengeliggjøres av lokale værforhold, naturhendelser og sabotasje. I ekstreme tilfeller kan værforhold og naturhendelser utilgjengeliggjøre lokaler også i større områder, mens tilsiktet skading av lokaler vil være svært krevende å gjennomføre mange steder på en gang. Det kan også forekomme vær- og naturkatastrofer som potensielt kan ta ut strøm og nett i store områder.

Mangelfull tilgang til EVA som sentralt system kan også forårsakes av feil og hendelser internt (eksempelvis ved endringer og tilpasninger av programvare), og ved større utfall av nettlinjer (av ulike årsaker) fra nettleverandører.

Datahall kan bli uttilgjengelig som følge av kritiske hendelser, og/eller data kan tapes.

EVA kan også utsettes for store systematiske angrep fra trusselaktører gjennom eksempelvis DDos-angrep (tjenestenekt ved overbelastning) eller introduksjon av skadevare via ulike vektorer. Virus spres også i dagens IT-miljøer, da gjerne automatisert, ofte kalt en orm. Uansett om viruset spres som en orm eller ei, så kan det treffe valgsystemene og gjøre disse utilgjengelige.

Et tjenestenektangrep kan for eksempel angripe datasenteret til Valgdirektoratet slik at de ikke mottar data fra noen av kommunene. Et slikt angrep vil potensielt kunne holde valgsystemet nede over lengre tid. Det kan hindre kommunene i å overføre resultatet til EVA. Dette kan imidlertid gjøres når en har klart å blokkere tjenestenektangrepet. Dermed vil ikke en slik hendelse true riktigheten av resultatet; og trolig heller ikke hindre at valget kan gjennomføres, men det kan føre til tap av tillit og være svært ressurskrevende å håndtere.

Bortfall av tilgang til elektronisk manntall vil kunne være utfordrende for valggjennomføringen.

Trusler/virkemidler

Både statlige aktører og enkelte politiske og andre -interessegrupperinger vil kunne ha interesse av å hindre gjennomføring av valg. Først og fremst vil nok motivasjonen ligge i å vise evne (skape uro og frykt), og å skape mistillit til myndighetene og deres evne til å sikre prosessene rundt valg.

Også trusselaktører som ikke nødvendigvis har en politisk intensjon kan tenkes å angripe og sabotere valgsystemet, kun for å demonstrere at de klarer det (noe som kan gi status i enkelte miljøer).

Andre utilsiktede forhold som for eksempel strømbrudd og ekstremvær kan også true valggjennomføringen.

For å oppnå effekt av betydning vil trolig de fleste aktuelle aktører konsentrere seg om digitale angrep på systemene, slik som tjenestenekt eller skadevare som hindrer bruk av systemet.

Vurdering: Høy trussel

Barrierer og sårbarheter

Valg gjennomføres på en tid av året der vær og klima vanligvis er lite utfordrende. Dersom værmessige eller naturgitte hendelser berører tilgang til stemmelokaler skal det i dag foreligge beredskapsplaner i alle kommuner for flytting av stemmested til alternative lokaler. Dette er blant annet i Oslo gjennomført «uproblematisk» i forbindelse med brann. Utilgjengeliggjøring av ett eller en gruppe stemmelokaler vil trolig derfor gi liten konsekvens for valget.

Kritiske systemer som strøm- og nettilgang er underlagt krav om forsyningssikkerhet, og det vil normalt være god dekning av redundante løsninger. Langvarige utfall som berører store områder er ikke vanlig.

Trolig ligger det største konsekvenspotensialet for valget i at sentrale systemer faller ut over lang tid som følge av egne feil, eller angrep ved tjenestenekt eller introduksjon av skadevare som ødelegger eller utilgjengeliggjør informasjon. De fleste

systemer har god redundans, men omfattende angrep eller hendelser som berører også parallelle systemer vil være kritiske. Bruk av innsidere for å skade sentrale systemer vil kunne gi stor og målrettet effekt. Det foreligger manuelle beredskapsrutiner for å kunne gjennomføre avstemmingen på valgdagen (-e) også uten tilgang til elektronisk manntall og til EVA, men gjennomføringen vil kreve betydelige ressurser og tid dersom utfallet er stort og varer over tid. Dersom eksempelvis en trusselaktør skulle klare å hacke systemet og fjerne avkrysninger i manntallet, har systemene flere lag med deteksjon som alarmerer dette – og mulighet til å skifte over til et speilet miljø i løpet av svært kort tid.

Som beskrevet i kapittel 3.4 i denne rapporten finnes det en rekke aktører og komponenter som både kan fungere som barrierer, og potensielt utgjøre sårbarheter i systemene gjennom hele den digitale verdikjeden til valgsystemene. I tillegg til sårbarheter i kjernesystemer, hos kjerneaktører og i ulike kjernekomponenter, kompliseres og forlenges disse kjedene også ved at de er avhengige av annen infrastruktur som strøm og nett m.fl. Dette medfører at en sårbarhet som ligger langt unna «skadestedet», og i liten grad kan kontrolleres av den som beskytter verdiene, kan gi store konsekvenser om den utnyttes eller en uønsket feil/hendelse inntreffer.

Eksempelvis ble det distribuert virus gjennom programvareoppdateringer i et regnskapsprogram brukt flere steder i Ukraina. Dette viruset spredde seg først i Ukraina, men ble deretter distribuert ukontrollert også i på helt andre geografiske steder og bransjer. Blant annet fikk det danske shippingkonsernet Maersk store skader i IT miljøene sine (Referanse: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/). Videre har vi sett at komponenter fra IT miljøer også plutselig har blitt avdekket som veldig sårbare, og kan føre til tap av IT sikkerhet på en rekke ulike enheter. Blant annet ble det i 2017 oppdaget alvorlige feil i moderne prosessorer i måten de håndterer data på. I algoritmene som ble brukt i prosessoren for å gjøre den raskere, fantes det også muligheter for angripere å lese ut konfidensiell informasjon fra systemene som brukte dem (Referanse: https://meltdownattack.com/).

