Fagfellevurdert

Internasjonal POLITIKK
Skandinavisk tidsskrift for Internasjonale Studier

Årgang 80, Nummer 1, side 53–77, 2022, ISSN 1891-1757, www.tidsskriftet-ip.no, Publisert februar 2022

Kommersiell sporing – nasjonal risiko

Vivi Ringnes Wilhelmsen*
Institutt for forsvarsstudier, Forsvarets høgskole, Norge

Sammendrag

Omfattende kommersiell datasporing og salg av svært detaljerte digitale profiler for markedsføring kan utnyttes og manipuleres av fremmede makter for spionasje, sabotasje og *subversion*. Datasettenes digitale natur medfører større detaljgrad, maskinlesbarhet optimalisert for automatisering, lange tidsserier, sanntidspotensial og mindre ressurskrevende datainnhenting sammenlignet med analoge metoder. Et globalt, uoversiktlig datamarked er sårbart for dataangrep og manglende verdikjedekontroll. Påstått anonymisering er ikke tilfredsstillende, og økt lagrings- og prosesseringskraft gjør datasettene stadig mer sårbare for reidentifikasjon. Samfunnsdigitalisering, smarte enheter og overvåkningskapitalismen intensiverer og forenkler inntrengningen i den private sfære. Morgendagens ledere kan i teorien spores fra vugge til grav, den store datamengden kan utlede informasjon som burde være gradert. Overvåkningskapitalismen, i kombinasjon med åpenhetens dilemma, tilsier at store datamengder i fri dressur derfor bør være en kilde til bekymring. Samlet vil de strategiske effektene av persondata kunne få potensielle konsekvenser for både samfunns- og statssikkerheten. I det digitale rom blir derfor personvernsikkerhetsdilemma en falsk dikotomi. En demokratisk stat vil aldri kunne kontrollere borgernes totale digitale liv. Stadig økt overvåkning vil alltid møte kritikk knyttet til at det utfordrer demokratiske prinsipper. Og statens overvåkningsmonopol er utfordret. Artikkelen konkluderer derfor med at vi i større grad bør anse personvern som et kollektivt anliggende, og at sterk personvernlovgivning kan være et verktøy for nasjonal sikkerhet.

Nøkkelord: overvåkningskapitalisme · kommersiell data · etterretning · nasjonal sikkerhet · påvirkningsoperasjoner · personvern

*Kontaktinformasjon: Vivi Ringnes Wilhelmsen, e-post: vwilhelmsen@mil.no

Citation: Wilhelmsen, V. R. (2022). Kommersiell sporing – nasjonal risiko. Internasjonal Politikk, 80(1), 53–77. http://dx.doi.org/10.23865/intpol.v80.3096

Innledning

I 2020 avdekket Forbrukerrådet at sjekkeappen Grindr, «verdens største sosiale nettverksapp for homofile, lesbiske, transpersoner og skeive», solgte brukerinformasjon til tredjeparter uten brukernes viten (Forbrukerrådet, 2020; NTB, 2019). Amerikanske sikkerhetsmyndigheter advarte da om at "*the personal data it collects could be exploited by Beijing to blackmail individuals with security clearances*" (NTB, 2019; Wells & O'Keeffe, 2019). Et datainnbrudd hos et selskap affiliert med det amerikanske republikanske parti, som sammenstilte kommersielt innhentet data for markedsføringsformål, eksponerte 200 millioner amerikaneres antatte religiøse tilknytning, etnisitet, politiske overbevisning og holdning til kontroversielle temaer som våpenpolitikk, abortrettigheter og stamcelleforskning (Borgesius et al., 2018, s. 87). Studenter ved Harvard har kombinert datasett fra kommersielle datatilbydere og det mørke nettet for å identifisere nærmere 1000 personer som har digitale profiler på utroskapsnettsider og er sårbare for utpressing da de er gifte, har barn og høy inntekt. En annen gruppe sammenstilte kredittvurdering, kontaktinformasjon og hjemmeadresser for flere høytstående politikere (Dawson, 2021, s. 70).[1]

Den følgende artikkelen ønsker å belyse hvorfor dette er av bekymring langt forbi personvern og den enkeltes kontroll over egen informasjon. Kommersielt innsamlet data kan billig og effektivt evalueres og manipuleres av de som vil kartlegge norske sivilsamfunn, gjennomføre inntrengingsforsøk i digitale strukturer, identifisere nøkkelpersonells sårbarheter, eller påvirke og undergrave vårt nasjonale fellesskap slik at vi står svakere i en krise eller konflikt.

Spionasje, desinformasjon og påvirkningsoperasjoner levde i beste velgående i den analoge verden. Men tilgang på rådata var en ressurskrevende prosess med åpenbar sårbarhet for agenters sikkerhet, feilslutninger og skjeve datagrunnlag. I løpet av de to siste tiårenes digitale revolusjon har nordmenns liv derimot flyttet inn på internett. Stadig flere av våre intime interaksjoner finner sted i det digitale rom – vær det med romantisk partner, sosialt nettverk, frivilligheten eller forvaltningen. Dataavtrykket vårt kan brukes til å optimalisere formidling og tjenester, avlede verdifull informasjon om for eksempel infrastruktur og sykdomsspredning, tilrettelegge for ytringsfrihet og knytte mennesker sammen på tvers av landegrenser. Høyverdige mål, men innsikt i enkeltpersoners mottagelighet for påvirkning samt kartlegging av holdning og atferdsmønstre, er også informasjon som kan misbrukes. Og drivkraften er våre digitale fotavtrykk, altså registrering og analyse av digitale handlinger.

Parallelt med den såkalte digitale revolusjon, har det globale trusselbildet endret seg. Det er i skrivende stund tyve år siden angrepet på World Trade Center og den påfølgende krigen mot terror. Solo-terrorister rekruttert og opplært i internettforum,

[1] I tillegg kommer datainnbrudd hos offentlig forvaltning. Datainnbruddet i Østre Toten kommune ga f.eks. uautorisert tilgang til systemer for barnevern, sosialhjelp, helseinformasjon, personnummer og bankkonto (NorSIS, 2021; Østre Toten kommune, 2021). Denne informasjonen er bekreftet lagt ut på det mørke nettet.

media-savvy[2] organisasjoner som IS, globale pedofilinettverk, samt bekymring for «konspirasjonsfabrikker» og ekkokamre, har bidratt til et økende fokus på internettets tveeggete natur. Gjerne da i forbindelse med *hybride trusler*. At alle får tilgang til globale plattformer, inviterer nye stemmer inn og kan forbedre informasjonsflyt. Men den samme mangelen på «portvoktere» (som redaktøransvar) forenkler spredning av ulovlig, ondsinnet eller skadelig informasjon. Politiets sikkerhetstjeneste (PST) og Etterretningstjenestens årlige trusselvurderinger har for eksempel de senere årene fremhevet etterretning mot enkeltpersoner og grupperinger, påvirkningsoperasjoner, nettverksoperasjoner og kilderekruttering som trusler mot grunnleggende nasjonale interesser, med flere henvisninger til den digitale dimensjonen (Etterretningstjenesten, 2019, 2020, 2021; Politiets sikkerhetstjeneste, 2019, 2020, 2021).

En retorisk forlengelse av en digitalisert trusselforståelse med globale forgreininger resulterer i argumentasjon om at nasjonale sikkerhetsmyndigheter må ha tilgang til mer informasjon om hva som skjer i det digitale rom. Argumentasjonen baserer seg i logikken at mer data gir et bedre kunnskapsgrunnlag. Terminologisk kan dette omtales som personvern-sikkerhetsdilemma, hvor borgerne tillater (bytter) økt statlig overvåkning for å gjøre samfunnet tryggere.[3] Data blir dermed en verdifull ressurs, en betaling den enkelte veksler mot bedre politikk eller beskyttelse. Vi så denne tendensen senest i debatt om ny lov om Etterretningstjenesten (Bakke-Jensen, 2020; Datatilsynet, 2019a; Wilhelmsen, 2019), sporingsappene Smittestopp 1 og 2 (Nordal, 2020) og Operasjon Trojan Shield (Kolsrud, 2021; Skille & Holm-Nilsen, 2021). Muligens vil et foreslått forbud mot bistand til påvirkningsvirksomhet og mulig utvidelse av PSTs lagring av åpne kilder, føre til en tilsvarende debatt (se for eksempel Døvik & Skille, 2021; Justis- og beredskapsdepartementet, 2021; Kollsrud, 2021; Langemyr, 2021).

Med stadig mer gjennomsyrende digitale tjenester, har plattformtilbydernes (ofte omtalt som *Big Tech*) forretningsmodell og økonomiske muskler også fått økt oppmerksomhet.[4] Den såkalte *overvåkningskapitalismen*, et begrep attribuert til Soshana Zuboff (2015, 2020), beskriver et markedssystem hvor persondata byttes mot adgang til digitale tjenester. Datagrunnlaget brukes så for å skreddersy annonsering og eksponering[5] som en direkte konsekvens av (antatt) personlighet, interesser, livssituasjon, nettverk og så videre. Insentivet blir et stadig mer finmasket

[2] Altså kompetanse på bruk av medieteknikker og kommunikasjonsflater for å skape oppmerksomhet om egen agenda og handlinger.

[3] Versjoner av daværende president Clintons lignelse mellom kryptering og et tveegget sverd, hvor beskyttelse av lovlydige borgere blir et skjold for terrorister og kriminelle, gir gjenklang i en rekke av dagens overvåkningsdebatter.

[4] Det er slående hvilket stemningsskifte plattformer som Facebook har gjennomgått fra den arabiske våren (hvor Facebook ble omtalt som tilrettelegger og demokratisk motor) til i dag (hvor fokus primært er på monopolmakt, manglende beskyttelse av menneskerettigheter (f.eks. rohingyaene i Myanmar), verktøy for påvirkningsoperasjoner (som USAs presidentvalg 2016) og kommersiell overvåkning og manipulasjon (som er fokus i denne artikkelen).

[5] Eksponering vil si hvilket innhold mottager introduseres for, ofte via reklamebannere.

datamateriale i den tro at mer data gir høyere grad av individualisering, som igjen resulterer i bedre gjennomslag for et produkt, en tjeneste eller et (politisk) budskap. I tillegg til de store teknologigigantene, er driveren i denne datahøstingen et såkalt tredjepartsmarked hvor mindre aktører kan profitere på å mate sin informasjon inn i en global databørs. Konsekvensen blir et globalt sammensurium av dataleverandører (kilder), -formidlere og -konsumenter som alle supplerer til sporing av den enkeltes atferd og preferanser med varierende kvalitet på anonymisering og beskyttelse.

Det store dataomfanget har i flere tilfeller vist seg å kunne gi inngripende informasjon om både enkeltindivider og gruppers gjøren og laden. Dette har åpenbare likheter med det Nasjonal sikkerhetsmyndighet (NSM) omtaler som *åpenhetens dilemma:* verdien vi tilskriver et åpent samfunn kan svekke vår felles sikkerhet fordi omfanget og sammenkobling av informasjon kan avdekke innsikt som burde konstituert gradering og kan deretter «*benyttes for å planlegge og gjennomføre sikkerhetstruende virksomhet mot Norge og norske interesser*» (NSM, 2020 s. 31).

