FFI-RAPPORT

17/16605

Teknologiske muligheter for Tolletaten

breddestudie

Thor Engøy
Jan Ivar Botnan
Kristin Hammarstrøm Løkken
Tomas Roll Frømyr
Morten Aronsen
Audun Stolpe
Tom Arild Blix
Idar Dyrdal
Lars Aurdal

Teknologiske muligheter for Tolletaten

breddestudie

Thor Engøy
Jan Ivar Botnan
Kristin Hammarstrøm Løkken
Tomas Roll Frømyr
Morten Aronsen
Audun Stolpe
Tom Arild Blix
Idar Dyrdal
Lars Aurdal

Forsvarets forskningsinstitutt (FFI) 27. oktober 2017

Emneord

Teknologi
Sensorer
Maskinlæring
Automatisering
IKT

FFI-rapport
FFI-RAPPORT 17/16605

Prosjektnummer
530201

ISBN
P: 978-82-464-2974-8
E: 978-82-464-2975-5

Godkjent av
Jan Ivar Botnan, *forskningsleder*
Janet Martha Blatny, a*vdelingssjef*

Sammendrag

Tolletaten har gitt Forsvarets forskningsinstitutt (FFI) oppdrag om å gjennomføre en teknologisk mulighetsstudie som kan bidra til etatens strategi for utvikling av organisasjonen på kort, mellomlang og lang sikt. Denne rapporten tar for seg anvendelse av sensorer og maskinlæring, og peker på gryende muligheter innen automatisering og digitalisering av vareflyten.

Befaringer hos Tolletaten, på Oslo havn, postsentralen på Alnabru, tollkontoret på Gardermoen og grensestasjonen på Svinesund, har gitt FFIs prosjektgruppe bakgrunn for å forstå teknologienes mulige anvendelse for Tolletaten.

Av de sensorteknologiene som er interessante kan nevnes kjemiske detektorer, TeraHertz, hyperspektral avbildning, radar samt forskjellige teknologier for deteksjon og overvåkning av fartøy på sjøen. Alle sensorteknologier, såvel som andre kilder til informasjon, kan brukes som grunnlag for maskinlæring. Et datasett som består av sensordata sammenholdt med en domeneeksperts tolkning av dataene må etableres først. Etter opplæring vil maskinen kunne finne mønstre og sammenhenger som man er ute etter f.eks. i en strøm av sensordata. Vi gir noen eksempler på hvordan maskinlæring (dyp læring) kan anvendes på sensorsystemer som Tolletaten bruker i dag, ANPR og røntgen. Et datasystem med flere ulike sensorer og informasjonskilder kan over tid lære seg hva som er normalt, og deretter melde fra om avvik fra normalsituasjonen. Dette vil kunne understøtte bedre planlegging og utnyttelse av Tolletatens ressurser.

Disse teknologiene kan bidra til å forbedre treffprosenten ved utvelgelse av objekter for kontroll. For å få oversikt over de ulovlige varestrømmene må det i tillegg gjennomføres kontroller basert på statistiske metoder. Hvis disse ulovlige varestrømmene skal stanses må antall kontroller øke vesentlig. Automatisering og robotisering innen post- og varemottak, kontroll av konteinere og overvåking av varestrømmer vil i fremtiden gi mulighet for et slikt økt kontrollvolum.

Teknologier som “blockchain” og “internet of things” vil sannsynligvis forbedre informasjontilgangen som følger vareflyten og dermed gi grunnlag for bedre kontroll. Hvordan data lagres, bearbeides og tilgjengeliggjøres vil endre seg gjennom skytjenester og bruk av lenkede data (“semantic web”). Imidlertid innebærer også teknologiutviklingen en trussel ved at kriminelle tar i bruk lett tilgjengelige løsninger for å anonymisere datatrafikk og taletjenester.

Summary

The Norwegian Customs Agency has tasked The Norwegian Defense Research Establishment (FFI) to carry out a technology feasibility study that can contribute to the agency's strategy for developing the organization in the short, medium and long term. This report deals with the use of sensors and machine learning, and points to emerging opportunities in automation and digitization of the flow of goods.

Visits to customs stations at Oslo harbour, Alnabru mail center, Oslo Airport Gardermoen and Svinesund border station, have been carried out and given the FFI team background for understanding the possible application of the technologies within the Customs Agency.

Sensor technologies that are of interest include chemical detectors, TeraHertz, hyperspectral imagery, radar and various technologies for detection and surveillance of vessels at sea. All sensor technologies, as well as other sources of information, can be used as the basis for machine learning. A data set consisting of sensor data along with a domain expert's interpretation of the data must be prepared first. After training, the machine will be able to find patterns that are sought after, for example in a stream of sensor data. We provide some examples of how machine learning (deep learning) can be applied to sensor systems the Agency is currently using, ANPR and X-ray. A computer system with several different sensors and sources of information can over time learn what is normal, and then report deviations from the normal situation. This may support better planning and utilization of the Customs Agency's resources.

These technologies can help improve the hit rate in selecting objects for control. In addition, in order to estimate the illegal goods flows, checks must be performed based on statistical methods. If these illegal goods are to be stopped, the number of checks must increase significantly. Automation and introduction of advanced robots in mail processing, control of containers and monitoring of goods flows will in the future support this required increase in control volume.

Technologies like "blockchain" and "internet of things" are likely to improve the information quality that follows the flow of goods and thus provide a better basis for control. How data is stored, processed and made available will change through cloud services and use of linked data ("semantic web"). However, technology development also poses a threat from criminal use of readily available solutions such as anonymous data traffic and voice services.

Innhold

Forord 7

1 Innledning 9
- 1.1 Prosjektgruppens sammensetning 9
- 1.2 Avgrensning 9
- 1.3 Innføring i Tolletatens organisasjon og oppgaver 10
- 1.4 Teknologiske temaer som ikke er behandlet 10
- 1.5 Lagring og utnyttelse av data 11
- 1.6 Leseveiledning 12

2 Sensorer og informasjonskilder 13
- 2.1 Kameraer 13
- 2.2 Røntgen 16
- 2.3 Promptgamma aktiveringsanalyse 17
- 2.4 Kjemiske detektorer 18
- 2.5 Terahertz-teknologi 20
- 2.6 Hyperspektral avbildning 21
- 2.7 Networked Intelligent Underwater Sensors 23
- 2.8 Liten navigasjonsradar ESM 24
- 2.9 Satellittbaserte sensorer 26
  - 2.9.1 Mindre satellitter 26
  - 2.9.2 Navigasjonsradardetektor på satellitt 26
  - 2.9.3 Elektro-optisk på satellitt 27
  - 2.9.4 Satellittbaserte radarsystemer 27
  - 2.9.5 Maritim overvåkning fra satellitt 27
- 2.10 Radar 28
- 2.11 Akustiske sensorer 29
- 2.12 Registre i innland og utland 31
- 2.13 Biometri 31
  - 2.13.1 Anvendelse 32
- 2.14 BarentsWatch 33
- 2.15 Utvidet virkelighet 34

3 Dataanalyse og maskinlæring 36
- 3.1 Mønstergjenkjenning 37
- 3.2 Dyp læring (deep learning) 39
- 3.3 Pattern of life 41
- 3.4 Veiledet og ikke-veiledet maskinlæring 41
- 3.5 Anvendelse for Tolletaten 42
  - 3.5.1 Pattern of life 42
  - 3.5.2 Maskinlæring på to nivåer 43

3.5.3 Maskinlæring og røntgen 44
3.5.4 Maskinlæring og ANPR 45
3.5.5 Gjenkjenning av varer vha. bildeanalyse 46

4 Automatisering og robotisering 47
4.1 Anvendelser innen post- og varemottak 47
4.2 Anvendelser ved innførsel av konteinere 48
4.3 Overvåking av varestrømmer 49
4.3.1 Merking med RFID 49
4.3.2 Forsegling 50
4.3.3 Tilstandsovervåkning (av enkeltpakker) 50
4.3.4 Droner til sporing av kjøretøy 51
4.3.5 Selvkjørende tollpatrulje 51

5 Relevante IKT-trender 52
5.1 Nye nettverksprotokoller/Dark Web 53
5.1.1 Mørknettet 53
5.1.2 Tor-nettverket 54
5.1.3 Dark Web og kriminalitetsbekjempelse 54
5.2 Blockchain 55
5.2.1 Blockchain og vareflyt 56
5.2.2 Modenhet 57
5.2.3 Blockchain kombinert med Tor-teknologi 58
5.3 Lagringsløsninger, analyseverktøy, infrastrukturkonsepter 58
5.3.1 Tingenes internett 59
5.3.2 Semantic Web-teknologier 60
5.3.3 Stordatateknologier (*Big Data*) 63
5.3.4 Skytjenester (Cloud computing) 64
5.4 Web Processing Service 66
5.4.1 Anvendelser og muligheter 67
5.4.2 Klassifikasjon generelt 67

6 Konklusjon og anbefalinger 69
6.1 Sensorer 69
6.2 Maskinlæring 69
6.3 Automatisering 70
6.4 IKT-trender 70
6.5 Anbefalinger 71

Vedlegg

A Bidragsytere til rapporten 73

Referanser 74

Forord

Denne rapporten har blitt til i tett samarbeid med Tolletaten. For å bli kjent med etaten, har vi blitt invitert på flere befaringer og fått se hvordan tollerne jobber. Vi har besøkt Oslo havn, operasjonssentralen i Oslo, Toll- og vareførselseksjonen Alnabru, postmottakene Alnabru og Robsrud, samt Gardermoen og Svinesund.

Under alle våre befaringer og i arbeidsmøter har vi blitt møtt stor med velvilje og åpenhet. Forskernes nysgjerrighet og mer eller mindre klare spørsmål har blitt tatt imot og tålmodig besvart. Vi lært å kjenne en operativ etat og mennesker med engasjement og klar bevissthet om sitt samfunnsoppdrag. Det har vært motiverende og klargjørende for arbeidet som nå er gjort. Alle vi har møtt fortjener ros og takk. Spesielt vil vi også uttrykke vår takknemlighet til dem som har satt rammene for oppgaven og organisert vår rundtur og innføring i Tolletatens oppgaver og organisering, prosjektansvarlig Espen Closs, IT-direktør Jan Erik Ressem og fagdirektør Øivind Bohn Vestli. Deres kommentarer til første utkast har bidratt til å gjøre rapporten klarere og vesentlig mer lesbar. Forhåpentligvis er dette starten på en lengre reise hvor vi kan samarbeide om å bygge et sikrere Norge.

Kjeller, 15. juni 2017

Thor
Jan Ivar
Kristin
Tomas
Morten
Audun
Tom
Idar
Lars

Denne rapporten er tidligere utgitt som FFI-rapport 17/01295 Unntatt O˙entlighet og overlevert Tolletaten som delleveranse til PA nr 1 under avtale FFI-80266/Toll-17/03955. Tolletaten har øns-ket å gjøre rapporten o˙entlig tilgjengelig. Rapporten utgis herved som ugradert endret kun med rapportnummer og denne tilføyelsen.

Kjeller, 27. oktober 2017

Thor Engøy

1 Innledning

Tolletaten har gitt Forsvarets forskningsinstitutt (FFI) oppdrag om å gjennomføre en teknologisk mulighetsstudie som kan bidra til etatens strategi for utvikling av organisasjonen på kort, mellomlang og lang sikt. I første omgang skal studien favne bredt og

- gi oversikt over mulige teknologiområder for Tolletaten med et spesielt fokus på kunstig intelligens, maskinlæring og sensorsystemer,
- identifisere og anbefale utvalgte teknologiområder for videre analyse og
- hvis mulig, identifisere teknologiområder som kan ha konsekvenser for organisering på kort sikt.

Foreliggende rapport inneholder resultatene av denne teknologiske breddestudien.

1.1 Prosjektgruppens sammensetning

Tiden for gjennomføring av studien har vært styrende for hvordan arbeidet har vært langt an. I stedet for et bredt studium av forskningslitteraturen ("review article") gjennomført av et fåtall forskere, som ville ha krevd mer tid, har FFI valgt å hente inn til sammen ni forskere på tvers av avdelingene på FFI slik at bredden i den faglige bakgrunnen og teknologiske erfaringen vil være tilstrekkelig til å løse oppdraget. De fleste har kun arbeidet deltid med oppdraget. Der det har vært nødvendig eller formålstjenlig er det også hentet inn teknisk underlagsmateriale fra andre medarbeidere på FFI.

Avdelingstilhørigheten til prosjektmedarbeiderne er som følger:

- Avdeling Beskyttelse og samfunnssikkerhet: forsker Thor Engøy, forskningssjef Jan Ivar Botnan, forsker Kristin Hammarstrøm Løkken, forsker Tomas Roll Frømyr
- Avdeling Maritime systemer: forsker Morten Aronsen, forsker Tom Arild Blix
- Avdeling Cybersystemer og elektronisk krigføring: forsker Audun Stolpe
- Avdeling Landsystemer: forsker Idar Dyrdal
- Avdeling Luft- og romsystemer: forsker Lars Aurdal.

1.2 Avgrensning

Samfunnsoppdraget til Tolletaten kan forenklet deles inn i to ulike hovedoppgaver:

- Bidra til effektiv lovlige inn- og utførsel av varer over landegrensene. De som fremlegger varer til fortolling skal møtes med en korrekt, enkel og hurtig saksbehandling.
- Kontrollere og stanse ulovlig inn- og utførsel av varer over landegrensene. De som forsøker å føre inn eller ut varer som er forbudt skal med høy grad av sannsynlighet bli oppdaget og forhindret fra å gjøre dette.

Prosjektgruppen har i dette arbeidet hovedsakelig hatt kontrolloppdraget for øye ved vurdering av de ulike teknologienes mulige anvendelser for Tolletaten. Ulovlige varer bestilles eller tas med over landegrensene av personer. Oppdagelse av slik ulovlig vareførsel er derfor nært knyttet til personetterretning. Det er i dette arbeidet ikke gjort forsøk på å sortere bort teknologiske muligheter basert på juridiske og etiske begrensninger.

I oppdraget bes vi spesielt om å vurdere hvordan kunstig intelligens og tilstøtende teknologier kan påvirke Tolletatens arbeid i framtiden. Kunstig intelligens har vært en "hellig gral" innen forskning i årtier uten at dette kan sies å ha hatt spesielt stor innflytelse på det praktiske liv generelt. Utviklingen har vært langsom, og utfordringene ofte større enn man trodde. I de siste fem årene har man imidlertid sett en rivende utvikling innenfor fagfeltet nevrale nett og ulike løsninger basert på nevrale nett kan i dag konkurrere med mennesker på avgrensede oppgaver. Dette området omtales ofte som "dyp læring" (engelsk "deep learning"). Gitt de gode resultatene som oppnås med løsninger basert på denne typen teknologier har vi valgt å fokusere vår vurdering av metoder innen kunstig intelligens til dyp læring.

1.3 Innføring i Tolletatens organisasjon og oppgaver

Oppdragsgiver har gitt prosjektgruppen orienteringer om Tolletatens oppgaver og organisering, pågående strategiarbeid, etablering av Tolletatens etterretningssenter, og anskaffelse av nye IT-løsninger (TREFF-prosjektet) og organisert arbeidsmøter for uformell idéutveksling knyttet til teknologiske muligheter. Dette har vært nyttig bakgrunn og start for arbeidet. I tillegg har prosjektgruppen fått anledning til å observere og gjøre seg kjent med utførelse av tollernes oppgaver ved Oslo havn, Postens godssenter på Alnabru og Østlandsterminalen på Robsrud, Gardermoen lufthavn og Svinesund. Å direkte kunne se hvordan oppgaver løses i praksis og diskutere med erfarne betjenter de utfordringer de møter, har vært meget nyttig for å kunne vurdere de mulige teknologienes relevans for Tolletaten.

1.4 Teknologiske temaer som ikke er behandlet

Organisatoriske forutsetninger for innføring av teknologi
Teknologien skal være et verktøy for mennesker og støtte utførelse av et oppdrag. Innføring av teknologi krever utdanning av personell og tilpasning av organisasjonen for å bli vellykket. Innvolvering av sluttbrukerne er nødvendig, tidlig i prosessen gjennom behovs- og kravformulering og helt fram til test og evaluering av de teknologiske løsningene. Betydningen av disse forutsetningene kan ikke overvurderes.

Utvikling av kommunikasjonsteknologi generelt og de muligheter det gir
Kommunikasjonsteknologi kan utnyttes til sporing og overvåking av personer mistenkt for ulovlige vareførsel. For eksempel kan en tenke seg at sms-er og annen kommunikasjon som utveksles like før og etter grensepassering blir registrert og utnyttet til å finne mønstre som gir bedre objektutvelgelse. Tråløse nettverk forventes å ha høy overføringskapasitet og gi enkel tilgang til all relevant informasjon for tollere der de befinner seg.

Kjente og mindre relevante sensorteknologier
Det er mange sensortyper som er alminnelig kjent og kommersielt tilgjengelig. Slike sensorer kan selvfølgelig utnyttes, f.eks. i kombinasjon med andre sensorer, men er ikke funnet nødvendig å omtales særskilt. Avanserte sensorer som bruker magnetisk resonans (MR) er utelatt fordi det synes å være et begrenset bruksområde for Tolletaten. Avbildning av personer vil kunne avsløre innvendig smugling av forbudte stoffer uten å påføre ioniserende stråling som personrøntgen gir. Teknologien vil imidlertid sette magnetiske materialer i bevegelse og derfor være uegnet for skanning av kjøretøy eller varer.

Karakterisering av personer basert på sensordata
Det arbeides mye med å utvikle indikatorer og algoritmer for å finne personer med onde hensikter. Klassifisering av sinnsstemning ("emotion classification"[1]) er å si noe om hva en person føler ut ifra hva man kan observere, uten nødvendigvis å interagere med personen. Pustefrekvens, puls, perspirasjon og ansiktsuttrykk er eksempler på egenskaper som kan si noe om hvorvidt en person er nervøs. Med gode sensorer og programvare vil det være mulig å måle dette på avstand. I den grad mennesker oppfører seg annerledes når de er nervøse, kan dette registreres av gode overvåkningskameraer, f.eks. i en ankomsthall.

1.5 Lagring og utnyttelse av data

Sensordata og informasjon fra andre kilder kan bearbeides og utnyttes på forskjellige måter. Den enkleste måten er at en person (toller) ser på informasjon fra en kilde og tar en beslutning på grunnlag av egen erfaring med tilsvarende saker. I praksis vil en toller bruke informasjon fra flere kilder. For å treffe riktige beslutninger er det nødvendig at all relevant informasjon er tilgjengelig for beslutningstaker. Dette forutsetter god kommunikasjonsinfrastruktur, tilstrekkelig båndbredde og regnekraft og godt tilrettelagte grensesnitt for presentasjon av informasjonen, fra enkeltkilder så vel som sammenstilt informasjon fra flere kilder.

Sensorer bør utnyttes kontinuerlig og gjøre det mulig å skanne all transport av varer over landegrensene. Alle sensordata, bilder og tilhørende informasjon bør lagres. Ved kontroller må alle funn logges, også negative funn. Datalagringen vil være en viktig forutsetning for maskinlæring, som er et overgripende tema i denne rapporten. Behovet for store datamengder i maskinlæring fordrer at data deles mellom tolldistriktene f.eks. gjennom sentralisert lagring. Det kan også være aktuelt å dele visse former for data med andre land, f.eks. røntgenbilder av biler eller kofferter.