I Lysne-utvalgets utredning om digitale sårbarheter fra 2015 (https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf) adresseres utfordringen ved sårbarheter i lange og uoversiktlige digitale verdikjeder knyttet til kritiske samfunnsfunksjoner. De samme utfordringene vil i stor grad også gjelde for valgsystemer og valgprosesser i en stadig mer digitalisert hverdag. Problemstillingen viser viktigheten av å ikke bare beskytte system og verdier mot muligheten for feil, hendelser og angrep (da det vil være nærmest umulig å ha oversikt over og håndtere alle sammenhenger og mulige sårbarheter), men også fokusere på å kunne oppdage hendelser og angrep, og håndtere dem slik at skade elimineres eller minimeres.

I tillegg til betydelige tekniske barrierer, vil beredskapsrutiner, manuell telling, prosesser, protokoller og godkjenninger vil i dag redusere konsekvensene knyttet til mange av hendelsene/angrepene i den digitale verdikjeden. Ved økende avhengighet av digitale systemer vil sårbarheten øke.

Per i dag foreligger ikke hjemmel i norsk lovverk for å utsette gjennomføringen av valg dersom systemer eller lokaler blir utilgjengelige eller dersom en annen trusselsituasjon skulle tilsi det. Det medfører at valget gjennomføres også eksempelvis dersom mange skulle bli forhindret fra å stemme, eller myndighetene ikke klarer å gjennomføre prosesser. Eneste alternativ er da å underkjenne selve valget i etterkant – og gjennomføre nytt valg. Et vellykket angrep i stort omfang vil derfor kunne få betydelig konsekvenser.

Vurdering: Middels sårbarhet

Konsekvenser for krav til valgprosessen:

Fri deltagelse	*Opplyst og informert*	*Korrekt*	*Gjennomføres som planlagt*	*Tillit*
Utilgjengelige lokaler eller systemer vil kunne vanskeliggjøre deltakelse for velgere, men om denne effekten vurderes som av betydning vil trolig nytt valg gjennomføres			Omfattende angrep vil kunne ha stor betydning for muligheten til å gjennomføre valget effektivt, og i verste fall medføre behov for ny valggjennomføring	Dersom valget ikke kan gjennomføres pga. enten feil eller angrep på valgsystemer vil det kunne ha stor negativ effekt på tilliten til myndigheter og systemer

Liten konsekvens	Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Stor konsekvens	Stor konsekvens

Kunnskapsstyrke	
Kjente sårbarheter og angrepsformer – selv om beskyttelse ikke er enkel mot alt	Høy
Overførbarhet	
Uttak av systemtilgang i stort omfang vil måtte være sentralt rettet	Lav
Endringshastighet	
Både angrepsmetoder og beskyttelsestiltak endrer seg med digitalisering	Middels

Oppsummering	
Samlet vurdering – Omfattende systemutfall vil kunne ha store konsekvenser for valggjennomføring, og påvirke tilliten til systemer og myndigheter i stor grad	*Styrbarhet* – Sikring av systemer, parallelle rutiner og muligheter for å flytte et valg kan i stor grad reguleres.
Høy	Middels

Aktuelle tiltak

- Personellsikring for medarbeidere med tilgang til kritiske systemer (Valgdirektoratet, leverandører, kommuner)
- Hjemmel og mulighet for å flytte tidspunkt for valggjennomføring ved omfattende hendelser
- Teknisk sikring og krav sentralt og lokalt
- Opprettholde parallelle gjennomføringsmuligheter (manntall, registrering, telling og registrering av stemmer mm)
- Gode beredskapsplaner på alle nivåer (sentralt og lokalt) – hendelseshåndtering
- Redundant infrastruktur både på lokaler og systemer/komponenter

18. Brudd på konfidensialitet

Hendelse/fenomen: Brudd på konfidensialitet

Beskrivelse

Et viktig prinsipp ved gjennomføring av valg i Norge (ref. valgloven) er at valget skal være hemmelig. Dvs. at alle skal kunne avlegge sin stemme uten at noen vet hva du har stemt. Dette prinsippet håndheves strengt i valglokalene i dag ved at ingen har tilgang til stemmebåsen når velgeren foretar sin avstemming. Det finners enkelte unntak der velgerne pga. funksjonsnedsettelse har behov for hjelp til gjennomføring. En kan også se for seg muligheter for en trusselaktør for å overvåke (i det skjulte) stemmebåser.

Prinsippet om hemmelige valg og krav til tiltak for å sikre dette, er et område som vil kunne bli betydelig utfordret dersom både identifisering av velgeren og stemmegiving foregår digitalt. Informasjonen vil da med all sannsynlighet kunne gjenfinnes og koples sammen også senere og av andre. Dersom valg også kan foregå hjemmefra eller andre steder som ikke er under oppsyn som valglokale, vil man i praksis vite svært lite om hvorvidt avstemmingen til den enkelte er «fri» eller «hemmelig».

Et annet konfidensialitetsaspekt er om informasjon om prognoser og resultater (f.eks. fra forhåndsstemmer) blir tilgjengelig og «lekket» før valglokalene stenger. Slike foreløpige resultater ville da kunne påvirke både om og hva enkelte velgere stemmer.

Også informasjon om hvem som har stemt (avkryssede manntall) kan tenkes å være sensitiv for enkelte velgere og velgergrupper, og påvirke friheten i valget. Informasjonen kan også benyttes til å kartlegge over tid hvem som ikke avlegger stemmer, og som lettere kan benyttes som identitet for å kunne avlegge flere stemmer.

Med dagens omfattende bruk av digitale plattformer, og i forlengelsen av diskusjonen om bruk av innsamling av informasjon og kunstig intelligens/maskinlæring for å sammenstille og analysere informasjonen om den enkelte fremkommer også spørsmålet om kunnskap og informasjon rundt velgernes politiske syn og preferanser. Selv om det som skjer i stemmebåsen er hemmelig, vil en rekke digitale systemer samle inn og sammenstille informasjon og så predikere med stor nøyaktighet hva den enkelte av oss kommer til å stemme/har stemt. Som beskrevet i fenomenvurderingen av ekkokamre og mikromålretting av informasjon, er slik analyse allerede utbredt og tilgjengelig. Her finnes eldre eksempler, men utviklingen på dette området har eksplodert de siste par årene https://www.psypost.org/2017/10/scientists-find-facebook-likes-can-accurately-predict-youre-going-vote-49801.