Alle offentlige strategier tilsier at Norge skal forbli et foregangsland i digitalisering av samfunn og borgernes hverdag. Dette kan gi mange goder, som optimalisering av (offentlige) tjenester og nye forretningsideer. Men digitalisering er et tveegget sverd, og våre digitale liv leves ikke i et vakuum. Som et av verdens mest digitaliserte land, er Norge sannsynligvis et av de landene som er mest sårbare for datalekkasje og potensielle konsekvenser for statssikkerheten.[6]

Denne artikkelen argumenterer for at åpenhetens dilemma i møte med overvåkningskapitalismen, utfordrer statens tradisjonelle overvåkningsmonopol og dermed også personvernsikkerhetsdilemmaet. Kommersiell digital overvåkning har blitt så omfattende at det medfører en stor datalekkasje inn i et uoversiktlig, globalt marked. Artikkelen vil vise eksempler på hvordan data har blitt anvendt for etterretning og sporing av enkeltpersoner, tilrettelegging for dataangrep, kartlegging av skjermede lokalisasjoner, samt som et verktøy i påvirkningsoperasjoner rettet mot grupper. Kimen til bekymring er altså at manglende datakontroll kan bli en akselerator. Fantasi og kreativitet tilsier at vi stadig vil finne nye bruksområder for billige, tilgjengelige og gjenbrukbare datasett. Hverken kontroll over globale kommersielle tilbyderes forretninger eller borgernes digitale liv er realistisk. Dermed bør personvernlovgiving,

[6] Dette fremheves fordi man kan argumentere for at våre egne sikkerhetstjenester kan ha nytte av datasettene i sitt arbeid. Både internett og personvernlovgivningens globale natur vil sette rammevilkår for norsk handlingsrom. Og det som skjer internasjonalt, vil få ringvirkninger i Norge. Eksempelvis kan man trekke frem vanskeligheten med filtrering av norsk informasjon under tilrettelagt innhenting og gammel personvernlovgivning versus GDPR. Man kan dermed stille det betimelige spørsmålet om sterkere personvernlovgivning vil svekke tjenestenes kunnskapstilgang. Det er en viktig diskusjon å ta, men da denne artikkelen primært adresserer norsk datalekkasje, er det utenfor tekstens omfang. Som et av verdens mest digitaliserte land, og med strengt regulerte sikkerhetstjenester, kan man også diskutere om de risiko den norske sårbarheten og angrepsflaten representerer, oppveier for en gevinst våre egne tjenester kan oppnå.

ledet av et tydelig føre-var-prinsipp og helhetlig risikoforståelse, heller anses som et kollektivt sikkerhetsverktøy enn en forvaltningsmessig tvangstrøye.

Teksten er strukturert som følger: Først vil artikkelen gjennomgå hva data er og hvordan kommersiell sporings insentiv er å samle mest mulig data. Her er det nødvendig å gå i noe detalj for å sikre leseren det nødvendige kunnskapsgrunnlaget til å vurdere de påfølgende argument. Så vil artikkelen belyse hvorfor påstått anonymisering av data i mange tilfeller er en illusjon, og dermed ikke tilbyr den påståtte skjerming. Deretter vil analysen vise hvordan kommersiell data kan utnyttes og manipuleres i den grad at det kan få strategiske effekter for nasjonal sikkerhet. Artikkelen viser at datasettene kan anvendes som «bensin» for cyberoperasjoner slik de kategoriseres av Thomas Rid (*espionage*, *sabotage* og *subversion*) og Ben Buchanan (*spionasje*, *angrep* og *detabilisering*) (Buchanan, 2020; Rid, 2013). Avslutningsvis argumenterer artikkelen for at omfattende digitale sporing, med påfølgende salg av inngripende innsikt i enkeltpersoners liv, påtvinger en revisjon av den etablerte forståelsen av personvern og overvåkning som motstående poler i sikkerhetsdebatten.

Hva er data og kommersiell sporing?

En cyberoffiser ved Jørstadmoen oppsummerer godt i sitt NRK-sitat våren 2020: «Der ligger såpass mye innebygget i både iPhone og andre dingser at det ikke er lett å ha kontroll [på hvilken data som samles inn]» (Gundersen et al., 2020).

Digital data er et mangesidig begrep, som brukes i en rekke betydninger. Busby et al. (2012, referert i Christl & Spiekerman, 2016, s. 84) deler data inn i frivillig, observert og analysedata basert på innsamlingsmetoden. Data kan diskuteres basert på type (f.eks. persondata versus metadata, gjerne beskrevet som *data om data*), hvem som har innhentet data (primær-, sekundær- og tredjepartsdata), eller i hvilken grad den er behandlet, hvilke kilder som sammenstilles, eller hva data kan brukes til (f.eks. kartlegging, prediksjon, mønstergjenkjenning, identifikasjon av uteliggere). Felles for alle subgrupperingene er at informasjon samles, lagres og (skal) anvendes i aggregert eller ikke-aggregert format for å informere om en person eller et fenomen. Når datapunkter systematisk samstilles for analyse eller videre sammenkobling med andre kilder, omtales det her som datasett.

Digitalisering, særlig etter inntoget av sosiale medier, har skapt historiske mengder data om den enkeltes atferd og interesser. Data kan samles i lange tidsserier, kan effektivt digitalt prosesseres, og krever betraktelig mindre lagringsplass enn analoge kilder. Materialet er også mindre hemmet av ønske om å presentere en idealisert versjon av oss selv, og antall kilder er betraktelig større enn ved tradisjonell tekstproduksjon (Park, 2014, s. 2).

Rent teknisk er digital sporing ikke spesielt sofistikert. Det er omfanget og informasjonsdelingen som er utfordrende, da dagens digitale sporing, eller overvåkning, går langt forbi annonsevirksomhet. Den mest allment kjente sporingen på nett,

cookies, er små tekstbiter implementert i nettsider for å huske tidligere besøk, brukerpreferanser (språk eller oppløsning) eller lignende (som varer i en handlekurv). De fleste digitale brukere i Europa har nok trykket en form for samtykkeerklæring hvor de godkjenner at «vi husker deg slik at du skal få en bedre brukeropplevelse». Avhengig av hvordan samtykkeerklæringen er utformet, ser man også opplistet samarbeidspartnere som er til stede på en enkelt nettside. For eksempel er Google Analytics mye brukt for å samle data om brukeropplevelse og -atferd.[7] Facebook Pixel, en vanlig funksjonalitet på nettider, tilrettelegger for sporing på tvers av nettsider, plattformer, enheter og apper. Facebooks populære Software Development Kits (SDK), en slags hyllevare for apputviklere, har informasjonsdeling som standard og deler til dels sensitiv informasjon som seksuell orientering (Forbrukerrådet, 2020, s. 122). Individuell informasjonskontroll blir tilnærmet umulig, når Egan (2019) viser at gjennomsnittspersonen har rundt 80 apper på sin smarttelefon, hvis forretningsmodell oftest funderes i videresalg av data. Gjennom mobile ID-nummer og annonse-ID kan man bygge en kontinuerlig digital profil på tvers av det interaksjon, nettside eller informasjonssøk.

Overvåkningskapitalisme og *surveillance by design*

Overvåkningskapitalisme, som beskrevet innledningsvis, er en nyttig terminologi for å beskrive hvordan stadig mer finmasket digital sporing har blitt den økonomiske motoren i det digitale økosystemet (se f.eks. Amnesty International, 2019; Forbrukerrådet, 2020; Silverman, 2017; Zuboff, 2015, 2020). Forretningsmodellen til teknologigiganter som Google, Apple, Facebook, Baidu, Alibaba og Tecent funderes alle i lovnaden om å nå den rette mottageren i sitt mest mottagelige øyeblikk. Google og Facebook genererer for eksempel henholdsvis 84 % og 98 % av sine inntekter fra datadrevet innsiktsformidling (Perrin & Verna, 2019). Å kalle dem sosiale *plattformer* kan dermed anses som misvisende, da denne ordbruken indikerer en nøytral tilrettelegger uten egen, aktiv handling.

Tredjepartsmarkedet, med såkalte dataforhandlere og -tilbydere, tilrettelegger for kapitalisering på datainnsamlingen gjennom identifikasjon av mulige innganger for markedsføring eller for optimalisering av eget produkt med påfølgende markedsandeler. Allerede i 2013 anslo en høring i Senate Committee on Commerce, Science and Transportation at mellom 3500 og 4000 selskaper globalt kan anses som tredjepartsaktører (Dixon, 2013). Selskapene samkjører datasett fra primærkilder som offentlige registre, sosiale medier, kundeklubber, spørreundersøkelser, apper og søkehistorikk før datainnsikten videreformidles i segmenter basert på opp til tusenvis av karakteristika. I et internasjonalt kommersielt annonsemarked

[7] En full gjennomgang av innsamlingsmetoder er utenfor denne artikkelens mulighet, og påfølgende eksempler er derfor kun ment som illustrasjoner på noen av metodene som brukes for datafangst.

samles og formidles så omfattende datasett med stor detaljgrad (se f.eks. Amnesty International, 2019; Christl & Spiekerman, 2016; Dawson, 2021; Forbrukerrådet, 2020; Gundersen, 2020a; Nordal, 2020; Tweetman & Bergmanis-Korats, 2020; Zuboff, 2015). Og «mer-innsikten» generert ved sammenkoblingen selges så til en rekke aktører, som igjen kan sammenstille datasett til en helhetlig onlineprofil ut ifra egne strategiske mål (Christl & Spiekerman, 2016, s. 91–92).

Den digitale profilen oppdateres altså hyppig og fra flere kilder. Amnesty International (2019, s. 16) har vist at Googles operativsystem Android, med over 2,5 milliarder brukere, deler 900 datapunkter per døgn, inkludert lokalisasjonsdata.[8] En 2016-studie fant at informasjon ble delt på tvers i 60 % av verdens 1000 mest populære nettsider (Englehardt & Narayanan, 2016, s. 11). Teknologirådet rapporterte samme år at det i gjennomsnitt er 46 tredjepartsaktører til stede på norske nettaviser, og at mellom 100 og 200 informasjonskapsler samler data om besøkendes atferd (Barland, 2016). Forbrukerrådet (2020, s. 17) viser at appene i snitt videreformidler informasjon til ti tredjepartsaktører. Og Binns et al. (2018, s. 8) finner at en av ti apper sender data til mer enn en lokalisasjon. Betaling for applikasjoner er heller ingen garanti for mindre sporing. I 2015 fant en studie av populære apper i Australia, Brasil, Tyskland og ISA at brorparten av gratis (95 %) og kjøpte (66 %) apper deler personinformasjon med tredjeparter (Seneviratne et al., 2015, s. 17).

