

Maskinlæring som trussel mot informasjonsintegriteten i samfunnet.

Amund Strandå Kristiansen

Innholdsfortegnelse

1. Innledning	2
1.1. Definisjoner	3
1.1.1. Informasjon	3
1.1.2. Integritet	3
1.1.3. Tillit	3
1.1.4. Maskinlæring	4
2. Informasjonssamfunnet tillater en å velge sin egen virkelighet	4
2.1. Innledning	4
2.2. Historisk sett	4
2.3. Moderne utfordringer med konsensus-modellen	5
2.4. "Jeg så det med mine egne øyne"	6
2.4.1. Kommersielle drivere av utviklingen	6
2.5. Falsk informasjon og ekkokammer som manipuleringsverktøy	7
3. GAN-nettverk	7
3.1. Innledning	7
3.2. Beskrivelse av teknologien	7
3.3. Illustrasjon av fremgangen til GAN-nettverk	8
3.3.1. Bilder	8
3.3.2. Tekst	9
3.3.3. Video	12
3.3.4. Lyd	12
3.3.5. Eksempel fra virkeligheten	13
3.4. GAN-nettverk som virkelighetsprodusenter	13
4. Lavtillitsforvaltning	14
4.1. Innledning	14
4.2. Den norske modellen under press	15
4.3. Konsekvenser av tiltaksfall	15
5. Systemer uten krav om tillit	15
5.1. Innledning	15

5.2.	Blockchain som desentralisert autoritet.....	15
5.3.	Krav til en slik løsning.....	16
5.4.	Andre mulige løsninger	17
5.4.1.	Lovgivning	17
5.4.2.	Maskinlæring for å motarbeide maskinlæring.....	17
6.	Oppsummering	18
7.	Referanser.....	18
8.	Vedlegg	20

1. Innledning

I denne oppgaven vil jeg legge frem argumenter for at den aggressive teknologiske utviklingen, særlig knyttet til maskinlæring, herunder *GAN-nettverk*¹ representerer en trussel mot informasjonsintegritet, i forvaltningen, og i samfunnet generelt. Faren er at den enkelte ikke lenger vil kunne ha tillit til informasjon han er i kontakt med, og dermed ikke vil kunne oppleve verden på samme måte som vi har blitt vant til i informasjonssamfunnet. Dermed trues også tilliten mellom parter i samfunnet. Hovedmekanismen for dette er at det blir stadig vanskeligere å skille mellom falske og ekte opplysninger samt at falske opplysninger kan produseres langt enklere enn tidligere- og til og med enklere en reelle opplysninger.

Ettersom stadig flere og større oppgaver blir automatisert øker samfunnets slagside mot feil i informasjonssystemer- enten feilinformasjon har blitt introdusert til systemet, opplysninger har blitt manipulert, eller opplysningene sammenstilles på en uheldig måte. Dette mener jeg over tid kan føre til et tap av tillit lik den vi har sett mellom mennesker og massemedia, særlig i utlandet.²

Senere i oppgaven vil jeg først ta for meg samfunnsmessige forhold som kan hjelpe eller bremse denne utviklingen ved å se til mediebransjen, som i mange land alt opplever at tilliten synker drastisk, før jeg undersøker hvordan maskinlæringsteknologi kan benyttes til å prolifere falske opplysninger. Til slutt vil jeg se på hvordan forvaltningen kan motvirke tap av tillit gjennom teknologiske løsninger som blockchain-teknologi, og jeg vurderer kort forskjellige juridiske regimer egnet til å regulere teknologien.

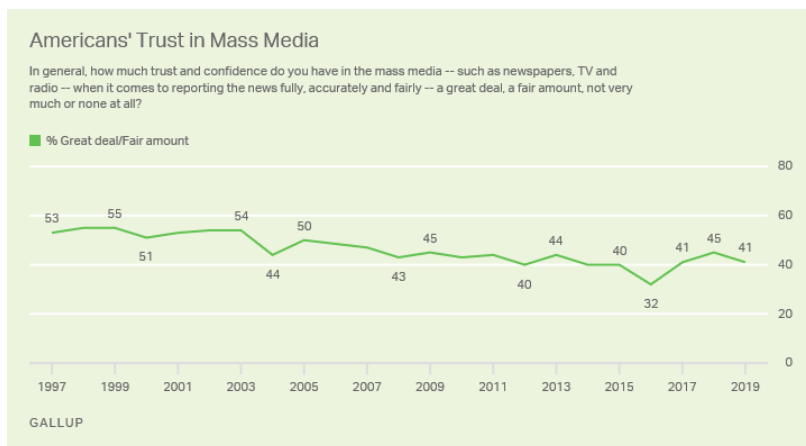
Motivasjonen til å skrive denne artikkelen er å belyse en konsekvens av framveksten av kunstig intelligens jeg oppfatter som underbelyst og lite utforsket: Mens maskinlæring i det abstrakte presenteres i et svært positivt lys³, skrives det regelmessig artikler om at hele stater er på defensiven grunnet proliferingen av falske nyheter⁴- uten at det knyttes noen sammenheng mellom disse to elementene.

¹ Se kapittel 2 samt Figur 1

² (BRENAN 2019)

³ Se Vedlegg 1

⁴ Se Vedlegg 2



Figur 1: Amerikaneres tillit til media over tid. På en 20-årsperiode har ca 20% av de som pleide å stole på media, mistet tilliten. (BRENAN 2019)

1.1. Definisjoner

1.1.1. Informasjon

Informasjon kan defineres på mange måter. Sentralt i denne oppgaven er at informasjon har til hensikt å informere eller opplyse mottakeren⁵, dvs. å angi fakta om virkeligheten som er nyttig for den gitte mottakeren. Det innebærer at en også kan overlevere et budskap som kan utgi seg for å være objektivt- altså basert i virkeligheten, uten at det faktisk er det. En kan da snakke om falsk informasjon, eller, som jeg ofte er innom i denne oppgaven "fake news".

1.1.2. Integritet

I og med at oppgaven har et teknisk og forvaltningsmessig fundament henter jeg integritetsbegrepet mitt fra Cybersecurity-feltet med utgangspunkt i den vanlige betydningen av ordet.

Med integritet menes at en har selvstendig kontroll over det man eier, ofte seg selv: En kan handle som en selv ønsker. I en forlengelse av denne definisjonen finner vi at personer, organisasjoner, eller ting kan forbindes med høy, eller god, integritet. Organisasjonen er rettferdig og lar seg ikke påvirke på utilbørlige måter, den er forutsigbar.⁶

Ideen om informasjonintegritet hentet fra cybersecurity-verdenen er kanskje nærmest beslektet med den bredere definisjonen. For at informasjon skal anses å ha høy integritet må en ha tillit til at opplysningene ikke kan ha blitt endret.⁷ En forlengelse av denne definisjonen vil være at en kan ha tillit til riktigheten av opplysninger, og dermed beslutninger som strømmer ut av denne informasjonen.

1.1.3. Tillit

Tillit er dermed integritetens motpart. Har en tillit til noe innebærer det at en mener det innehar høy integritet. I en forlengelse av dette kan systemer kan ha tillit til hverandre enten som standard, eller

⁵ (Rossen 2018)

⁶ (Store Norske leksikon u.d.)

⁷ (Mahler 2019)

oppnå det for eksempel gjennom fremvisning av sertifikater eller inntasting av passord. I denne oppgaven vil jeg primært fokusere på tillit som noe vi mennesker har til forvaltningen og til digitale tjenester. En kan også se for seg en modell hvor samfunnet som helhet har en viss integritet, og vi som deler av helhet en har tillit til denne. Siden våre viktigste samfunnsfunksjoner forvaltes gjennom datasystemer er vår tillit til disse funksjonene uløselig knyttet til informasjonintegritet: En kan ikke unngå å miste tillit til forvaltningen dersom datasystemene feilaktig konkluderer med at du har svindlet til deg bostøtte.⁸

1.1.4. Maskinlæring

I denne oppgaven vil jeg diskutere maskinlæring som en teknologi rent overordnet, og fokusere på en form for maskinlæring spesielt: GAN (*Generative Adversarial Networks*) spesielt. Om maskinlæring generelt er det tilstrekkelig å legge til grunn at maskinlæring er teknologi som lar datasystemer produsere store mengder informasjon med begrenset input fra mennesker. Inntil veldig nylig har informasjon generert av slike systemer vært av en kvalitet som gjør den lett å skille fra virkelige opplysninger- men som jeg kommer tilbake til under forandrer dette seg fort.