Under fenomenet mikromålretting av informasjon, er også bruken av valgomater diskutert.

Selv om konfidensialiteten ved avstemming ivaretas og opprettholdes, kan verdien av hemmelige valg tenkes å bli mindre i fremtiden, med referanse til betraktningene over.

Trusler/virkemidler

Å innhente informasjon om hva den enkelte velger har stemt gjennom overvåking av stemmebåser o.l., vil både være teknisk og/eller personellmessig krevende, og for de aller fleste trusselaktører ha svært begrenset verdi, utover helt lokale og begrensede tilfeller med spesifikk agenda. En avsløring av f.eks. overvåking av stemmebåser ville imidlertid ha en viss negativ effekt på tilliten til valgprosessen.

Mye større potensial ligger trolig i å få tilgang til og benytte seg av informasjon som samles inn via digitale plattformer i forkant av et valg, slik at større grupper kan eksponeres og påvirkes. Temaet er adressert der fenomenet mikromålretting adresseres.

Avkryssede manntallslister vil kunne ha verdi for en trusselaktør som ønsker å kunne avlegge flere stemmer ved å benytte seg av andres identitet. En kartlegging av hvem som «aldri» stemmer gir et godt utgangspunkt for hvilke identiteter som kan utnyttes mest mulig risikofritt. Med det manuelle innslaget i dagens avtemmingsprosess (med personlig oppmøte), vil imidlertid en slik form for valgjuks være svært ressurskrevende å gjennomføre i noe større format.

I en tenkt utvikling der både identifisering av velgeren og avstemmingen utføres elektronisk (valgmaskiner, internettvalg o.a.), vil potensialet for en trusselaktør øke. Dette både med tanke på å avsløre hva som er stemt – og benytte kunnskap om identiteter som kan forfalskes for å avlegge flere stemmer. En avsløring av hva en velger har stemt – eller et tilfelle av at stemmer har blitt avlagt ved bruk av andres identitet vil kunne ha en svært stor negativ effekt på tilliten til valgsystemene.

Vurdering: Lav trussel

Barrierer og sårbarheter

At valget er hemmelig har vært og er et viktig prinsipp for Norge og for mange velgere. Ingen skal «skremmes fra» å stemme i tråd med sin frie vilje, fordi noen finner ut hva du har stemt/stemmer. For de aller fleste velgere er dette prinsippet godt ivaretatt under valget i dag; med unntak for noen enkelte velgergrupper med behov for hjelp og tilrettelegging i stemmebåsene.

Manuelle prosesser rundt avstemming utgjør i dag en betydelig barriere, som utfordres dersom både identifisering av velgeren og avstemmingen foregår elektronisk.

Avkryssede manntallslister i EVA kan tenkes å nås elektronisk av en trusselaktør, og en lekkasje av slike vil kunne ha stor negativ effekt på tilliten til systemene. Omfattende bruk av informasjonen i manntallet for å avlegge falske stemmer vil imidlertid ha begrenset konsekvens (eller være svært ressurskrevende) på grunn av de manuelle elementene i avstemmingsprosessene.

Hvorvidt verdien av hemmelige valg utfordres gjennom informasjonen om velgerne som samles og analyseres mellom valggjennomføringene, bør utredes videre (og adresseres også i andre hendelsesbeskrivelser i denne rapporten).

Vurdering: medium sårbarhet

Konsekvenser for krav til valgprosessen:

Fri deltagelse	*Opplyst og informert*	*Korrekt*	*Gjennomføres som planlagt*	*Tillit*
Kjennskap til at valget ikke er hemmelig vil kunne skremme velgere fra å delta i valget – og gi mulighet for å påvirke pga. frykt				Kjennskap til at prinsippet om hemmelige valg er brutt på noen måte vil potensielt ha stor negativ effekt på tilliten til prosessen i dag
Noe konsekvens	Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Stor konsekvens

Kunnskapsstyrke

Det er god kunnskap om konfidensialitet i eksisterende prosess, men begrenset med kunnskap om effekten av digitale analyser og av prosessendring	Middels

Overførbarhet

Stedsuavhengig	Høy

Endringshastighet

Digitalisering av valg vil endre sårbarheten på dette området	Middels

Oppsummering	
Samlet vurdering – Begrenset utfordring i valgutførelse i dag, men kommende og mulige endringer gjør temaet svært aktuelt	*Styrbarhet* – Valg av prosess (digitaliseringsfart) er styrbar. Utviklingen for informasjon på nett er delvis regulerbar.
Middels	Middels

Aktuelle tiltak

- Begrense digitalisering som gjør både identifisering av velger og stemmen digital
- Trinn for trinn sikring av konfidensialitet gjennom tekniske og andre tiltak ved ytterligere digitalisering av valg
- Forske på/utrede effekt av personinformasjon og analyser på nett på konfidensialitet vedrørende politiske preferanser
- Teknisk beskyttelse av informasjon om valgresultater (for å hindre for tidlig publisering)
- Sikringstiltak for beskyttelse av manntallslister i EVA

19. Ufrivillige feil ved valggjennomføring

Hendelse/fenomen: Ufrivillige feil ved valggjennomføring

Beskrivelse

Det foreligger en rekke muligheter for å gjøre feil i forbindelse med gjennomføringen av valg. Dette kan dreie seg om prosessuelle feil ifht valglovverket, tekniske feil med en rekke ulike konsekvenser og tilsvarende for menneskelige feil i gjennomføringen.

Feil av denne typen vil ofte være tett knyttet til kompetanse for involverte valgmedarbeidere på sentralt og lokalt nivå. I de ulike kommunene vil det være svært varierende grad av kontinuitet og kompetanse både på teknisk område, og for valggjennomføring. Dette er en naturlig følge av stor variasjon i kommunenes størrelse, muligheter til å ha dedikerte valgmedarbeidere, og hvorvidt involvert personell er tilstede og involverte i korte eller lange perioder.

Konkrete potensielle feil og mangler ved gjennomføringen av valg er i stor grad adressert i risikovurderinger og tiltaksplaner både i kommunene, i Valgdirektoratet og i Kommunal- og moderniseringsdepartementet – og vil derfor ikke bli behandlet i ytterligere detalj i denne utredningen.