De digitale profilene prises etter omfang og hvor sikkert den kan knyttes til en unik ID. Det økonomiske insentivet er dermed å innhente så mye informasjon som mulig, og så nært knyttet opp til et individ som lovlig. Axciom, en av verdens største dataforhandlere, hevder for eksempel å inneha profiler på alle amerikanere samt 2,5 milliarder mennesker i 60 land (Nadler et al., 2018, s. 11). I eget markedsføringsmateriell tilbyr de kunder tilgang til en online database som dekker 65 % av verdens digitale populasjon, katalogisert med over 10 000 attributter (karakteristika) for å «allow the brands to build a complete view of the consumer» (Acxiom, 2020).[9] Et annet viktig moment er at datadrevet innsikt overføres innad i nettverk og på tvers av grupper med lignende karakteristika. Det etableres såkalte «speilpublikum» som også kan generere innsikt om personer som har valgt å stå utenfor en tjeneste (som Facebook), hvor maskinlære bruker stratifisert utvelgelse for å overføre detaljert innsikt mellom mennesker som deler gitte variabler (Hareide, 2021, s. 12). I tillegg anvendes data om og fra ditt nettverk (som familie, kollegaer og venner). Den enkeltes dataavtrykk er derfor langt utenfor den enkeltes kontroll.[10]

[8] Tallet er basert på analyser når telefonen ikke er i bruk, så det faktiske antallet kan være betraktelig høyere.

[9] Åpenbart bør slik selvpromotering behandles med nødvendig skepsis, men at såpass omfattende datasett tilbys enhver som vil betale, bør være en kime til bekymring.

[10] Overførbarheten i de store datasettene medfører også at den enkeltes personvernspreferanser og datakontroll mindre relevant, noe som er et sentralt element når man diskuterer personvern som en individuell preferanse.

I hvilken grad modelleringen er vellykket, vil selvfølgelig variere avhengig av datasammenstillingen og metodikk. Men fordi atferd og preferanser predikeres gjennom nettverkseffekter og ved hjelp av utvalgsmodellering fundert i svært store datasett basert på en stor populasjon, er det høy sannsynlighet for at trender og tendenser kan identifiseres.

Anonymitet er en (u)beleilig illusjon

Datasett er oftest anonymisert gjennom fjerning av direkte identifikatorer som navn og e-postadresser. I mange tilfeller er det derfor mer korrekt å snakke om en *pseudonymisering.*[11] Ofte baserer reidentifisering seg på en kjent, statistisk risiko: datamaterialet blir så finmasket at anonymiteten ikke blir reell. Som ulike kombinasjoner av kjønn, alder, antall barn inkludert deres kjønn og alder, sivil status, interesser, type digitalt utstyr og dennes karakteristika, bosted og bostedstype, og så videre. Journalister benyttet for eksempel reidentifisering for å avdekke Donald Trumps 1985–1994 selvangivelser (Brogan, 2019). Og her kommer vi til kjernen i hvorfor anonymisering i beste fall er en luftspeiling. Rocher et al. (2019) har gjennom enkel maskinlære korrekt identifisert hele 99,98 % av enkeltindivider i en milliardpopulasjon, til tross for at datasettene bestod av standard informasjon, var ukomplett, og anonymisert. Oppsummert konkluderer forskerne ved Imperial College med at:

> Companies and governments have downplayed the risk of re-identification […]. Our findings […] demonstrate that an attacker could easily and accurately estimate the likelihood that the record they found belongs to the person they are looking for. (Sitert i Brogan, 2019)

Det er en åpenbar logisk brist i at anonyme data skal resultere i et individualisert, skreddersydd budskap eller brukeropplevelse. Uavhengig av om budskapet er et kommersielt produkt, politisk informasjon eller en konspirasjonsteori, forutsetter såkalt *personalisering* innsikt i livssituasjon, interesser og/eller trykkpunkter. Og underlaget til denne personaliseringen, innsikten i brukernes liv, avgjør verdisettingen av kommersielle plattformer som Facebook, Google og Amazon. Hal Varian, Googles sjefsøkonom, siteres for eksempel med at selskapets strategiske mål er at «vi skal vite hva du ønsker og gi deg det før du ber om det» (sitert i Hareide, 2021, s. 13).

En annen effektiv – og litt tabloid – måte å av-anonymisere data, er ved hjelp av lokalisasjonsdata. Altså, datapunkter som med korte intervaller forteller hvor en person (hens smarttelefon) befinner seg. Dette er en grunnleggende funksjonalitet i

[11] Datatilsynet definerer pseudonymisering som «Å avidentifisere personopplysninger slik at de ikke kan knyttes til en bestemt person uten bruk av tilleggsopplysninger (for eksempel en koblingsnøkkel) som lagres adskilt og tilstrekkelig sikkert. Pseudonymiserte personopplysninger er ikke anonyme».

mange apper. De fleste mennesker beveger seg primært mellom et par lokalisasjoner, og tilgang gir dermed grunnlag for enkel identifikasjon gjennom åpne kilder. Ved hjelp av fire lokalisasjonspunkter, kunne forskere identifisere 95 % av enkeltmennesker (Forbrukerrådet, 2020, s. 83). Skjermet militært personell, kadetter på øvelse, statsråder og USAs president Donald Trump, er alle blitt sporet av journalister gjennom lokalisasjonsdata (se f.eks. Furuly et al., 2020; Gundersen, 2020a, 2021; Gundersen et al., 2020; Karlsen, 2019; Vigsnæs & Kjelland-Mørdre, 2019; Thompson & Werzel, 2019; Aale, 2019). Geo-fencing («en digital innhegning») benytter samme metodikk, men tar utgangspunkt i en spesifisert geografisk lokalisasjon, som en militærleir eller Stortinget, og identifiserer enheter (og deres eiere) innenfor innhegningen. Deretter kan man forfølge eierne av gitte enheters bevegelsesmønstre og atferd i det digitale rom. *The New York Times* brukte eksempelvis kun minutter på å kartlegge nøkkelpersonell i CIA og NSA gjennom lokalisasjonsdata samlet på parkeringsplassen (Thompson & Werzel, 2019). Deretter identifiserte de hjemmeadresser, familier og nettverk. Paul Ohm, jusprofessor ved Georgetown University, slår fast at «Really precise, longitudinal geolocation information is absolutely impossible to anonymize. DNA is probably the only thing that's harder to anonymize than precise geolocation information» (sitert i Thompson & Werzel, 2019).

Kommersiell data, etterretning og påvirkningsoperasjoner

> *The best advertising captures people's attention, change their perception and prompts them to take action*. (Googles markedsføringsmateriell, sitert i Nadler et al., 2018, s. 10)

Grunnmuren i den kommersielt forankrede overvåkningskapitalismen er profilering, altså (automatisert) identifikasjon av enkeltmenneskers statusmarkører og atferd i store datamengder. Til sammenligning stadfester Bigo et al. (2013) at hensikten med automatisert etterretning (*automated intelligence*) for nasjonal sikkerhet er «*to detect suspicious behaviour of individuals within a large group of citizens*» (Verhelst et al., 2020, s. 2). Sitatene illustrerer en lik mentalitet i troen på at automatisert sammenkobling og analyse av store datasett kan utlede merinnsikt i et individs atferd. Og i forlengelse hvordan denne kan påvirkes.

Bonfanti (2018, s. 110–111) beskriver *cyber intelligence* som informasjon anskaffet via eller som stammer fra cyberspace, i tillegg til informasjon som informerer om cyberrelaterte tema. Det er altså ikke en forutsetning at informasjonen skal være lovlig innhentet. Dette er et viktig poeng i denne artikkelen, da et svartebørsmarked, med anslått verdi på 1,5 milliarder amerikanske dollar, formidler datasett med svært sensitiv informasjon vedrørende identifiserbare enkeltpersoner.[12] Mye stammer fra

[12] De økonomiske overslagene for svartebørsmarkedet er usikre. Såkalte *Fullz, «the motherload of personal data on an individual»*, har en kostpris på mellom 17 og 60 dollar.

datainnbrudd hos kommersielle tilbydere og offentlige institusjoner med påfølgende salg. Etter datainnbruddet i Østre Toten kommune bekreftet for eksempel både kommunen selv og NorSIS at data var lagt ut for salg på svartebørs, og at denne kunne misbrukes for utpressing, ID-tyveri e.l. (NorSIS, 2021; Østre Toten kommune, 2021). Svartebørshandel krever nærmest ingen tekniske ferdigheter og økonomiske muskler, og er en relativt enkel tilgang til personsensitiv informasjon og konfidensiell kommunikasjon som kredittkortinformasjon, medisinsk historikk, passinformasjon og geolokalisasjon (Armor, 2019; Tweetman & Bergmanis-Korats, 2020, s. 17). Noen selgere har faktisk kundeservice og tilbyr såkalte *Fullz*, «*the motherload of personal data on an individual*», på bestilling (Armor, 2019).

Etter det amerikanske presidentvalget i 2016, og påfølgende anklager om utenlandsk innblanding i Storbritannias brexit-avstemning, har påvirkningsoperasjoner rettet mot befolkningsgrupper (særlig under valg) fått mye oppmerksomhet. Her ble det samme digitale verktøy som nasjonale partier har til disposisjon (herunder mikromålretting), utnyttet av utenlandske aktører (se også Nadler et al., 2018). Dog påvirkning kan være legitimt og ønskelig i et demokrati,[13] så blir det problematisk når avsender er fordekt, og når koordinerte påvirkningsaktiviteter ønsker å svekke mottager. Forsvarets forskningsinstitutt (FFI) tilbyr en god forståelse av påvirkningsoperasjoner som «en aktørs koordinerte bruk av illegitime og fordekte metoder for å påvirke meninger og virkelighetsoppfatninger hos mennesker og grupper uten at de er klar over det, i den hensikt å skape forutsetninger for å oppnå egne strategiske mål» (Sivertsen et al., 2021, s. 15). Major Jess Dawson (2021, s. 68–69) ved Army Cyber Institute anser den primære forskjellen mellom (legitim) politisk mikromålretting og (illegitim) militære informasjonsoperasjoner som *hvem som utfører operasjonen* og *hvem som er målet*, fordi begges formål er å «develop insights on how best to persuade the target to change its behavior to one that is more favorable to [US] interests».[14] Det er altså klare fellesnevnere i formål og verktøy på tvers av (datadrevne) militære operasjoner, kommersielt salg av varer og tjenester, og datadrevet promotering av legitime politisk budskap.

I hvilken grad påvirkningsoperasjoner og desinformasjon har effekt, i betydning i hvilken grad en «aktør eller stat kan endre virkelighetsoppfatningen hos mennesker og grupper utenfor deres juridiske kontroll (C-SPI, 2020)», er vanskelig å måle og dermed omdiskutert. Holdninger, preferanser og tillit formes over tid og ulikt hos forskjellige mottagere. Og påvirkningsoperasjoner kan ha brede samfunnsmessige ringvirkninger på tvers av sektorer. Eksempelvis vil befolkingens tro på styringsmaktenes gode intensjon og gjennomføringsevne ha konsekvenser for beredskap, villighet

[13] Enkeltpersoner, interessegrupper og politiske partier ønsker å påvirke rammebetingelser og politikk. Deres tilgang og påfølgende ambisjon om medbestemmelse er en demokratisk forutsetning.