2. Informasjonssamfunnet tillater en å velge sin egen virkelighet

2.1. Innledning

I dette kapittelet vil jeg kort forklare hvordan jeg velger å se for meg samfunnet: Samfunnet er et system hvor individer i dag selv kan beslutte å delta i grupperinger ut ifra hvilken informasjon de best liker. Jeg vil peke på at denne utviklingen kombinert med bevisst feilinformasjon har ført til senket tillit i stor skala.

2.2. Historisk sett

Fra et historisk perspektiv har maktgrupper i samfunnene hatt mulighet til å bestemme hvilke opplysninger som må anses som korrekte, mer eller mindre uavhengig av hva virkeligheten tilsier.⁹ Denne makten har vært brukt til å skape konsensus rundt ideer som religion og styresett- ofte til ulempe for hele eller deler av befolkningen. Ettersom samfunnet har blitt mer liberalt og teknologiske fremskritt har det blitt vanskeligere å kontrollere informasjonsflyten, og det har blitt enklere å bekrefte eller avkrefte opplysninger. I takt med dette har mange samfunn innrettet seg etter utviklingen og lagt opp til fri informasjonsflyt så langt det er hensiktsmessig.¹⁰

Overordnet sett kan en si at en har gått fra en situasjon der det er få dommere som angir hvilke opplysninger som er de riktige, til at alle nå er dommere og kan ta stilling til -og handle basert på de opplysningene vi ønsker og gjennom dette oppnår et konsensus rundt hva som er korrekt.

⁸ Noe fra martines master

⁹ (Grøn 2019)

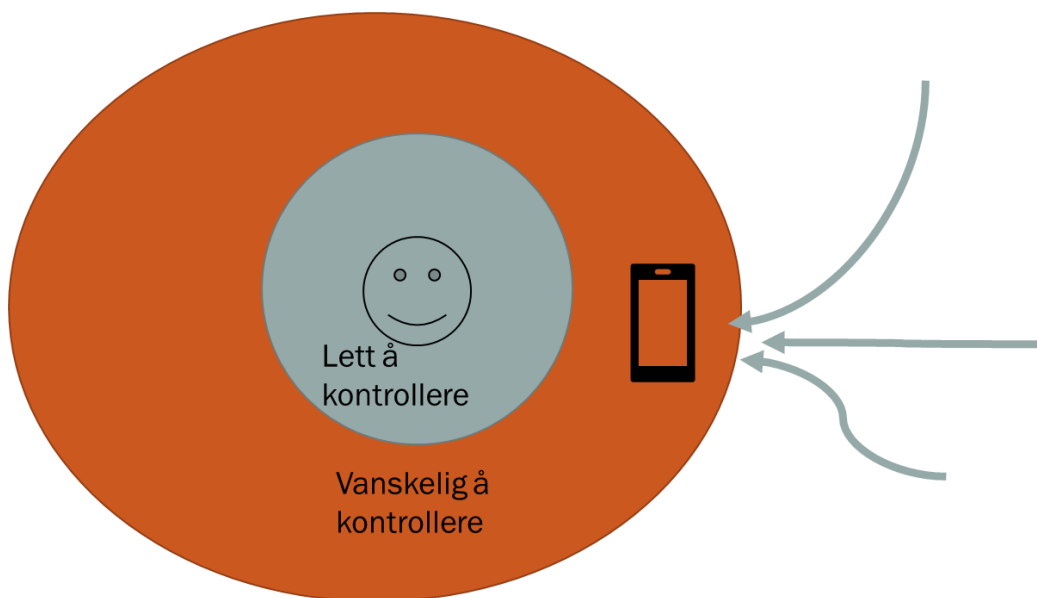
¹⁰ Offentleglova

2.3. Moderne utfordringer med konsensus-modellen

Ettersom informasjonsteknologi (Jeg inkluderer her også teknologi som analoge telefoner og TV) har utviklet seg har det blitt enklere å tilegne seg informasjon. Enhver kan oppsøke eller bli eksponert for informasjon om et gitt tema, og bygge sin virkelighetsoppfatning på denne.

Det har ikke bare blitt enklere å finne informasjon- det har blitt mye mer av den: Informasjon blir gjort tilgjengelig for første gang eller ny-publisert på internett gjennom menneskelig arbeid, men også kameraer, GPs 'er, rutere og et vell av andre sensorer laster kontinuerlig opp informasjon som indekseres aggregeres, og kan søkes på. På denne måten har individets "virkelighetshorisont" blitt utvidet betydelig.

Denne "utvidede virkelighetshorisonten" bærer med seg et vell av fordeler: Der en tidligere måtte være rik og privilegert for å kunne se og ta direkte stilling til ting som skjedde i fremmede land, kan en nå åpne en nettavis for å få det på direkten. En snakker derfor ofte om at diskursen blir demokratisert- i kontekst av denne oppgaven kan en si at vi får flere "dommere" som kan ta stilling til informasjon og hva som stemmer overens med virkeligheten.



Figur 2: Modellen illustrerer at et individs rekkevidde er blitt langt større, men opplysninger hentet gjennom digitale kanaler er også vanskeligere å få etterprøvd personlig- en er dermed avhengig av et konsensus.

Som illustrert i modellen over har individer en nærliggende sfære hvor informasjon kan testes opp mot virkeligheten- melder telefonen om regn kan en stikke hånden ut av vinduet for å teste dette. Denne virkelighetsoppfatningen ligger dermed i stor grad fast- men den har kort rekkevidde.

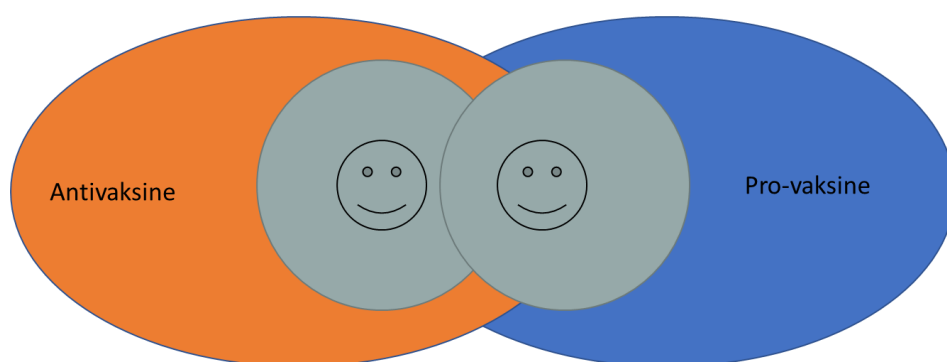
For å kunne benytte seg av den utvidede sfæren må en enten opptre ukritisk, en må finne konsensus, eller en må benytte seg av et mellomledd en har tillit til- som f.eks. en avis. Siste alternativ er å opptre ukritisk: En ser utover horisonten og plukker opp informasjon basert på egne forestillinger.

Om en imidlertid ikke skuer ut i denne større sfæren teknologi har gitt tilgang til, stiller en med et stort handikapp: En kan ikke delta i diskursen på lik linje med andre, og en går glipp av et vell av opplevelser en ellers kunne observert som tredjepart. En snakker om et digitalt klasseskille- de som har verktøyene som trengs for å utforske den videre verden gjennom digitale kanaler, og de som

ikke har det¹¹. Ut i fra dette kan en trygt konstatere at det å oppleve verdenen gjennom digitale verktøy er viktig, og at det er viktig at alle deltar- ulempen er stor for de som ikke gjør det. Den "utvidede virkelighetshorisonten" har blitt en del av samfunnet til en slik grad at en ikke tenker på at de fleste inntrykk en har i løpet av en dag kanskje ikke engang er opplevd direkte¹²

2.4. "Jeg så det med mine egne øyne"

En fremvoksende sideeffekt av at så mye informasjon er tilgjengelig for alle, er at en ikke lenger som samfunn kan forkaste feilinformasjon og finne et konsensus i samme grad som tidligere: Et godt eksempel på dette er vaksinenektene som har kommet til å være i fremgang på verdensbasis, og har egne helsenettsider og informasjonskanaler.¹³ En gruppe som har et annet synspunkt en staten, storsamfunnet, eller simpelthen majoriteten kan enkelt finne sammen og forsterke og verifisere gruppens fakta.



Figur 3: De personene har nært overlappende "Nære virkeligheter" og "Digitale virkeligheter", men ender opp med do vidt forskjellige standpunkt fordi de er del av forskjellige kretser på internett.