Store variasjoner i mengden beslaglagte varer fra år til år peker på at transportmetoder og -ruter er i stadig endring. For å kunne si noe om størrelsen på de ulovlige varestrømmene, f.eks. narkotika, er det viktig å foreta en systematisk prøvetaking som ikke er forutinntatt eller skjevfordelt. Randomiserte utvalg av kontroller av både gods og personer er derfor viktig å gjennomføre kontinuerlig. Foruten å gi grunnlag for å anslå de faktiske varestrømmene vil slike kontroller gjøre det mulig å oppdage nye mønstre i den ulovlige vareførselen. Data generert på denne måten vil også være nødvendig som grunnlag for avansert maskinlæring.

[1] "Emotion classification" må ikke forveksles med "sentiment analysis", som dreier seg om å kartlegge befolkningens holdninger til et tema, typisk på grunnlag av store datamengder i form av tekst. Svaret på en analyse kan være så enkelt som at folk stort sett er positivt innstilt til temaet.

1.6 Leseveiledning

Denne rapporten har fire hovedkapitler: kapittel 2 Sensorer og andre informasjonskilder, kapittel 3 Dataanalyse og maskinlæring, kapittel 3 Automatisering og robotisering og kapittel 5 Relvante IKT-trender. Disse kapitlene inneholder beskrivelse av teknologier som vi regner relevante for Tolletaten i dag eller på lengre sikt og som derfor fortjener omtale. Imidlertid kan disse kapitlene inneholde detaljer som ikke alle lesere vil finne like interessante. Vi har derfor forsøkt å gi et ekstrakt av innholdet først i hvert kapittel i form av en tabell over de mest relevante teknologiene og deres anvendelsesområder. Det er i denne tabellen i tillegg antydet en grad av modenhet til teknologien og hvor lett teknologien kan innføres av Tolletaten (gjennomførbarhet). Denne vurderingen av modenhet og gjennomførbarhet er meget overordnet og foreløpig og er basert kun på prosjektgruppens begrensede kjennskap til og forståelse av Tolletatens oppgaver og utfordringer. Vi tar forbehold om at disse vurderingene vil kunne endres ved nærmere studier av teknologi og foreslått anvendelse.

Den utålmodige leser kan hoppe rett til rapportens siste kapittel. Kapittel 6, Konklusjon og anbefalinger, gir en oppsummering av resultatene fra hovedkapitlene og en nedkortet liste over teknologier som anbefales for videre studier.

2 Sensorer og informasjonskilder

Teknologi og anvendelsesområde	Mod.	Gj.f.
TeraHertz: Inspeksjon av gods, deteksjon av eksplosiver.		
Biometri: Sikker ID av personer.		
Hyperspektral avbildning: Skille fra hverandre objekter og materialer som visuelt ser like ut.		
Røntgen: Oppdage ulovlige varer.		
Kjemiske detektorer: Detektere og identifisere ulovlige og farlige stoffer.		
Promptgamma aktiveringsanalyse:Inspeksjon av gods, oppdage farlige stoffer.		
Akustiske sensorer: Deteksjon og mulig klassifisering av bl.a. droner og kjøretøy		
Radar: Deteksjon og klassifisering av droner.		
NILUS: Deteksjon av farkoster på og under vann.		
LINE/NRD: Deteksjon av navigasjonsradarer. Samarbeid med BarentsWatch.		
Satellittsensorer: Deteksjon og identifikasjon av fartøy. Samarbeid med Barents-Watch.		

Tabell 2.1 *Tabellen viser ulike anvendelser av sensorteknologi som er omtalt i dette kapitlet. Teknologisk modenhetsnivå (Mod.) og gjennomførbarhet (Gj.f.) for Tolletaten er antydet med fargekode: grønn = høy, gul = medium, og rød = liten.*

Dette kapitlet handler om sensorer og informasjonskilder og gir en oversikt over noen mulige anvendelser av sensorteknologi som kan være aktuelle for Tolletaten. Tabell 2.1 viser et utdrag av teknologier som vi anser som nye og nyttige for Tolletaten, og gir et estimat av modenhet og gjennomførbarhet. Røntgen og kamerateknologi antas å være godt kjent for Tolletaten, og er derfor ikke med i tabellen, selv om de omhandles i dette kapitlet.

Alle teknologiene og informasjonskildene som beskrives i dette kapitlet kan tenkes brukt som input til maskinlæring, både hver for seg for å øke produktiviteten og treffsikkerheten, og sammen med andre sensorer og informasjonskilder for å avdekke større mønstre og sammenhenger. Maskinlæring er tema for kapittel 3.

I tillegg til deteksjon, kontroll og klassifisering som beskrevet over, er det aktuelt med generell overvåkning av områder. Eksempler kan være grenseoverganger og områder hvor personer oppholder seg etter at de har forlatt fly, ferge el.l. og til de har passert tollen. I slike områder kan det være aktuelt å bruke sensorinformasjonen til å utføre Pattern of life (POL)-analyser, og på det grunnlaget detektere avvik fra normal flyt. Se mer om dette i avsnitt 3.3 og 3.5.1.

2.1 Kameraer

Kameraer som virker i den synlige delen av det elektromagnetiske spekteret (eventuelt kameraer som også inkluderer det nære infrarøde området (Near Infrared (NIR))) har lenge vært brukt innen

overvåking og kontroll og har også stor verdi for anvendelser innen toll. De typiske kameraene som brukes for dette formålet er relativt billige, noe som gjør at de kan brukes på mange steder og i mange sammenhenger. Kameraene kan også gjøres små og er derfor enkle å montere og beskytte, det er også mulig å montere dem slik at de er vanskelige å oppdage. En ny trend er miniatyriserte kameraer som kan bæres på kroppen, noe som gir omfattende muligheter for å dokumentere konkrete situasjoner og forhold som en toller møter i sitt daglige virke.

En rekke parametre styrer kameraenes ytelse, vi vil her raskt diskutere de mest sentrale for den typen kameraer som kan anvendes innen toll.

- **Pikselstørrelse:** Kameraets sensor er inndelt i et rutemønster der hver rute er en piksel. Hver piksel kan telle antallet fotoner som treffer den innenfor en viss tid (lukkertiden). Dersom mange fotoner treffer innenfor en gitt tid vil pikselen representere et lyst punkt i det endelige bildet, om få fotoner treffer vil pikselen være mørk. Siden fotoner treffer hele sensorflaten er det rimelig at dersom pikslene er **store** vil de kunne samle flere fotoner på samme tid (en nyttig analogi her er en bøtte som skal brukes for å samle regndråper,- jo større diameter i bøtteåpningen, jo raskere vil den kunne samle en ønsket mengde vann). Store piksler tillater kort lukkertid i kameraet slik at raske bevegelser kan fryses. Tilsvarende vil store piksler egne seg i dårlig lys fordi de kan samle tilstrekkelig mange fotoner også når lysforholdene ikke er ideelle.
- **Pikselantall:** Antallet piksler i rutemønsteret på sensoren er en av faktorene som avgjør oppløsningen til sensoren. Sterkt forenklet kan man si at mange piksler typisk gir høyere oppløsning.
- **Sensorstørrelse:** Kameraets sensor består av piksler i et rutemønster på en plate av silisium, denne platen med piksler omtales gjerne som sensoren. Det er krevende å lage slike silisiumplater og jo større platen er, jo dyrere vil den være. Størrelsen på platen avhenger av to ting, hvor mange piksler den skal bære, og hvor store hver piksel er. Sensorer med mange store piksler (en stor piksel vil typisk være på $25\mu m^2$) vil være mye mer kostbar enn en piksel med få og små piksler (i moderne mobiltelefoner vil kameraet ofte ha piksler som er bare ca. $1\mu m^2$ store).
- **Optikk:** Optikken avgjør i siste instans hvor godt man kan fokusere lyset ned på sensoren. En dyr sensor med høy oppløsning og følsomhet krever presis (og dermed dyr) optikk for å levere sitt fulle potensiale.
- **Farger eller gråtoner:** Avhengig av hva slags filter som legges på hver enkelt piksel kan sensoren levere bilder i tre kanaler, rødt grønt og blått (RGB) som gir mulighet for fargebilder, eller i bare en kanal som gir gråtonebilder. Dersom skarphet og/eller lysfølsomhet er svært kritisk velger man gjerne gråtonesensorer da disse har de beste egenskapene for disse to parametrene. Mange kameraer som leveres i markedet for sikkerhetskameraer har i tillegg til følsomhet i hele den synlige delen av spekteret også en følsomhet som strekker seg et stykke ut i det nære infrarøde området (NIR). Dette gjøres for å maksimalisere lysfølsomheten siden dette er en viktig parameter for disse kameraene.

Kameraer kan naturligvis brukes innen et stort antall mulige anvendelser for toll. Vi vil i det følgende ta for oss noen typiske anvendelser og beskrive hvilke parametre som kan tenkes å være førende for valg av kamera (sensor) i de ulike tilfellene.

- **Fastmonterte kameraer for overvåking av trafikk av biler og personer:** Dette er en vanlig

bruk av kameraer, og er utbredt innen toll og betalingssystemer. På grunn av at scenen som overvåkes ofte endrer seg i høy hastighet må kameraene kunne operere med kort lukkertid for å fange raske bevegelser, i tillegg vil ofte lysforholdene være krevende noe som også dikterer store piksler. Denne typen kameraer brukes ofte for lesing av bilskilt, gjerne omtalt som Automatic Number Plate Recognition (ANPR).

- **Kameraer montert i biler og på personer:** Etterhvert som digitale kameraer har blitt billigere og bedre har det blitt vanlig å lage dem slik at de lett kan monteres i biler og på personer (et godt eksempel på et slikt produkt laget for det sivile markedet er GoPro kameraene som monteres på personer for å dokumentere ulike ting bæreren gjør). Denne anvendelsen av kameraer kan brukes for dokumentasjon og situasjonsforståelse. Typisk er dette relativt små kameraer noe som gjerne dikterer en liten sensor. Kameraene har ofte høy oppløsning, siden prisen er lav vil dette bety små piksler og denne typen kameraer vil ofte egne seg dårlig i lavt lys, de produserer også ofte relativt støyfulle bilder.
- **Stereokameraer:** En mindre utbredt bruk av kameraer er å montere dem i par slik at de kombinerte bildene fra begge kameraene danner grunnlag for å beregne stereobilder. Denne typen bilder gjør det mulig å estimere avstanden fra kameraene til objekter i en scene de ser på og dette kan ha en rekke anvendelser for toll. En enkel bruk av slike stereopar kunne for eksempel være å estimere dimensjoner av biler som kjører i land fra ferger, man kunne også tenke seg å bruke dette for å bestemme et kjøretøys bakkeklaring eller andre forhold som kan si noe om kjøretøyets last. I utgangspunktet kan de fleste kameraer brukes i stereopar og det stilles ingen spesielle krav til kameraene som skal inngå i et stereopar.

I det tradisjonelle markedet for kameraer til overvåkning og kontroll har fokus ofte vært på kameraer med kort lukkertid som er svært følsomme (kameraer som kan fange raske bevegelser og som har gode lavlysegenskaper med andre ord). Siden dette fordrer store piksler har man ofte ofret oppløsning for å holde kameraprisen på et akseptabelt nivå. Selv om dette kan virke som et logisk valg har dette også negative konsekvenser.

Et eksempel på dette er lavoppløste gråtonekameraer for bruk i ANPR. Her er oppløsningen ofte så lav at den delen av moderne skilt som beskriver bilens nasjonalitet (gjerne i nedre venstre hjørne av skiltet) ikke kan leses med automatiske systemer for skiltlesing (ANPR). I moderne systemer for ANPR avgjøres derfor ofte bilens nasjonalitet ut fra en semantisk analyse av selve skiltet **uten** at det tas hensyn til de symbolene som faktisk sier i hvilket land bilen er registrert.

Dette er naturligvis uheldig i og med at det reduserer treffsikkerheten i ANPR-systemet. Utviklingen innen sensorteknologi har imidlertid vært rivende de siste årene og det er i dag god grunn til å spørre om de samme begrensningene i valg av kamera bør gjelde. I framtidige anskaffelser av kamerasystemer for Tolletaten bør leverandøruavhengige spesialister på kameraer og deres anvendelser trekkes inn for å bistå i valget av teknologi. Ikke minst er det kritisk at kamerasystemer ikke velges isolert, men at man tar hensyn til både den manuelle tolkningen som kameraene skal bidra til og, ikke minst, den automatiske tolkningen som skal utføres på bildene. For ANPR-anvendelsen vil moderne høykvalitetskameraer åpne for uttrekking av mer informasjon enn selve kjennetegnet. Nasjonalitetstegnet i skiltet vil kunne tolkes, videre vil ofte bilmerke og farge (dersom fargekameraer benyttes), kunne leses.

2.2 Røntgen

For Tolletaten er røntgen en viktig sensorteknologi for inspeksjon av gods. Det genereres daglig store mengder bilder basert på gjennomlysning av bagasje, post, pakker, biler, vogntog, fraktkonteinere. I noen tilfeller utføres også røntgen på mennesker, med dertil egnet utstyr. Innen sikkerhetssektoren har det blitt vanlig å screene totalvolumet av gods som passerer et kontrollpunkt, mens ved tollpassering benyttes røntgen på utvalgte objekter til utvelgelse for kontroll, samt i selve objektkontrollen. Tollerens tolkning av røntgenbildet er grunnlag for eventuell videre inspeksjon. Noen instrumenter har mulighet for automatisert gjenkjennelse av narkotiske stoffer, eksplosiver og tilsvarende, men disse blir ofte ikke benyttet fordi mengden falske positive utslag oppleves som uakseptabelt høy.

Tolkningen av røntgenbilder er derfor i dag vesentlig erfaringsbasert, der kontrollørens evne til å gjenkjenne ulovlig gods utvikles over tid. Det er ikke tilrettelagt for systematisk lagring, annotering og utveksling av bildeinformasjon mellom ulike kontrollpunkter og regioner med tanke på læring. Røntgenbilder kan bli vedlagt sakspapirer, lagret på intranett og i instrumentspesifikke databaser ved eventuelle funn. Falske positive og negative kontroller lagres ikke. I noen tilfeller gjøres det forsøk på å bygge opp større mengder bildemateriale, eksempelvis referansebilder av ulike bilmodeller. Etaten har ikke et fellessystem for å lagre, merke og søke i slike data.

Opptak av røntgenbilder er enkeltvis en rask prosess, men den samlede tiden eller ressursforbruket etaten benytter på å tilrettelegge for, ta opp og tolke bilder er likevel stor. I mange arbeidsprosesser gir bildet også grunnlag for vurdering av videre inspeksjon. Resultatløse objektkontroller, for eksempel grunnet falske positive eller røntgenbilder som vanskelig lar seg tolke, er svært kapasitetsbindende. Åpenbart er falske negative funn uønsket, siden de i verste fall fører til en mislykket objektkontroll. Reelle prosessforbedringer er nødvendig. Mulighetsrommet for å forbedre dagens utnyttelse av røntgen som deteksjonsmetode er relativt stort og det spenner fra et lavt ambisjonsnivå der relativt enkle grep i liten grad endrer dagens rutiner, til større investeringer og nye metoder som kan ligge utenfor handlingsrommet for etaten. Under nevnes ulike anvendelsesområder for røntgen:

- **Bildedatabase:** En bildelagrings- og behandlingsløsning for alle typer røntgenbilder av gods kan gi en rekke muligheter for deling av informasjon med etterretningskjeden og mellom regionene, samt danne grunnlag for kurs, læring og mentorering. Systemet bør i størst mulig grad automatisere de daglige rutinene, slik at bilder lagres og katalogiseres korrekt uten å påføre kontrolløren merarbeid. Videre må det gi kontrolløren mulighet til enkelt å annotere og notere metadata til bildene, slik at vurderinger kontrolløren finner det nyttig å dele, fanges opp.
- **Metoder:** Problemstillinger knyttet til instrumentering kan sorteres etter størrelsen på hva man ønsker å ta bilde av. For mindre enheter slik som pakker og postsekker, kan man benytte instrumentering tilsvarende bagasjerøntgen. Forskjellen i røntgenpenetrasjon mellom ulike organiske materialer, slik som militære eksplosiver, narkotika og bøker er målbar og ofte tilgjengelig i litteraturen. Det er derfor en relativt enkel sak å lage deteksjonsalgoritmer som skiller de ulike materialene. Røntgenstrålingens evne til gjennomlysning er avhengig av strålingens energinivå. For inspeksjon av stykkgods vil enklere strålekilder med energinivå mellom 50 og 500 keV være tilstrekkelig, mens større systemer for konteinere og tilsvarende benytter strålekilder i området 5 til 10 MeV.
- **Multispektral bildedannelse:** Fra et enkelt røntgenbilde er det ikke mulig å skille mellom et objekts tykkelse og dets materialegenskaper. Vi kan med andre ord ikke si noe om objektet er

tynt og tungt eller tykt og lett. Det er imidlertid utviklingsmuligheter for både strålekilder og røntgendetektorer tilsvarende utviklingen innen avbildning i synlig lys, der man har gått fra sort-hvitt til farge og nå videre til multi- og hyperspektral avbildning. Dette har gitt enormt utvidede muligheter for nye bildebehandlingsmetoder.

- **Ulike bildeperspektiv og tomografi:** Røntgenbilder der ulike objekter overlapper er utfordrende å tolke. Særskilt gjelder dette større enheter som konteinere, men også postsekker og større pakker. Ved å gjennomlyse kontrollobjektet fra flere vinkler, kan det være enklere å avsløre innholdet. Tomografiske metoder, slik som Computertomografi (CT) røntgen, er en sammenstilling der objektet gjennomlyses fra et antall vinkler og programvare automatisk beregner et bilde med dybdeinformasjon. Instrumenter som skal levere en slik kapasitet må nødvendigvis være vesentlig mer kompliserte enn tradisjonelle røntgenmaskiner. Det er uklart om CT-maskinene som er kommersielt tilgjengelige i dag er hensiktsmessige, men CT er en teknologi man må forvente vil kunne gi bedre operativ ytelse enn tradisjonell røntgen for typisk pakke- og baggasjekontroll. Innenfor fagfeltet Augmented Reality (AR) foregår det en rask utvikling av både utstyr og algoritmer. Etter en 3D-scanning i røntgentomografen, kan operatøren, iført Virtual Reality (VR)-briller, søke etter anomalier i 3D-beskrivelsen av objektet. Søket kan være manuelt eller støttet av bildeanalyse. Bruk av bildeanalyse er normalt å anbefale, selv om det krever utvikling og trening av algoritmer. Det finnes imidlertid åpent tilgjengelig mange standardmetoder som kan benyttes, eller som det i det minste kan bygges videre på. Dyp læring (basert på nevrale nett) er en betegnelse på nye metoder som trolig kan gi gode resultater. Detekterte anomalier kan markeres manuelt eller automatisk med f.eks. fargelegging.
- **Tilbakespredt røntgen:** Bildedannelsen omtalt til nå, har basert seg på en gjennomlysning, der det er strålens evne til å penetrere kontrollobjektet som danner en kontrast. Tilbakespredt røntgen vil normalt ikke penetrere de største objektene, men fordi detektor og strålekilde står på samme side, vil man få signal så langt inn som signalet penetrerer. Det er mulig å kombinere detektorer for gjennomlysning og tilbakespredt røntgen i samme enhet. Kommersielle løsninger finnes.
- **Andre målemetoder:** Andre typer stråling kan benyttes som komplementerende teknikker til røntgen. Magnetisk Resonans (MR), pulset gammastråling og nøytronstrålingsteknikker slik som pulset høyenergi nøytronstråling (PFNA) er eksempler på teknikker som, for forskjellige formål, kan kombineres med røntgen for å øke deteksjonsgraden. Det er lite som tyder på at det er nye teknikker under utvikling som kommer til å erstatte røntgen.