[14] Mikromålretting bygger i større grad på informasjon som er nært knyttet til deg som individ, og som analyserer personopplysninger samlet inn fra en rekke ulike kilder om atferd, interesser og verdier (sitat Datatilsynet, 2019b).

til å betale skatt, stemmegivning osv. Men det er vanskelig å spore om en eventuell reduksjon i tillit er et resultat av økte sosio-økonomiske forskjeller, avsløringer av korrupte politikere, effekt av politikk på den enkeltes hverdag, *eller* utenlandske strategiske narrativ med formål om destabilisering.[15]

Debatt rundt påvirkningsoperasjoners effekt omhandler også i hvilken grad utenlandske aktører har den nødvendige innsikten i sosio-kulturelle og lingvistiske forhold (se f.eks. Schia & Gjesvik, 2020). Førstnevnte innvending er utenfor denne artikkelens omfang. Det må imidlertid legges som et grunnpremiss at *hvis* man aksepterer at stater kan forme innbyggeres holdninger (f.eks. gjennom kampanjer), *hvis* man aksepterer at (datadrevet) markedsføring kan forme (politiske) preferanser og synspunkter, og *hvis* man aksepterer at store datasett kan generere inngripende kjennskap til personers trykkpunkter (sårbarheter), og *hvis* man anerkjenner eksistensgrunnlaget til overvåkningskapitalismen, *så* må man også akseptere at kommersielle datasett har en rolle i risikovurderinger relatert til påvirkningsoperasjoner. Det sekundære aspektet, at utenlandske påvirkningsagenter stiller svakere, er derimot svært interessant når man diskuterer kommersielle datasett. Fordi det kan utledes kontinuerlig («live») innsikt i trender, språkbruk, kulturelle koder og så videre, bør man vurdere i hvilken grad kommersielle datasett kan kompensere for den (påståtte) konkurranseulempen utenlandske agenter har.

Datadrevede cyberoperasjoner: Spionasje, sabotasje og subversion

Globalisering og digitalisering har endret verktøyene utenlandske påvirkningsagenter og etterretningsoffiserer har til disposisjon. Men formålet er det samme: endre målets atferd, eller svekke målet (Herzog, 2011; ISC, 2020; Mueller, 2019; Rid, 2019; sitert i Dowling, 2021, s. 3). Thomas Rids *Cyber War Will Not Take Place* og Ben Buchanans *The Hacker and the State* tilbyr gode rammeverk for å forstå hva cyberoperasjoner er, og hva de kan oppnå. For lesbarhetens skyld vil denne artikkelen benytte Rids terminologi, men definisjonene er overlappende.

Thomas Rid avviste i 2012 at cyberkrig, i betydningen et slags Cyber-Pearl-Harbor-angrep hvor samfunnet lammes, vil bli en realitet. Rid argumenterer derimot for at den reelle cyber-trusselen bør forstås som strategisk bruk av cyberdomenet for spionasje, sabotasje og *subversion* (Rid, 2013).[16] Ben Buchanans 2020-bok deler

[15] Et *strategisk narrativ* kan forstås som kimen i den langsiktige historiefortellingen / tolking av begivenheter som en aktør ønsker å fremme. De mest effektfulle påvirkningsoperasjoner har sannsynligvis en kime av sannhet, tilpasser seg lokale forutsetninger (som konfliktlinjer, språk og visuelt uttrykk), samt utnytter psykologiske variabler som repetisjon (*cognitive easing*), emosjonelle triggere, inn/ut-grupper og bekreftelsesbias.

[16] Rid definerer som følgende «Sabotage is a deliberate attempt to weaken or destroy an economic or military system»; «Espionage is an attempt to penetrate an adversarial system for purposes of extracting sensitive or protected information» og «Subversion is the deliberate attempt to undermine the authority, the integrity, and the constitution of an established authority or order» (Rid, 2012, s. 16–22).

tilsvarende cyberangreps effekt på geopolitiske forhold inn i tre kategorier: spionasje, angrep og destabilisering. Rid og Buchanans relaterte rammeverk er særlig nyttig fordi de illustrerer at trusler i cyberdomenet ikke er *enten* påvirkningsoperasjoner *eller* nettverksoperasjoner. Og at risikoforståelsen vedrørende cyberdomenet bør implementeres langs hele krise-krig-spekteret. Rid skriver for eksempel at «all past and present political cyberattacks are merely sophisticated versions of three activities that are as old as warfare itself: subversion, espionage, and sabotage», og at cyberangrep «have a significant utility in undermining social trust in established institutions», «are ideal instruments of sabotage» og «cyber-espionage is entirely non-violent yet most dangerous» (Cavelty & Rid, 2018, s. 131; Rid, 2012, s. 6).[17] Cyberoperasjoner anses dermed både som et supplement til tradisjonelle krigsoperasjoner eller langsiktig svekkelse av et samfunns samhold, forutsetninger og konkurranseevne. Og en risikovurdering bør dermed orienteres således.

Artikkelen vil nå gjennomgå på hvilken måte kommersielle datasett kan tilrettelegge for og forsterke gjennomslaget til henholdsvis spionasje, sabotasje og *subversion*.

Spionasje og sabotasje

Spionasje og sabotasje vil bli behandlet som to produkter av det samme verktøyet i denne analysen, da den risiko ved kommersielle datasett baseres i fare for uautorisert tilgang. I henhold til Tomas Rids terminologi vil sabotasje forstås som «*a deliberate attempt to weaken or destroy an economic or military system*» (Rid, 2012, s. 16). Spionasje brukes derimot i betydningen «*an attempt to penetrate an adversarial system for purposes of extracting sensitive or protected information. It may be either social or technical in nature*» (Rid, 2012, s. 20). Så både der hvor sabotasje ønsker å ødelegge, og hvor spionasje ønsker å tilrane seg informasjon, er tilgang essensielt.

Siden 2005 er 33 land mistenkt for å sponse cyberoperasjoner. I 2019 ble det rapportert om 76 operasjoner, primært innbrudd for spionasjeformål (Council on Foreign Relations, 2020). Lotrionte (2014–2015, s. 444–445) slår fast at cyberspionasje er den foretrukne metoden for både statlige og ikke-statlige aktørers informasjonsinnhenting, særlig etterretningsorganisasjoner (sitert i Paterson & Hanley, 2020). Rekruttering av kilder, samt fremmed etterretning, fremheves i de senere års nasjonale trusselvurderinger. PST skriver for eksempel at «rekruttering av kilder og agenter, kartlegging av virksomheter og kritisk infrastruktur samt nettverksoperasjoner, vil utgjøre de mest alvorlige utfordringene knyttet til fremmede staters etterretningsvirksomhet i 2018» (Politiets sikkerhetstjeneste, 2018, s. 4). Datasettene

[17] Martin Libicki og hans like kritiserer Rids smale forståelse av krig, men en redegjørelse av debatten er utenfor denne artikkelens ambisjonsnivå da den ikke retter seg inn mot cyberkrig. Derimot fokuserer den på hvordan kommersielle datasett kan akselerere gjennomslag og effekt, kategorisert ihht. Rid og Buchanans rammeverk.

kan forenkle kartlegging av nøkkelpersoners atferd og større miljøer, motivert av et ønske om «generell oversikt, kontroll over politiske motstandere, sette press på politiske eksilmiljø, eller med formål om å forstyrre eller svekke norsk forsvarsevne i en potensiell krisesituasjon» (Politiets sikkerhetstjeneste, 2018).

De store dataformidlere kategoriserer brukeratferd i kundeorienterte kategorier, med karakteristika av detaljert og mulig sensitiv natur. Facebook benytter for eksempel et klassifiseringssystem med 52 000 attributter for sine 2 milliarder brukere (Nadler et al., 2018, s. 12). Sekstiåtte Facebook-likes skal, ifølge Dawson (2021, s. 67), være nok til å predikere hudfarge, seksuell orientering, politisk tilhørighet, alkohol- og narkotikamisbruk, samt familiehistorikk som skilsmisse. Experian tilbyr kategoriserte profiler basert på 181 forskjellige etnisiteter, religioner og nasjonaliteter. Dette krysskobles opp mot interessemarkører, familiære forhold, inntekt, politisk tilknytning og yrke. Tidligere fremhevet artikkelen den seksuelt sensitive informasjonen Grindr delte. Det er også rapporter om at personsensitiv informasjon er delt fra muslimske bønneapper, blant annet hvor ofte en person ber kan så brukes som en proxy for hvor troende en person er. I 2013 fant en amerikansk senatskomite at Experian hadde solgt lister over personer definert som «finansielt sårbare» (Christl & Spiekerman, 2016, s. 104), åpenbart relevant informasjon for noen som ønsker å kartlegge nøkkelpersonell. Forskere ved Stanford University analyserte et par hundre menneskers telefon-metadata gjennom et par måneder. I dette relativt lille datasettet identifiserte de finansielle problemer, medisinske tilstander (inkludert behov for abort), ekteskapelige forhold, våpenkjøp, samt bruk av narkotiske stoffer som cannabis (Donohue, 2016, s. 40).[18] I Norge har NRK kjøpt lokalisasjonsdata fra 140 000 enheter, tilknyttet titusener av nordmenn, inkludert militære offiserer, pasienter ved psykiatriske institusjoner og sykehus, brukere av krisesentre, samt politikere. Bellingcat, i samarbeid med The Insider, Der Spiegel og CNN, har i en rekke artikler presentert FSB-agenters identitet, karrierer, reisemønstre, familier og lignende. I flere av artiklene er avsløringene basert på krysskobling og tidsserieanalyse av datasett med mobilhistorikk, telekom og reiselogger (som passasjerlister) ansamlet over lengre tid (Bellingcat, 2020a, 2020b; Furuly et al., 2020; Gundersen, 2020b, 2020c, 2021; Gundersen et al., 2020).

NATO Strategic Communication Center of Excellences rapport, *The current digital arena and its risks to serving military personnel*, fremhever faren for at militære motstandere kan innhente nok persondata til å påvirke måls atferd (Bay &

[18] I tillegg til store mengder ikke-sensitiv informasjon relatert til nettverk, jobb og familier. Ironisk nok er metadata (i motsetning til innholdsdata) gjerne presentert som mindre inngripende, til tross for at dets maskinelle natur er langt mer effektivt som analysegrunnlag. I tillegg er det mindre sårbart enn innholdsdata for feilrepresentasjon, da metadata ikke kontrolleres av den som skaper dataen (Donohue, 2016, s. 41). Kapittel 2 i Donohues bok presenterer en god gjennomgang av metadatas (data om data) etterretningspotensial.

Biteniece, 2019).[19] Henrik Tweetman og Gundars Bergmanis-Korats har i rapporten *Databrokers and Security* allerede fremhevet risikoen for at kommersielt anskaffet informasjon fra offentlige etater, lojalitetsprogrammer og digitale tjenester kan brukes i kartlegging og utpressing av forsvarspersonell (Tweetman & Bergmanis-Korats, 2020). De hevder at profileringspotensialet er så stort at risikoen tilsvarer en nasjonal sikkerhetsutfordring, og at Forsvaret bør anse data som kritisk infrastruktur. Jessica Dawson på sin side argumenterer for at militæret i USA bør «[defend] servicemembers' digital privacy as a national security risk» (2021, s. 63) Det er dermed betimelig å spørre seg om denne risikoen er mindre for ikke-militært nøkkelpersonell og befolkningen som helhet i et totalforsvarsperspektiv.