Sagt med andre ord oppnår hvert enkelt individ sitt eget ekkokammer, alt etter hvilket standpunkt de ønsker å holde seg til- det vil som regel alltid være mulig å finne andre til å forsterke standpunktet.

2.4.1. Kommersielle drivere av utviklingen

En faktor som underbygger konstruksjonen av disse alternative virkelighetsoppfatningene, er at kommersielle aktører som Facebook og Google har fordel i å forsterke disse: Tjenestene deres tjener penger på reklame ut ifra hvor mange som ser reklamen og hvor ofte de klikker på den. For å få flere klikk og kikk på reklamene ønsker de dermed å holde brukerne på siden, og det oppnår de best ved å ikke eksponere den for noe den kan oppfatte som ubehagelig eller kontroversielt. Dermed har de utviklet innfløkte systemer for å identifisere brukere, og å servere dem opplysninger de i størst mulig grad vil være komfortable med.¹⁴

¹¹ (Kunnskapsdepartementet 2018)

¹² Aviser, bøker, og viderefortelling er eldre verktøy med samme oppgave, men aldri før har "alle" hatt tilgang til slike mengder informasjon på en slik måte: Inntrykk er blitt mye rikere fordi en kan koble bilder, video, og lydklipp dynamisk og med langt høyere kvalitet en tidligere.

¹³ (NRK 2019)

¹⁴ (DuckDuckGo 2018)

2.5. Falsk informasjon og ekkokammer som manipuleringsverktøy

Som hintet til i forrige kapittel er det kanskje særlig politiske meninger som er kontroversielle og en identifiseres ut fra. I studien fra DuckDuckGo er det tema som er politisk ladet i USA en ser størst variasjon i resultatene. Det er også her folk opplever at det er størst splittelse i folks virkelighetsoppfatning- men det er selvsagt de som holder med det andre standpunktet som tar feil.¹⁵ Gitt at folk tilsynelatende ganske velvillig låser seg inn i ekkokammer de finner behagelige, er det ikke overraskende at større aktører en bare bekymrede antivaksine-foreldre har sett verdien av å systematisk spre falsk informasjon.¹⁶

De siste årene har et sentralt tema vært at fiendtlige aktører skal ha benyttet "fake news" til å spre farlige synspunkt i andre stater. Mest oppslag har det vært rundt de Russiske kampanjene i Ukraina¹⁷ og i USA¹⁸. Hvor Russland angivelig brukte store kontorer fulle av personer til å produsere artikler, kommentarer, facebook-grupper og annet innhold med hensikt å svekke Ukraineres støtte til krigen i Øst-Ukraina, og styrke støtten til outsider-kandidater som Bernie Sanders og Donald Trump, henholdsvis. Uavhengig av de målene og suksessen til disse kampanjene viser forskning i USA tydelig at et av resultatene ble økt politisk polarisering og mer mistro til media.¹⁹ Det er derfor sterk grunn til å tro flere falske fakta fører til økt polarisering og mistro nokså uavhengig av målet med å spre de falske faktaene: Mer grums i vannet fører uansett til en skitnere dam.

3. GAN-nettverk

3.1. Innledning

I dette kapittelet vil jeg diskutere GAN-nettverk- en maskinlæringsteknologi. Den sentrale tanken er at GAN-nettverk kan fungere som generatorer av falske opplysninger- og at produsenter av falske artikler, rapporter, videoer mv. vil ha et fundamentalt fortrinn over produsenter av ekte opplysninger- som jo må undersøke virkeligheten, og så forholde seg til det de observerer. Jeg vil også redegjøre for teknologiens fremgang og eksempler på hva GAN-nettverk allerede kan produsere av overbevisende innhold.

3.2. Beskrivelse av teknologien

GAN-nettverk er som nevnt en form for maskinlæring. *Generative Adversarial Networks* fungerer grunnleggende sett ved at en part ("Forfalskeren") forsøker å lage et produkt den andre parten ("Banken") ikke kan skille fra bakgrunns materialet (Ekte pengesedler). Forfalskeren får poeng basert på hvor god banken synes resultatet er, og kan dermed opp eller nedprioritere hvilke egenskaper som skal prioriteres i neste omgang. Gjennom millioner av runder med dette kan system trenes til å generere nye produkter innenfor hva som helst som er matet inn i en maskin, og hvor en har tilstrekkelig bakgrunns materiale til å tillate forfalskeren å gi poeng på en hensiktsmessig måte. Et sentralt element er at "forfalskeren" aldri ser bakgrunns materialet, men (Som regel) starter med tilfeldig støy som utgangspunkt- dermed kan et slikt system generaliseres til hva som helst, og

¹⁵ (Fletcher 2017)

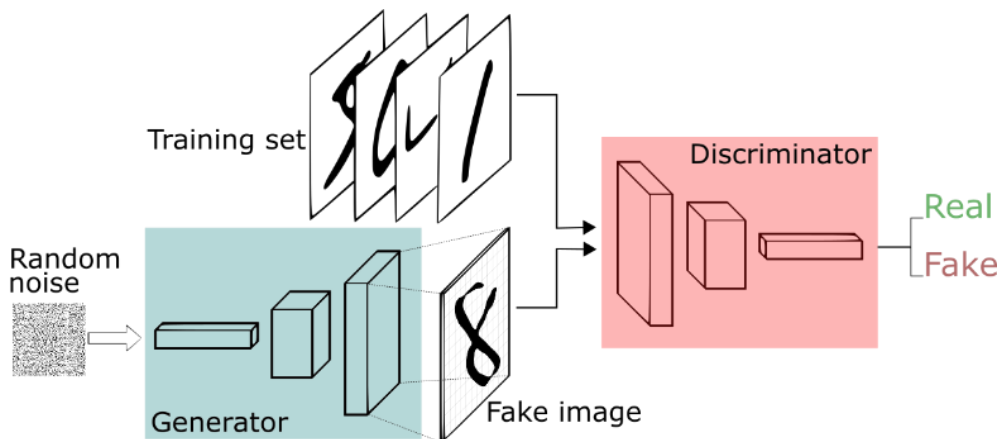
¹⁶ Deres standpunkt vil selvsagt være at pro-vaksineleger er de som sprer løgner- og dermed står en på stedet hvil.

¹⁷ (Cain 2019)

¹⁸ (BBC 2019)

¹⁹ (BRENAN 2019)

mennesker må ikke arbeide for å identifisere de fundamentale egenskapene med bakgrunnsmateriale- for det finner systemet helt på egenhånd.²⁰²¹ Se nedenfor for eksempler på slike produkter, og hvordan teknologien har utviklet seg.



22

Figur 4: Illustrasjon av hvordan en GAN-modell fungerer overordnet sett. Generatoren baserer seg på støy og nærmer seg gradvis et riktig resultat. Dermed trenger ikke mennesker å definere egenskaper for hva systemet skal generere.

3.3. Illustrasjon av fremgangen til GAN-nettverk

Det er viktig å merke seg at GAN-nettverk som konsept bare har eksistert siden 2014. Det er derfor veldig usikkert hvordan teknologien, eller lignende teknologier, vil utvikle seg. Det er imidlertid konstatert at utviklingen har gått raskt, og at den overordnede systemmodellen har vist seg å være effektiv i flere sammenhenger. En kan også konstatere at det allerede i dag kan genereres falskt innhold som mangler noen tilknytning til virkeligheten, men samtidig ser realistisk ut. Under følger en serie eksempler på verktøy jeg anser som særlig nyttige til å spre falsk informasjon i samfunnet, spesielt i sammenheng.

3.3.1. Bilder

Det heter seg at en tror det når man ser det. Om en ønsker å ta stilling til en hendelse er det naturlig å be om et bilde slik at en kan danne seg sitt eget inntrykk. Historisk sett har manipulering av bilder foregått, men en overvekt av bilder fra enhver hendelse har i moderne tid kunne brukes til å skape et helhetlig bilde av hendelsen. Med et system for å generere realistiske falske bilder, kan det tenkes at en skaper en overflod av bilder som gjengir hendelsen på den ønskede måten- og dermed kan hevde at de ekte bildene er de falske. Slik kan en også skaffe bevis for ting som aldri har skjedd.