2.3 Promptgamma aktiveringsanalyse

Ved å studere sammensetning av atomkjerner i et prøvevolum vil det være mulig å bestemme hvilke stoffer det består av. Noen atomkjerner er ustabile og sender ut gammastråler med karakteristisk energi. Passiv deteksjon av gammakvanter kan brukes til å bestemme mengden av slike ustabile kjerner.

Måleteknikken kan gjøres mer anvendelig ved å tilføre en nøytronkilde. De fleste atomkjerner reagerer umiddelbart på bombardering med hurtige nøytroner ved å sende ut karakteriske gammastråler. Et gammaspektrometer kan dermed detektere mange flere av de ulike atomkjernene som finnes i prøvevolumet og mengdeforholdet mellom dem.

Pga. gammastrålenes gjennomtrengningsevne er det er mulig å detektere stoffer gjennom de fleste typer materialer. I industrien brukes måleteknikken f.eks. til å overvåke elementsammensetning under produksjon av sement. Det er også laget instrumenter for å bestemme eventuelt innhold av kjemiske stridsmidler i ukjente beholdere (f.eks. umerkede artillerigranater). Prøvevolumet er typisk liter (eller mindre). Nøytronbestrålingen gir liten restaktivitet og teknikken regnes som ikke-destruktiv. Pakken som undersøkes trenger ikke åpnes. Det gjenstår å utvikle analysen til å skille på ulike organiske stoffer.

Anvendelsesområdet for Tolletaten er innenfor (automatisk) skanning av pakker og konteinere for å bestemme eventuelt innhold av ulovlige og farlige stoffer. Selv om teknologien synes å være robust nok og kostnadene er moderate, er modenheten for slik anvendelse fortsatt lav. På sikt er dette imidlertid en teknologi som det kan være verdt å følge med på.

2.4 Kjemiske detektorer

Narkotiske stoffer, medikamenter og andre trusselstoffer utgjør en vesentlig del av den ulovlige vareflyten. Ved kontrollpunktene møter kontrollører daglig et stort antall substanser man må ta stilling til om skal beslaglegges og sendes til tollaboratoriet. Ved enkelte kontrollpunkter har man anskaffet laser-raman spektrometer (heretter raman) for kjemisk bestemmelse av væsker og faste stoffer, mens de fleste kontrollpunkter benytter kontrollørens erfaring og sanser samt ulike typer prøvekit bestående av prøvepapir man kan påføre stoffer og se etter utslag. I enkelte tilfeller kan det være farlig å lukte på kjemikaliene, som for noen sedativer slik som fentanyler.

Med riktig opplæring av operatøren, er raman en effektiv teknikk som raskt måler prøven med et minimum av forarbeid. Signalet sammenlignes med et bibliotek av kjente stoffer og en treff-verdi oppgis. Ved tilstrekkelig samsvar kan prøven beslaglegges. Nye og ukjente stoffer kan karakteriseres ved tollaboratoriet og man kan oppdatere biblioteker i takt med endringen i hva som innføres. Teknikken benytter en relativt kraftig laserstråle som belyser et lite område. Dersom prøven er mørk er det fare for at prøven blir svært varm og i verste fall antenner. Det er i liten grad hensiktsmessig å benytte raman på slike materialer. Det finnes komplementerende teknikker til laser-raman spektroskopi som vil kunne øke effektiviteten ved kontrollpunktene. Tradisjonelt benytter man Infrarød (IR) spektroskopi, som dekker en rekke stoffer som er uegnet for raman. Det finnes i dag små brukervennlige instrumenter også for IR som kan egne seg for bruk ved kontrollpunktene.

FFI arbeider med beredskap mot kjemiske, biologiske og radiologiske våpen (CBR-våpen) og eksplosiver, samt tiltak mot at de samme substanser skal bli anvendt i forbindelse med terrorisme. Et viktig tiltak er å oppdage forsendelser av slike stoffer til spesielt utsatte mottagere som viktige myndighetspersoner. FFI har arbeidet med utvelgelse av sensorer og etablering av prosedyrer ved post- og varemottak. Dette har gitt erfaringer med ulike typer teknologi som også kan være aktuelle for Tolletaten.

Sensorer for deteksjon av kjemiske, biologiske og radiologiske trusselstoffer i luft er på ulike trinn i utviklingsprosessen. Mens radiologiske sensorer er små og enkle, og trenger liten grad av vedlikehold, er biologiske sensorer på den annen side ennå tidlig i utviklingen. Sensorer for kjemiske trusselstoffer og giftige industrikjemikalier (Toxic industrial chemicals (TIC)) er i en

mellomstilling, der det finnes mange ulike sensorer tilgjengelig på markedet. De fleste sensorene er såkalte punkt-sensorer, det vil si at de detekterer CBR-trusselstoffer som transporteres til sensoren med luften som suges inn i detektoren.

Teknologier brukt i kjemiske punktsensorer er gjengitt i tabell 2.2.

Teknologi	**Beskrivelse**	**Modenhet**	**Detektor /Monitor**	**Prøvetilstand**
Akustiske overflatebølger (SAW)	En sensor for hver kjemisk forbindelse	Ny, fremdeles ustabil teknikk	Begge	Gass
Kolorimetriske sensorer	Våtkjemisk teknikk, bl.a. deteksjonspapir	Brukt i mange år	Detektor	Gass, væske
Elektrokjemiske sensorer	En sensor for hver kjemisk forbindelse	Brukt i mange år	Begge	Gass
Flammespektrometri	Kan detektere trusselstoffer som inneholder fosfor, svovel, arsen eller nitrogen	Brukt i mange år	Begge	Gass
Fotoionisasjonssensorer	Detekterer stoffer med ionisasjonspotensial over en bestemt verdi	Brukt i flere år	Begge	Gass
Halvlederteknologi	Benytter en array av halvleder sensorer	Forholdsvis ny teknikk	Begge	Gass
Infrarød spektrometri (IR)	For forholdsvis rene forbindelser	Brukt i mange år	Detektor	Gass/ væske/ faste
Ionemobilitetspektrometri (IMS)	Kan skille mellom noen trusselstoffer	Brukt i mange år	Begge	Gass
Massespektrometri (MS)	Kan identifisere trusselstoffer	Brukt i mange år	Begge	Gass/ væske/ faste
Pulset elementanalyse vha nøytroner (PELAN)	Kan klassifisere innholdet i lukkede konteinere	Ny teknikk	Detektor	Væske/ faste
Raman spektrometri	Kan se gjennom glass og klar plast	Brukt i mange år	Detektor	Væske/ faste
Ultralyd (PASS)	Kan klassifisere innholdet i lukkede konteinere	Ny teknikk	Detektor	Væske/ faste

Tabell 2.2 *En oversikt over teknologier brukt i kjemiske punktsensorer.*

Det er i dag få elektroniske sensorer på markedet for deteksjon av kjemiske stoffer i væske- og fastform som er egnet for bruk utenfor laboratorier. De mest benyttede teknikkene egnet for feltbruk er de tidligere nevnte raman og IR. Det som tradisjonelt har vært brukt er deteksjonspapir. Disse kan

trykkes mot mistenkelige væskedråper og skifter farge dersom de kommer i kontakt med kjemiske trusselstoffer. De er billige og enkle i bruk, men utfordringen er at de gir fargeomslag også for en del vanlige løsemidler, dvs. at de kan gi falske positive signaler. Det finnes også spesielt tilleggsutstyr til noen kjemiske gass-sensorer som gjør at brukeren kan varme opp et lite område av prøveoverflaten og overføre væskeformige stoffer og faste partikler til gassform som deretter suges inn i sensoren. Ionemobilitetsspektrometri (IMS) er et eksempel på denne typen metode. IMS benyttes i stadig større grad i post- og varemottak og i sikkerhetskontroller.

Punkt-sensorer for gassdeteksjon er avhengige av at det er detekterbare mengder av trusselstoffene i luften som suges inn i sensoren. Dette er en utfordring dersom stoffene er godt emballert i en pakke som er relativt gasstett. Sensorene utviser ikke samme sensitivitet som hunder, men vil kunne ha anvendelse i f.eks. robotiserte kontrollsystemer. Et slikt system kan designes slik at pakker legges i en gasstett beholder en viss tid for å øke deteksjonssannsynligheten. Dette kan føre til at trusselstoffer i gass- eller aerosolform kan slippe ut av pakken og oppkonsentreres i den lufttette beholderen. Forsøk utført ved FFI har vist at denne teknikken øker sannsynligheten for å kunne detektere kjemiske stridsmidler i små pakker. Økningen i følsomhet ved bruk av denne teknikken er svært avhengig av type emballasje og hvilket trusselstoff det dreier seg om. FFI har ikke utført eksperimenter med narkotika, men prinsippet med konsentrasjon i lukket beholder vil være det samme.

Andre teknikker som kan nevnes er Spatially Offset Raman Spectroscopy (SORS) og Laser-Induced Breakdown Spectroscopy (LIBS). SORS er en variant av raman spektroskopi som tillater nøyaktig analyse av objekter tildekket av klær, plast, papir eller lignende. En laserstråle går inn i materialet gjennom diffus spredning og man detekterer raman-strålingen som blir sendt tilbake. Laserstrålen vil ikke kunne trenge særlig dypt inn i prøven og vil for eksempel bli stoppet av flere lag emballasje. LIBS baserer seg på å punktoppvarme et mikroskopisk område av en overflate og danne en liten plasmasky. Elementsammensetningen i prøven bestemmes fra plasmaets fluorescens, men teknikken kan potensielt også benyttes til å bestemme kjemisk sammensetning av organiske forbindelser, slik som eksplosiver og narkotiske stoffer. Under kontrollerte omgivelser har man med LIBS demonstrert avstandsdeteksjon over flere meter, men teknikken er relativt ny og fortsatt under utvikling.

En tredje metode, kalt magnetisk resonans relaxometri, er også beskrevet til bruk for deteksjon av skjulte væskeformige eksplosiver og ulovlige legemidler eller narkotika i uåpnede beholdere. Teknikken har vist seg effektiv for deteksjon i ikke-metalliske flasker, uavhengig av størrelse eller form. Forsøk har vært knyttet til sikkerhetskontroller, der det ikke er hensiktsmessig å åpne flaskene.

Det skjer en stor utvikling innen Micro Eletro Mechanical Systems (MEMS) som muliggjør blant annet miniatyrisering av systemer for kjemisk analyse, såkalt lab-on-a-chip. Dette øker mulighetene for å benytte deteksjonsmetoder og oppkonsentreringsmetoder i små sensorpakker som tidligere kun var egnet for laboratoriebruk. MEMS-kretser kan egne seg for deteksjon av både biologiske og kjemiske stoffer.

2.5 Terahertz-teknologi

Frekvensområdet som regnes som Terahertzområdet, 0.1 – 10 THz, grenser mot radardomenet for de laveste frekvensene og infrarøddomenet for de høyeste frekvensene. Mangel på kilder i

dette frekvensområdet gjorde at det tidligere kun var interessant for astronomiske anvendelser. På 1990-tallet ble kildene utviklet og forskningen på feltet økte kraftig. I all hovedsak har dette resultert i tre anvendelser: avbildning, spektroskopi og ikke-destruktiv testing. Enkeltfrekvenskilder, med frekvenser under 1 THz, er brukt for å avbilde mistenkelige objekter som for eksempel våpen. Spektroskopi, hvor bredbåndskilder er benyttet, brukes for å gjenkjenne eksplosiver, illegale stoffer som for eksempel narkotika eller for å inspisere farmasøytiske stoffer under fremstillingsprosessen. I ikke-destruktiv testing brukes bredbåndskilder til å avdekke feil i materialer som kan ha oppstått under belastning. Delaminering i kompositttmaterialer som er utsatt for store krefter kan avdekkes med THz teknologi[1].

THz-strålingens største begrensning er vann, som oftest i form av vanndamp i atmosfæren. Vanndamp absorberer THz stråling særdeles effektivt, noe som gjør at strålingen dempes etter få meter gjennom atmosfæren. Derfor virker THz-teknologi best når avstanden mellom kilden og målet, og mellom målet og detektor, er kort. Spektroskopi og ikke-destruktiv testing i laboratoriet fungerer bra fordi avstandene ar korte. Også inspeksjon av bagasje og brev er lovende anvendelser. De fleste innpakningsmaterialer, som papir, papp, plast og tøy, er transparente for THz stråler. Elektrisk ledende materialer, som metaller, derimot blokkerer THz-stråling.

På noen flyplasser anvendes THz-avbildningsteknologi for å avdekke mistenkelige gjenstander som er skjult på kroppen (body skanner). Fraunhofer instituttet(Tyskland) har utviklet et apparat som ligner på en kopimaskin og som skanner brev sendt til innsatte i fengsel for å detektere kontrabande.

Figur 2.1 *Person som skjuler knivblad oppdaget med THz-teknologi.*

2.6 Hyperspektral avbildning

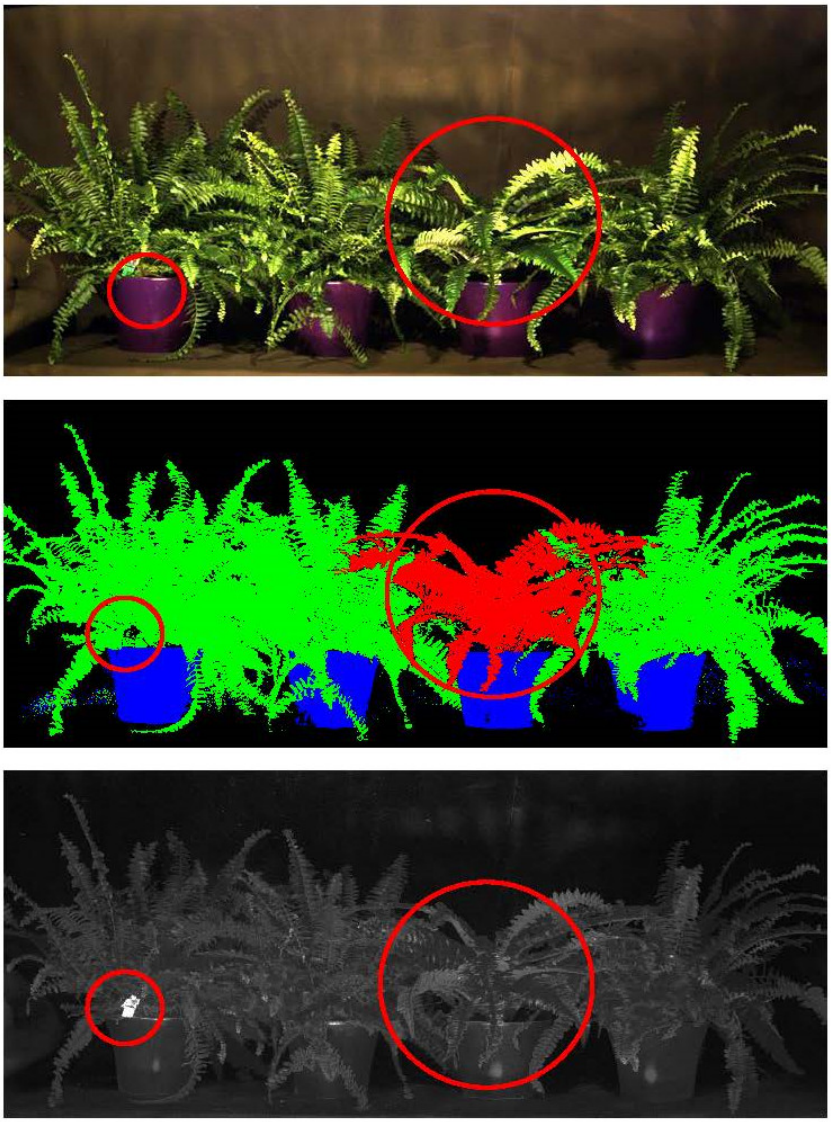
Det er velkjent at spektroskopi i det synlige frekvensområdet kan brukes for å identifisere kjemiske stoffer. Konvensjonelt gjøres spektroskopi ved å ta en prøve og måle den med et laboratorieinstrument. Det finnes også håndholdte spektrometre av ulike slag for punktmålinger direkte på overflaten av et ukjent stoff. I hyperspektral avbildning bruker man et spesialisert kamera som måler spekteret til

lyset som kommer inn i hver piksel i et bilde. På denne måten kan man raskt gjøre spektroskopisk måling i et stort antall punkter over en stor flate. Denne teknologien er illustrert i Figur 2.2 der et hyperspektralt kamera har tatt bilde av en oppstilling planter (ekte og kunstig) med et lite objekt laget av avvikende materialer (Legomann). I det konvensjonelle bildet, som tilsvarer manuell inspeksjon, er det vanskelig å finne den kunstige planten, eller det lille objektet. Ved hjelp av ulike typer prosessering kan man imidlertid framheve disse materialene tydelig. I det ene tilfellet er det gjort spektral klassifikasjon for å skille ut tre materialtyper, inklusiv den kunstige planten. I det andre tilfellet er det gjort spektral avviksdeteksjon for å finne det lille objektet laget av materialer som avviker fra resten av oppsettet.

I tilknytning til tollvesenets anvendelser kan det være aktuelt å bruke hyperspektral avbildning for å oppdage stoffer av spesiell interesse, for eksempel narkotika eller eksplosiver. En annen aktuell anvendelse er å skille mellom forskjellige materialer som er visuelt like, for eksempel for å identifisere forfalskede produkter. Det er viktig å være klar over at hyperspektral avbildning bare er følsom for materialet i overflaten av objektet som avbildes, avhengig av hvor dypt lyset trenger inn. Dette begrenser anvendelsesområdet en god del, siden man for eksempel ikke kan inspisere innsiden av en pakke uten å åpne den (medmindre emballasjen er gjennomsiktig). Noen tenkbare bruksscenarier er:

- Deteksjon av søl av interessante stoffer, for eksempel utenpå pakker eller på gulvet i et lasterom.
- Rask sjekk av mange pakker med tilsynelatende likt innhold for å undersøke om noen har et avvikende innhold.
- Sammenligning av et produkt mot en kjent referanse ved mistanke om forfalskning.
- Monitorering av pakker på et samlebånd for å kjenne igjen en type emballasje som har vært brukt tidligere på pakker med innhold av interesse. (Tilsvarende metoder brukes for sortering av resirkulert avfall.)

Hyperspektrale bilder må prosesseres for å få fram den ønskede informasjonen. Slike prosesseringssystemer må være skreddersydd for anvendelsen. Etablering og drift av et hyperspektralt system krever følgelig en del kompetanse. Eksempler på kommersielle systemer kan finnes på `www.neo.no` eller `www.chemimage.com`.



Figur 2.2 *Figuren viser bilder tatt i ulike spektralområder som viser hvordan en legofigur (rød ring til venstre) og en kunstig plante (rød ring til høyre) fremtrer avhengig av bølgelengde.*

2.7 Networked Intelligent Underwater Sensors

Networked Intelligent Underwater Sensors (NILUS) består av relativt små sensornoder som droppes ned på havbunnen. Nodene kan plukkes opp igjen ved at man benytter den integrerte oppblåsbare løfteposen. NILUS sensornodene har passiv akustikk og magnetiske sensorer, og en lokal autonom signalprosesseringsenhet som automatisk oppdager passerende mål. Informasjon fra sensornodene sendes til et eventuelt operasjonssenter gjennom et undervannskommunikasjonsnettverk bestående av akustiske modem og videre gjennom en gatewaybøye utstyrt med akustisk modem og radiomodem[2].

Figur 2.3 *NILUS sensor node (til venstre) med akustisk modem (til høyre)*

Disse sensorene vil kunne oppdage for eksempel små undervannsbåter som man kan se for seg frakter ulovlige varer. Enkeltkomponentene i systemet er moden teknologi, men sammensetningen av komponenter og bruken er på prototypenivå. Kablede, permanente systemer av denne typen undervannssensorer eksisterer. Fordelen med NILUS er at det er lett deployerbart.