Kategorien «sabotasje» har muligens mindre intuitiv risiko knyttet til kommersielle datasett, da cyber-sabotasje kan anses som teknologisk i sin natur. Vi skal ikke presentere en fullstendig oversikt over de mange formene for cybersabotasje, men derimot begrense oss til å påpeke at ødeleggelsene varierer i kompleksitet (*sophistication*), målrettethet og effekt. Eksempelvis anses Stuxnet som en svært sofistikert operasjon som har krevd mye ressurser og innsidekunnskap. Løsepengeviruset Not Petya spredde seg globalt og infiserte sannsynligvis langt ut over avsenders hensikt, med store økonomiske konsekvenser for blant annet shippingselskapet Maersk. Nord-Koreas angrep på Sony Pictures etter en uflatterende film om Kim Jong-un, fikk konsekvenser av økonomisk og prinsipiell art,[20] men anses som teknisk usofistikert (Buchanan, 2020). Og under cyberangrepet i Estland (2007) og under Syriakonflikten, ble DDoS-angrep brukt som både en form for cyber-graffiti, for å hindre tilgang på informasjon og signalisere hackernes pondus.

Ikke alle typer cyber-sabotasje kan tilrettelegges av kommersielle datasett. Men det er verdt å merke seg at sabotasjeoperasjoner kan ta utgangspunkt i såkalte «menneskelige svakheter», typisk at noen klikker på en link, bruker svake passord, laster ned et dokument eller på en annen måte gir uautorisert tilgang. Denne type målrettet manipulasjon, ofte omtalt som *spearphishing* eller *catphishing*, er skreddersydd elektronisk kommunikasjon som bruker kjennskap til mottageren for å lure hen til å utføre en handling som strider mot egeninteresse.[21] Personaliseringen sikter på

[19] Rapporten fokuserte på mengde data forskere kunne innhente fra soldater på øvelse. Både fra åpne kilder og *social engineering*. I tillegg til skreddersydd budskapsformidling, fremhever NATOs analyse fire ondsinnede bruksområder for kommersiell data: manipulasjon, bedrageri, innhenting av sensitiv informasjon og strategiske lekkasjer av uflatterende eller kompromitterende informasjon, «doxing» (Bay & Biteniece, 2019, s. 8).

[20] Ansattes personinformasjon ble lekket med påfølgende søksmål mot selskapet. Terrortrusler mot kinoer som viste filmen medførte mye mindre distribusjon enn planlagt. Men man kan også spørre seg om hackernes reaksjon medførte mye mer oppmerksomhet enn filmen i seg selv hadde klart å skape.

[21] Dette kan ses som en personalisert versjon av phishing, hvor store mengder forespørsler sendes ut med håp om at det store kvanta vil tilsi at noen utfører ønsket handling (som å klikke på linken). Grad av målretting, spearphishing, varierer selvfølgelig, men et mer sofistikert eksempel

å øke innholdets troverdighet eller redusere mottagerens forsvarsverk (skepsis), slik at datainnbruddet eller løsepengevirus lykkes. Igjen er nok kvalitet på personaliseringen den essensielle variabel for suksess, men sannsynligvis har kunnskapsgrunnlag potensial for å øke gjennomslag. Sikkerhetsselskapet Fire Eye rapporterer for eksempel at opptil 70 % av mottagere åpner spearphising-eposter og at hele 50 % klikker på link eller åpner vedlegg som sprer viruset (Murnane, 2016).

Cyberdomenet har altså tilrettelagt for nye angrepsflater og sårbarheter innen både spionasje og sabotasje. Datarikdom blir «bensin» i kartleggingsanalysen og den sosial manipulasjonen. Men

> «Political subversion is a greater threat because it serves to undermine the sovereignty and democratic principles of the target state and represents an existential threat. It challenges the values, beliefs and independence of the state and its citizens». (Paterson & Hanley, 2020)

Vi vil derfor nå rette oppmerksomheten mot subversion (undergraving), med særlig fokus på påvirkningsoperasjoner, og hvorfor kommersielle datasett også bør inkluderes i denne risikovurderingen.

Subversion

Politiske krigføring, et begrep attribuert til George Kennan, er anvendelsen av alle midler en stat har til disposisjon utenom krig for å påtvinge en annen sin vilje (Lucas & Mistry, 2009). Paterson og Hanley (2020) anser politisk krigføring [i det digitale rom] som en fellesbetegnelse for informasjonskrigføring og subversion, som konstituerer en essensiell trussel da det undergraver institusjoners legitimitet og autoritet. Thomas Rid bruker *subversion* i betydning «the deliberate attempt to undermine the authority, the integrity, and the constitution of an established authority or order» (Rid, 2012, s. 22). Subversion kan også forstås som «statecraft designed to directly influence domestic politics in a target in a manner prejudicial to its foreign policy interests» gjennom enten å svekke målets posisjon eller å endre målets politikk (Kastner & Wohlforth, 2021; Wohlforth, 2020, s. 461). Ben Buchanan bruker tilsvarende begrepet «destabilization», altså destabilisering av det fundament tillitt og samhørighet bygger på. Subversion, direkte oversatt til «undergraving» på norsk, kan dermed forstås som strategiske operasjoner med hensikt å erodere den grunnmuren samfunnet vårt står på. Dette er relatert til hybride trusler med siktet om å «utnytte

---

kan være nok etterretning samlet i et datainnbrudd til å etterligne (*impersonate*) en CFO slik at organisasjonen overfører midler til manipulators konto. Et mindre sofistikert og ressurskrevende eksempel kan være at overvåkning i sosiale medier identifiserer en persons interesser (som veteranbiler, mammaklubber, oppussing) og bruker dette for å oppnå kontakt og relasjone, være det for catphishing eller for å optimalisere sannsynlighet for at mottager klikker på en særlig interessant link.

politiske, økonomiske og sosiale svakheter i et samfunn» (Disen, 2018, s. 18).[22] Det retter seg derfor både mot statssikkerheten og samfunnssikkerheten; man kan si at der konvensjonell krigføring er *war on government*, så kan hybrid krigføring forstås som *war on governance* (Galeotti, 2015).

Weissmann et al. (2017) stadfester at sammensatte trusler (herunder desinformasjon, propaganda, villedning, spionasje, sabotasje, datainnbrudd og påvirkning gjennom sosiale medier) har blitt fremtredende trekk ved væpnet konflikt og fredstid (Sivertsen et al., 2021, s. 9, 16). Virkemidlene kan sorteres innunder tre kategorier: propaganda og desinformasjon; (materiell) støtte til innenlandske grupperinger; initiering av vold gjennom for eksempel støtte til opprørere/rebeller, sabotasje av infrastruktur og snikmord (Kastner & Wohlforth, 2021; Wohlforth, 2020). Stordata blir i økende grad anvendt som driver i informasjonsoperasjoner og strategiske narrativ, med konsekvens at utenlandsk påvirkning er blitt delvis synonymt med cyber-påvirkning (Jamieson, 2020; Morgan, 2018; O'Connor et al., 2020; sitert i Dowling, 2021, s. 2; Paterson & Hanley, 2020, s. 445).[23]

Sverre Disen skrev i 2018 at «i utgangspunktet vil de fleste påvirkningsoperasjoner søke å overbevise ulike grupper av strategiske tilhørere om riktigheten av et bestemt narrativ, altså 'selge inn' en bestemt fremstilling av hva som er en objektiv sannhet» (Disen, s. 23). Salg av et narrativ i påvirkningsoperasjoner og markedsføring har åpenbare overlapp, noe som tilsier at overførbarheten bør være til stede i verktøyene kampanjene benytter (herunder kommersielle datasett og datadrevet, personalisert markedsføring). Også Jessica Dawson ved Army Cyber Institute fremhever data som drivkraft i utenlandske påvirkningsoperasjoner (Dawson, 2021, s. 63).

Å forutse noens preferanser eller handlinger er en ting. Å forme (*shape*) atferd gir helt andre muligheter (Østbø, 2021, s. 437). Det er derfor viktig å huske på at et sentralt element i datadrevet markedsføring er å identifisere *hvem* som er mest mottagelig, *når* mottageren er mest mottagelig, og på *hvilken måte* budskapet bør formidles (se Kaptein et al., 2015; Nadler et al., 2018, s. 15). Forskjellige individer og grupper utsettes for ulike «nudges» avhengig av hva som gir best gjennomslag (Sætra, 2020, s. 2). Basert på kommersielt innsamlet data om verdier, interesser og atferd, skreddersys påvirkningens narrativ med «issues which are important to an individual, adapting the format and language to meet the individual needs and

[22] Hybride trusler er et omdiskutert begrep som brukes i mange forskjellige betydninger. Det kan forstås som «statlige og ikke-statlige aktørers koordinering og synkronisering av militære, politiske, økonomiske, sivile og informasjonsmessige virkemidler» (Caspari, 2021). For en utførlig presentasjon av de mange forståelsene og de konsekvenser det får for norsk beredskap, se Caspari (2021).
[23] Cordey (2019, s. 28) deler henholdsvis cyber-påvirkningsoperasjoner inn i *cyber-enabled technical influence operations* og *cyber-enabled social influence operations*. Førstnevnte baserer seg på bruk av cyberkapabiliteter for å påvirke målets atferd (f.eks. DDoS, hacking og doxing), mens sistnevnte manipulerer målets holdning og beslutningsprosess gjennom falskt digitalt innhold, trolling og bots. Førstnevnte gruppes relevans for kommersielle datasett relaterer seg dermed til spionasje og sabotasje (gjennom etterretning og sikre tilgang), den andre gruppen faller innunder subversion og mer spesifikt påvirkningsoperasjoner.

interests for maximum effect» (Borgesius et al., 2018). Basert på predikativ analyse, målinger fundert i store datasett og kontinuerlige tilbakemeldingssykluser gjennom såkalt A/B- og multivariat-testing, eksperimenterer og foredles påvirkningens narrativ for å endre holdning eller atferd (Christl, 2017, s. 6).[24] I artikkelen «When nudge comes to shove» argumenterer tilsvarende Henrik Sætra for at dyptgripende innsikt i preferanser, verdier og sårbarheter multipliserer gjennomslagskraften til påvirkning i den grad at han sammenligner det med presisjonsbombing (Sætra, 2020, s. 101).