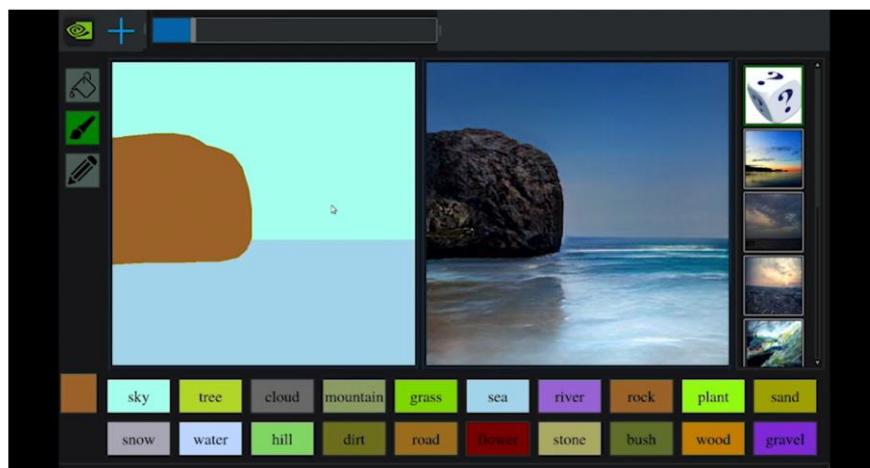
²⁰ Her er selvsagt mye detaljer skrevet vekk.

²¹ (Ian J. Goodfellow* 2014)

²² (Floydhub 2019) For øvrig en god innledning til teknologien- med mange gode eksempler.



Over er en serie GAN-genererte ansikt de siste årene. Allerede i 2016 var det mulig å generere ansikt som så fotorealistiske ut- begrensningen lå i at det ikke eksisterte datakraft til å generere resultater i høyere oppløsning. Ettersom tiden har gått har datakraft økt og den generelle modellen har blitt tilpasset forskjellige bruksområder for å øke effektiviteten. Resultatet er at en f.eks. kan opprette en Facebook-profil med en egengenerert representasjon av en person. Bildet vil ikke kunne identifiseres som stjålet og det vil være vanskelig å bekrefte at profilen er falsk.



24

Dette verktøyet utviklet av Nvidia kan direkte generere nær fotorealistiske landskap basert på en brukers tegninger. Igjen blir det vanskelig, ved hjelp av bildesøk, å konstatere om dette stedet eksisterer eller ikke. Som nevnt over kan slike verktøy potensielt brukes for å skape bevis for falske hendelser.

3.3.2. Tekst

Kanskje det viktigste verktøyet for å spre informasjon er skriftlige opplysninger- enten det er gjenfortellinger eller rene data-ark. En artikkel med falskt innhold kan i utgangspunktet produseres

²³ (Goodfellow 2019)

²⁴ (Salian 2019)

like enkelt som en artikkel med reelt innhold- men med et GAN-nettverk som produserer det samme blir balansen en annen.²⁵

Input:

A train carriage containing controlled nuclear materials was stolen in Cincinnati today. Its whereabouts are unknown.

Resultat:

The incident occurred on the downtown train line, which runs from Covington and Ashland stations.

In an email to Ohio news outlets, the U.S. Department of Energy said it is working with the Federal Railroad Administration to find the thief.

“The theft of this nuclear material will have significant negative consequences on public and environmental health, our workforce and the economy of our nation,” said Tom Hicks, the U.S. Energy Secretary, in a statement. “Our top priority is to secure the theft and ensure it doesn’t happen again.”

The stolen material was taken from the University of Cincinnati’s Research Triangle Park nuclear research site, according to a news release from Department officials.

The Nuclear Regulatory Commission did not immediately release any information.

According to the release, the U.S. Department of Energy’s Office of Nuclear Material Safety and Security is leading that team’s investigation.

“The safety of people, the environment and the nation’s nuclear stockpile is our highest priority,” Hicks said. “We will get to the bottom of this and make no excuses.”²⁶

Teksten markert som resultat over er generert av *GPT-2*-modellen. Teksten beskriver en hendelse som aldri har funnet sted, men som for alle i nærheten av Cincinnati nok ville ha vært overbevisende nok til å unngå toget akkurat denne dagen. Det er viktig å bemerke seg at systemet ikke er begrenset til å skrive nyhetsartikler- den valgte å svare inputen på denne måten. Det er altså et generelt system som svarer på input på en av flere mulige måter. Under får systemet matet inn en tekst og så spørsmål, hvor maskinen skal fylle inn svarene. Systemet er ikke på forhånd innstilt på å svare på spørsmål, men "forstår" at det skal gjøres slik:

Input er i vanlig skrift/ **Resultat er i fet skrift:**

The 2008 Summer Olympics torch relay was run from March 24 until August 8, 2008, prior to the 2008 Summer Olympics, with the theme of “one world, one dream”. Plans for the relay were announced on April 26, 2007, in Beijing, China. The relay, also called by the organizers as the “Journey of Harmony”, lasted 129 days and carried the torch 137,000 km (85,000 mi) – the longest distance of any Olympic torch relay since the tradition was started ahead of the 1936 Summer Olympics.

²⁵ Se kap. 3.4

²⁶ (Alec Radford 2019)

After being lit at the birthplace of the Olympic Games in Olympia, Greece on March 24, the torch traveled to the Panathinaiko Stadium in Athens, and then to Beijing, arriving on March 31. From Beijing, the torch was following a route passing through six continents. The torch has visited cities along the Silk Road, symbolizing ancient links between China and the rest of the world. The relay also included an ascent with the flame to the top of Mount Everest on the border of Nepal and Tibet, China from the Chinese side, which was closed specially for the event.

Q: What was the theme?

A: **"one world, one dream"**.

Q: What was the length of the race?

A: **137,000 km**

Q: Was it larger than previous ones?

A: **No**

Q: Where did the race begin?

A: **Olympia, Greece**

Q: Is there anything notable about that place?

A: **birthplace of Olympic Games**

Q: Where did they go after?

A: **Athens**

Q: How many days was the race?

A: **seven**

Q: Did they visit any notable landmarks?

A: **Panathinaiko Stadium**

Q: And did they climb any mountains?

A:

Target answers: unknown or yes

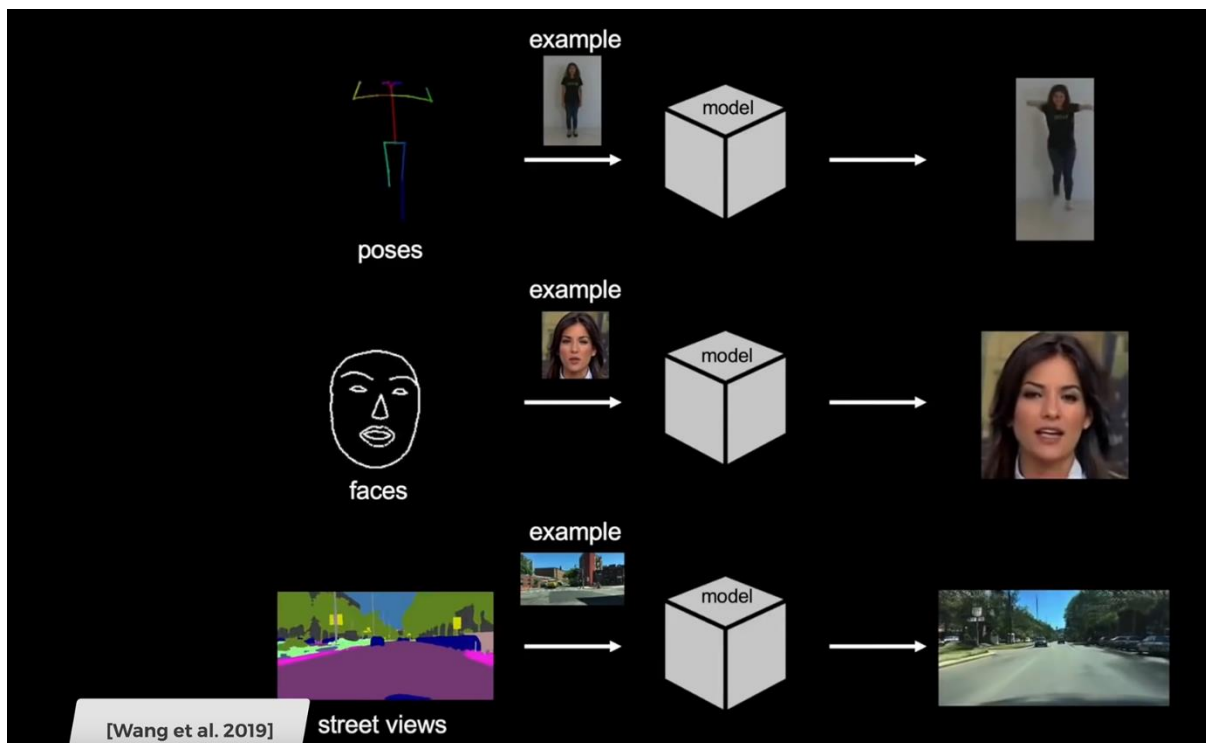
Model answer: **Everest**²⁷

Som demonstrert over kan altså et GAN-nettverk benyttes til å generere flere typer skriftlig innhold som ligger nært opp mot det et menneske ville produsere, og med en demonstrert forståelse for hva inputen er. Et GAN-nettverk vil dermed kunne gjøres til en "ekspert" på et tema før det stilles til å skrive om det. Om en på dette stadiet gir falske opplysninger, eller lar systemet fylle inn sine egne parameter, vil det kunne skrive høyst realistiske tekster. Et eksempel kan være at en lærer et system opp på artikler om folkemord, for så å sette den løs i å skrive slik artikler selv: På kort tid vil det eksistere artikler som omhandler folkemord i hver eneste by begått av hver eneste gruppe- og det å skille de reelle historiske hendelsene vil med tiden bli vanskelig.