2.8 Liten navigasjonsradar ESM

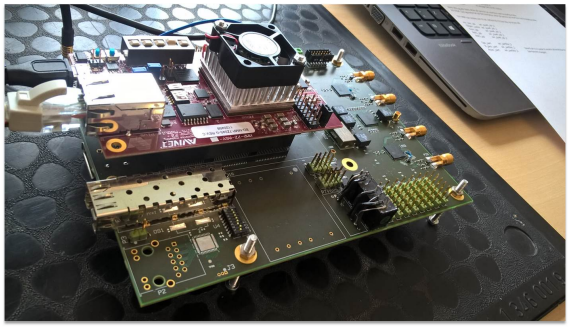
Et skips navigasjonsradar er en aktiv sensor som sender ut radarstråler. Disse strålene kan detekteres av en radardetektor, og ved hjelp av to eller flere slike sensorer kan man bestemme skipets posisjon. Elektroniske Støttetiltak (ESM) er i militær sammenheng fagfeltet som blant annet søker å oppdage, identifisere og lokalisere utsendt elektromagnetisk energi. Typisk vil ESM bruke passive sensorer for deteksjon og geolokalisering av radio- og radar-emittere.

Overvåkning med Automatic Identification System (AIS) er avhengig av skipperens velvillige medvirkning til å bli overvåket. Overvåkning basert på skipenes navigasjonsradar er i langt mindre grad det, siden skipperen vil kvie seg for å slå av sin navigasjonsradar. AIS og ESM kan derfor sammen gi et mer pålitelig sjøbilde og kan faktisk utpeke skip som manipulerer sin AIS-informasjon.

FFI har utviklet en testsensor kalt Liten navigasjonsradar ESM (LINE). Versjon 1 av denne ble demonstrert i forbindelse med lokalisering av skip i sann tid ved Ørland under en Nato-øvelse og senere i Unmanned aerial vehicle (UAV) på Frohavet og i Andfjorden.

Radardetektorene kan verifisere at fartøyene faktisk er der deres AIS-sender sier at de er, ved å finne den egentlige posisjonen til navigasjonsradarene på hvert av fartøyene. Avvik mellom signalene fra båtenes AIS-sender og de signalene radardetektorene plukker opp, kan selvsagt skyldes feil på

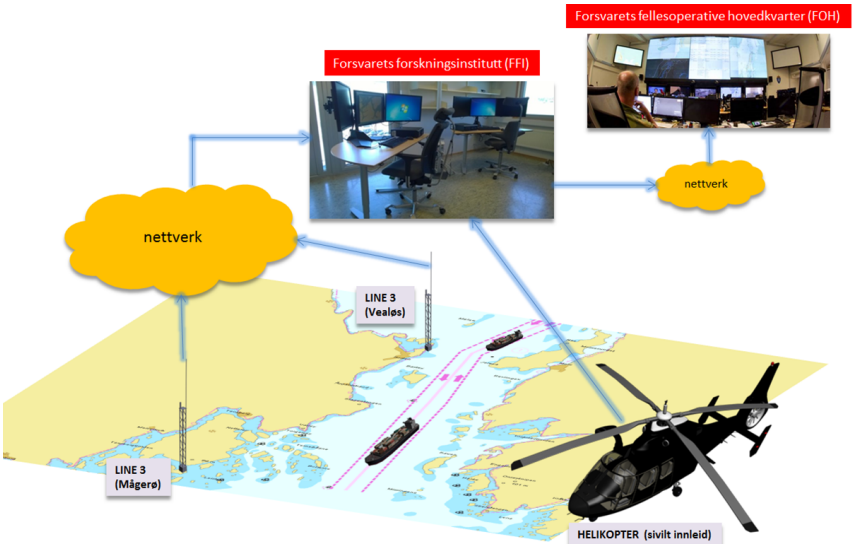
utstyret i båtene. Det kan også være avvik fordi båtene manipulerer signalene, for eksempel fordi de vil skjule tjuvfiske, smugling eller andre lovbrudd [3].



Figur 2.4 *Prototype av LINE 3.*

En forenklet, industrialisert versjon (LINE 3) vil trolig bli svært rimelig og kan utplasseres langs kysten i et stort antall. Dette sensornettverket blir helt uavhengig av Global Positioning System (GPS) og andre satellittbaserte systemer, som er svært lette å forstyrre. I et samarbeidsprosjekt i Nordsjøområdet utredes nå landbaserte systemer for sikrere navigasjon. Dette er i tråd med visjonen til International Maritime Organization (IMO) om sikker e-navigasjon. LINE kan være en aktuell kandidat.

En test skal gjennomføres i samarbeid med Forsvarets operative hovedkvarter (FOH), Kystverket og muligens Tolletaten i Oslofjorden. Tre LINE 3 sensorer skal settes opp og NorSAT-3 (se kapittel 2.9) skal simuleres av et helikopter (se figur 2.5). Målsetningen er å verifisere konseptet for følging, klassifikasjon og avviksdeteksjon i sanntid. En kjede av LINE sensorer vil anslagsvis kunne dekke kystområdene med omtrent tjue kilometers avstand. LINE vil foreløpig få navnet Navigasjonsradardetektor (NRD) når den plasseres på en satellitt.



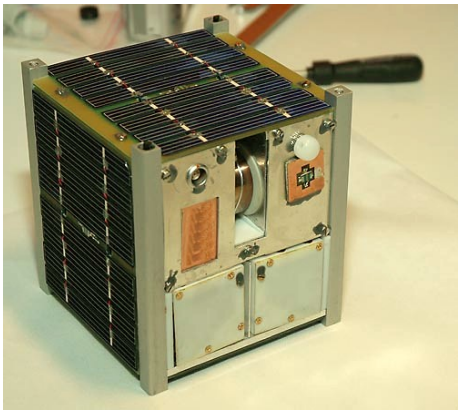
Figur 2.5 *Operativt perspektiv av CD&E med helikoptersimulert NRD på satellitt sammen med landbaserte stasjoner.*

2.9 Satellittbaserte sensorer

En satellitt kan defineres som et objekt som går i bane rundt jorda. Tradisjonelt har disse vært brukt til kommunikasjon og kringkasting samt noe jordobservasjon. Satellittbilder ifm. værvarsling er eksempel på det siste. I de senere år har begrepet "New space" dukket opp. Dette har sammenheng med at verdensrommet har blitt mer tilgjengelig, ikke bare for statlige aktører, men også for kommersielle aktører. Ny teknologi og lavere kostnader i forbindelse med oppskyting av satellitter gjør at flere aktører beveger seg inn på satellitt-markedet. Disse aktørene er i stand til å utvikle og bygge små satellitter svært raskt, og få dem i bane til svært lav kostnad per satellitt.

2.9.1 Mindre satellitter

Mikrosatellitter er en klasse av veldig små satellitter. Med den utviklingen i teknologi som har vært, har det blitt mulig å bygge satellitter med en vekt fra noen gram til noen få kilo. Slike små satellitter beskrives ofte som "CubeSats". En typisk CubeSat er formet som en kube som er 10 × 10 × 10 cm. Den er laget slik at den kan monteres i en standard oppskytingsadapter, slik at oppskytningskostnadene kan holdes lave. En slik CubeSat vises i figur 2.6 Denne minste størrelsen beskrives som 1 U. Større satellitter beskrives typisk som 16 U el.l.



Figur 2.6 *Den norske CubeSat nCube-2 (kilde:* `http://ncube.no/utviklingen-av-ncube-2/`*, 16. mai 2017).*

2.9.2 Navigasjonsradardetektor på satellitt

Alle skip over en viss størrelse er pålagt å sende ut AIS-signal som identifiserer fartøyet og dets posisjon og destinasjon. Deteksjon av Automatic Identification System (AIS) med den norske satellitten AISSat-1 fra 2010 har gitt gode resultater for overvåkning av skipstrafikk. AIS er svært nyttig for maritim overvåking, men er avhengig av at skipene faktisk følger internasjonale regler. AISSat-erfaringen viser at noen rapporterer feil posisjon, og slår av AIS-senderen i perioder. Andre bytter identitet rett som det er. For å fange opp disse, arbeides det med en videreutvikling av konseptet. Det er ønskelig å kunne oppdage ikke-kooperative fartøyer med et sensorsystem som er under nasjonal kontroll.

Foruten dobbel ytelse på AIS-mottaker anses det mulig å få på plass en rombasert ESM-kapasitet innen få år. Dette vil gjøre det mulig å oppdage fartøy som seiler uten AIS, men som har navigasjonsradar på. Prototypen LINE 3 er snart klar, se kapittel 2.8. Den kan gjøre alle målinger som mikrosatellitter trenger for å peile og skille det store antallet skipsradarer som en satellitt vil observere i en radius på 2800 kilometer, i 600 kilometers høyde. Satellittsensoren har foreløpig navnet NRD.

2.9.3 Elektro-optisk på satellitt

FFI jobber med konsept for lavlyskamera med oppløsning på ca 10m som planlagt plassert på en satellitt. Man planlegger en kapasitet for deteksjon av mål på minimum 30 m som vil tilsvare ca 3 piksler. I en tollsammenheng vil man kanskje se for seg et behov for deteksjon av mindre fartøy (10 m) som medfører et større krav til optikken, og det vil igjen bli kostnadsdrivende. Hvis man i tillegg ønsker å klassifisere fartøy, vil man stille enda større krav til optikken.

2.9.4 Satellittbaserte radarsystemer

Det utvikles stadig nye og mer avanserte radarinstrumenter med nye kapasiteter. Norge har i dag en avtale med Canada som gir tilgang til data for offentlig bruk fra den kommersielle satellitten Radarsat-2. Canada planlegger å skyte opp tre nye radarsatellitter i 2017-18, og er interessert i å fortsette samarbeidet med Norge. De nye satellittene vil også bli utstyrt med AIS-mottaker, noe som vil gjøre det mulig å sammenstille observasjoner av skip fra synthetic aperture radar (SAR) og AIS. Dette vil øke evnen til å identifisere unormal aktivitet. Norge er også med i et europeisk samarbeid gjennom European Space Agency (ESA), som vil ha to radarsatellitter i polar bane fra 2014. Utfordringen for Norge vil være å få prioritet til bruk over våre områder[3].

2.9.5 Maritim overvåkning fra satellitt

Figur 2.7 *AIS Sat-1.*

FFI har bidratt til utviklingen av to nanosatellitter på 20 × 20 × 20 cm. i lav jordbane, utstyrt med AIS-mottakere for å overvåke skipstrafikk utenfor rekkevidden til landbaserte basestasjoner. I tillegg til å overvåke skipstrafikk i norske interesseområder, bidrar satellittene til å etablere et globalt maritim situasjonsbilde. Satellittene har godt dekningsområde i nord[2].

[2] `http://www.heavens-above.com/`

FFI har erfaring med bruk av radarbilder fra store satellitter som Radarsat og den nye europeiske Sentinel-1. Radarbilder gir oversikten både i mørke og gjennom skydekke. Det er imidlertid vanskelig å identifisere skip kun med radar. Andre teknikker er derfor også interessante og lar seg kanskje realisere fortere, for eksempel lavlyskamera, som er svært lysfølsomme kameraer, og radardetektorer. FFI forsker på begge teknikkene og bruken av dem på små satellitter[3].

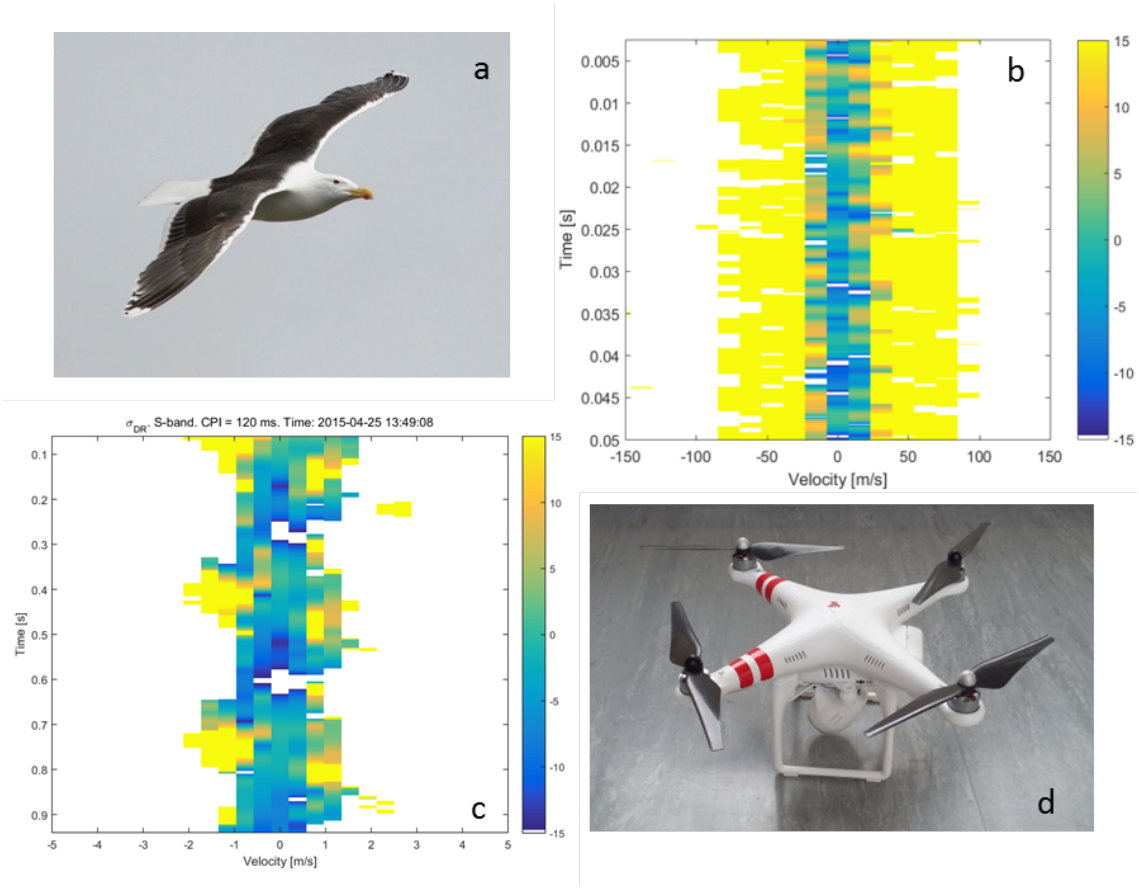
2.10 Radar

Radar er godt egnet til å detektere objekter på avstand, f.eks. personell eller farkoster på bakken, i luft og på sjø, og har derfor stort potensiale innen overvåking av grenseområder. Et eksempel på anvendelse av radar er overvåkning av skipstrafikk, som ble nevnt i avsnitt 2.9 om satellittbaserte sensorer. En annen aktuell anvendelse for Tolletaten kan være dronedeteksjon ved hjelp av radar. Antallet slike små, ubemannede luftfartøy i luftrommet omkring oss har økt dramatisk de siste årene. Ubemannede luftsystemer har ofte vært assosiert med militær bruk, like fullt er økningen i droneaktivitet de siste årene i stor grad knyttet til sivil bruk. Faktorer som lav pris, stor tilgjengelighet og enkel operasjon av fartøyene antas å bidra til denne utviklingen.

Den økte bruken av mikro- og mini-droner, begreper her brukt om farkoster under henholdsvis 2 kg og mellom 2 og 20 kg, stiller strengere krav til overvåkning for å opprettholde sikkerhet i luften, på bakken og til havs enn hva man tidligere har vært vant til. Dette gjelder både på militær og sivil side. En aktuell problemstilling er knyttet til hvordan man for eksempel kan forhindre dronebasert smugling og rekognosering ved grenseoverganger.

Deteksjon, målfølging og klassifikasjon er tre viktige oppgaver for systemer som har til oppgave å motvirke illegal bruk av droner. Dronene må detekteres og skilles ut fra bakgrunnsstøy, refleksjoner fra andre uinteressante objekter (clutter) og interferens fra andre radiosystemer. Videre må hvert enkelt mål kunne skilles fra andre og spores i rommet over tid. Klassifikasjon av målet er svært relevant ettersom droner må kunne skilles fra andre mål med liknende radartverrsnitt og bevegelsesmønster, eksempelvis fugler. Disse tre oppgavene antas å være løsbare ved nøye konfigurering av radaren. Mer detaljert klassifikasjon i form av identifikasjon av dronetype kan være mulig basert på radardata alene hvis systemet utvikles med tanke på dette.

En forutsetning for deteksjon er fri sikt mellom radar og målet. Dette kan være en utfordring for små, lavtflygende droner, der vegetasjon og terrengformasjoner ofte er til hinder for deteksjon. Målets størrelse (radartverrsnittet) påvirker også deteksjonsavstanden. Droner reflekterer langt mindre effekt enn f.eks. et småfly, med tilsvarende kortere deteksjonsavstand. Små droner har forøvrig ofte et radartverrsnitt sammenlignbart med fugler. Å skille mellom droner og fugler med sammenlignbart radartverrsnitt og bevegelsesmønster har vist seg å være en hovedutfordring for droneovervåkning med radar, se [4]. I denne sammenheng er klassifikasjon av målet viktig. Sannsynligheten for riktig klassifikasjon avhenger av mange faktorer, men kan påvirkes gjennom valg av radarparametere. Høy bærefrekvens og fullpolarimetriske målinger har bl.a. vist seg å være nyttig. Figur 1 viser et eksempel på kombinasjon av mikro-Doppler informasjon og en polarimetrisk parameter samlet inn med det eksperimentelle radarsystemet BirdRAD i S-bånd.



Figur 2.8 *Klassifikasjon av fugl og drone med radar i S-bånd. a - Fotografi av Svartbak. b - Differensiell RCS av DJI Phantom II drone i form av spektrogram. c - Differensiell RCS av Svartbak i form av spektrogram. d - Fotografi av DJI Phantom II drone.*

Radar som frittstående sensor antas å kunne gi god ytelse innen overvåkning av droner når denne designes for formålet. Radarens styrker er knyttet til deteksjon av mål i bevegelse, god rekkevidde, penetrasjonsevne i vegetasjon (dersom dette vektlegges gjennom valg av lav bærefrekvens), og ytelse uavhengig av lys- og vær-forhold. Likeledes kan grovklassifikasjon av dronen være mulig basert på radar alene. Høyere grad av klassifikasjon, samt vurdering av eventuell last og bestykning kan være mulig basert på fusjon med andre sensorer.