Gjennom sanntids-mikromålretting basert i (kommersielle) datasett, kan påvirkningsagenter altså i teorien tilpasse hvilket sub-budskap, i hvilken språkdrakt, og til hvem et narrativ formidles. En studie fra University of Oxford indikerer at sosiale medier, datadrevet markedsføring og søkeordoptimalisering i stadig økende grad anvendes for påvirkning (Bradshaw & Howard, 2018, s. 3). Ifølge Bradshaw og Howard (2019, s. i), kan det identifiseres valgmanipulasjon i 70 land, opp fra 48 land i 2018 og 28 land i 2017. Forfatterne konkluderer med at «*although there is nothing necessarily new about propaganda, the affordance of social networking technologies – algorithms, automation, and big data – change the scale, scope, and precision of how information is transmitted in the digitale age*» (Bradshaw & Howard, 2019, s. 11). Denne type profilering ligger også til grunn for Googles *Redirect Method*, hvor data fra Google Ads identifiserte mennesker sårbare for islamistisk radikalisering. Deretter ble mulige IS-krigere kontinuerlig eksponert for alternative narrativ gjennom søkeordsoptimalisering og skreddersydde annonser i tekst, bilde og video (Google, 2016). Omfattende datainnsikt vil også til en viss grad kompensere for sosio-kulturelle ulikheter mellom avsender og mottager, ved at avsender kan få kontinuerlig oppdatert underlagsinformasjon og svært spesifisert tilbakemelding. I ovennevnte Google-eksperiment økte for eksempel klikkraten med over 70 % i både det engelsktalende og det arabiske publikum (Google, 2016).[25]

NSM fremhever i *Risiko 2020* at åpen, kommersiell informasjon fra sensorer i mobiltelefoner, smartklokker, strømmålere, elektroniske dørlåser og alarmsystemer, satellitter og flybilder, action-kamera, droner og avanserte kjøretøy, kan være en betydelig sikkerhetsutfordring (NSM, 2020 s. 31).[26] Jo mer «treningsdata» algoritmer tilbys, jo bedre grunnlag har den for å identifisere markører, mønstre og uteliggere. Gjennom maskinlære forbereder maskinen også egen teknikk, i motsetning

[24] A/B-testing vil si at to randomiserte grupper eksponeres for to ulike landingsider, innhold e.l. Multivariat er det samme, men med flere grupperinger som eksponeres for nyanser av det samme budskapet, utforming av nettsted etc. Dette er vanlig i digital tjenesteutvikling og kommunikasjonsfag for å optimalisere produktutvikling.

[25] Klikkerate er et forholdstall som viser hvor ofte publikum utfører en ønsket handling, f.eks. klikke på en annonse. I kommunikasjon og markedsføring er det en etablert KPI for hvor vellykket et budskap er.

[26] Salg av datasett fra en rekke datainnbrudd på tidligere nevnte svartebørsmarked, tilsier at informasjon ikke nødvendigvis er «trygg» selv om innsamler benytter bedre anonymisering eller frasier seg den økonomiske gevinsten i tredjepartanvendelse (ikke salg eller deling ut over egen organisasjon).

til at utvikleren instruerer hvert steg (Verhelst et al., 2020, s. 2977).[27] Analysen blir dermed stadig mer selvgående (eller autonom). Verhelst et al. (2020) trekker frem at det (heldigvis) er relativt få terrorister og radikaliserte, og at det reduserer implementering av maskinlære i terrorbekjempelse. Datasettene vil naturlig nok være betraktelig større når man behandler befolkningen som helhet på jakt etter sårbarheter (som utroskap, økonomiske utfordringer, rusmiddelbruk eller aggressiv digital atferd), nøkkelpersoners geografiske og digitale bevegelser, nettverk, sikkerhetsprosedyrer og potente konfliktlinjer. Takket være økt kapasitet, mer sofistikert teknisk arkitektur og grafikkprosessorer (GPU), øker også muligheten for å kombinere flere kilder av ulike format og organisering (Pastor-Galindo et al., 2020, s. 10285).

Algoritmer kan jobbe delvis selvstendig, i stort omfang, og svært raskt. Så der Sætra sammenlignet datadrevet *nudging* med presisjonsbombing, så kan man også hevde at den totale mengden av påvirkning kan sammenlignes med teppebombing. I 2018 hevdet for eksempel Facebook at ett av deres systemer, ved hjelp av maskinlære, gjennomførte 200 trillioner prediksjoner hver eneste dag (Amnesty International, 2019). Brad Pascale, leder for Trumps 2016 digitale presidentkampanje, testet mellom 40 000 og 50 000 budskap hver eneste dag (Bashyakarlya et al., 2019, s. 18). Omfanget ga kampanjen et sterkt kunnskapsgrunnlag for donasjonsinnhenting og budskapsgjennomslag. Prediksjonene bygget også et omfattende datasett på den digitale følgerskare, som igjen kunne anvendes til kontinuerlige «temperaturmålinger» på sinnsstemningen i velgermassen – uten de feilkilder som små utvalg og egenrapportering er sårbare for. Hinds og Joinson (2019, s. 205) viser til en rekke studier som påviser at både menneske- og databaserte studier lykkes i å identifisere personlighetstrekk basert på nettatferd og sosiale medier (se f.eks. Schwartz et al., 2013; Vazire & Gosling, 2004; Waggoner et al., 2009; Youyou et al., 2015, 2017). De viser også til to metastudier som indikerer at datamaskiner har bedre prediksjonsevne enn mennesker og konkluderer med at «as our interaction with technology continues to grow apace, the oportunities to study personality and predict behavor are unprecedented» (Hinds & Joinson, 2019, s. 209).[28] Analyser drevet av de samme datasettene som denne artikkelen ønsker å fremheve risikoen ved.

Samfunn karakterisert av god styring og tillit til myndighetene, økonomisk vitalitet, høy tilfredsstilhet i befolkningen, samt få etniske, historiske eller religiøse motsetninger kan anses som vanskelige mål for hybrid krigføring (Disen, 2018, s. 18). Denne anskuelsen har vært nærliggende både for risikoforståelse og foreslåtte tiltak mot påvirkningsoperasjoner (se f.eks. Hågen Karlsen, 2021). Som en

[27] Sårbarhet for bias, spuriøse korrelasjoner, samt falske positive og negative treff, springer hovedsakelig ut av for små datasett. Manglende innsyn i beslutningsgrunnlag (også kalt *black boxing*) vil derimot sannsynligvis bare øke etter hvert som automatisert maskinlære benyttes i økende grad for å behandle svært store datasett.

[28] se Azucar et al., 2018; Tskhay & Rule, 2014; begge referert på side 205.

forlengelse av denne logikken bør narrativ som strategisk understreker økte sosio-økonomiske forskjeller, dårlig forvaltning eller forsterker samfunnsgruppers motsetninger antas å være en sentral komponent i vellykkede påvirkningsoperasjoner. Påvirkningsoperasjoner retter seg direkte inn mot (gryende) konfliktlinjer i samfunnet og søker å forsterke disse. Datarike kommersielle kunnskapsgrunnlag som tilgjengeliggjør skreddersydd kobling mellom narrativ og mottager, sårbarhetsanalyser hos publikum og kontinuerlig tilbakemelding (*feedback-loop*), samt etablering av digitale trykkamre,[29] bør dermed være en kilde til bekymring.

Vi trenger en reell risikoforståelse

> *I Norge skal det være trygt å bruke digitale tjenester. Privatpersoner og virksomheter skal ha tillitt til at den nasjonale sikkerheten, den enkeltes velferd og demokratiske rettigheter blir ivaretatt i et digitalisert samfunn.* (Nasjonal strategi for digital sikkerhet, 2019, s. 7)

De nasjonale trusselvurderingene fremhever andre staters interesse for norske bedrifter, forvaltning, borgere og politiske prosesser. Derimot er samtalen rundt trygg dataforvaltning i nasjonalt sikkerhetsøyemed begrenset.[30] Arbeid som *Data Brokers and Security* fra NATO Strategic Communication Center of Excellence (2020), Carrie Corderos kongressnotat «The National Security Imperative of Protecting User Data» (2019) og Jesscia Dawsons «Microtargeting as Information Warfare» (2021), kan anses som arbeid til etterlevelse. For en fremmed stat eller aktør kan det være verdifullt å vite hvilket bål de bør helle bensin på, hva som rører seg i samfunnet, hvem eller hva som er de svake ledd, og hvordan påvirkningskampanjer maksimerer gjennomslag. Artikkelen har vist at mulighet for segmentering ned til svært små grupper og geografiske områder, innebærer en rekke sikkerhetsutfordringer knyttet til kartlegging, manipulasjon, rekruttering og utpressing på både gruppe- og individnivå. Nøkkelpersoner er også sivile privatpersoner med nettverk. Morgendagens politikere og forsvarspersonell er tilsvarende del av et samfunn hvor apper, sosiale medier og annonsører gjennomsyrer hverdagen. De har familier som skaper sårbarheter, eksponeres for nyhetsbildet og påvirkes av opinionen rundt seg. Morgendagens nøkkelpersonell kan i teorien spores fra vugge til grav. Risikovurderinger bør derfor som et absolutt minimum ikke begrenses til en nåtidig evaluering av hva datasett kan informere om og anvendes for.

En forutsetning for et digitalisert Norge, er en digital kompetent befolkning som tar i bruk ny teknologi etter hvert som den utvikles. Alle nasjonale strategier tilsier

[29] Dag Hareide bruker «trykkamre» i stedet for det mer etablerte «ekkokamre», da han hevder at uniforme digitale grupperinger primært forsterker eksisterende tendenser, «sannheter» og emosjoner. I stedet for at dette blir kastet frem og tilbake (ekko), skaper dette en forsterkningseffekt (derav trykk) (Hareide, 2020).

[30] Dog enkelte fremhever behovet for en nasjonal skytjeneste inspirert av tyske Bundescloud (se f.eks. Bredeveien, 2021; Gundersen et al., 2021; Håkonsen, 2021).

at optimalisering av datagrunnlag samlet gjennom «smarte byer», Internet of Things (IoT) og digitalisert forvaltning vil være en strategisk samfunnsprioritet. Dette fører til at antall sensorer og den enkeltes dataavtrykk vil mangedobles i de kommende år. Dog noe sporing er nødvendig for individualisert funksjonalitet og brukervennlighet, så er overvåkningskapitalismen symptomatisk på et system som går langt forbi ambisjon om markedsføring. Vi har vist at store datamengder representerer en reell risiko for at informasjon som burde vært gradert, tilgjengeliggjøres. Fordi data er kommersielt formidlet i et globalt marked, er det ikke noe overoppsyn med hvem som akkumulerer data til hvilket formål, eller noen form for føre-var-prinsipper fundert i en type utløpsdato eller hjemfallsregel. Artikkelen har også vist at den enkeltes personvernspreferanser ikke er en tilfredsstillende sikkerhetsmekanisme. Ei heller en korrekt anskuelse av risiko. Når konsekvensen er kollektiv, bør ikke mulig gradert informasjon reduseres til den enkeltes «personverns-smerteterskel».