²⁷ (Alec Radford 2019)

3.3.3. Video

Nært beslektet med bildemedia finner vi video. Videomanipulering hører kanskje for de fleste til innenfor filmbransjen- men også her er utviklingen enorm og det finnes system som bare behøver et enkelt bilde for input før det kan generere hendelsesforløp totalt uten rot i virkeligheten.



28 29
,

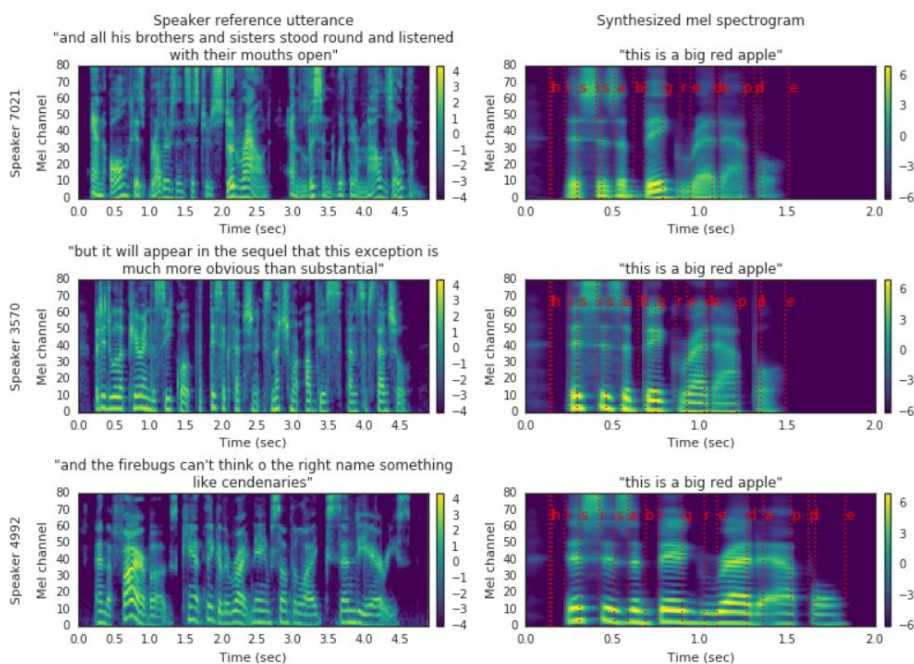
På bildet over ser vi utdrag fra en videopresentasjon av systemet: Basert på et enkelt bilde av en person kan systemet bruke personen som en dukke til henholdsvis dansing og snakking. Basert på et gatebilde og en enkel modell kan en nær fotorealistisk kjøretur genereres. Muligheten for å oppkonstruere hele hendelsesforløp basert på svært lite input er reel- både i det store: At en skaper video av et terrorangrep for å agitere til konflikt, og i det små: At noen sprer en video der du uttaler deg rasistisk. For å gjøre illusjonen komplett behøves imidlertid et siste element:

3.3.4. Lyd

Et siste element som må til for å skape en overbevisende virkelighetspresentasjon, er lyd. I film i dag benytter en allerede foley-artister og lydbibliotek til det aller meste, men om en skal skape noe som skal ha skjedd i virkeligheten må en ha tilgang til virkelige personers stemmer.

²⁸ (Two minute papers 2019) (Kilde til Video)

²⁹ (Catanzaro 2019) (Forskningsartikkel)



30

Som illustrert ovenfor kan dette GAN-nettverket produsere et "stemme-avtrykk" basert på bare 5 sekunders lydopptak. Systemet behøver ikke å ha hørt et individ uttale alle lyder eller en lang rekke ord for å skape et realistisk resultat³¹- altså er det ikke bare kjente personer som er utsatt for å bli etterlignet. Enhver som har sendt et videoklipp med lyd av seg selv kan i teorien bli "klonet", og ens stemme kan brukes til å spre et hvilket som helst budskap.

3.3.5. Eksempel fra virkeligheten.

Et nyere eksempel som ble vidt sirkulert som ekte, er en video av Mark Zuckerberg som uttrykker at han har stjålet data fra millioner av borgere og gjennom dette kan kontrollere dem og deres fremtid.³² Særlig i det mindre formatet Instagram oppfordrer til gjennom å først og fremst være en telefon-app ser videoen realistisk nok ut til at det vil ta en viss innsats, selv for en person som er kjent med teknologien, å bekrefte eller avkrefte om videoen er sannferdig.

3.4. GAN-nettverk som virkelighetsprodusenter

Som beskrevet ovenfor er moderne kunstig intelligens i dag kapabel til å konfigurere til å produsere mange typer innhold som er realistisk eller nært realistisk i mange sammenhenger. Konsekvensen av dette er at digitalt innhold som strekker seg utover den nære horisonten til enhver tid kan være falskt, samtidig som det vil være med på å forme livet til alle som har kontakt med den videre verden. En kan på denne måten si at GAN-nettverk er med på å forme den faktiske virkeligheten: Det kan tenkes at mange finner opplysninger og konklusjoner som er lett å være enig i blant GAN-nettverks artikler, videoer, eller taler- og etter hvert også handler og baserer livene sine på disse opplysningene.

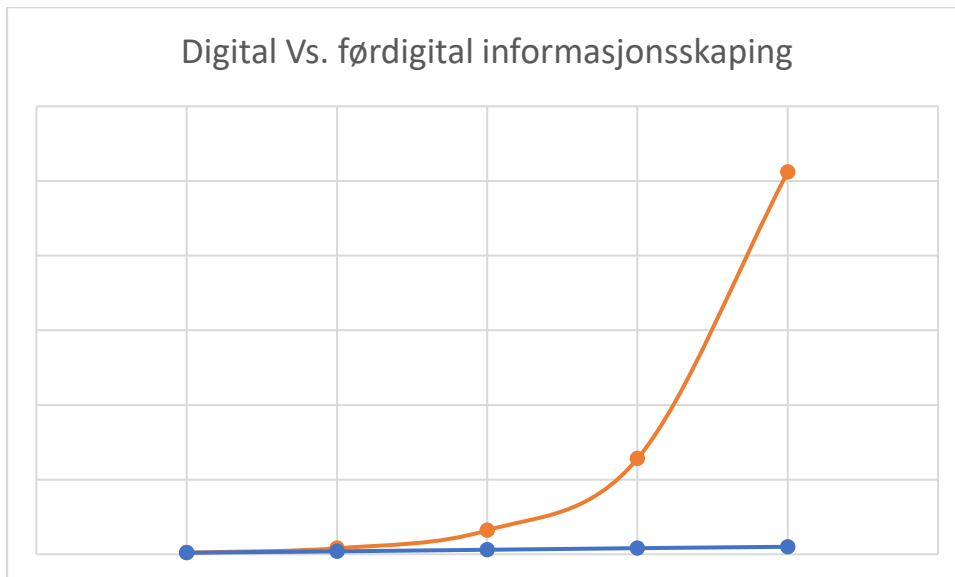
³⁰ (Ye Jia * 2018)

³¹ (Ye Jia * 2018)

³² (Posters 2019)

Det er like nærliggende å tenke at mange ikke lenger vil klare å ha tillit til noen informasjonskanaler lengre- alle sier jo vidt forskjellige ting! For disse blir kanskje løsningen å være ekstremt kildekritisk, eller å begrense sin "virkelighetshorizont". En slik person vil sannsynligvis tro på mange færre feile ting, men vil samtidig være langt mindre oppdatert på utviklingen rundt seg.