Trusler/virkemidler

Menneskelige og tekniske feil og kombinasjoner av disse kan føre til at systemer og funksjoner svikter og at valget ikke kan gjennomføres effektivt. Feil og mangler kan også medføre redusert legitimitet ved at formalkrav ikke oppfylles.

Manglende kompetanse og feil i utførelse av gjennomføringen kan også svekke både tekniske og organisatoriske sikkerhetsbarrierer.

Feil i valggjennomføringen kan i betydelig grad svekke tillit til prosess og myndigheter.

Vurdering: Høy trussel

Barrierer og sårbarheter

Det foreligger til dels omfattende veiledningsmateriell og standarder, og tilgang til opplæring og rådgivning for kommunene som skal gjennomføre valget. Valgdirektoratet jobber aktivt med å videreføre, forbedre og styrke arbeidet med veiledning og opplæring. Både materiell og opplæring gis gode skussmål fra kommunene, og oppslutningen fremstår som stor. Imidlertid er hverken veiledninger eller opplæring obligatorisk for kommunene og valgmedarbeiderne, noe som gjør barrieren også mot feil mindre solid. Det er også en økende sårbarhet at krav til IT-utstyr og sikring av dette (i tråd med veiledninger) blir mer krevende kompetansemessig.

Valg gjennomføres kun over en periode hvert annet år, noe som gir utfordringer med å opparbeide og opprettholde kompetanse. I enkelte kommuner vil det være fast ansatte valgmedarbeidere, eller medarbeidere som ivaretar den samme oppgaven over flere år, mens det i mange kommuner vil være en oppgave som tilfaller funksjoner kun i valgperioden -og kanskje bare for ett enkelt valg. Dette kan øke sårbarheten for at det gjøres feil i valggjennomføringene.

Valgforum – som er kommunenes interesseorganisasjon knyttet til valg, har også etablert diskusjonsforum på Facebook der valgmedarbeidere kan utveksle erfaringer og gi hverandre råd knyttet til krav og gjennomføring. Et slikt forum kan være en styrkende barriere mot feil i gjennomføringen, men også en potensiell sårbarhet ved at det som kommuniseres ikke kvalitetssikres av myndighetene.

En viktig barriere mot feil er også høy grad av tillit til og respekt for de demokratiske prosessene i det norske samfunnet, noe som gjør at kommunene har høyt fokus på å sikre ivaretakelse av gjennomføringen.

Vurdering: Medium sårbarhet

Konsekvenser for krav til valgprosessen:				
Fri deltagelse	*Opplyst og informert*	*Korrekt*	*Gjennomføres som planlagt*	*Tillit*
		Kan påvirke korrekt gjennomføring/resultat – men vil trolig avdekkes og rettes opp pga. rutiner og parallelle prosesser/kontroller	Feil i valggjennomføringen kan medføre forsinkelser og mangler ved gjennomføringen	Svekker innbyggernes tiltro til myndigheter og valgprosess
Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Liten konsekvens	Noe konsekvens	Stor konsekvens

Kunnskapsstyrke	
Kjente utfordringer	Høy

Overførbarhet	
Gjelder i alle kommuner og sentralt	Høy

Endringshastighet	
Kompetansekrav til valgmedarbeidere vil være i stadig endring, spesielt med tanke på krav til IKT-sikkerhet	Middels

Oppsummering	
Samlet vurdering – Økende krav til kompetanse for å håndtere valg sikkert, feil kan få større konsekvenser	*Styrbarhet* – Både krav til kompetanse, personellsikkerhet og til rutiner og teknikk kan reguleres av myndighetene om ønskelig
Middels	Høy

Aktuelle tiltak

- Regulatoriske krav til:
  - Kompetanse for valgmedarbeidere
  - Personellsikkerhet for valgmedarbeidere
  - Oppsett, vedlikehold, oppbevaring og håndtering av utstyr og systemer involvert i valg
- Online rådgivningsstøtte til valgmedarbeidere 24/7
- Gode planer for beredskap/hendelseshåndtering ved feil
- Videreføring av utvikling av veiledningsmateriell og opplæring av valgmedarbeidere

20. Lav valgoppslutning

Hendelse/fenomen: Lav valgoppslutning

Beskrivelse

Lav valgoppslutning er et demokratisk problem, i større grad enn en sikkerhetsutfordring. Lav valgoppslutning er derimot ofte en negativ konsekvens av sikkerhetsutfordringer, og et resultat av at tilliten til myndigheter, demokratiske prosesser og valgsystemer svekkes.

En motivasjon for at eksempelvis enkelte statlige aktører kan «angripe» valg i Norge, vil være å svekke tillit, redusere oppslutning om valgprosessene og med dette undergrave demokratiet som styreform.

En av utfordringene knyttet til redusert valgdeltakelse ligger i legitimiteten av valget som representativ for folkets vilje, spesielt om valgoppslutning også blir utpreget forskjellig i ulike grupperinger/folkegrupper, aldersgrupper osv.

En samfunnstrend (om enn ikke utpreget i Norge per i dag) er økende grad av «utenforskap» der folkegrupper sanksjonerer/protesterer ved å blant annet ikke delta i de demokratiske prosessene.

Trusler/virkemidler

For de fleste av fenomenene som betraktes i denne utredningen, der bevisste aktører står bak et «angrep» på valget, vil redusert tillit og mulig redusert valgoppslutning være en mulig konsekvens når fenomenene realiseres. SE derfor beskrivelser underøvrige fenomener.

Vurdering: Høy trussel

Barrierer og sårbarheter

Høy tillit i samfunnet og til myndigheter og demokratiske prosesser er trolig den fremste barrieren i Norge mot redusert oppslutning om valget. I tillegg pekes det på en rekke eksisterende eller anbefalte barrierer i tilknytning til fenomener og hendelser som er diskutert; og tilsvarende for sårbarheter.