Artikkelen ønsker ikke å etterlate inntrykket av at kommersielle datasett gir fremmede makter en universell mirakelkur for å realisere ethvert mål. Derimot ønsker vi å nyansere risikoforståelsen ved gjennomdigitalisering av hverdagen. Artikkelen har vist hvordan overvåkningskapitalismen, i kombinasjon med åpenhetens dilemma, tilsier at store datamengder i fri dressur bør være en kilde til bekymring uten at dette tolkes som at alle muligheter må realiseres eller at all data er farlig. Det bør heller forstås som en mulig kilde for multiplikatoreffekt, enten for grad av gjennomslag eller omfang. Et globalt, uoversiktlig datamarked er sårbart for dataangrep og manglende verdikjedekontroll. Datasettenes digitale natur medfører større detaljgrad, maskinlesbarhet optimalisert for automatisering, lange tidsserier, sanntidspotensial og mindre ressurskrevende datainnhenting sammenlignet med analoge metoder. Påstått anonymisering har vi vist at ikke er tilfredsstillende, et problem som sannsynligvis bare vil øke etter hvert som økt lagrings- og prosesseringskraft gjør datasettene mer sårbare for reidentifikasjon. Samfunnsdigitalisering, smarte enheter og overvåkningskapitalismen intensiverer og forenkler inntrengningen i den private sfære. Samlet vil dette høyst sannsynlig øke de strategiske effektene av persondata med potensielle konsekvenser for statssikkerheten.[31]

Innledningsvis redegjorde vi for hvordan det klassiske *personvern-sikkerhetsdilemma* kan anses som et bytteforhold eller en balansegang mellom borgernes rett til personvern versus deres rett til sikkerhet (Verhelst et al., 2020, s. 2976). Når kollektivt fravær av fare settes opp mot en individuelt abstrakt gode, reduseres datakontroll til den enkeltes smerteterskel mellom nåtidig brukervennlighet og bidrag

[31] NSMs *Risiko 2020* skriver i sin vurdering at «en av årsakene til at verdien av informasjon øker, er at kapasiteten for automatisert dataanalyse øker eksponentielt og prosesser automatiseres. Dette muliggjør sammenstilling og nye former for analyse av det enorme volumet av åpen informasjon. Mengden åpen informasjon og muligheten til å sammenstille informasjon digitalt innebærer en betydelig risiko for at trusselaktører får innsikt i forhold vi ønsker å skjerme eller burde skjerme. Slik sett er trussel aktørens kostand og risiko knyttet til innhenting betydelig redusert i forhold til for 10–20 år siden».

i sikkerhetsdugnaden. Et noe svekket personvern og en abstrakt «Big Brother» i et land karakterisert av svært høy tillit til myndighetene, kan resultere i en falsk trygghet eller manglende tiltakslyst. Særlig hvis debatten primært fokuserer på metadata og anonymisert data, senest observert i prosessen rundt ny etterretningstjenestelov (Wilhelmsen, 2019). Personvernsargumentene blir formulert av sivile aktører som Datatilsynet, Advokatforeningen og Forbrukerombudet med fokus på nedkjølingseffekt, individets rettigheter og menneskerettigheter som ytringsfriheten. Dette er viktige, prinsipielle aspekter i hvorfor vi bør begrense den massive innsamlingen av kommersiell data om nordmenn.

Men det er dermed også en reell fare for at datafangst, omfang av videresalg og mulighetsrommet for anvendelse undervurderes fra et sikkerhetsperspektiv. Denne artikkelen konkluderer med at personvernsikkerhetsdilemmaet blir en falsk dikotomi i møtet med overvåkningskapitalismen. En demokratisk stat vil aldri kunne kontrollere borgernes totale digitale liv. Stadig økt overvåkning vil alltid møte kritikk knyttet til at det utfordrer demokratiske prinsipper. Et sterkt personvern kan dermed bli et verktøy for sikring. Uten å komme i konflikt med informasjonsfrihet, kildevern, rett til privatliv, og ytringsfrihet tilsvarende hva statlig, digital overvåkningsregimer beskyldes for.

Nasjonal sikkerhet og individuell datakontroll er ikke motstående poler. Dette er et feilaktig narrativ som blir en hemsko for realiseringen av de sikkerhetsutfordringene denne artikkelen har påpekt. Vi må avvise motsetningsforholdet mellom personvern og sikkerhet. Vi bytter ikke det ene mot det andre. Derimot kan de gjensidig styrke hverandre. Vi bør spørre oss om datakontroll og personvern i større grad bør anses som et kollektivt sikkerhetsanliggende. Og om den mest tilgjengelige sikkerhetsmekanisme er begrensning av dataakkumulasjonen gjennom sterk personlovgivning og nasjonal datakontroll.

Om forfatteren

Vivi Ringnes Wilhelmsen er forsker ved Institutt for forsvarsstudier (IFS). Hun har en master i statsvitenskap fra Universitetet i Oslo og en master i International Relations fra Geneva School of Diplomacy and International Relations.

Referanser

Acxiom. (2020). *Acxiom data: Comprehensive global data and insights*. Hentet 28.08.2020 fra www.acxiom.com/customer-data/

Amnesty International. (2019). *Surveillance gigants: How the business model of Google nad Facebook threatens human rights*. Amnesty International. https://www.amnesty.org/en/documents/document/?indexNumber=pol30%2F1404%2F2019&language=en

Armor. (2019). *The Armor 2019 black market report: A look inside the dark web*. www.armor.com/resources/report/the-dark-market-report/

Bakke-Jensen, F. (2020, 14. september). Ny e-lov gir bedre beskyttelse mot digitale angrep (Tale/innlegg). *Stavanger Aftenblad*. Hentet 13.02.2022 fra https://www.regjeringen.no/no/dokumentarkiv/regjeringen-solberg/aktuelt-regjeringen-solberg/fd/taler-og-innlegg/ministeren/taler-og-innlegg-av-forsvarsminister-frank-bakke-jensen/2020/elovenbeskytter/id2741266/

Barland, M. (2016, 28. januar 2016). *Hva er overvåkningsøkonomien?* Teknologirådet. https://teknologiradet.no/hva-er-overvakingsokonomien/

Bashyakarlya, V., Hankey, S., Mcintyre, A., Renno, R. & Wright, G. (2019). *Personal data: Political persuasion inside the influence industry. How it works.* http://cdn.ttc.io/s/tacticaltech.org/influence-industry.pdf

Bay, S. & Biteniece, N. (2019). *The current digital arena and its risk to serving military personnel.* NATO Stratcom CEO. https://stratcomcoe.org/pdfjs/?file=/cuploads/pfiles/nato_report_-_hacking_humans_the_current_digital_arena_and_its_risks_to_serving_military_personnel.pdf?zoom=page-fit

Bellingcat. (2020a, 14. desember). *FSB team of chemical weapon experts implicated in Alex Navalny Novichock poisoning*. Bellingcat. www.bellingcat.com/news/uk-and-europe/2020/12/14/fsb-team-of-chemical-weapons-experts-implicated-in-alexey-navalny-novichok-poisoning/

Bellingcat. (2020b, 14. desember). *Hunting the hunters: How we identified Navalny's FSB stalkers*. Bellingcat.

Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T. & Shadbolt, N. (2018). *Third party tracking in the mobile ecosystem*. 10th ACM Conference on web science.

Bonfanti, M. E. (2018). Cyber intelligence: In pursuit of a better understanding for an emerging pratice. *Cyber, Intelligence and Security*, *2*(1).

Bradshaw, S. & Howard, P. N. (2018). *Challenging truth and trust: A global inventory of social media manipulation*. University of Oxford.

Bradshaw, S. & Howard, P. N. (2019). *The global disinformation disorder: 2019 Global Inventory of organized social media manipulation*. Oxford University.

Bredeveien, J. M. (2021, 12. mai). Hvem skal eie våre norske data? *Dagsavisen.* https://www.dagsavisen.no/debatt/kommentar/2021/05/12/hvem-skal-eie-vare-norske-data/

Borgesius, F. J. Z., Möller, J., Kruikemeier, S., Ó Fathaigh, R., Irion, K., Dobber, T., Bodo, B. & de Vreese, C. (2018). Online political microtargeting: Promises and threats for democracy. *Utrecht Law Review*, *14*(1), 82–96. https://doi.org/10.18352/ulr.420

Brogan, C. (2019, 23. juli). Anonymising personal data "not enough to protect privacy" shows new study. *Imperial College News*.

Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of geopolitics*. Harvard University Press.

C-SPI, F. F. (2020, 21. august 2020). *Slik skal FFI forske på påvirkningsoperasjoner*. Hentet 29. juni 2020 fra https://www.ffi.no/aktuelt/nyheter/slik-skal-ffi-forske-pa-pavirkningsoperasjoner

Caspari, B. C. (2021). *Norges forståelse av hybride trusler: Effektene av ulike konseptualiseringer på myndighetenes samarbeid* [Masteroppgave, Universitetet i Stavanger]. https://hdl.handle.net/11250/2835861.

Cavelty, M. D. & Rid, T. (2018). Thomas Rid, Cyber war will not take place [Bokanmeldelse]. *European Review of International Studies*, *5*(1), 131–134.

Christl, W. (2017). *Corporate surveillance in everyday life: How companies collect, combine, analyze, trade and use personal data on billions*. Cracked Labs. https://crackedlabs.org/en/corporate-surveillance

Christl, W. & Spiekerman, S. (2016). *Networks of control. A report on corporate surveillance, digital tracking, big data and privacy*. Facultas.

Cordey, S. (2019). *Cyber influence operations: An overview and comparative analysis* (Cyberdefense trend analysis Issue. Center for Security Studies CSS.

Council on Foreign Relations. (2020). *Cyberoperation tracker: Operations by country*. www.crf.org/cyber-operations/#Map

Datatilsynet. (2019a). *Datatilsynet sier nei til digital masseovervåkning av norske borgere*.

Datatilsynet. (2019b, 20. juni). *Målretting av politiske budskap*. https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/malretting-av-politiske-budskap/

Dawson, J. (2021). Microtargeting as information warfare. *The Cyber Defense Review*, *6*(1), 63–80. https://doi.org/10.31235/osf.io/5wzuq

Disen, S. (2018). *Lavintensiv hybridangrep på Norge i en fremtidig konflikt*. FFI.

Dixon, P. (2013, 18. desember). *What information do data brokers have on consumers?* Senate Commerce Committee hearing.

Donohue, L. K. (2016). *The future of foreign intelligence: Privacy and surveillance in a digital age*. Oxford University Press.

Dowling, M.-E. (2021). Democracy under siege: Foreign interference in a digital era. *Australian Journal of International Affairs*, 1–5. https://doi.org/10.1080/10357718.2021.1909534

Døvik, O. & Skille, Ø. B. (2021, 6. oktober). *Vil la PST lagre informasjon fra åpne kilder i 15 år*. NRK. https://www.nrk.no/norge/pst-skal-fa-lagre-informasjon-fra-apne-kilder-1.15680296

Egan, E. (2019). *Now you can see and control the data that apps and websites share with Facebook.* http://about.fb.com/news/2019/08/off-facebook-activity/