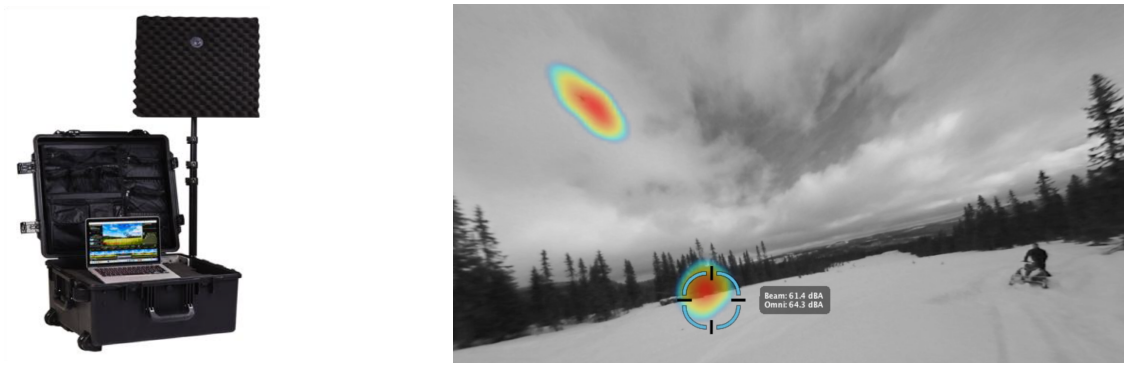
2.11 Akustiske sensorer

Akustiske sensorer kan brukes til deteksjon, gjenkjenning og følging av kjøretøy på bakken (veitrafikk) og farkoster i luft og på sjø, og kan derfor i likhet med radar ha en funksjon innen overvåking av grenseområder. Slike sensorer skiller seg imidlertid fra elektro-optiske sensorer (kameraer, radar, laser mm.) ved at de er tilnærmet uavhengige av fri sikt og helt uavhengige av lysforhold. Dette gir i prinsippet heldøgns- og helårsdekning under praktisk talt alle vær- og terrengforhold. Man kan imidlertid ikke forvente samme rekkevidde som med f.eks. radar.

Akustiske sensorer er godt egnet til å supplere andre sensortyper for å gi et mer fullstendig dekningsområde enn det som kan oppnås ved direkte-sikt sensorer alene. De kan derfor inngå i deteksjonssystemer for å oppdage f.eks. droner som passerer grensen. Slike droner kan tenkes å frakte smuglergods eller brukes til rekognosering (overvåking av grensestasjoner, for å avdekke grensekontroll før biler med smuglergods blir sendt over). Et annet mulig anvendelsesområde for akustiske sensorer kan være deteksjon av kjøretøy i kombinasjon med ANPR, slik at alle grensepasseringer med motoriserte kjøretøy detekteres, uavhengig av nummerskiltets synlighet/lesbarhet.

Deteksjonsrekkevidden avhenger bl.a. av kildens lydstyrke, og vil forøvrig variere mye med forplantningsforholdene, som i sin tur er bestemt av vær-, terreng- og bakkeforhold, samt støy fra omgivelsene (bakgrunnsstøy). Under gunstige forhold kan i sær lavfrekvent lyd (f.eks. helikoptre) detekteres på svært lang avstand (10 - 20 km), selv med terrenghindringer i mellom. For små droner er deteksjon på noen få hundre meters avstand mer realistisk. Her foregår det imidlertid mye forskning for tiden (også på FFI) for å avklare mulighetene som ligger i akustisk dronedeteksjon. Potensialet som ligger i dyp læring (se avsnitt 3.2) for både deteksjon og gjenkjenning (klassifisering) av bl.a. droner i et komplisert lydbilde, er så langt vi vet lite utprøvd pr. i dag.

Det finnes flere akustiske sensorer på markedet som først og fremst er beregnet på militære anvendelser. De fleste er såkalte skuddeteksjonssystemer, men det finnes også systemer for deteksjon av helikoptre og lokalisering av artilleri.



Figur 2.9 *Akustisk sensor fra SquareHead Technologies til venstre. Bildet til høyre viser et eksempel på deteksjon av drone (øverst til venstre i bildet) og stridsvogn (nederst i bildet).*

Det norske firmaet Squarehead Technologies har utviklet en sensor med tilhørende programvare, spesifikt for deteksjon, gjenkjennig og følging av droner. Her benyttes paneler med 16 x 16 mikrofoner (MEMS) for å registrere lyden. Prosessoren i systemet foretar retningsbestemming ved hjelp av ulike typer stråleforming (beamforming). Dette gjør det mulig å følge flere droner (generelt lydkilder) på en gang, og angi type drone. I øyeblikket kan systemet skille mellom noen få utvalgte typer. Panelet er utstyrt med et web-kamera, og detekterte lydkilder kan markeres i bildet. Figur 2.9 viser systemet og et eksemplel på et bilde fra systemet, med overlagrede akustiske «hot spots» fra henholdsvis drone og stridsvogn. Systemet er under kontinuerlig utvikling.

2.12 Registre i innland og utland

Myndigheter og aktører innen vareførsel besitter hver for seg ulike typer informasjon som til sammen kan belyse om en gitt pakke er innført iht. lover og forskrifter eller om det er grunnlag for mistanke om ulovligheter. Dette kan f. eks. være lister over bankkonti, forretningsforetak, kundelister, leverte og bestilte varer, leveringsadresse. Registrene vil gjerne være knyttet til navn på person. Lovlig grunnlag og avtaler med aktørene om at slike data skal gjøres tilgjengelig må på plass. Det vil i denne sammenheng være en fordel om det er mulig å gjøre oppslag i andre registre, enn Tolletatens egne, uten å lagre disse dataene.

2.13 Biometri

Systemer for automatisk identifisering av personer er under utvikling for flere formål. Relevante teknologier basert på ansikt, iris, fingeravtrykk, ganglag, DNA, stemme og kroppslige proporsjoner er i dag modne for anvendelser eller i rask utvikling. Alt ligger derfor teknologisk til rette for bruk av biometriske data for gjenkjenning eller identifisering av personer. Utfordringene er knyttet til personvern og beslutning om å bygge opp informasjonsdatabaser som er tilgjengelige for brukerne, f.eks. tollbetjenten.

Man kan i prinsippet skille personer ved å sammenligne nesten hva som helst ved kroppen, gitt at man kan måle med en tilstrekkelig nøyaktighet. Av praktiske og historiske årsaker er DNA, ansikt, fingeravtrykk, og iris metoder der det finnes aksepterte standarder som gjør det forholdsvis lett og interessant å utveksle informasjon mellom etater. Bortsett fra DNA har International Civil Aviation Organization (ICAO) definert hvordan disse fire modalitetene kan inkluderes i elektronisk lesbare pass og er derfor av særskilt interesse ved grensepasseringer. European Union (EU) har definert identitetskort som er maskinlesbare etter ICAO-standarden og de fleste landene i EU har tatt dette i bruk. Norge har også vedtatt å utstede slike Identifikasjon (ID) kort og ordningen forventes å tre i kraft i 2018.

Biometri har i stor grad vært knyttet til kriminalitetsbekjempelse fordi undersøkelser av fingeravtrykk og DNA har hatt stor suksess i teknisk etterforskning. Overvåkning, straff og innskrenkninger i privatlivet har dominert diskusjonene rundt biometriske systemer i Europa, mens det for eksempel i India i mye større grad fokuseres på de positive sidene. Deres nye statlige biometriske identifikasjonssystem, Aadhaar, er basert på fingeravtrykk og iris-skann og skal forvalte identitet på en sikker måte. Det er nøkkelen til å gi analfabeter et alternativ til vanlig legitimasjon og dermed mulighet for banktjenester og trygdeytelser. Mer enn 99% av Indias 1,1 milliarder innbyggere er nå (2017) registrert i systemet. Samtidig har privat sektor i vesten, som blant annet bankvesen, kortutstedere, sikkerhetsindustri og elektronikkprodusenter begynt å vurdere biometriske løsninger fordi de har potensial til å kunne lages sikrere og på sikt driftes rimeligere enn dagens alternativer. Dette er elementer som vil bli vektlagt i utformingen av lovgrunnlaget. På samme måte som vi i dag har et helt annet forhold til å dele private opplysninger med kommersielle aktører på grunn av revolusjonen i sosiale medier, vil sannsynligvis allmennheten ha et annet syn på biometriske ID-metoder om ti år.

Selv om en av Tolletatens primæroppgave er kontroll av objekter og ikke personer, er personopplysninger og informasjonsinnhenting rettet mot individer i mange tilfeller avgjørende for å avdekke

ulovlig innførsel. USA har både i justis- og forsvarssektoren investert tungt i informasjonssystemer som baserer seg på å dele personinformasjon basert på biometriske data. Landet er en sterk drivkraft for utvidet samarbeid mellom nasjoner og internasjonale organisasjoner for en mer effektiv bekjempelse av internasjonal kriminalitet og terrorisme. Dette gjenspeiles i organisasjoner som North Atlantic Treaty Organization (NATO) og Interpol. EU-databaser som Schengen Information System (SIS) II og visasystemet Visa Information System (VIS) inneholder nå biometriske data. For effektivt å kunne innhente og behandle slike data og sammenstille dem med egne trafikk- og kontrolldata, vil det være nødvendig med en plattform for håndtering av biometriske modaliteter. Dette inkluderer et system for innhenting av biometriske data ved kontrollpunkter, oppslag i biometriske data (biometrisk matching), utveksling med andre etater og en sammenkobling av de biometriske dataene med andre relevante data i saksbehandling og etterretning.

Biometriske data gir mulighet for å bygge informasjonssystemer som gir styrket personvern. Datautveksling mellom etater kan gjøres mer målrettet og tilgang til personinformasjon bedre koblet til tjenstlige behov. Man kan enklere skille på hvem som innsamler informasjon, hvem som lagrer informasjon og til sist hvem som eier og gir tilgang til informasjon. Dette kan man også gjøre uten bruk av biometriske data, men det kan lettere automatiseres og effektiviseres ved hjelp av biometri. Et eksempel på dette er "ping&ring-konseptet" som utvikles i NATO. I et operasjonsområde vil det kunne være flere land som opererer under en felles samarbeidsavtale som er restriktiv og begrenser informasjon som utveksles. Bilaterale avtaler vil gjerne gi større frihet til deling, men da kan ikke dataene legges i felles NATO-system. Ved å sette opp et nettverk av separate nasjonale systemer kan man tenke seg at land A sender ut et fingeravtrykk og ber partnernasjoner om informasjon knyttet til dette. Landene velger så respons basert på de bilaterale avtalene og utveksler det de har hjemmel for. Dette kan være både helautomatiske systemer eller manuelt autorisert. Systemet kan enkelt utvides utover operasjonsområder og ved behov ta inn organisasjoner som Interpol. I takt med at politiet og andre aktuelle nasjonale og utenlandske samarbeidspartnere for Tolletaten tar i bruk biometri vil "ping&ring-nettverk" bli mer aktuelt for å utnytte hjemmelsgrunnlaget som foreligger for samarbeid og utveksling av personinformasjon.

2.13.1 Anvendelse

Biometri kan ha en rekke anvendelsesområder innen persondeteksjon, -sporing, -identifikasjon, -verifikasjon og -informasjonsforvaltning. Innovasjonen innen området foregår både konseptuelt og teknologisk.

Vi kan skille mellom biometriske systemer for overvåkningsformål og systemer der personen samarbeider ved opptak av biometri. Passkontroll er et eksempel på det siste. Personen oppgir en identitet og systemet har et sett med sensorer (kamera, fingeravtrykksleser) som registrerer egenskaper ved personen. Dataene sammenholdes med hva som er lagret på identiteten i en database eller medbrakt på id-kortet. Slike en-til-en søk er i dag datateknisk trivielt og kommersialisert. Ytelsen er bedre enn for manuell passkontroll.

Man kan tenke seg et system der personer som krysser en grense ved en flyplass eller havneanlegg, kan gå gjennom en sone uten å vise identitetspapirer, men der kamera gjør ansiktsgjenkjenning slik at kun de som ikke gjenkjennes, blir bedt om å vise legitimasjon. Dette er mye mer utfordrende å få effektivt fordi man ikke vet hvilken identitet man skal sammenligne med. Man må i utgangspunktet

søke mot alle data i hele databasen, et en-til-mange søk. Det gjøres mye forskning på å effektivisere denne typen søk, men det er krevende når databaser blir så store som hele populasjoner. Det stilles også større krav til sensorer for å danne akseptable bilder som kan sammenlignes med passbilder, når de er tatt fra ulike vinkler og under varierende lysforhold. Det er en teknologiutvikling på både sensorer og gjenkjenningsteknologier som gjør denne typen identifisering stadig mer aktuell. Federal Bureau of Investigation (FBI) faset inn 2. generasjon av Next Generation Identification System (NGI) i 2011. Det benytter multimodal matching og kan gi treff selv om foto eller fingeravtrykk alene ikke er godt nok for et entydig treff. Utviklingen av avanserte algoritmer som kan sammenstille ulike data for gjenkjenning, vil trolig kunne gå raskt i takt med utviklingen innen dyp læring.

Ved mange kontrollpunkter benyttes overvåkningskamera for å avdekke mistenkelig aktivitet. Operatørene bygger seg erfaring om hvilke mønstre som er vanlige og hva de bør reagere på. Et system som kan gjenkjenne og skille personer fra hverandre ved bruk av bildegjenkjenning, vil kunne oppdage avvikende aktivitet uten at personen nødvendigvis identifiseres. Det kan gi alarm eller merke enkeltpersoner og følge dem gjennom området, bytte kamera automatisk og lagre sporet i tilfelle det fører til en kontroll med funn. Videre kan systemet brukes til å bygge en statistisk normaltilstand slik at det kan reagere på anomaliteter. Slike systemer vil kunne gi både beslutningsstøtte operativt og data til etterretningsarbeidet.

2.14 BarentsWatch

Informasjonstilgangen i det maritime domenet er så stor at det er svært utfordrende å rette fokus og ressurser mot viktige objekter, hendelser og aktører. Tolletaten har derfor behov for automatiske prosesseringssystemer som kan analysere de store mengdene data og informasjon og presentere et fåtall relevante objekter å følge med på i sitt situasjonsbilde. Videre kan dette situasjonsbildet kobles sammen med historikk fra ulovlige og normale transporter og gjøre at overvåkingsfokus og prioritering av øvrige ressurser forbedres ytterligere.

Svært forenklet kan vi si at maritim situasjonsbevissthet er knyttet til:

1. tilgang til tidsriktig strøm av data og informasjon av tilstrekkelig kvalitet,
2. teknologiske løsninger for å behandle volumet av data og informasjon mottatt,
3. trente analytikere for å vurdere operasjonelle konsekvenser av informasjonen og
4. muligheter for å dele informasjon med de som måtte trenge den.

Tolletaten bør, sammen med deltakerne i BarentsWatch-prosjektet og eventuelt andre statlige etater, se på muligheten for å utvikle smarte fellesløsninger. Dette innebærer, fra laveste til høyeste ambisjonsnivå, å utvikle:

1. enkle logiske algoritmer som analyserer de mer statiske dataene (navn på skip, IMO nummer, internasjonale kallesignaler, etc.), sammenstiller og tilgjengeliggjør de i Barents Watch eller for brukernes egne applikasjoner. Det bør tas vare på avviksdata.
2. algoritmer som analyserer de dynamiske dataene (posisjon, fart, manøvertype etc.), sammenstiller og tilgjengeliggjør de i Barents Watch eller for brukernes egne applikasjoner. Data fra sensorer som verifiserer skipsposisjoner må integreres for å avdekke uregelmessigheter i rapporterte posisjoner.

3. algoritmer som analyserer annen tilgjengelig informasjon om mannskap, passasjerer, last, svartelister på fartøy og personer, etterretning, etc., sammenstiller og tilgjengeliggjør de i Barents Watch eller brukernes egne applikasjoner.

Normal oppførsel for et skip er ikke en statisk størrelse, men varierer både med situasjonen og type skip [5][6]. Å definere et slikt variabelt sett med normalsituasjoner er ikke trivielt, men kan f.eks. gjøres gjennom *Pattern of Life* analyse, dersom tilstrekkelig data er tilgjengelig, se kapittel 3.3. Gitt at en normalsituasjon er definert kan avvik fra denne detekteres.

Samarbeidsprosjekter som Barents Watch er avhengig av aktive og kravstore brukere som både tar i bruk de informasjonskildene som er tilgjengelige og som ser etter muligheter for forbedringer. Nye bakkebaserte og rombaserte passive og aktive sensorer (f.eks. LINE/NRD og nye AIS-kilder) vil kunne gjøres tilgjengelig hvis flere etater ønsker det. Dette vil øke evnen til deteksjon og sporing av ulovlig trafikk langs kysten. Ved å videreføre sin involvering i Barents Watch med en robust brukergruppe og melde inn sine ønsker og behov, vil Tolletatens situasjonsbevissthet i det maritime domenet kunne forbedres.

2.15 Utvidet virkelighet

Utvidet virkelighet (engelsk: AR) er en samlebetegnelse på presentasjonsteknologier for sensorinformasjon som ikke hindrer bruken av menneskets egne sanser, men heller koder om sensorinformasjonen til signaler som kan oppfattes av sansene. Sagt på en annen måte gjør teknologien sensorinformasjonen sansbar og legger den til den direkte informasjonen fra omgivelsene som sansene fanger inn. Arketypen på AR-teknologi er jagerpilotenes hjelmskjerm, "Head Up Display", hvor det projiseres et bilde, f.eks. radarspor, målposisjon eller lignende, som er synlig for piloten samtidig som han ser omgivelsene gjennom glasset i cockpiten. Mellom sensor og projsert bilde foretas dataprosessering av sensorinformasjonen og pilotens bevegelser slik at informasjonen presenteres korrekt overlagt det naturlige synsbilde av omgivelsene.

Teknologien er moden og allerede tilgjengelig i det sivile markedet. Spillet Pokemon Go bruker GPS-lokalisering av virtuelle dyr som kun blir synlig på skjermen når mobiltelefonen er i nærheten av det virtuelle dyrets virkelige oppholdsted. Microsoft Hololens har demonstrert anvendelser innen medisin, design og arktitektur såvel som bygg- og anleggsarbeid. Både bilde og lyd kan brukes for å orientere personen ift. virkelige eller virtuelle fenomener og objekter. Spedisjonsfirmaet DHL har pekt på DHL Trend Report “Augmented Reality” at AR vil kunne være et nyttig verktøy innen flere deler av logistikken, ifm. lasting og lossing, navigering, kundestøtte og utplukk av pakker.

En mulig anvendelse for Tolletaten er å tilgjengeliggjøre sensordata mens man leter etter et mistenkelig objekt i en pakke eller konteiner. For eksempel kan et røntgenbilde av en pakke bli synlig som et orientert 3D-bilde overlagt eget synsbilde. Mens man snur eller åpner pakken vil det prosesserte bildet orienteres på samme måte og lettere gjøre det mulig å finne et mistenkelig objekt.

[3], som blant annet beskriver AR i lasting og lossing, transport, kundestøtte, utplukk etc.

[3] http://www.dhl.com/content/dam/downloads/g0/about_us/logistics_insights/csi_augmented_reality_report_290414.pdf

Figur 2.10 *Illustrasjon av utvidet virkelighet (engelsk: Augmented Reality (AR)). Data fra ulike sensorer supplerer det som øyet (og andre sanser) oppfatter og vha. dataprosessering presenterer dataene for øyet. Hentet fra: DHL Trend Report "Augmented Reality" 2014*

3 Dataanalyse og maskinlæring

Teknologi og anvendelsesområde	Mod.	Gj.f.
Tolkning av røntgenbilder basert på maskinlæring/dyp læring		
Avviksdeteksjon basert på dyp læring		
Gjenkjenning av varer basert på bildeanalyse		
Maskinlæring og ANPR		
Maskinlæring kan anvendes på alle sensorteknologier med en viss modenhet.		
Maskinlæring kan anvendes på heterogene data.		

Tabell 3.1 *Tabellen viser ulike anvendelser av maskinlæring som er omtalt i dette kapitlet. Teknologisk modenhetsnivå (Mod.) og gjennomførbarhet (Gj.f.) er indikert med farger som angir graden av oppnåelse: grønn = høy, gul = medium, og rød = liten.*

Dette kapitlet tar for seg ulike sider ved fagfeltet maskinlæring. De mest aktuelle anvendelsene for Tolletaten er oppsummert i tabell 3.1. Tabellen anslår teknologiens modenhet og gjennomførbarhet for de ulike anvendelsene.