Vurdering: Medium sårbarhet

Konsekvenser for krav til valgprosessen:

Fri deltagelse	*Opplyst og informert*	*Korrekt*	*Gjennomføres som planlagt*	*Tillit*
Om hele grupper «melder seg ut» av demokratiske prosesser vil medlemmer ikke oppleve reell mulighet for deltakelse	«Utenforskap» og isolasjon i ekkokamre og grupperinger vil kunne hindre tilgang til bred informasjon			Om grupper melder seg ut og valgoppslutningen synker betydelig, vil valget miste sin legitimitet og tilliten til prosesser og myndigheter synke
Liten konsekvens	Liten konsekvens	Ingen/nesten ingen konsekvens	Ingen/nesten ingen konsekvens	Svært stor konsekvens

Kunnskapsstyrke

Kompleks problemstilling med mange faktorer	Middels

Overførbarhet	
Kan forekomme overalt	Høy
Endringshastighet	
Samfunnstrender i endring	Middels
Oppsummering	
Samlet vurdering – Høy valgdeltakelse er en grunnleggende forutsetning for demokratiske prosesser	*Styrbarhet* – Mange faktorer kan påvirkes, men i liten grad reguleres
Middels	Middels
Aktuelle tiltak	
Se beskrivelser under andre hendelser og fenomener.	

Vedlegg 3 Benyttet underlagsmateriale

I gjennomføringen av utredningen har gruppen benyttet en stor mengde ulike kilder og underlagsmateriale. Adresser/linker til en del av dette er samlet i vedlegget her, da gruppen vurderer at mye kan være av interesse for leserne også.

https://www.darkreading.com/vulnerabilities---threats/election-security-isnt-as-bad-as-people-think-/a/d-id/1333579

https://www.aftenposten.no/norge/i/k6oB/Svindlernes-falske-ID-er-blir-ikke-slettet

https://www.skatteetaten.no/person/folkeregister/om/modernisering/ny-informasjon/

https://www.vg.no/nyheter/innenriks/i/P3zq7e/store-utfordringer-kan-bruke-falske-dokumenter-for-aa-svindle-til-seg-foererkort

https://www.ffi.no/no/Rapporter/15-00811.pdf

https://www.rand.org/topics/information-operations.html

http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-08.pdf

https://www.brookings.edu/2018/10/19/the-real-security-threat-to-the-2018-midterm-elections-is-low-voter-confidence/

https://www.sciencedirect.com/science/article/pii/S1353485811701234

https://www.euractiv.com/section/global-europe/news/montenegro-hit-by-cyber-attacks-on-election-day/

https://www.forbes.com/sites/kalevleetaru/2018/11/08/estonias-online-voting-would-solve-a-lot-of-our-election-problems/

https://estoniaevoting.org/

https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

https://www.politico.eu/article/europe-cyber-sanctions-hoped-to-fend-off-election-hackers/

https://www.politico.eu/article/europe-most-hackable-election-voter-security-catalonia-european-parliament-disinformation/

https://www.securityweek.com/leap-cyber-attacks-against-elections-oecd-countries-canada

https://www.stiftung-nv.de/sites/default/files/securing_democracy_in_cyberspace.pdf

https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/election-cybersecurity-challenges-and-opportunities/view

https://www.csis.org/analysis/csis-election-cybersecurity-scorecard-outlook-2018-2020-and-beyond

http://aceproject.org/election-technology-and-cyber-security-standards

https://www.politico.eu/article/europe-most-hackable-election-voter-security-catalonia-european-parliament-disinformation/

https://news.microsoft.com/on-the-issues/videos/security-democracy-collaborating-on-election-security/

https://techcrunch.com/2018/08/24/facebook-microsoft-dhs-nass-nased-election-officials/?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=xgFEwHaEtP1fwzn_-M0lGA

https://www.technologyreview.com/s/611850/why-security-experts-hate-that-blockchain-voting-will-be-used-in-the-midterm-elections/

https://www.nap.edu/read/25120/chapter/4

https://www.nrk.no/hordaland/mangler-regler-for-politisk-nettreklame-1.14474786

https://www.digi.no/artikler/tor-ikke-frigi-ny-ai-algoritme-som-dikter-opp-historier-kan-lage-troverdige-falske-nyheter/458294?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter-2019-02-19

https://www.aftenposten.no/article/ap-qn926E.html

https://www.regjeringen.no/no/aktuelt/sikrer-to-uavhengige-opptellinger-ved-valg/id2629370/

https://www.idea.int/news-media/news/cybersecurity-and-elections-international-idea-round-table-summary

https://www.coe.int/en/web/electoral-management-bodies-conference/programme

https://cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process/page8

https://www.cyberscoop.com/secure-elections-act-reintroduced/

https://www.wired.com/story/secure-elections-budget-congress/

https://www.belfercenter.org/index.php/publication/state-and-local-election-cybersecurity-playbook

https://www.belfercenter.org/publication/election-cyber-incident-communications-coordination-guide

https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=3547&context=facpub

https://digitalcommons.wcupa.edu/cgi/viewcontent.cgi?article=1002&context=crimjust_facpub

https://www.politico.com/newsletters/morning-cybersecurity/2018/05/03/pennsylvania-experts-review-election-cybersecurity-202733

https://democrats-homeland.house.gov/news/press-releases/election-security-task-force-releases-final-report-recommendations

https://www.cisecurity.org/elections-resources/

https://www.defcon.org/images/defcon-25/Election%20Security%20White%20Paper_Praetz_12062017.pdf

https://motherboard.vice.com/en_us/article/kb7py9/this-is-why-we-still-cant-vote-online

https://www.ifes.org/sites/default/files/2018_heat_cybersecurity_in_elections.pdf

https://www.ria.ee/en/news/european-union-members-share-advice-cyber-security-elections.html

https://research.bournemouth.ac.uk/project/hybrid-warfare-and-election-meddling-assessing-the-digital-threat-to-democracy/

https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/NCSC%20-%20guidance%20for%20local%20authorities%20during%20the%20General%20Election_0.pdf

https://e-estonia.com/solutions/e-governance/i-voting/

https://motherboard.vice.com/en_us/article/gvyv34/how-secure-is-estonias-e-voting-system

https://www.bloomberg.com/news/articles/2017-06-14/germany-builds-an-election-firewall-to-fight-russian-hackers