Et motargument er at det jo alt finnes flust av falske opplysninger, og kildekritikk er jo en egenskap som fokuseres på barneskolen av, men maskinlæring vil kunne fundamentalt endre forholdet mellom ekte og falske opplysninger:



Figur 5: Illustrasjon av at det uten digitale verktøy var et nokså lineære forhold mellom innsats: 1 time skrijving, og resultat: En artikkel. Med GAN-maskinlæring kan en spekulere i at f.eks. 1 million timer utvikling kan gi et nært ubegrenset antall artikler.

Det nokså lineære forholdet mellom innsats og produsert informasjon vil ikke lenger være gjeldende om maskinlæringssystemer kommer i vid drift. Disse systemene kan, om konfigurert til det, generere tusenvis av artikler i minuttet og dermed enkelt utkonkurrere reelle informasjonsskapere. En vil dermed selv med ekstrem kildekritikk bli eksponert for og internalisere falske opplysninger gjennom at disse opplysningene etterhvert trekker inn i dine valgte informasjonskilder.

4. Lavtillitssforvaltning

4.1. Innledning

I denne delen av oppgaven vil jeg diskutere et mulig utfall av at falske opplysninger oversvømmer det digitale landskapet til en slik grad at opplysninger innhentet gjennom digitale kanaler ikke lenger kan stoles på.

4.2. Den norske modellen under press

I Norge i dag lever vi i et miljø av gjensidig tillit mellom staten og borgerne.³³

Forvaltningsinstitusjoner har i stor grad tillit til sin befolkning, og jeg vil hevde at det samme er sant den andre veien: Vi kan som hovedregel få innsyn i viktige dokumenter, vi fyller selv ut skattemeldingen som bare unntaksvis blir etterkontrollert, og det samme gjelder for bostatus når vi er studenter. Dette fungerer som regel greit, kanskje fordi vi er ærlige og vil gjengjelde den tilliten vi føler til staten, eller kanskje vi rett og slett ikke tror vi kan lyge og komme unna med det.

Men hva om vi ikke lenger har tillit til institusjonene våre: Vi har ikke helt oversikt over hva de gjør og hva de sier- for hver dag kommer det uttalelser tilsynelatende ekte, men stikk i strid med den offisielle linjen. Kanskje vil vi ikke lenger føle at vi kan stole på disse, og kanskje føler vi ikke lenger at de har mulighet til å ta oss i løgnen? Og videre: Hva viss forvaltningens tidligere så sikre registre etter hvert infiltreres av uriktige opplysninger?

4.3. Konsekvenser av tiltssfall

Tillit har blitt omtalt som "den nye oljen".³⁴ Fordi det tillater oppgaver i samfunnet å gjennomføres med liten "overhead" knyttet til verifisering, oppfølging, korrigering, osv. Generelt scorer land hvor det er høy tillit mellom partene, også høy på økonomisk og sosial velferd.

Om tilliten i samfunnet skulle falle som følge av at informasjonsintegriteten forvitres, vil det kunne føre med seg store effektivitetstap: En vil for eksempel ikke lenger kunne bruke innsendte bilder som identifikasjon: For å sikre at du er den du er vill sannsynligvis fysisk oppmøte være eneste realistiske metode. Det samme gjelder for forvaltningen, som ikke lenger overbevisende forkynne budskap digitalt- og hvem som helst kan jo generere stempel og en ordlyd som høres korrekt ut, så brev er nok ute av bildet og. Kanskje må en så langt tilbake til at politiet eller andre autoriteter må forkynne små og store budskap for å oppnå at de blir etterfulgt. Man ender altså opp med at digitalisering paradoksalt nok hemmer digitalisering.

5. Systemer uten krav om tillit.

5.1. Innledning

Som kort skissert overfor er det store ulemper knyttet til å miste tilliten mellom parter i samfunnet. Imidlertid finnes det alt blockchain-baserte systemer som av natur ikke krever tillit til motparten(e), og dermed er egnet til å loggføre og verifisere informasjon.

5.2. Blockchain som desentralisert autoritet

Blockchain er en av hovedideene som underbygger Bitcoin. Kort forklart innebærer en blockchain at hver eneste transaksjon skrives ned til en felles kvittering, som alle parter får en verifisert kopi av. Om en kvittering på noe tidspunkt skulle avvike fra de tusenvis av andre, like kvitteringene, forkastes avvikerens. Utgangspunktet var at dette systemet skulle sikre monetære transaksjoner av Bitcoin, men teknologiens prinsipper er også nyttig til andre formål.³⁵

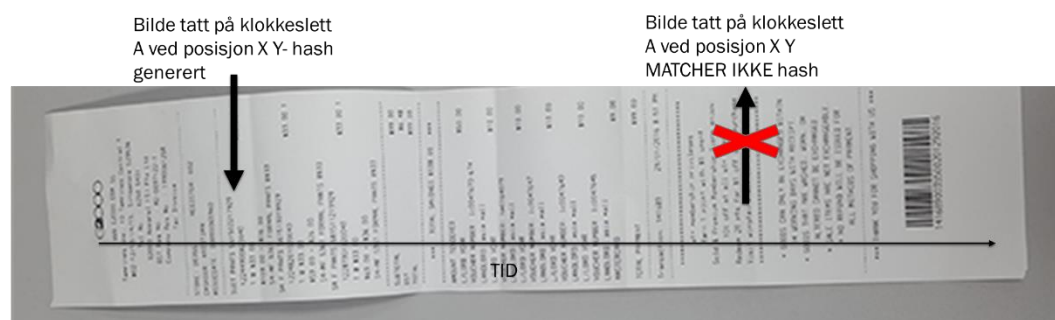
³³ (Kleven 2016)

³⁴ (VIGSNES 2017)

³⁵ (Parkins 2015)

Et sentralt aspekt ved denne modellen er at hver enkelt part ikke må ha tillit til noen annen part: Om en forsøker å lure systemet, vil hans versjon av virkeligheten bli forkastet- eneste måte å endre på konsensusen som ender opp med å bli skrevet ned, er å kontrollere over 50% av "kvitteringskriverene", og siden hver enkelt svindler ønsker å få forfalsket sine verdier separat, er det nesten umulig å overvinne majoriteten som alltid er i enighet.

Om en setter denne teknologien i kontekst av et samfunn hvor ingen kan enes om hva som er riktig representasjon av virkeligheten, ser en fort verdien. Nettverket kunne teoretisk sett brukes direkte til å holde avstemninger om hva som har skjedd eller ikke skjedd- men dette vil være lite heldig fordi en da lett kan komme under tyranni fra en liten majoritet (F.eks. Kan majoriteten, som er EU-motstandere, få bokført at EU er forferdelig, selv om den store minoriteten er nøytrale eller positive). En mer nærliggende løsning er å bruke teknologiens mulighet til å loggføre hendelser på en tillitsløs måte for å verifisere enkeltopplysninger:



Figur 6: Figuren illustrerer at et bilde loggføres via en unik Hash-kode. Om dette bildet senere forsøkes publisert igjen kan det kontrolleres mot Blockchain-kvitteringen for å undersøke om bildet er identisk. Om det ikke er det kan det trygt forkastes.

Som vist ovenfor kan en generere Hash-koder³⁶ ut ifra den visuelle dataen i f.eks. et bilde samt bildets metadata, for så å lagre dette i Block-chainen. Om en på et senere tidspunkt er usikker på bildets ekthet, kan en kontrollere hashen. Om bildet senere blir vist et annet sted, kan en kontrollere opp mot hash-koden i Block-chainen.

5.3. Krav til en slik løsning

I og med at det genereres så enorme mengder informasjon i dag, må det antas at det er upraktisk å lagre hash-koder basert på alt i en Block-chain. Det må derfor eksistere kriterier for hva som skal sikres på denne måten, og ikke. Et annet problem er at en fortsatt ikke kan konstatere hvorvidt informasjonen som er representert på Block-chain er ekte- en kan bare konstatere hva som er originalen. Dermed er ikke det fundamentale problemet knyttet løst: En har bare oppnådd å stadfeste original-media, ikke å luke ut falske opplysninger. En videreutvikling av dette er at en oppretter "verifiserte" og "ikke-verifiserte" kategoriseringer i media, men dette skaper sine egne problemer for presse- og ytringsfrihet.