Maskinlæring er et fagfelt i grenselandet mellom statistikk, matematikk og informasjonsvitenskap. Fokus for dette fagfeltet er metoder som i større eller mindre grad gir maskiner mulighet til å treffe beslutninger basert på tilgjengelige data. Et dagsaktuelt eksempel på et slikt system er fingeravtrykksleseren som nå finnes på mange ulike håndholdte enheter som for eksempel mobiltelefoner. Systemet er designet slik at det kan analysere data fra en fingeravtrykksleser for så å avgjøre om et gitt fingeravtrykk er eierens fingeravtrykk. Systemet har altså lært seg å kjenne igjen en gitt persons fingeravtrykk (har altså lært noe om sine omgivelser) og kan, basert på dette, ta ulike avgjørelser.

Som fagfelt har maskinlæring røtter tilbake til årene rundt 1950 og har siden dette vært i rivende utvikling. En viktig gren innen forskningen i dette store fagfeltet har vært utviklingen av systemer som på et eller annet nivå etterligner menneskehjernens antatte måte å gjøre beregninger på. Allerede i 1957 foreslo Frank Rosenblatt at man kunne bruke et såkalt perseptron (en enkel modell for et biologisk nevron) for å gjøre beregninger. Disse tidlige arbeidene ga senere opphav til forskning på såkalte nevrale nett, et forskningsfelt som har vært en underdisplin av maskinlæring siden den gang.

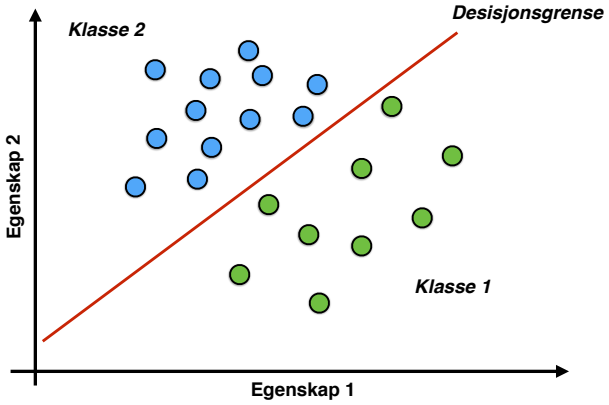
Selv om nevrale nett lenge har vært gjenstand for omfattende forskning var resultatene ikke spesielt imponerende og ønsket om at man skulle kunne klare å etterligne menneskehjernens ytelse virket lenge som et svært fjernt håp. I de siste årene, grovt anslått i tiden etter 2010, har dette imidlertid forandret seg kraftig.

Denne utviklingen kan forklares på en rekke måter, men det virker naturlig å peke på to drivkrefter som har hatt en spesiell innflytelse. En underliggende årsak har vært den dramatiske endringen i tilgangen på billig datakraft, en utvikling man kan takke spillindustrien for. I dag kan rimelige grafikkkort for massemarkedet yte 10 teraflops (10 milliarder flyttallsoperasjoner per sekund) over

tid, noe som gjør at dagens nevrale nett kan være enormt mye større og mer komplekse enn hva man tidligere har kunnet bruke. En annen årsak er at man i den senere tiden har gjort metodiske framskritt som har vist seg å være nøkler for å oppnå bedre ytelse, her er det rimelig spesielt å peke på såkalte konvolusjonsnett som en kritisk teknologi for bedret ytelse.

3.1 Mønstergjenkjenning

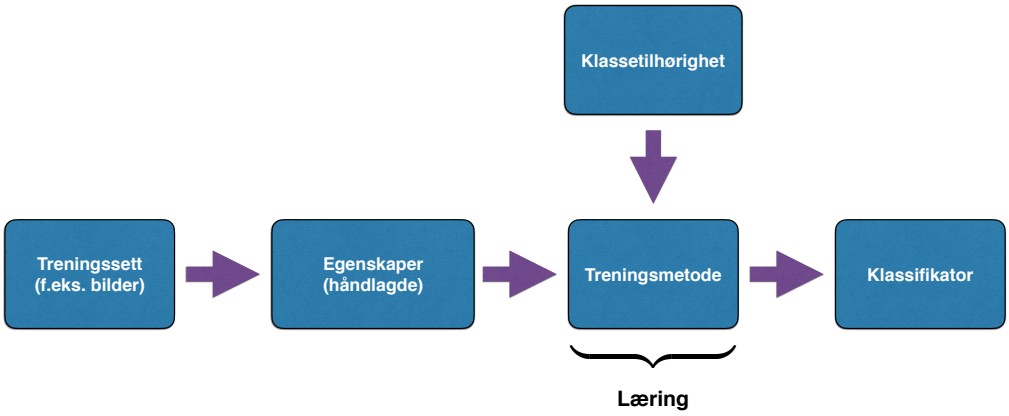
Fagfeltet mønstergjenkjenning dreier seg i hovedsak om å klassifisere objekter av interesse til én av flere mulige klasser eller kategorier. Objektene (*mønstrene*) kan være trykte bokstaver, håndskrevne tegn eller fysiske gjenstander i bilder, elektromagnetiske signaler, ulike tilstander i f.eks. medisinsk sammenheng, og mye mer. Tradisjonelt trener man her opp en *klassifikator* til å skille mellom forskjellige kategorier ut fra karakteristika (egenskaper) ved objektene, dvs. man ønsker å lære en maskin til å skille mellom klassene (ref. begrepet *maskinlæring*), basert på eksempler på objekter fra ulike klasser. Egenskapene er tallstørrelser (målinger) avledet fra objektene. For et objekt i et bilde kan f.eks. høyde, bredde eller omkrets være mulige egenskaper.



Figur 3.1 *Eksempel på objekter fra to klasser (henholdsvis grønne og blå sirkler), representert ved to målte tallstørrelser (egenskap 1 og egenskap 2). Den røde linjen (desisjonsgrensen) deler her dette todimensjonale egenskapsrommet inn i separate regioner, én for hver klasse. Ukjente objekter blir klassifisert til den region de havner i, dvs. hvilken side av desisjonsgrensen de ligger på.*

Figur 3.1 viser et eksempel med to egenskaper plottet mot hverandre for et utvalg av eksempler fra to klasser. La oss si at problemet består i å avgjøre hvorvidt en kunstgjenstand laget av tre er ekte eller en forfalskning, der ekte gjenstander typisk er laget av lyst trevirke med lav kornethet i veden, og la egenskap 1 være lysheten og egenskap 2 være kornetheten. Hvis nå de grønne sirklene representerer ekte gjenstander og de blå falske, kan man trene opp en klassifikator for å skille mellom falske og ekte gjenstander. Den heltrukne linjen er en såkalt desisjonsgrense som deler inn rommet i regioner svarende til hver av klassene man ønsker å skille mellom. I dette eksempelet skiller desisjonsgrensen perfekt mellom eksempelobjektene fra de to klassene, men dette vil generelt ikke være tilfelle. Målet med treningen (maskinlæringen) er å komme frem til desisjonsgrenser som skiller klassene best mulig, slik at sannsynligheten for å tilordne et objekt til feil klasse blir så lav som mulig.

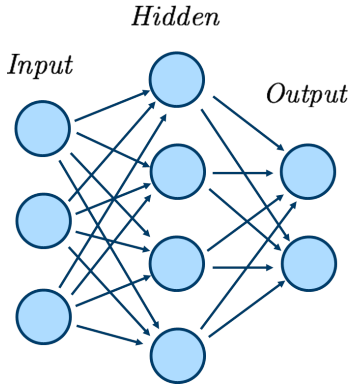
Maskinlæring foretas vanligvis ved såkalt *veiledet læring*, som forutsetter at klassetilhørigheten til eksempelobjektene er kjent. Gangen i denne prosessen er illustrert i figur 3.2. Ut fra objektene i treningssettet (til venstre i figuren) vil man tradisjonelt gjøre et valg av egenskaper basert på á priori kunnskap om problemstillingen. Tallverdiene til disse egenskapene blir beregnet i den såkalte egenskapsuttrekkeren for hvert av objektene i treningssettet. Her vil det typisk foretas en form for bilde- eller signalanalyse, avhengig av hva slags data som er input til klassifiseringsprosessen. Treningsobjektene, representert ved de valgte egenskapene, brukes til trening av klassifikatoren. Målet med treningsprosessen er å dele egenskapsrommet inn i adskilte regioner som gir minst mulig overlapp mellom klassene. Liten overlapp leder til relativt sikker klassifisering (lav feilrate). Bruk av flere egenskaper gir vanligvis mer informasjon for klassifisering, og derved lavere feilrate. Tradisjonelt er egenskapene valgt på forhånd, og er ikke en del av selve treningsprosessen.



Figur 3.2 *Illustrasjon av prinsippet for veiledet læring. Et sett av objekter, representert ved utvalgte (håndlagde) egenskaper, og med kjent klassetilhørighet (treningssettet) tas som input til en av mange mulige treningsmetoder for å generere en klassifikator.*

Metodene for trening av klassifikatorer har i hovedsak utgangspunkt i sannsynlighetsregning, der treningssettet brukes til å estimere de statistiske fordelingene for hver av klassene. Klassifikatoren kan da konstrueres ut fra disse fordelingene, slik at sannsynligheten for å klassifisere feil blir så lav som mulig, ut fra den tilgjengelige informasjonen. Alternativt kan man bestemme seg for formen på klassifikatoren (lineær, kvadratisk eller av høyere orden), og bruke treningssettet til å finne optimale verdier for parametrene som inngår i klassifikatoren. Eksempler på slike metoder er de såkalte Perseptron- og relaksasjonsalgoritmene og Support Vector maskiner (SVM). I den sistnevnte metoden forutsettes i utgangspunktet at klassene er lineært separable (dvs. at de kan separeres av en lineær klassifikator), men metodikken kan generaliseres for å trene klassifikatorer av høyere orden. Forøvrig kan Perseptronmetodikken generaliseres. Dette leder til nevrale nett, som er en mye brukt klassifikatortype som trenes ved såkalt "back-propagation" (se figur 3.3). Trening av ulike typer klassifikatorer er beskrevet i bl.a. [7].

Et beslutningstre er en klassifikatortype som i sin enkleste form bruker de valgte egenskapene sekvensielt. Slike trær kan også trenes automatisk, og kan ofte gi en mer robust klassifikator (dvs. mindre utsatt for overtrening) enn andre metoder som bruker mange egenskaper samtidig. I



Figur 3.3 *Illustrasjon av et enkelt nevralt nett med ett skjult lag. Inputlaget tar imot egenskapene (i dette tilfellet tre egenskaper), mens outputlaget gir en tiltro til hver av klassene (i dette tilfellet to mulige klasser). Klassen med størst tiltro blir valgt. I hver node i det skjulte laget og i outputlaget beregnes det en tallverdi ut fra inputverdiene fra laget foran. Et nevralt nett kan ha mange skjulte lag.*

senere år har det vist seg at en "skog" av slike trær kan gi svært gode resultater, ved å kombinere klassifiseringsresultatet fra mange forskjellige beslutningstrær. Spesielt gjelder dette en såkalt "random forest". Her genereres et stort antall trær ved bl.a. å bruke et tilfeldig utvalg av egenskapene i en tilfeldig rekkefølge.

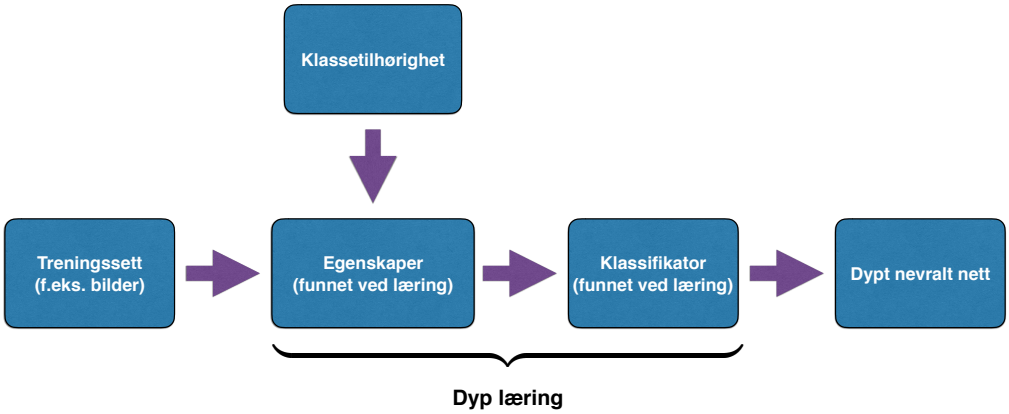
Av andre metoder innen mønstergjenkjenning kan nevnes såkalte *strukturelle metoder*, der det benyttes en symbolsk representasjon (f.eks. som "stort", "lite", "langstrakt", "rødt") av objektene eller deler av objektene. Objektene beskrives i slike metoder som en sammenstilling av delobjekter på flere nivåer (hierarkisk beskrivelse). Strukturelle metoder er nyttige dersom antall mulige klasser er stort og objektene kan brytes ned i enkeltkomponenter som er lette å gjenkjenne. Metoder er til en viss grad beslektet med kunnskapsbaserte systemer og ekspertsystemer.

Dype nett og dyp læring, som beskrives nærmere i neste avsnitt, er en videreføring av nevrale nett, og har de siste årene gitt svært gode resultater bl.a. innen bildeanalyse. Hovedforskjellen mellom tradisjonell maskinlæring og dyp læring er at i det siste tilfellet blir også valget av egenskaper for objektene en del av treningsprosessen. Dette er illustrert i 3.4. Et dypt nett for klassifisering av bilder består typisk av et antall "konvolusjonslag", med en tradisjonell klassifikator (typisk et nevralt nett) på toppen (se figur 3.5).

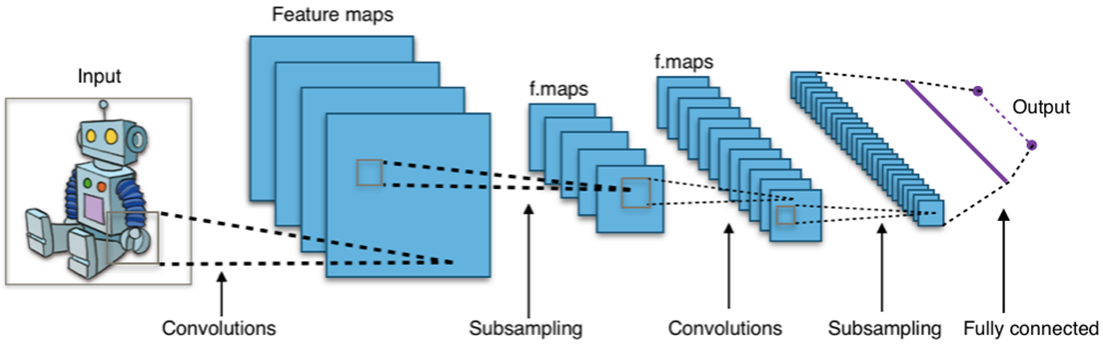
Konvolusjonslagene kan her betraktes som egenskapsuttrekkere, med den forskjellen at disse også blir trent ved å utnytte klassetilhørigheten til objekter i treningsbildene.

3.2 Dyp læring (deep learning)

I tiden etter 2010 har store nevrale nett blitt en mer og mer dominerende teknologisk base for maskinlæring. Milepæler i den siste tiden har for eksempel vært at nevrale nett nå brukes for å spille go (komplisert japansk brettspill) på toppnivå. Videre slår nå nevrale nett mennesker i en rekke komplekse bildegjenkjenningsoppgaver.



Figur 3.4 *Gangen i dyp læring. Her blir både egenskapsuttrekkeren og klassifikatoren funnet ved trening.*



Figur 3.5 *Illustrasjon av et dypt nevralt nett, med konvolusjonslagene til venstre og et ordinært nevralt nett til høyre (kilde:Aphex34).*

Den underliggende teknologien omtales gjerne som *deep learning* (dyp læring), der *dyp* refererer til antall såkalte *lag* i de nevrale nettene som benyttes. I praksis kan man si at dyp læring er det fagfeltet som arbeider med store og komplekse nevrale nett for å løse maksinlæringsoppgaver.

Fordelen ved bruk av dyp læring for slike anvendelser er den svært gode ytelsen som disse systemene ofte oppnår. Videre er analysen typisk rask slik at en høy analyserate kan opprettholdes. Den primære ulempen er at disse systemene må trenes med data, for at dette skal virke tilfredsstillende kreves det ofte svært store datamengder. Dette problemet forsterkes ved at dataene ofte må sorteres manuelt for å indikere for systemene for eksempel hva som er et funn og hva som ikke er det. Det er viktig å påpeke at dette er en rent praktisk utfordring knyttet til bruken av disse metodene, ikke en svakhet som påvirker ytelse.

3.3 Pattern of life

Det finnes ingen formell definisjon av konseptet POL. "Pattern of life" kan oversettes med livsmønster. Livsmønsteret til en person er en type informasjon som kan abstraheres fra personens daglige gjøremål og si noe om hva som er normalt for denne personen. En persons POL vil kunne bestå av hvor han pleier å oppholde seg, reiseruter, hva han ser på tv, hvem han kommuniserer med etc. Hvis man samler inn tilstrekkelig informasjon over tid, vil det kunne danne seg et mønster - et pattern of life - for denne personen. På dette grunnlaget kan det genereres prediksjoner om personens oppførsel i fremtiden.

Hvis man har POL fra tilstrekkelig mange personer, vil det være mulig å gjøre antagelser om en person ut ifra hva man vet om andre personer med tilsvarende POL. Det vil for eksempel være rimelig å anta at en person som parkerer bilen utenfor barnehagen i ti minutter på vei til og fra jobb hver dag har barn i barnehagealder, eller at en person som handler på Vinmonopolet hver uke også drikker alkohol innimellom.

Det kan genereres pattern of life for andre enheter enn personer. Et typisk eksempel er overvåkning av biltrafikk i et område. Et mønster kan da være at det er tett trafikk om morgenen i 8-tiden og om ettermiddagen i 16-tiden, mens det er mindre trafikk ellers på dagen og lite om natten.

Prediksjoner som genereres i forbindelse med POL-analyser kan ha flere anvendelser. Et anvendelsesområde er avviksdeteksjon. Når datasystemet har en forventning om fremtidig tilstand, kan det si ifra hvis forventningen ikke blir innfridd. Man har da en uvanlig situasjon, som det kan være verdt å undersøke nærmere. Prediksjonene fra POL kan også gi grunnlag for en mer optimal ressursallokering, fordi man har en forventning om hva som vil skje i fremtiden.

POL er i utgangspunktet et system som gir informasjon om hva som er normalt, genererer prediksjoner og melder fra om avvik. Så er det opp til mennesker å ta avgjørelsen om hvordan prediksjoner og avvik skal håndteres. Eventuell læring av dette, med informasjon om ønskelige og ikke-ønskelige tilstander eller endringer, kan mates tilbake inn i datasystemet, slik at maskinen selv kan ta avgjørelser. Da begynner vi å snakke om maskinlæring.

3.4 Veiledet og ikke-veiledet maskinlæring

Det finnes flere måter å lære opp en maskin på. Man kan skille mellom veiledet (supervised) og ikke-veiledet (unsupervised) maskinlæring. Veiledet maskinlæring krever at man trener opp maskinene med kjente data. Det vil si at for hver input, finnes det et riktig svar. For et røntgenbilde av en pakke vil dette bety at man må fortelle maskinen hvorvidt det var noe å finne i pakken eller ikke. Etter et stort antall slike læringspar (bilde og fasit), vil maskinen på egenhånd generere noen kriterier som den bruker til å plukke ut bilder som passer inn i mønsteret for funn.

ikke-veiledet maskinlæring går ut på å ganske enkelt mate maskinen med informasjon uten å si noe mer om riktige eller gale svar. Maskinen vil da kunne lære seg hva som er "normalt", for så å kunne gi beskjed dersom noe avviker fra normalen. Dette er mest relevant for å finne mønstre i en samling data over tid, for eksempel ANPR-data eller (etterretnings)data fra flere kilder.