https://www.kth.se/tcs/about-tcs/news-tcs/stora-brister-i-elektroniska-valsystem-1.298429

https://www.duo.uio.no/bitstream/handle/10852/52489/Risvik_Master.pdf?sequence=1

https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf

https://forsvaret.no/fakta_/ForsvaretDocuments/Fokus2018_bokmaal_oppslag_godkjent.pdf

https://www.pst.no/trusselvurdering-2018/

https://nsm.stat.no/aktuelt/risiko-2018/

https://norsis.no/trusler-trender-2017-18/

https://www.nsr-org.no/moerketall/

https://www.regjeringen.no/no/dep/kmd/org/styrer-rad-og-utvalg/valglovutvalget/mandat-for-valglovutvalget/id2577295/

https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

https://defcon.org/images/defcon-26/DEF%20CON%2026%20voting%20village%20report.pdf

https://www.pst.no/globalassets/artikler/trusselvurderinger/psts-trusselvurdering-2019.pdf

https://fr-ca.facebook.com/pg/ndebatt/posts/

https://www.nupi.no/Arrangementer/2017/Paavirkningsoperasjoner-og-desinformasjon-som-verdensfenomen

https://www.vg.no/nyheter/utenriks/i/0EdWdG/kina-vil-bli-supermakt-i-norske-farvann

https://forsvaret.no/fokus

https://www.pst.no/globalassets/artikler/trusselvurderinger/psts-trusselvurdering-2019.pdf

https://www.aftenposten.no/meninger/debatt/i/oRGkvK/Hva-er-en-klok-NATO-politikk-overfor-Russland--Julie-Wilhelmsen-og-Kristian-Lundby-Gjerde

https://www.ffi.no/no/Rapporter/18-00080.pdf

https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435

https://www.nupi.no/Skole/HHD-Artikler/2017/EU-kriser-aarsaker-og-muligheter

https://www.pst.no/globalassets/artikler/trusselvurderinger/psts-trusselvurdering-2019.pdf

https://forsvaret.no/fokus

https://www.nature.com/articles/s41599-019-0227-8

https://www.ffi.no/no/Rapporter/18-00080.pdf

https://www.ft.com/content/d8205ea0-3a6a-11e9-b72b-2c7f526ca5d0

https://www.rferl.org/a/eu-official-names-russia-as-main-disrupter-of-elections-in-europe/29600810.html

https://www.nrk.no/nyheter/cambridge-analytica-1.13973142

https://www.aftenposten.no/norge/politikk/i/RAVQW/Arbeiderpartiet-utsatt-for-hacker-angrep

https://www.recordedfuture.com/apt10-cyberespionage-campaign/

https://thehustle.co/dark-overlord-hacker-cybercrime-software-engineer-hiring/

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

https://www.symantec.com/content/en/us/home_homeoffice/media/pdf/norton_cybercrime_exposed_booklet.pdf

https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html

https://motherboard.vice.com/en_us/article/zmakk3/researchers-find-critical-backdoor-in-swiss-online-voting-system

https://www.politico.eu/article/europe-cyber-sanctions-hoped-to-fend-off-election-hackers/

Vedlegg 4 Analyse av Russland som dimensjonerende trusselaktør

Russland er en dimensjonerende aktør for Norge både med tanke på vår geografiske beliggenhet, internasjonale interesser, og Russlands kapasitet. Det er derfor gjort en grundigere analyse av Russland med tanke på intensjoner, virkemidler/metoder og kapasitet. Analysen er basert på åpne etterretningskilder

Analyse

Aktørene har en rekke virkemidler til disposisjon, men de mer ressurskrevende er det bare de statlige aktørene som kan ta i bruk. Virkemidlene er i hovedsak rettet inn mot informasjonsdomenet. Noen virkemidler rettes mot infrastruktur og fysiske objekter. Kort oppsummert kan man si at informasjonsdomenet vil benyttes for å påvirke meninger hos befolkning og mennesker i maktposisjoner. Informasjonen formidles på alle tenkelige plattformer og vil være fordreid for å oppnå avsenders målsetninger. Virkemidler som rettes mot objekter vil av natur være ødeleggende og tas i bruk for å sette objektet ut av funksjon. Dette kan typisk være cyberangrep mot valgutstyr, fysisk ødeleggelse av adkomstveier eller bygningsmasse eller angrep på mennesker.

Russland er uten tvil den viktigste aktøren som påvirker Norges forsvars- og sikkerhetspolitiske tenkning og handlinger. Dette er grunnet vår geostrategiske plassering og Norges nasjonale interesser i Arktis og Nordområdene, inkludert den sentrale betydningen av Svalbard. Det er derfor hensiktsmessig å se på de virkemidlene Russland benytter for å påvirke og øke innflytelse mot Norge.

Russland er langt viktigere for Norge enn Norge er for Russland i dette asymmetriske forholdet. Russland har i senere år økt sin militære aktivitet i Barentshavet og modernisert sitt forsvar i betydelig grad. For norske beslutningstagere skaper det betydelig bekymring om hva som er Moskvas intensjoner og planer som kan ramme Norges nasjonale strategiske interesser. Bekymringen skaper samtidig et stort rom for mistolkning og potensial for overdrivelser i forhold til tolkning av russisk aktivitet generelt. Dette bidrar til en sårbarhet på norsk side.[24]

En helhetlig virkemiddelbruk
Russland bruker alle statens virkemidler, som en integrert del av sin militære doktrine for å fremme og sikre Russlands forsvars- og sikkerhetspolitiske interesser. Dette har noe misvisende blitt omtalt som *hybridkrigføring* og er fremsatt som noe nytt, noe det ikke er. Russland har lang erfaring med å anvende konvensjonelle og ikke-konvensjonelle virkemidler for å sikre sine interesser og påvirke utvikling i Russlands favør enklest mulig og til minst mulig kostnad. Alle former for myk eller hard voldsmakt er helhetlig integrert i den russiske verktøykassa. Erfaringene og fremgangsmåten for Russlands evne og vilje til å bruke bredden av statens maktvirkemidler ble vel dokumentert under den kalde krigen.[25]

Formålet med virkemiddelbruken
Tema og sak kan være forskjellig fra tidligere, men metodene er langt på vei de samme som før. I dag bygger Russland et narrativ (en historie), der fakta ikke er viktig. Den fortalte historien er at:

Ingen kan stole på noen

[24] https://www.aftenposten.no/meninger/debatt/i/oRGkvK/Hva-er-en-klok-NATO-politikk-overfor-Russland--Julie-Wilhelmsen-og-Kristian-Lundby-Gjerde

[25] https://www.ffi.no/no/Rapporter/18-00080.pdf

Spredning av falske nyheter og propaganda synes generelt å være tonet noe ned til fordel for push- og biprodukter (spin-offs) som genereres av å fordreie informasjon som i utgangspunktet er sann eller delvis sann. Russland ønsker å fremstille liberaldemokratiet som udemokratisk, ved å påpeke at det er korrupt, ineffektivt, byråkratisk og kaotisk. Russland selger inn ideen om at Europa, inkludert Norden, mangler kompetanse og evne til å håndtere egne kriser som terrorisme og immigrasjonsstrømmer, og at Vestens statslederne i bunn og grunn er amerikanske nikkedukker. Hovedmålet er å splitte det nasjonale samholdet og undergrave offisielle versjoner av prosess i saker og hendelser.[26]

1. delmål
Russlands første delmål er å svekke USA og splitte NATO og EU for å begrense deres innflytelse i russisk strategisk sfære, og samtidig opprettholde intern politisk kontroll i Russland. Intern politisk kontroll opprettholdes gjennom en sterkt økt sentralisert politikk, hvor svært få har tilgang på reell makt utover Putins indre sirkel. Aktiviteten mot Vesten underbygges av en rekke eksempler:[27]

1 økt høyreekstremisme i europeiske partier, fremvekst av ekstreme høyrestrømninger i Europa og svekket støtte til EU;
2 Russlands økte lån på $11.7 millioner til det høyreekstreme partiet Nasjonal Front i Frankrike;
3 vold fra immigrasjonsmiljøer brukes som bevis på at regjeringene ikke har kontroll og ikke kan stoles på;
4 oppnåelsen av et mer lydhørt publikum til Russlands konservative, nasjonalistiske og autoritære styresett gjennom en rekke strategiske informasjonskampanjer;
5 europeisk og skandinavisk folkeopinion har delvis endret syn på EU, NATO og USA gjennom en rekke strategiske informasjonskampanjer.

2. delmål
Sekundært ønsker Russland å sette Vesten i dårligst mulig lys. Dette blir forsøkt oppnådd gjennom å portrettere Vesten som:[28]

- dekadent;
- arrogant mot andre kulturer;
- ustabilt;
- splittet;
- overfylt av ulovlige innvandrere;
- på randen av kollaps.

3. delmål
Russland ønsker seg nasjonalistiske, konservative og isolasjonistiske regjeringer i andre land, da disse antas å være mindre villige til å blande seg inn i Russlands interesser og indre anliggender. Målsettingen er å påvirke disse landenes politiske beslutningstaking i russisk favør og sikre innflytelse over nasjonalforsamlinger for å påvirke politikere til å oppheve sanksjoner mot Russland og generelt føre en mer russiskvennlig politikk.

Russland har aktivt forsøkt å påvirke valgprosesser og utfall av valg i USA, Nederland, Frankrike og Tyskland, samt å påvirke Brexit-diskusjonen i Storbritannia. Dette viser at Russland er villig til å ta politisk risiko og bære de politiske kostnadene som kommer med slik aktivitet. Det er p.t. uklart om Russland har

[26] https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435

[27] https://www.nupi.no/Skole/HHD-Artikler/2017/EU-kriser-aarsaker-og-muligheter

[28] https://www.pst.no/globalassets/artikler/trusselvurderinger/psts-trusselvurdering-2019.pdf

hatt noen substansiell rolle i påvirkning av valgprosessen i Sverige. Hensikten bak slik politisk krigføring er å polarisere den nasjonale debatten rundt demokratiet, svekke tilliten til demokratiet, påvirke befolkningens oppfatninger og disse landenes innenrikspolitiske persepsjon i russisk favør. Valgprosesser er i økende grad gjenstand for politisk manipulering.[29]

Innflytelses- og påvirkningsoperasjoner
Alle land driver med informasjonsoperasjoner og påvirkningskampanjer, så dette er ikke unikt for Russland.

Innflytelses- og påvirkningsoperasjoner er først og fremst billig, og det medfører begrenset risiko for den som utfører dem. De etterlater seg kaos og usikkerhet, noe som kan tjene Russlands interesser ved å tåkelegge andre politiske forhold som man ikke ønsker oppmerksomhet rundt. Russland forsøker å balansere legitim politisk påvirkning (åpen) og ulovlig politisk påvirkning (lukket).[30]

Virkemidlene i påvirkningsoperasjoner oppnår best resultat når de er helhetlige og integrerte. Samtidig er det krevende og vanskelig å styre utfallet av slike operasjoner, siden det er så mange faktorer som spiller inn på resultatet. Blant annet kan koordineringen av egne ressurser i operasjonen være mangefasettert og lide av mangel på enhetlig ledelse.

Det er svært vanskelig å finne håndfaste bevis på målrettede informasjons- og/eller påvirkningsoperasjoner, da de er nesten umulig å spore. Aktører har en høy grad av operasjonsbevissthet og de løper en begrenset risiko. Regelverk og internasjonal rett er ikke godt nok tilrettelagt for straffeforfølgelse i forhold til slike operasjoner. [31]

Den store nye variabelen i moderne tid er økte muligheter for cyberangrep, trollfabrikker, nettroll og hacking av kommunikasjonssystemer. Sabotasjepotensiale er enormt.[32]

Virkemidler
Virkemidler kan skreddersys og brukes sammen om hverandre og med åpent diplomati for størst mulig påvirkningseffekt. Virkemidlene som benyttes er[33]:

- konsistent historiefortelling (narrativ);
- STRATCOM – styrt kommunikasjon for å begrense avstanden mellom talehandling og annen handling;
- politisk dialog for å påvirke sak/prosess;
- propaganda;
- spredning av konspirasjonsteorier;
- etterretning;
- kartlegging av nettverk, fagmiljøer og kompetanse-/nøkkelpersoner;
- finansiering av partier og organisasjoner;
- betaling og korrumpering av nøkkelpersonell;
- massiv flyt av penger for å kjøpe støtte[34];
- utplassering av agenter i tenketanker og forskningsmiljø;

[29] https://forsvaret.no/fokus Etterretningstjenesten trusselvurdering Fokus, 2018, 2019.