³⁶ Den digitale dataen prosesseres av en algoritme som gir tilbake en kort tekst-streng som er unik for akkurat dette bildet. Fordi algoritmen inneholder en stor grad av støy, vil selv små endringer i dataen resultere i en totalt annerledes Hash-kode.

5.4. Andre mulige løsninger

5.4.1. Lovgivning

Det finnes allerede minst et eksempel på at det er implementert lovgivning med hensikt å hemme spredningen av falske opplysninger:³⁷ I Singapore har den autoritære regjeringen nettopp benyttet en lov³⁸ som tillater dem å komme med advarsler om falsk informasjon samt detaljerte motsvar, uavhengig av hvorvidt publiseringsmediet ønsker det. I dette tilfellet har Facebook tilsynelatende stilt seg negativ til å sette informasjonen som nå er stemplet som falsk, under tvil, men de hadde ingen valg gitt lovgivningen i landet.

Dette illustrer at løsninger gjennom lovgivning er vanskelig å implementere på en god måte: I dette tilfellet var innlegget publisert av en populær politisk dissident, og det er en åpenbar interesse for den Singaporiske regjeringen at innlegget diskrediteres og hindres fra å spres.

Lovgivning som tillater staten å markere opplysninger som falske er dermed grunnleggende problematiske både fra et pressefrihets- og talefrihetsperspektiv, og slik autoritær lovgivning kan fort bli et yndet verktøy gitt at feil personer får regjeringsmakt.

En kan tenke seg en mykere løsning hvor det opprettes ordninger (Som kort nevnt ovenfor) hvor staten tilbyr verifiseringstjenester til journalister og andre parter en forutsetter har en demonstrert presseetisk kompetanse. Informasjon fra disse kan aggregeres enten gjennom aviser eller gjennom en statlig tjeneste, med mål om å opprettholde en privilegert informasjonsstrøm av høy kvalitet.

Også her møter en på problemer hvor det kan oppfattes at staten favoriserer personer som er positive til regjeringen og gir disse en plattform, fremfor andre som er negative. Kanskje kan denne ordningen styres av et uavhengig organ- men da er en tilbake på den selvjustis-modellen vi har i dag: At Pressens Faglige Utvalg vurderer konkrete artikler fra medlemsorganisasjoner. En slik modell kan imidlertid bare fungere så langt folk flest har tillit til PFU's upartiskhet- noe som også må forutsettes å være under angrep i en slik fremtid jeg har skissert.

En annen innfallsvinkel er å ulovliggjøre villig publisering av falsk informasjon med formål om å villed- men her møter en umiddelbart problemer med å skille satire, humor, parodi, kritikk, osv. fra de faktiske Falske opplysningene. Også en slik lov vil kunne misbrukes.

Min posisjon blir dermed at statlig regulering sannsynligvis vil føre til en svekkelse av tillitsforholdet mellom borger og stat i stor grad på samme måte som spredning av falske opplysninger vil gjøre det samme. Må en ty til vid fattende lovgivning kan en på denne måten sies å allerede ha tapt- den liberale samfunnsordenen svekkes uansett.

5.4.2. Maskinlæring for å motarbeide maskinlæring

En løsning som er foreslått for å unngå proliferering av falske opplysninger, er at en konfigurerer GAN-systemer til å lære seg å gjenkjenne falske opplysninger. Pr. i dag kan slike "Detektiv-nettverk" detektere falske bilder og videoer med relativt stor nøyaktighet, men de må være trent til den konkrete oppgaven (å detektere video, bilder, tekst, eller lyd), og de krever mye datakraft.³⁹

Slike nettverk vil imidlertid like fort kunne bli integrert i GAN-nettverket som genererer de falske opplysningene- slik at "kontrolløren" nå bare vil gi poeng dersom informasjonen ikke fanges opp som

³⁷ (Bhavan Jaipragas 2019)

³⁸ Protection From Online Falsehoods and Manipulation Act (POFMA)

³⁹ (Zellers 2019)

falsk av GAN-systemet laget til nettopp dette. Vi har kommet så langt at det er utviklet maskinlæringsystemer som lærer å identifisere effektive og gode oppbygninger av GAN-nettverk. Med andre må en forvente at realismen til de falske opplysningene bare øke.⁴⁰

6. Oppsummering

I denne artikkelen har jeg lagt frem et argument for at maskinlæring, og særlig GAN-nettverk er en trussel for samfunnet. Grunnen til det er at en potensiell stor overvekt av falske opplysninger vil svekke tilliten mellom aktører i samfunnet. Følgene av dette kan være varierte, men basert på inntrykk fra USA og Ukraina hvor det er sannsynlig at mindre sofistikerte, men lignende metoder har blitt brukt, er det grunn til å tro at følgene kan være negative både i den sosiale og i den økonomiske sfæren

Jeg har også undersøkt løsninger for å sikre at falske opplysninger ikke infiltrerer samfunnet, og kommet frem til at det mest hensiktsmessige er å bekjempe teknologi med teknologi, fordi lovgivning sannsynligvis vil komme til å innskrenke nettopp den samfunnsordenen den søker å beskytte. Av teknologiske løsninger virker Blockchain-teknologi mest lovende fordi det tillater parter å verifisere opplysninger opp mot seg selv, med hensikt å verifisere at filen ikke er tuklet med. Problemet med å skille falske opplysninger fra ekte opplysninger er dog ikke løst. Basert på informasjonen presentert i denne artikkelen, mener jeg at en forutsetning for fortsatt sunn samfunnsutvikling, herunder med høy velstand og gjensidig tillit mellom borgere og forvaltning, er at problemstillinger rundt falske opplysninger blir bedre kjent, og at utvikling av løsninger på denne problematikken settes på sakordenen i langt større grad enn i dag.

7. Referanser

Alec Radford, Jeffrey Wu, Rewon Child, David Luan, Dario Amodei. «Language Models are Unsupervised Multitask Learners.» 2019: 24.

BBC. *BBC.com*. 9 10 2019. (funnet 12 1, 2019).

Bhavan Jaipragas, Dewey Sim. *South China Morning Post*. 30 11 2019. <https://www.scmp.com/week-asia/politics/article/3040045/facebook-urges-singapore-government-respect-free-expression-it> (funnet 12 2, 2019).

BRENAN, MEGAN. *Gallup.com*. 25 9 2019. <https://news.gallup.com/poll/267047/americans-trust-mass-media-edges-down.aspx>.

Cain, Geoffrey. *The New Republic*. 29 3 2019. (funnet 3 29, 2019).

Catanzaro, Ting-Chun Wang and Ming-Yu Liu and Andrew Tao and Guilin Liu and Jan Kautz and Bryan. «Few-shot Video-to-Video Synthesis.» I *Advances in Neural Information Processing Systems (NeurIPS)*. 2019.

⁴⁰ (Xinyu Gong 2019)

DuckDuckGo. *Measuring the "Filter Bubble": How Google is influencing what you click*. DuckDuckGo, 2018.

Fletcher, Nic Newman and Richard. «Bias, Bullshit and Lies.» *DIGITAL NEWS PROJECT*, 2017: 20-24.

Floydhub. *Generative Adversarial Networks - The Story So Far*. 21 6 2019. (funnet 12 1, 2019).

Goodfellow, Ian. *Twitter.com*. 15 1 2019.
https://twitter.com/goodfellow_ian/status/1084973596236144640 (funnet 12 1, 2019).

Grøn, Øyvind. *SNL*. 10 9 2019. https://snl.no/Galileo_Galilei (funnet 11 25, 2019).

Ian J. Goodfellow*, Jean Pouget-Abadie†, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair‡, Aaron Courville, Yoshua Bengio§. «Generative Adversarial Nets.» *NIPS Proceedings*6, 2014.

Kleven, Øyvinn. «Nordmenn på tillitstoppen i Europa.» *SSB, Samfunnsspeilet 2/2016*, 2016: 13-18.

Kunnskapsdepartementet. *Bekymret for digitalt klaseskille*. 03 12 2018.
<https://www.regjeringen.no/no/aktuelt/bekymret-for-digitalt-klaseskille/id2621106/> (funnet 11 26, 2019).

Mahler, Tobias. «Introduction to Cybersecurity Regulation (Presentasjon).» 21 1 2019.

NRK. *NRK*. 1 12 2019. https://www.nrk.no/norge/who_-vaksineskepsis-en-av-vare-storste-helseutfordringer-1.14432567 (funnet 2019).