Englehardt, S. & Narayanan, A. (2016). *Online tracking: A 1-million-site measurement and analysis*. Conference on Computer and Communications Security. https://dl.acm.org/doi/abs/10.1145/2976749.2978313
Etterretningstjenesten. (2019). *Fokus 2019*. https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus
Etterretningstjenesten. (2020). *Fokus 2020*. https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus
Etterretningstjenesten. (2021). *Fokus 2021*. https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus
Forbrukerrådet. (2020). *Out of control: how consumers are exploited by the online advertising industry*.
Furuly, T., Lied, H. & Gundersen, M. (2020, 9. mai). *Avslørt av mobilen*. NRK.
Galeotti, M. (2015, 19. august). *Hybrid war as war on governanace* [Intervju]. https://smallwarsjournal.com/jrnl/art/hybrid-war-as-a-war-on-governance
Google. (2016). *The redirect method*. https://redirectmethod.org
Gundersen, M. (2020a, 15. september). *Over 700 nordmenn kartlagt av kinesisk selskap*. NRK Beta.
Gundersen, M. (2020b, 24. august). *Secret Service kjøpte data om amerikanske mobilers bevegelser*. NRK Beta.
Gundersen, M. (2020c, 3. desember). *Telefonen spionerte på meg. Slik fant jeg overvåkerne*. NRK Beta. https://nrkbeta.no/2020/12/03/telefonen-spionerte-pa-meg-slik-fant-jeg-overvakerne/
Gundersen, M. (2021, 22. februar). *Nato-rapport: disse selskapene truer rikets sikkerhet*. NRK Beta.
Gundersen, M., Skille, Ø. B. & Døvik, O. (2021, 7. juni 2021). *Senterpartiet mener Norge trenger en «nasjonal sky»*. NRK Beta. https://nrkbeta.no/2021/06/07/senterpartiet-mener-norge-trenger-en-nasjonal-sky/
Gundersen, M., Skille, Ø. B. & Lied, H. (2020, 18. mai). *Når mobilen blir fienden*. NRK.
Hareide, D. (2020). *Menneske og teknomaktene*. Aschehoug.
Hareide, D. (2021). Vi er alle borgere i Digitalistan: Teknomaktene og norske motstandsbevegelser I A. Rolstadås, A. Krokan, G. E. D. Øien, M. Rolfsen, G. Sand, H. Syse, L. M. Husby & T. I. Waag (Red.), *Den digitale hverdagen*. John Grieg Forlag. https://www.ntva.no/publikasjoner/den-digitale-hverdagen/
Hinds, J. & Joinson, A. (2019). Human and computer personality prediction from digital footprints. *Current Directions in Psychological Science*, *28*(2), 204–211. https://doi.org/10.1177/0963721419827849
Håkonsen, K. D. (2021, 18. oktober). *Forsvarsansatte vil ha offentlige data vekk fra private skytjenester: – Høygradert informasjon kan komme på avveie*. https://frifagbevegelse.no/ntlmagasinet/forsvarsansatte-vil-ha-offentlige-data-vekk-fra-private-skytjenester–hoygradert-informasjon-kan-komme-pa-avveie-6.158.823571.2d9887dc73
Justis- og beredskapsdepartementet. (2021). *Høring om endringer i straffeloven mv. – påvirkningsvirksomhet*. https://www.regjeringen.no/no/dokumenter/horing-om-endringer-i-straffeloven-mv.-pavirkningsvirksomhet/id2849395/
Kaptein, M., Markopoulos, B., de Ruyter, B. & Aarts, E. (2015). Personalizating persuasive technologies: Explicit and implicit personalization using persuasion profiles. *International Journal of Human Computer Studies*, *77*, 38–51. https://doi.org/10.1016/j.ijhcs.2015.01.004
Karlsen, G. H. (2021). Hvordan kan vi beskytte valg mot fremmed påvirkning? *Internasjonal Politikk*, *79*(1), 90–113. https://doi.org/10.23865/intpol.v79.2309
Karlsen, J. (2019, 24. mars). *Soldaters Tinder-bruk på øvelse bekymrer*. Forsvarets forum.
Kastner, J. & Wohlforth, W. C. (2021). A measure short of war: The retur of great-power subversion. *Foreign Affairs*, *July/August*.
Kollsrud, K. (2021, 19. august). *Forslag om «påvirkningsforbud» får bred kritikk fra juristmiljøene*. Rett24. https://rett24.no/articles/forslag-om-pavirkningsforbud-far-bred-kritikk-fra-juristmiljoene
Kolsrud, K. (2021, 10. juni). *Derfor nekter tingretten FBI-dokumenter i «Trojan Shield»-saken*. Rett24. https://rett24.no/articles/derfor-nekter-tingretten-fbi-dokumenter-i-trojan-shield-saken
Langemyr, H. (2021, 18. august). Naivt lovforslag om påvirkning. *Dagsavisen*. https://www.dagsavisen.no/debatt/kommentar/2021/08/18/naivt-lovforslag-om-pavirkning/
Lucas, S. & Mistry, K. (2009). Illusions of coherence: George F. Kennan, U.S. strategy and political warfare in the early cold war, 1946–1950★. *Diplomatic History*, *33*(1), 39–66. https://doi.org/10.1111/j.1467-7709.2008.00746.x
Murnane, K. (2016, 26. oktober). How John Podesta's emails were hacked and how to prevent it from appening to you. *Forbes*.
Nadler, A., Crain, M. & Donovan, J. (2018). *Weaponizing the digital influence machine: The political perils of online tech*. Data & Society. https://datasociety.net/library/weaponizing-the-digital-influence-machine/
Nasjonal strategi for digital sikkerhet. (2019). *Nasjonal strategi for digital sikkerhet*. Justis- og beredskapsdepartementet & Forsvarsdepartementet.
Nordal, A. G. (2020, 21. desember). Føler seg trygge på personvernet i den nye smittestopp-appen. *Tekna Magasinet*. https://www.tekna.no/magasinet/foler-seg-trygge-pa-personvernet-i-den-nye-smittestopp-appen/

NorSIS, N. s. f. i. (2021, 8. april). *Dataangrepet i Østre Toten kommune: Minst 9000 dokumenter og store e-postmengder stjålet.* https://norsis.no/dataangrepet-i-ostre-toten-kommune-minst-9000-dokumenter-og-store-e-postmengder-stjalet/

NSM, N. S. (2020). *Risiko 2020*. Nasjonal sikkerhetsmyndighet NSM.

NTB. (2019, 28. mars 2019). USA pålegger kinesisk selskap å selge Grindr. *Aftenposten*. https://www.aftenposten.no/verden/i/jd0mOA/usa-paalegger-kinesisk-selskap-aa-selge-grindr

Park, G., Schwartz, H. A., Eichstaedt, J. C., Kern, M. L., Kosinski, M., Stillwell, D. J., Ungar, L. H. & Seligman, M. E. P. (2014). Automatic personality assessment through social media language. *Journal of Personality and Social Psychology*. http://dx.doi.org/10.1037/pspp0000020

Pastor-Galindo, J., Nespoli, P., Gómez Mármol, F. & Martínez Pérez, G. (2020). The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. *IEEE Access*, *8*, 10282–10304. https://doi.org/10.1109/ACCESS.2020.2965257

Paterson, T. & Hanley, L. (2020). Political warfare in the digital age: Cyber subversion, information operations and deep fakes. *Australian Journal of International Affairs*, *74*(4), 439–454.

Perrin, N. & Verna, P. (2019, 11. juni). *eMarketer*. https://www.emarketer.com/content/podcast-regulating-the-tech-giants-why-now

Politiets sikkerhetstjeneste. (2018). *Trusselvurdering 2018*. https://www.pst.no/trusselvurdering-2018/

Politiets sikkerhetstjeneste. (2019). *Trusselvurdering 2019*. https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2019/

Politiets sikkerhetstjeneste. (2020). *Nasjonal trusselvurdering 2020*. https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2020/

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

Rid, T. (2012). Cyber war will not take place. *The Journal of Strategic Studies*, *35*(1), 5–32.

Rid, T. (2013). *Cyberwar will not take place*. Oxford University Press.

Rocher, L., Hendrickx, J. M. & de Montjoye, Y. (2019). Estimating the sucess of reidentifications in incomplete datasets using generative models. *Nat Commune*, *10*(3069). https://doi.org/10.1038/s41467-019-10933-3

Schia, N. N. & Gjesvik, L. (2020). Hacking democracy: Managing influence campaigns and disinformation in the digital age. *Journal of Cyber Policy*, *5*(3), 413–428. https://doi.org/10.1080/23738871.2020.1820060

Seneviratne, S., Kolamunna, H. & Seneviratne, A. (2015). *A measurement study of tracking in paid mobile applications*. 8th ACM Conference on Security & Privacy in Wireless nad Mobile Networks (WiSec '15), New York, USA.

Silverman, J. (2017). Privacy under surveillance capitalism. *Social Research: An International Quarterly*, *84*(1), 147–164.

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

Skille, Ø. B. & Holm-Nilsen, S. (2021, 8. juni). *Slik lurte politi over hele verden kriminelle med en «kryptert» app.* NRK. https://www.nrk.no/norge/slik-lurte-politi-over-hele-verden-kriminelle-med-en-_kryptert_-app-1.15527880

Sætra, H. S. (2020). When the nudge comes to shove: Liberty and nudging in the era of big data. *Technology in Society*, *59*(101130).

Thompson, S. A. & Werzel, C. (2019, 19. desember). Twelve million phones, one dataset, zero privacy. *New York Times*.

Tweetman, H. & Bergmanis-Korats, G. (2020). *Data brokers and security*. NATO Strategic Communications Center of Excllence.

Verhelst, H. M., Stannat, A. W. & Mecacci, G. (2020). Machine learning against terrorism: How big data collection and analysis influences the privacy-security dilemma. *Science and Engineering Ethics*, *26*(6), 2975–2984. https://doi.org/10.1007/s11948-020-00254-w

Vigsnæs, M. K. & Kjelland-Mørdre, I. (2019, 2. august). *Toppolitikere avslører hvor de er via treningsapp*. NRK.

Wells, G. & O'Keeffe, K. (2019, 27. mars). U.S. orders Chinese firm to sell dating app Grindr over blackmail risk. *The Wall Street Journal*. https://www.wsj.com/articles/u-s-orders-chinese-company-to-sell-grindr-app-11553717942

Wilhelmsen, V. R. (2019). *Ny etterretningslov – nasjonal sikkerhet eller digital masseovervåkning?* Civita.

Wohlforth, W. C. (2020). Realism and great power subversion. *International Relations*, *34*(4), 459–481. https://doi.org/10.1177/0047117820968858

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospect of an information civilization. *Journal of Information Technology, 30*, 75–89.

Zuboff, S. (2020, 24. januar). You are now remotely controlled. *New York Times*.

Østbø, J. (2021). Hybrid surveillance capitalism: Sber's model for Russia's modernization. *Post-Soviet Affairs*, *37*(5), 435–452. https://doi.org/10.1080/1060586X.2021.1966216

Østre Toten kommune. (2021, 8. april). *Varsel om personopplysninger på avveie*. https://www.ototen.no/_f/p1/i42329283-e953-4a69-b352-8cf19e344dd4/dataangrepet-varsling-massevarsling.pdf

Aale, P. K. (2019, 26. mars). Slik ble Russlands militæroperasjoner avslørt. Nå blir det mye vanskeligere. *Aftenposten*.

Abstract in English

Digital Tracking – a Matter of National Security?

More complex threat actors and risk assessments, e.g., hybrid threats, are often met with calls for increased government surveillance, which is of concern for democratic integrity. The two are therefore often presented as opposite poles. However, surveillance capitalism and the sale of extensive digital profiles can be manipulated and exploited by foreign powers for espionage, sabotage and subversion. The strategic effect is likely to increase as digitalization of governance, Smart Cities and IoT, as well as data storage and processing capacity, increase. The large amount of data can uncover information that should have been subject to clearance, tomorrow's leaders can in theory be tracked from infancy. In essence, the sale of personal data can have strategic effects on national security. As Surveillance capitalisms challenge the government surveillance monopoly, we should view privacy as a collective value for national defense.

Keywords: surveillance capitalism · national security · subversion · privacy