[30] https://www.nature.com/articles/s41599-019-0227-8

[31] https://www.ffi.no/no/Rapporter/18-00080.pdf

[32] https://www.ft.com/content/d8205ea0-3a6a-11e9-b72b-2c7f526ca5d0

[33] Det kan være verd å merke seg at russiske Sputnik og RT på norsk måtte legges ned
[34] korrupsjon er trolig et større problem enn falsk informasjon og propagandaoperasjoner

- rekruttering av informanter gjennom sosiale media/annet, ofte under dekke av å være diplomat, student, forsker eller NGO-ansatt;
- cyberangrep på LinkedIn, Facebook, Instagram, Twitter o.l.;
- brev- og dokumentforfalskning;
- svertekampanjer, gjerne i sosiale media, uten at det er begrenset til det;
- trusler og utpressing.

Målgrupper
Russland jobber målrettet og langsiktig med sjarmoffensiver mot aktører og miljøer som er bitre eller i opposisjon til det liberale demokratiet. De prioriterer både ekstreme høyre- og venstremiljøer for å skape splid og usikkerhet. De viktigste målgruppene er:[35]

- politikere, ledere av ungdomspartier;
- embedsmenn, forsvarsansatte, politi;
- medlemmer av Nobelkomiteen o.l.;
- NGO-ansatte;
- journalister;
- advokater;
- tenketanker, forskningsmiljø;
- konsulenter;
- eiendomsmeglere;
- russisk diaspora, innflyttere fra tidligere sovjetrepublikker;
- ungdomsmiljøer.

Trusselbildet mot valg og demokrati i Norge
Det er ikke usannsynlig at Russland kan ha interesse av å påvirke valg og demokratiske prosesser i Norge i forbindelse med det forstående valget. Mest sannsynlig besitter de en mengde informasjon om norske politikere og det norske politiske systemet de kan bruke for å direkte eller indirekte påvirke politiske beslutningsprosesser, herunder valg.

Hovedårsaken til at trusselen mot Norge fra Russland i forhold til valg og demokratiske prosesser likevel trolig er begrenset, er først og fremt den dype konsensusen i norsk utenrikspolitikk. Uavhengig av hvilken sammensetning av partier man lander ned på etter et valg, vil ikke den norske utenrikspolitikken substansielt endre seg. Andre forhold er den høye tilliten nordmenn har til demokratiet og den korte avstanden mellom statsledere og befolkningen. I tillegg har Russland en mengde aktører og saker som har langt høyere prioritet enn Norge.[36]

Dette til tross, det er flere sårbarheter som kan motivere russisk vilje og interesse av å true det norske valget og de demokratiske prosessene:

- den bilaterale dialogen mellom Norge og Russland er på frysepunktet;
- samarbeidet mellom USA og Norge kan i sum gi Russland incentiv til å angripe den nordiske styresettformen, ved gjennom valg å svekke tilliten til den nordiske politiske modellen. Russland kan undergrave tilliten, for derigjennom å forsinke eller så tvil om beslutningsprosesser på norsk side. Dette kan skje ved å skade eller å søke å påvirke personer, konkrete saker eller prosesser;
- det norske folks iboende tillit til de demokratiske prosessene, og derigjennom en mulig naivitet, kan forenkle et angrep;
- den lave sikkerhetspolitiske interessen blant folk flest og norske politikkere spesielt;

[35] https://www.rferl.org/a/eu-official-names-russia-as-main-disrupter-of-elections-in-europe/29600810.html

[36] https://www.pst.no/globalassets/artikler/trusselvurderinger/psts-trusselvurdering-2019.pdf

- den svake og til dels naive norske sikkerhetskulturen;
- det generelt lave kunnskapsnivået om nordområdepolitikk, og derigjennom muligheten for politisk splittelse om konfliktområder, herunder Svalbard. Norsk nordområdepolitikk er på kryssende kurs med en rekke nære internasjonale samarbeidspartnere, og det gir et økt rom for feiltolkninger og misforståelser i et mer spisset geopolitisk klima. Norge oppfattes i økende grad som mindre Russlandsvennlig og en pådriver for økt vestlig militær aktivitet i Nordområdene;
- den store distansen mellom den norske sentralmakten sentrert rundt det sentrale Østlandet og befolkningen i Nord-Troms og Finnmark gjør gjensidig forståelse og effektiv kommunikasjon vanskelig. Sentralmakten har behov for å forstå de forhold som eksisterer både lokalt og opp mot Russland. Samtidig har lokalbefolkningen behov for relevant styring og understøttelse fra politisk hold. Et svært godt eksempel på hvor vanskelig det er å bygge ned barrierer og oppnå økt gjensidig forståelse, så man i den nylige regionsdebatten. Samtidig foregår det lokalt et tett samarbeid med russisk næringsliv og befolkning. Kulturforståelsen er langt bedre og kommunikasjonen flyter langt lettere enn mot sentralmakten i Oslo. Denne sårbarheten får økt effekt gjennom et lavt folketall i Nord-Troms og Finnmark, der et mindre antall opinionsbærere kan nå frem til et stort prosentantall av befolkningen.

Forhold som kan medføre russisk påvirkning og trusler

- NATOs ballistiske missilforsvar;
- forskning på atomvåpen og ballistiske missiler;
- basepolitikken;
- amerikanske og allierte militære øvelser i Norge;
- F-35 Lightning II;
- bygging av etterretningsradar i Vardø;
- digitalt grenseforsvar;
- manglende norsk militær avskrekkingsevne;
- kritisk infrastruktur;
- utvikling på og av Svalbard;
- norsk våpenteknologi;
- norsk maritim teknologi;
- fiskeri;
- havrett og konflikter over rettigheter;
- energi- og petroleumssektoren;
- utvikling i og av NATO;
- økt militær aktivitet i Nordområdene.