Parkins, David. <https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things>. 31 10 2015. (funnet 12 2, 2019).

Posters, Bill. *Instagram.com*. 7 6 2019. <https://www.instagram.com/p/ByaVigGFP2U/> (funnet 12 2, 2019).

Rossen, Eirik. *SNL*. 17 2 2018. <https://snl.no/informasjon>.

Salian, Isha. *Stroke of Genius: GauGAN Turns Doodles into Stunning, Photorealistic Landscapes*. 18 3 2019. <https://blogs.nvidia.com/blog/2019/03/18/gaugan-photorealistic-landscapes-nvidia-research/?ncid=so-you-n1-78256>.

Store Norske leksikon. *SNL*. u.d. <https://snl.no/integritet> (funnet 11 25, 2019).

Two minute papers. *Youtube.com*. 30 11 2019. <https://www.youtube.com/watch?v=4J0cpdR7qec> (funnet 12 2, 2019).

Vatvedt, Martine. «Maskinlæring og åpenhet i digital forvaltning.» 2019: Bakgrunnsmateriale.

VIGSNES, EIRIK. «Tillit mer verdt enn oljen vår.» <https://www.forskningdagene.no/>, 25 8 2017.

Xinyu Gong, Shiyu Chang, Yifan Jiang, Zhangyang Wang. «arXiv:1908.03835.» 11 8 2019: 11.

Ye Jia *, Yu Zhang *, Ron J. Weiss *, Quan Wang, Jonathan Shen, Fei Ren, Zhifeng Chen, Patrick Nguyen, Ruoming Pang, Ignacio Lopez Moreno, Yonghui Wu. «Transfer Learning from Speaker Verification to Multispeaker Text-To-Speech Synthesis.» I *Advances in Neural Information Processing Systems 31*, 4485-4495. 2018.

Zellers, Rowan and Holtzman, Ari and Rashkin, Hannah and Bisk, Yonatan and Farhadi, Ali and Roesner, Franziska and Choi, Yejin. «Defending Against Neural Fake News.» *arXiv preprint arXiv:1905.12616*, 2019.

8. Vedlegg

Skjerm bilde tatt 25.11.2019: En svært enkel undersøkelse viser at 9/10 artikler om maskinklæring er positive eller nøytrale. Den resterende artikkelen handler om at "roboter vil ta over jobbene våre"-altså en helt annen problemstilling.



About 5,110 results (0.19 seconds)

**Tech p  agendaen for Norge og Slovenia**

Forskningsaktuelt SINTEF - 9 hours ago

Ved   kombinere mer etablerte metoder med maskinl ring, er m let   gj re den sv rt energikrevende prosessen med   smelte om kvarts til ...

**RFID og maskinl ring holder orden p  b kene i dette ...**

digi.no - Nov 18, 2019

RFID-teknologi tar seg av boksoreringen p  danske biblioteker. N  skal maskinl ringsalgoritmer hjelpe til med   forhindre overfylte bokhyller.

**Sjekk sykehjemmet som bruker maskinl ring for   spare str m**

Tu.no - Oct 28, 2019

Som ett av ytterst f  sykehjem her i landet har Rennes y bo- og rehabiliteringssenter i Ryfylke tatt i bruk maskinl ring for   spare str mutgifter.

**Det kan sp nde ben for rettsikkerheden, hvis maskinl ring ...**

Jyllands-Posten (Satire) (Blog) - Nov 24, 2019

Mange oppfatter beslutninger baseret p  data som neutrale. En sag fra USA viser imidlertid, at det ikke alltid er tilf eldet, og at brugen af data i ...

Mennesker skal l re om maskinl ring

Folkeskolen.dk - Nov 19, 2019

Maskinl ring fylder mere og mere i samfundet i dag, og der er brug for, at b rn og unge lærer at forst , hvordan s danne systemer fungerer.

**Digitaliseringen kan gi bedre mat – og mindre svinn**

Dagens N ringsliv - Nov 21, 2019

N  er vi i den spede begynnelsen av den fjerde, og vi kaller den matindustri 4.0: Smarte sensorer og roboter, kombinert med maskinl ring og ...

**- Allerede under registreringen bes man velge hvilket av FNs ...**

Kampanje - Nov 24, 2019

Maskinl ring og AI holder fortsatt stand som buzzwords. Enkelte kjente navn som Boost.AI er   finne p  stands. En artig vri p  maskinl ring ...

**Tror de kan redde liv med kunstig intelligens. Men trolig er det ...**

Aftenposten - Nov 16, 2019

IKKS benytter en type kunstig intelligens kalt maskinl ring. Maskinl ring blir trolig viktig i mange lignende prosjekter i fremtiden. Berge og ...

**B r vi frykte kunstig intelligens?**

Fredrikstad Blad - Oct 30, 2019

Veien til kunstig intelligens for empiristene er maskinl ring. I stedet for at mennesker gj r maskinene smarte ved   programmere maskinene ...

Roboter er p  full fart inn i jussen

forskning.no - Nov 5, 2019

L nekassen, for eksempel, bruker maskinl ring til   plukke ut studenter til bostedskontroll. Med denne fant L nekassen dobbelt s  mange ...


Skjerm bilde tatt 25.11.2019: Et lite utvalg av treffene på "falske nyheter" Falske nyheter knyttes til vanskelige sosiale og demokratiske problemstillinger.

Google

falske nyheter


Q All Images News Videos Maps More Settings Tools


About 111,000 results (0.21 seconds)

 **Må stilles ansvarlig for falske nyheter**
Dagbladet.no - 9 hours ago
Det ene er at plattformen har få mekanismer for å hindre konspirasjonsteorier, fabrikkasjoner og falske nyheter i å spre seg. Det andre er at ...
Sacha Baron Cohen raser mot Facebook: – Ville latt Hitler ...
TV 2 - Nov 22, 2019
Sacha Baron Cohen: Facebook hadde latt Hitler snakke fritt
ABC Nyheter - Nov 23, 2019
Sacha Baron Cohen: - Facebook ville latt Hitler få lov til å ...
In-Depth - Nettavisen - Nov 22, 2019
[View all](#)

Falske nyheter er ikke den største faren for demokratiet ...
Morgenbladet - Nov 14, 2019
Etter tre år med Donald Trump, og foran et nytt amerikansk valg, har den moralske panikken over «falske nyheter» og «det postfaktuelle» ...


Wikipedia-grunnleggeren lanserer nytt sosialt nettverk. Målet ...
Aftenposten - Nov 18, 2019
Nettverket er en forlengelse av prosjektet «Wikiritubune», en nyhetsside Wales lanserte i 2017 for å bekjempe falske nyheter. Prosjektet endte ...


 **Søster tror avdød fotballspiller lever**
Dagbladet.no - 6 hours ago
... bare har måttet takle det tragiske tapet av sin far, men også være vitne til nådeløse falske nyheter, trusler og personangrep i sosiale medier.


 **Tyskland ber Kina om å gi FN full tilgang til leirene i Xinjiang**
Adresseavisen - 1 hour ago
Tyskland ber Kina om å gi FN fullt innsyn i leirene i regionen Xinjiang, der lekkede dokumenter tyder på at det foregår hjernevask og tortur.

Er du usikker på om du klarer å skille usannheter fra fakta?
Fredrikstad Blad - Nov 11, 2019
Jeg vil anbefale boken «Falske nyheter» til alle som er usikre på om de klarer å skille usannheter fra fakta, og til alle andre som er opptatt av ...

– Som tatt ut av læreboka for valgmanipulasjon
NRK - Nov 4, 2019
«TROLLFABRIKK»: Redaksjonen i Folkeopplysningen produserte falske nyheter og valgmater for å lure elevene ved Lillestrøm videregående ...

 **Falsk pilot tatt på fersken på flyplassen**
ABC Nyheter - Nov 21, 2019
I to år hadde den indiske forretningsmannen lurt til seg fordeler på flyplasser i India, kledd i pilot-kostyme. Som tatt rett ut av ...

 **Forbud mot politisk reklame er feil medisin**
Adresseavisen - Nov 4, 2019
Nettjenesten Twitter innfører forbud mot all politisk reklame. Det er godt ment, men feil virkemiddel i kampen mot spredning av falske nyheter i ...
Bergens Tidende

 **Trump anklager riksrettsvitner for løgn**
ABC Nyheter - Nov 22, 2019
Jeg mener det er en falsk varsler. Se video øverst i artikkelen. Den amerikanske presidenten sa i intervjuet med programmet Fox & Friends at ...