3.5 Anvendelse for Tolletaten

Metoder fra dyp læring har en forbløffende envne til å detektere *hotspots* i bilder, områder som inneholder gitte typer objekter og strukturer. Dette kan brukes for å automatisere analyse av gjennomlysningsbilder fra ulike scannere brukt i fortolling.

Ved å analysere hendelsesforløp som serier av enkeltobservasjoner, kan nevrale nett brukes for å avsløre sekvenser av hendelser som har spesiell betydning. For eksempel kan man benytte denne typen metoder for å analysere sekvenser av bilnummer og lete etter rekkefølger av bilnumre som tyder på at en speiderbil kjører foran en bil som transporterer ulovlige varer.

3.5.1 Pattern of life

Pattern of life (POL)-analyser kan brukes både til avviksdeteksjon og ressursallokering.

Mulige anvendelsesområder for avviksdeteksjon kan være:

- Personer - etterretning: All tilgjengelig informasjon om en reisende person kan mates inn i en POL-analyse. Det kan dreie seg om personlig informasjon som kjønn, alder og bosted, og reiseinformasjon som f.eks. reisemål, medreisende og betalingsmidler. Ved å registrere denne type informasjon for alle reisende, vil man kunne finne noen mønstre som gjentar seg ofte, og andre som er mindre vanlige. Hvis maskinen finner en sammenheng mellom noen POL og ulovlig vareførsel, kan den gi beskjed om dette neste gang en person med denne typen POL er ute og reiser.
- Overvåkning av områder: Ved hjelp av overvåkningskameraer og andre sensorer, er det mulig å generere POL for et område. Et eksempel kan være bagasjehallen på en flyplass. Unormal flyt eller unormal oppførsel kan detekteres fordi datasystemet har en forventning om hva som er normalt.
- Datanettverk - Informasjons- og kommunikasjonsteknologi (IKT)-sikkerhet: Ved å logge normal datatrafikk, både i Tolletatens interne datasystemer og internett-trafikk, kan det genereres en POL, altså en beskrivelse av og forventning om normal aktivitet. Avvik fra normalen kan dermed detekteres. Dette kan tenkes å være et dataangrep, virus eller noe annet som må håndteres.

For Tolletaten kan det også være aktuelt å bruke POL-analyser i forbindelse med ressursallokering. Prediksjoner fra analysene kan si noe om hvor det vil være størst behov for personell. Et eksempel kan være fergetrafikken i Oslo. En kan tenke seg at selv om POL-analyser av passasjerlistene og tilhørende etterretningsinformasjon ikke har gitt noen utslag i forbindelse med innkommende ferger, så kan analyser av et bredere datamateriale si noe om hvorvidt den ene fergen har en høyere forventning om ulovlig vareførsel enn de andre. Hvis man må velge hvilken ferge man skal sette inn ressurser på, kan en slik analyse gi en pekepinn. Det kan også være mulig at et stort POL-system kan finne mønstre som tilsier økt bemanning enkelte steder i forbindelse med høytidsdager eller andre spesielle hendelser. På samme måte kan det avdekkes perioder med lavere forventning til ulovlig vareførsel eller trafikk i et område, slik at ressursene der kan brukes på noe annet.

3.5.2 Maskinlæring på to nivåer

Ethvert sensorsystem kan utvides med maskinlæring. Eksempler på dette kan være kamerasystemer som lærer å gjenkjenne ansikter, eller akustiske sensorsystemer som lærer å gjenkjenne lyden av en drone. Maskinlæring på ett sensorsystem kaller vi i det videre for *lavnivå maskinlæring*. I vår beskrivelse av *høynivå maskinlæring*, tar vi utgangspunkt i at all sensordata og etterretningsinformasjon kan sammenstilles og brukes til å generere ny kunnskap, idet maskinen finner mønstre og sammenhenger i kompliserte datasett (heterogene data). Figur 3.6 i avsnitt 3.5.4 om ANPR illustrerer maskinlæring (nevrale nett) på disse to nivåene. Det laveste nivået vises til venstre i figuren som et nevralt nett som gjenkjenner bilskilt. Det nevrale nettet til høyre i figuren illustrerer maskinlæring på et høyere nivå, hvor informasjon fra flere kilder er sammenstilt og anvendt i maskinlæringen.

Maskinlæring på én type sensordata, lavnivå maskinlæring: Den enkleste formen for maskinlæring på ett sensorsystem kan innføres i Tolletaten uten store endringer i infrastruktur. Her brukes røntgenbilder som eksempel, men maskinlæring kan anvendes på alle typer sensordata og etterretningsinformasjon. Maskinlæring kan anvendes på de røntgenbildene som i dag studeres av en toller. Den enkleste varianten av maskinlæring vil være at alle røntgenbildene lagres sammen med tollerens tolkning av bildet. Riktig svar i fasiten er da "dette objektet ville tolleren plukket ut for kontroll" eller "dette objektet ville ikke blitt plukket ut for kontroll". Det er også mulig å gi mer detaljert informasjon, som for eksempel at objektet ble plukket ut fordi det så ut til å inneholde tabletter. Når maskinen har fått trent seg opp på denne typen informasjon, vil den kunne gjøre de samme utvelgelsene som tollerne, og man vil få en mer stabil objekt-utvelger, samt at man vil kunne jobbe raskere (økt kvantitet). Det er verdt å merke seg at maskinen i denne situasjonen også vil lære å gjøre de samme feilene som tollerne gjør, og utvalgte objekter som senere viste seg å være negative vil fortsette å være lagret i systemet som positive, og disse objektene vil fortsatt bli valgt ut til kontroller. Dette kan løses ved å lære maskinen hvilke pakker det faktisk var ulovligheter i, i stedet for hvilke pakker som ble valgt ut for kontroll. Dette vil imidlertid kreve at alle objektene som skal brukes i treningssettet kontrolleres. Riktig svar i fasiten er da "her var det et funn" eller "her var det ikke et funn". Med et slikt treningssett, kan maskinen finne nye mønstre og sammenhenger, og på dette grunnlaget velge ut pakker til kontroll som tollerne selv ikke ville valgt ut, men som passer inn i et mønster som maskinen har funnet i forbindelse med beslag.

For å oppnå god veiledet maskinlæring, er det nødvendig med store datamengder, noe som kan være vanskelig å generere lokalt. Det kan være aktuelt å dele data mellom tolldistriktene slik at maskinlæring kan skje på et størt mulig datagrunnlag. Et eksempel er røntgenbilder av kjøretøy. Det finnes få bilder av en gitt modell, men ved å samle alle data fra alle distrikter og utføre maskinlæring på hele datasettet, utnyttes informasjonen på en god måte. Det kan også være aktuelt å dele sensordata med med andre land.

Maskinlæring på heterogene data, høynivå maskinlæring: Når en toller velger ut en pakke for kontroll, kan det være mer enn bare selve røntgenbildet som trigger mistenksomheten. Tolleren har kunnskaper og erfaringer som veileder ham eller henne i utvelgelsesprosessen. Dette kan vi overføre til maskinlæring. Det er da snakk om å sammenstille informasjon fra forskjellige kilder. Data fra alle sensorer og etterretning kan logges og mates inn i en maskin, sammen med forskjellige fasiter

som tollerne legger inn (beslag/ikke beslag). Når det gjøres et beslag, vil maskinen da kunne bruke all tilgjengelig informasjon for å danne et mønster i forbindelse med beslaget. Senere vil den da kunne si ifra når tilsvarende mønster dukker opp.

Maskinlæringen kan finne mønster i store mengder av informasjon. F.eks. hvem som reiste den samme strekningen i dagene før og etter at en person ble tatt for smugling. Den kan også finne helt andre mønstre som vi mennesker ikke tenker på, og ikke har kapasitet til å bearbeide. Når en smugler avsløres, kan informasjon om dette mates inn i maskinen slik at den kan gjenkjenne tilsvarende mønster en annen gang. For å unngå falske positiver når maskinen skal utføre utvelgelsen, er det viktig at negative funn også lagres. Det er for eksempel ikke ønskelig at alle personer med koffert velges ut for kontroll fordi en person med koffert hadde med seg noe ulovlig over grensen.

Et eksempel på sammenstilling av informasjon fra forskjellige kilder kan være ANPR og informasjon om brev og pakker. Hvis det finnes et mønster i hvordan en smugler kjører og hva slags post han sender og mottar, kan en maskin finne dette mønsteret. Det forutsettes da at all post avbildes (og eventuelt også måles og veies), og at det finnes en form for automatisk gjenkjenning av adressat, logging av avsenderland etc. Jo mer informasjon man har om pakken, jo mer detaljert kan mønsteret lages.

Eksempel: Person A og B har blitt stoppet på grensen og tatt for narkotikasmugling, på to forskjellige tidspunkt. Det er ingen sammenheng mellom disse beslagene, annet et at det er samme type narkotika. Beslagene registreres i et datasystem. I det samme systemet finnes det røntgenbilder og fargebilder av all post som har kommet til landet de siste to månedene, med tilhørende maskingenerert metainformasjon (størrelse, vekt, adressat, avsender ...). Ingen av pakkene til person A og B har blitt plukket ut for kontroll. Datasystemet vet nå at personene A og B er en smuglere. Systemet ser nå at begge disse har mottatt pakker som ser like ut på røntgen og som kommer fra samme land. Det er få andre som har mottatt slike pakker. Bilene til A og B er også registrert av ANPR-kamera i et område hvor ingen av dem bor eller jobber. Det finnes én person til som har mottatt en lignende pakke og hvis bil har vært observert i det samme området. Denne bilen er nå på vei mot grenseovergangen på Svinesund. Alarmen går.

3.5.3 Maskinlæring og røntgen

Tolletaten benytter i dag ulike typer for røntgen gjennomlysningsutstyr for en rekke anvendelser. Pakker i postmottak kan scannes, det samme kan hele kjøretøy ute ved tollstasjonene. Etter at scanningen er gjennomført må bildene analyseres. Dette kan gjøres manuelt, men potensialet for bruk av mønstergjenkjenningsalgoritmer er stort.

Utgangspunktet for bruk av mønstergjenkjenning på denne typen data er eksisterende databaser over røntgenbilder som viser både funn og mangel på funn. Ved å trene opp en mønstergjenkjenningsalgoritme (typisk vil metoder fra dyp læring brukes her) på disse dataene vil systemene, etter trening på et tilstrekkelig stort antall bilder, kunne detektere bilder som inneholder potensielle funn.

Dette kan gi en rekke fordeler for Tolletaten:

- **Økt kvantitet i analyser av objekter:** Det er slitsomt og krevende å inspisere bilder manuelt. Ved å bruke et automatisk system for å finne interessante kandidater kan mengden bilder som analyseres økes kraftig.

- **Nye kriterier for treff:** Maskinen kan læres opp på et sett av bilder hvor innholdet i de avbildede objektene er kontrollert og dokumentert. I de tilfellene hvor det var ulovlig innhold i en pakke som tollerne normalt ikke ville valgt ut til kontroll, vil maskinen da kunne finne nye mønstre og sammenhenger mellom bilde og treff. Maskinens utvalg vil da bli kvalitativt forskjellig fra det en toller ville valgt ut for kontroll, basert på egen erfarig (maskinlæring).
- **Håndtere komplekse geometrier og store datamengder:** Computertomografi (CT)-bilder (som blir mer og er vanlige for tollanvendelser) er tredimensjonale, og dermed vanskelige for mennesker å prosessere. Maskiner kan lese informasjon i flere dimensjoner. De kan også håndtere større datamengder enn mennesker, slik at de kan se bilder i sammenheng og finne mønstre som ikke er enkle for et menneske å oppdage. En godt trent maskin vil også kunne gjenkjenne et objekt i bildet selv om kontrasten er så svak at et menneske ikke ser det.

Et første forslag til en mulig anvendelse av dette er å trene et nevralt nett for å finne postpakker som inneholder piller (eller pillelignenede objekter). Dette er en viktig type pakke å undersøke rent tollmessig, samtidig som at problemet er tilstrekkelig begrenset til at det ikke er altfor krevende å komme i gang.

3.5.4 Maskinlæring og ANPR

Metoder for ANPR basert på nevrale nett (ofte referert til som *deep learning*) gir svært god ytelse. Dette åpner for en rekke interessante anvendelser av ANPR for Tolletaten.

Ytelsesmessig vil et moderne ANPR system av god kvalitet, og som er tilpasset norske forhold, kunne tilby en ytelse i god overkant av 90% riktig leste skilt i årsgjennomsnitt. Her er det betydelige årsvariasjoner med vintersesongen som den desidert vanskeligste på grunn av at snø og smuss akkumuleres på bilskitene. En slik gjenkjennelsesrate åpner for en rekke interessante anvendelser.

Den mest innlysende anvendelsen er naturligvis det å lese skilt og å sammenholde leste skilt med registere over biler man av en eller annen grunn ønsker å stoppe. Dette kan naturligvis også brukes for å hviteliste biler slik at biler som nettopp har vært kontrollert uten funn **ikke** stoppes for umiddelbare nye kontroller. Med slike strategier kan Tolletatens ressurser bedre fokuseres mot kjøretøy som har en reell interesse.

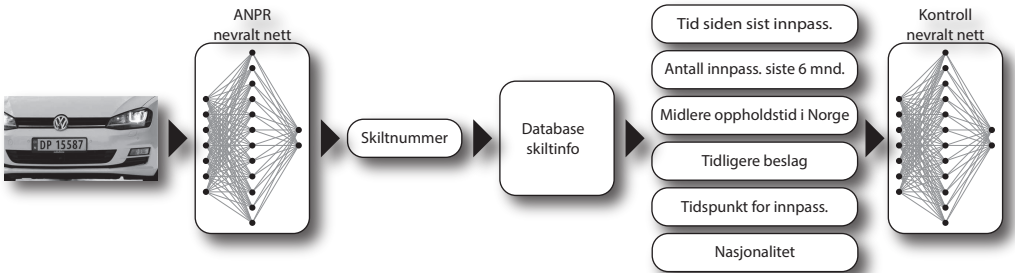
Tolletaten har per nå rett til å lagre et kjøretøys skiltinformasjon i inntil 6 måneder sammen med sted og tidspunkt for passeringen. Med dette som utgangspunkt kan man se for seg andre og mer sofistikerte anvendelser av ANPR. I de følgende avsnittene vil vi peke på noen slike muligheter. Denne typen anvendelser er nært koblet opp mot den typen anvendelser som ofte omtales som *pattern of life*, se seksjon 3.3.

En første mulig anvendelse er å lete etter bestemte mønstre i en lang serie av passeringer. Gitt at en bil stanses og det gjøres et funn kan det være interessant å lete etter biler som har passert samme grenseovergang i en gitt periode før beslaget ble gjort, dette kan brukes for å identifisere speiderbiler. Dersom samme bil har kjørt før bilen der beslaget ble gjort også ved andre tidligere passeringer er dette en god indikasjon på at det ene kjøretøyet speider for det andre.

Andre muligheter ligger i å lete etter biler som passerer ulike grenseoverganger i et mønster. Dette kan være en indikator på at fører av disse kjøretøyene ønsker å ungå å bli lagt merke til med hyppige passeringer på en bestemt grensestasjon.

Ved å sammenholde skiltinformasjon både ved inn og utkjørsel av et kjøretøy vil det være mulig å beregne hvor lenge en gitt bil har vært i Norge, det vil også, dersom oppholdstiden ikke er for lang, være mulig å indikere hvilke områder av Norge kjøretøyet kan ha besøkt. Dette kan brukes til å verifisere en førers historie for eksempel. Skulle Tolletaten få lov til å sammenholde sine ANPR registre med tilsvarende registre fra Autopass og andre bompenge og fergesystemer øker antallet muligheter for sporing enormt.

Et system som implementerer en slik løsning er illustrert i figur 3.6. Her benyttes først en ANPR løsning basert på nevrale nett for å lese skiltet på passerende biler. Det leste registreringsnummeret mates så inn i en database og en rekke relevante informasjonsbiter for det relevante kjøretøyet hentes ut. Denne informasjonen mates så inn i et nytt nevralt nett som er trent til å plukke ut kjøretøy for kontroll basert på den informasjonen som er hentet ut fra databasen.



Figur 3.6 *Anvendelse av et sammensatt system for maskinlæring for utvelgelse av kjøretøy til kontroll. Et bilde av et passerende kjøretøy mates inn i en modul for maskinlæring basert på nevrale nett. Denne leser skiltet og teksten fra skiltet brukes til å hente en betydelig mengde relevant passeringsinformasjon for dette kjøretøyet fra en database. I neste omgang benyttes et nytt maskinlæringssystem (dette også basert på nevrale nett) for evt. å velge bilen ut for kontroll.*

3.5.5 Gjenkjenning av varer vha. bildeanalyse

Bruk av automatisk bildesøk i tollsammenheng, er en teknologisk mulighet som kan bli praktisk anvendelig på lengre sikt (5-10 års perspektiv). La oss si at en toller blir konfrontert med en helt ukjent gjenstand (f.eks. innholdet i en pakke som er åpnet for inspeksjon). Hvordan skal man kunne finne ut om gjenstanden stemmer overens med tolldeklarasjonen, og eventuelt finne riktig tariffnummer dersom deklarasjonen er mangelfull? Tolleren tar et bilde av gjenstanden, systemet foretar et søk i en stor bildedatabase og returnerer forslag til hva gjenstanden kan være.

Man kan tenke seg at Tolletaten bygger opp en slik database over tid, eventuelt i samarbeid med andre lands tollvesen. Det finnes allerede i dag systemer for søk etter bilder med lignende innhold (Google mm.). En anvendelse her er for rettighetshavere av et gitt bilde å kunne finne om andre bruker bildet på sine nettsteder uten tillatelse. Man kunne tenke seg tilsvarende systemer som leter etter lignende gjenstander i bildet. Her dreier det seg om bildesøk ut fra informasjonen i selve bildet, ikke søk basert på tekst (stikkord) knyttet til bildet. Et slikt system kan bidra til effektivisering av vareflyt ved automatisk å finne tolltariffnummeret.

Realismen i dette, som et praktisk hjelpemiddel for Tolletaten, må undersøkes videre.

4 Automatisering og robotisering

Teknologi og anvendelsesområde	Mod.	Gj.f.
Automatisk dokumentasjon		
Automatisk forkontroll (med ulike sensorer)		
Anvende roboter for (ut)pakking og håndtering		
Merking med RFID		
Sporing av kjøretøy vha. droner		

Tabell 4.1 *Tabellen viser ulike anvendelser innen automatisering og robotisering som er omtalt i dette kapitlet. Teknologisk modenhetsnivå (Mod.) og gjennomførbarhet (Gj.f.) for Tolletaten er antydet med fargekode: grønn = høy, gul = medium, og rød = liten*

Automatisering og maskinell behandling har revolusjonert vareproduksjonen i de fleste industrier og ført til høyere produksjonsvolum, bedre kvalitet og lavere pris. Det forskes på stadig nye anvendelsesområder for roboter, også utenfor tradisjonell industriproduksjon, og spesielt der anvendelsene kan gi økt volum, bedre kvalitet og lavere kostnader kan det forventes store endringer.

Prosessene som Tolletaten utfører er i begrenset grad integrert eller innarbeidet i hele vareførselsprosessen. De ulike aktørene, som bestiller, leverandør og speditør, søker å optimalisere sine prosesser. Hvis samfunnets målsetting om å hindre innførsel av ulovlige varer var overordnet og premissgiver for hvordan hele vareførselsprosessen skulle designes ville det kunne stilles krav om tidligere og bedre kvalitet på informasjonen fra aktørene. Dette ville igjen kunne gi mer treffsikre fysiske kontroller.

I siste instans er det den fysiske kontrollen og beslaget som hindrer ulovlig innførsel. Selv med 100% treffsikkerhet vil de hovedsakelig manuelle kontrollressursene ikke kunne demme opp for mer enn en brøkdel av de varene som innføres ulovlig. En vesentlig økning i antall kontroller som gjennomføres kan vanskelig tenkes realisert uten automatisering av prosessene, herunder bruk av avanserte roboter.

4.1 Anvendelser innen post- og varemottak

Varer leveres i stor og økende grad som postpakker. Sortering av post gjøres i store anlegg med maskinell støtte. Tolletaten har adgang til å be om kontroll av postforsendelser f.eks. fra spesielle land. Utplukk for kontroll og selve den fysiske kontrollen er manuelle prosesser. Samlebåndet hvor posten transporteres gir også mulighet for hund å søke basert på lukt. Typisk vil pakker som plukkes ut for kontroll bli skannet med røntgen for å gi operatøren mulighet for å se etter tegn på ulovlige varer inne i pakken. Mistenkelige pakker åpnes manuelt. Innholdet undersøkes vha. syn, lukt og eventuelle tilgjengelige instrumenter. Hvis det ikke konstateres ulovlige funn, pakkes innholdet tilbake igjen.

Positive funn av ulovlige varer krever flere manuelle prosesser som dokumentasjon, midlertidig oppbevaring, oversendelse til politi og eventuelt destruksjon. Negative funn forsvarer ikke tilsvarende prosess og blir ikke dokumentert.

Det er tenkelig med flere forenklinger og effektiviseringer av denne kontrollprossessen ved bruk av automatisering og avanserte roboter.

Automatisk dokumentasjon
De pakkene som plukkes ut for kontroll kan dokumenteres ved automatisk oppretting av et digitalt saksdokument hvor all tilgjengelig informasjon om pakken lagres, det som på forhånd er kjent som avsender, adressat, og transportrute, og ulike fysiske egenskaper ved pakken som kan hentes fra ulike sensorer i mottaksprosessen f.eks. vekt, form og farge. Dette vil da ligge klart for kontrolløren slik at tilleggsinformasjon som røntgenbilde, foto av enkeltdeler i pakken, og data fra kontrollinstrumenter bare knyttes til saken. De ulike stegene i kontrollprosessen bør være så enkle som mulig og ha et fast oppsett, dvs. kreve minimalt med justering fra pakke til pakke. Positive funn vil være godt dokumentert og kreve minimale manuelle tillegg. Negative funn vil nærmest være selvdokumenterende.

Automatisk forkontroll
All tilgjengelig informasjon, herunder sensordata om pakken, bør brukes til suksessivt å sortere bort de pakkene som med mindre sannsynlighet har ulovlig innhold. Informasjonsteknologi (IT)-systemene bør ha tilgang til analyserte data fra tidligere funn (f.eks. vha. maskinlæring) og automatisk gjøre slik utsortering. De pakkene som når kontrolløren bør i størst mulig grad inneholde ulovlige varer eller skille seg ut på en annen måte slik at de fortjener nærmere dokumentasjon.

Robot for utpakking (av farlige pakker)
Innhold i postpakker kan være farlig for mennesker, f.eks. svært små mengder fentanyler. Avanserte roboter vil i fremtiden kunne ha tilsvarende fingernemhet og finmotorikk som mennesker. Slike roboter vil kunne åpne pakker, plukke ut mistenkelig gjenstander, foreta kjemiske analyser og sikre det farlige innholdet i en tett beholder.

Miniatyrroboter for undersøkelse og prøvetaking
Undersøkelse av kjøretøy eller pakninger hvor det er skjult ulovlige varer blant andre lovlige varer er tidkrevende. Et alternativ til å åpne eller plukke fra hverandre en større pakke kan være å finne og ta prøve av et mistenkelig materiale vha. svært små roboter som enten styres av en operatør eller autonomt søker gjennom et volum.

4.2 Anvendelser ved innførsel av konteinere

Konteinertransporten går for en stor del på kjøl. I havner hvor konteinere føres inn og lastes om til annet transportmiddel vil hele håndteringsprosessen understøttes maskinelt. I likhet med det som ovenfor er nevnt om post- og varemottak bør den prosessen inkludere en rekke trinn som bidrar til å sortere ut enheter som fortjener oppmerksomhet og manuell behandling av tollere.

Automatisk forkontroll
All tilgjengelig informasjon, hele transportruten, (konteiner)manifest, deklarasjon, sensordata som

kamerabilder og røntgenskanning av konteineren osv. bør brukes til suksessivt å sortere bort konteinere som har lav sannsynlighet for ulovlig innhold. Kun konteinere som enten har høy sannsynlighet for innhold av ulovlige varer eller som er plukket ut etter systematisk randomisert utvalg blir gjenstand for kontroll.

Automatisk dokumentasjon
De konteinerne som plukkes ut for kontroll kan dokumenteres ved automatisk oppretting av sak hvor all tilgjengelig informasjon om konteineren lagres. Dette ligger klart for kontrolløren slik at tilleggsinformasjon som røntgenbilde eller foto av enkeltpakker i konteineren, og data fra andre kontrollinstrumenter kan knyttes til saken.

Robot for (ut)pakking av konteinere
Innholdet i transportkonteinere er pakket av spesialister slik at volumet utnyttes best mulig. Kontroll av konteinere krever i dag manuell utpakking av flere personer og er både tidkrevende og tungt. I tillegg er det vanskelig å få alt tilbake på plass i samme volum etter gjennomført kontroll. Avanserte roboter vil i fremtiden kunne åpne konteinere, løfte ut enkeltpakker, fotografere, lese pakkeinformasjon, skanne vha. røntgen, holde orden på plassering i den opprinnelige pakkegeometrien og tilslutt kunne plassere alt tilbake der det sto i utgangspunktet.

Miniatyrroboter for undersøkelse og prøvetaking
Små roboter kan søke, enten styrt eller autonomt, etter mistenkelig materiale som ligger vanskelig til.

4.3 Overvåking av varestrømmer

Kontroll med både varestrømmer og om selve forsendelsen er manipulert eller åpnet underveis er del i det som med en fellesbetegnelse går under uttrykket “Total Asset Visibility”. Dette inkluderer hele kjeden fra varelager, transport og leveranse til mottaker. Det kreves internasjonale avtaler og krav for å få dette implementert i transportbransjen.

4.3.1 Merking med RFID

Det har vært gjort flere forsøk på merking av varer, fra konteinere og ned til enhetsnivå ved hjelp av Radio Frequenecy IDentification (RFID). Det finnes både aktive og passive RFID brikker som dekker flere frekvensbånd. Både LF (30-300 kHz), HF (3-30 MHz), UHF (0,3-3 GHz) og mikrobølge (2-30 GHz) benyttes. De laveste frekvensene egner seg for korte avstander (<0,5m) og kan leses av gjennom de fleste materialer. Typisk benyttes disse på enhetsnivå. De høyeste frekvensene kan benyttes over lange avstander, men her har emballasjen mye å si for lesbarheten. Disse benyttes på konteinernivå. RFID er i utstrakt bruk verden rundt, men det benyttes ulike frekvensbånd i UHF-området. Myndighetene har tilrettelagt for frivillig bruk av RFID uten at dette er utformet som et pålegg. Det er opp til distributører og leverandører å bestemme om teknologien skal tas i bruk. Flere og flere benytter seg imidlertid av RFID pga. ønsket om sporbarhet. Dette gjelder også i Norge der blant andre Posten og Nortura benytter RFID. I tillegg benyttes det ifm. merking av dyr. Teknologien er med andre ord moden, men det gjenstår å få på plass forpliktende

internasjonale avtaler (og ikke frivillighet) før systemene kan benyttes optimalt. Det finnes systemer som kan kjøpes i dag og benyttes effektivt for i hvert fall deler av varetransporten, men bruk av ulike frekvensområder krever flere installasjoner og internasjonale avtaler.

Figur 4.1 *RFID leser benyttet av Nortura.*

4.3.2 Forsegling

Sendinger som skal nå rette mottaker uten å bli åpnet av uvedkommende har tradisjonelt blitt forseglet, dvs. at pakkens åpning er dekket med et materiale som har et stempel (identitetsmerke) som kun avsender er i besittelse av. Brudd på forseglingen indikerer at pakken har blitt åpnet. For at informasjonen om en vare som transporteres fra avsender til mottaker skal være overens med det som avsender har deklarert, er det nødvendig at pakken ikke åpnes og innholdet endres. Myndighetene kan i prinsippet kreve at alle pakker blir forseglet. Brudd på forseglingen vil dermed være en indikator på en mistenkelig pakke som bør undersøkes. En måte å realisere pakkeforsegling på er å gi ansvaret til transportøren, f.eks. Posten eller speditører som er godkjent av myndighetene, eller å kreve bruk av standardiserte og ferdig merkede pakker som automatisk blir forseglet når de pakkes sammen av avsender eller ved mottak hos transportør. Forseglingen vil i tillegg kunne inneholde et merke som lar seg spore i et informasjonssystem. Typisk vil pakker skannes ved passering av et transportknutepunkt. Et slikt helhetlig system for forsegling og merking vil gi et omfattende datagrunnlag for å se på normalsituasjonen av varestrømmene og eventuelt oppdage avvik.

4.3.3 Tilstandsovervåkning (av enkeltpakker)

I tillegg til å bli klar over at en forsendelse ikke er iht. til oppgitt deklarasjon, f.eks. fordi den er endret under transport, er det ønskelig å vite mer om hva som har skjedd med pakken. Dette

kan gjøres ved å utstyre hver pakke med sensorer som detekterer endringer i tilstanden til pakken eller egenskaper i omgivelsene. Hvis slike enkle sensorer kan lages små og meget billige er det tenkelig at de kan være en del av kostnaden til å sende en pakke, en avansert form for frimerke. I prinsippet kan slike "frimerkesensorer" gjenbrukes. For myndighetene vil en slik overvåkning av pakketransportene peke på både hvor og når uønskede endringer skjer og kunne gi grunnlag for automatisk utvelgelse for objektkontroll og etterfølgende etterforskning og reaksjon.

4.3.4 Droner til sporing av kjøretøy

En transportør av ulovlige varer vil prøve å unngå å bli stoppet og kontrollert f.eks. ved å passere over en ubetjent grensestasjon. Selv om det oppdages en mistenkelig transport vha. ANPR, vil kontrollressursene i perioder være begrenset slik at det vil være vanskelig for tollbetjenter fra nærliggende områder å innhente og stanse et slikt kjøretøy.

Et alternativ kan være å spore kjøretøyet vha. flygende droner. Autonomien som kan bygges inn i selve farkostene vil gjøre at det er tilstrekkelig å angi mål og overordnede parametre for kontroll dronen. Langs veiakser vil det normalt være mobilnett som kan overføre styringsinformasjon til og sensordatastrøm fra dronen. Hvis dronene er tilstrekkelig små, kan det være mulig å feste dem til kjøretøyet midlertidig under transporten. Kontroll av kjøretøyet kan utføres ved bestemmelsestedet av andre tollbetjenter.

Droneteknologien begynner å bli moden og kommersielt tilgjengelig. Den skisserte anvendelsen avhenger av lovverk som regulerer slike farkoster og ressursene som bestiller har. Organisasjonsmessig vil dette kreve spesialkompetanse og utnyttelse av Tolletatens ressurser over større områder og på tvers av regionene.

4.3.5 Selvkjørende tollpatrulje

Selvkjørende biler kan, i likhet med flygende droner, følge etter mistenkelige kjøretøy. De kan også gi signal med lyd og lys til kjøretøyet om å stanse for kontroll. Tollbetjent kan tilkalles til stedet hvor kjøretøy har stanset. En fullstendig ubetjent kontroll vha. roboter er langt fram, men den ubetjente tollbilen kan være utstyrt med sensorer for å skanne varer og være en kommunikasjonskanal mellom kunde og tollbetjent på operasjonssentral.

5 Relevante IKT-trender

Teknologi og anvendelsesområde	Mod.	Gj.f.
TOR: illegal vareflyt (trussel)		N/A
I2P,Freenet: illegal vareflyt (trussel)		N/A
OTR, OSTN, ZRTP: anonym telefoni for kriminelle aktører (trussel)		N/A
Blockhain: automatisering av vareflytkontroll	Skalering	Standardisering
IoT: automatisering av vareflytkontroll		Standardisering
Semantic Web: analyse av lenkede data (fra ulike kilder på internett)	Få løsninger	
Stordata (Big Data): etteretning og prediktiv analyse	Kommersiell	
Skytjenester (Cloud Computing): sentralisert/distribuert lagring og beregning		Datasikkerhet
Web Processing Services: redusert lagrings- og beregningskrav til brukerklienter (grensesnitt for distribuerte tjenester)	Etablert standard	Tjenester må lages

Tabell 5.1 *Tabellen viser ulike IKT-relatert teknologi og anvendelse som er omtalt i dette kapitlet. Teknologisk modenhetsnivå (Mod.) og gjennomførbarhet (Gj.f.) for Tolletaten er antydet med fargkode: grønn = høy, gul = medium, og rød = liten.*

På et teknologiområde som utvikler seg så raskt som IKT, vil en trend kunne være en flyktig ting. Det vil derfor være ganske vanskelig å anslå hvorvidt en bestemt teknologi kommer til å være en langsiktig driver for utviklingen fremover.

For å identifisere hovedtendenser som kan være interessante for Tolletaten, har vi derfor valgt å heve blikket noe, og gruppere fremvoksende IKT-teknologier i to hovedgrupper basert på hvilke muligheter og utfordringer de representerer for toll. Dette er:

1. *Nye nettverksprotokoller/Dark Web*: En sterk trend er utviklingen av nye nettverksprotokoller på villedende rutingalgoritmer og krypteringsteknikker. Disse teknologien er designet for å gi anonymitet og å hindre sporbarhet online, og kalles derfor ofte *The Dark Web*. Flere og flere mennesker benytter Dark Web-tjenester i en eller annen form. Det er derfor å forvente at det stadig vil bli mer krevende for Tolletaten å drive kriminalitetsbekjempelse og å avsløre ulovlig vareflyt.
2. *Lagringsløsninger, analyseverktøy og infrastrukturkonsepter*: selv om tradisjonelle teknikker for Internettprotokoll (IP)-sporing og digital etterforskning har blitt noe svakere, så har analyseverktøyene blitt desto sterkere, og mengden informasjon vi er i stand til behandle langt større og mer variert. Moderne lagringsløsninger har beveget seg et godt stykke fra den tradisjonelle sentrale relasjonsdatabasen. Både databaser og analyseverktøy har akseptert *distribuert prosessering* som et grunnpremiss: et moderne datavarehus er som regel spredt over et stort antall maskiner som kan vokse ved behov, og nye analyseverktøy er i stand til å sammenstille og analysere informasjon på tvers av dokumenter, nettssteder og online-samfunn.

En teknologi som ikke passer naturlig inn i disse kategoriene, men som har potensielt interessante anvendelser for Tolletaten, er *blockhain* som vi diskuterer i et separat avsnitt.

5.1 Nye nettverksprotokoller/Dark Web

I de siste årene har det dukket opp en del nye nettverksprotokoller som er designet for anonym og kryptert kommunikasjon. Noen av disse er ment for trafikk på det ordinære internettet, mens andre etablerer alternative nettverker som, selv om de er en del av det fysiske internett, ikke er tilgjengelig gjennom en vanlig webbrowser. I en tid der personvernet er presset er dette teknologier med viktige og legitime anvendelser. Allikevel er det desverre belegg for å hevede at mer og mer kriminell aktivitet flyttes over på disse nettverkene [8].

Dersom Tolletaten ønsker å opprettholde kompetanse til å etterforske og overvåke f.eks. illegal vareflyt på nett, kan det derfor være viktig å følge med på disse teknologiene. Vi gir et overblikk over noen av de viktigste i dette avsnittet.

5.1.1 Mørknettet

Den andelen av nettrafikken som foregår anonymt og kryptert utgjør en slags nettverker i nettverket som er ugjennomsiktig for konvensjonell IP-basert overvåkingsteknologi. De kalles derfor gjerne *mørknettet* (*Dark Web*) med en sekkebetegnelse.

Internett, slik vi vanligvis bruker dette begrepet i dagligtale, er et datanettverk der maskiner kommuniserer med hverandre via IP-adresser. En IP-adresse er et tall som kan sammenliknes med et telefonnummer: alle enheter—telefoner, nettbrett, kjørecomputere e.a.—må ha en IP-adresse for å kunne kommunisere med andre enheter på internett.

IP-kommunikasjon er i utgangspunktet åpen, slik at det er mulig å overvåke internettrafikken. Selv ved kryptert overføring av data, er det mulig å se hvem som har sendt og mottatt dataene samt størrelsen på datapakkene. *Mørknettet* (*The Dark Web*) består av utvidelser av internettprotokollen som er spesifikt designet for å maskere IP-adresser og kryptere informasjon.

Mye av programvaren for anonymitet på internett formidles gjennom paraplyorganisasjonen “The Guardian Project”. Dette er en organisasjon som beskriver seg selv som et globalt kollektiv av programvareutviklere, designere og aktivister, forenet gjennom en målsetning om å utvikle open source mobilapplikasjoner for privatpersoner som ønsker å kommunisere fritt uten å bli overvåket. The Guardian Project tilbyr pr. i dag mobilapplikasjoner for privat og anonymisert chat, anonymisert IP-telefoni, kameraapplikasjoner som fjerner GPS-informasjon og annet. Noen av disse skisseres kort her:

- The Invisible Internet Project (I2P) er bygget på en videreutvikling av *onion*-protokollen (jf. avsnitt 5.1.2) kalt *garlic*. Garlic-protokollen krypterer datapakker og IP-adresser for å hindre IP-sporing og analyse av datatrafikk. Garlic er en overlagsteknologi; den er designet for trafikk til og fra vanlige, allerede tilgjengelige nettsteder og -tjenester. Den kan brukes til anonym Web-surfing, chatting, blogging og filoverføring.
- Freenet, i motsetning til I2P, er et *alternativt* nettverk, hvilket vil si at det ikke ruter trafikk til og fra ordinære maskiner og nettsteder: selv om Freenet tilbyr et vanlig webgrensesnitt og kan navigeres med en Freenet-browser på en ordinær laptop, så er stedene man kan besøke begrenset til de som med hensikt er opprettet innenfor Freenett infrastrukturen. Slik sett likner Freenet på et nettverk av skjulte Tor servere (jf. avsnitt 5.1.2).

- Off-the-Record Messaging (OTR) er en kryptografisk protokoll ment for direktekommunikasjon i sanntid. OTR er designet for å gi *deniable authentication*. Dette betyr at partene i en direkte samtale er i stand til å forsikre seg om hverandres respektive identitet uten at de i ettertid vil kunne knyttes til samtalen av en utenforstående tredjepart.
- Open Secure Telephony Network (OSTN) er en standard for å kryptere og anonymisere IP-telefoni.
- Zimmermann Real-Time Transport Protocol (ZRTP) er en kryptografisk nøkkeldelingsprotokoll for kryptering av Voice over IP. Som OSTN er denne protokollen designet for sikre og anonyme telefonsamtaler på mobile enheter over internett.

5.1.2 Tor-nettverket

De fleste nettsteder på mørknettet bruker programvare bygget over The onion router (TOR)-protokollen. Dette er en protokoll som krypterer IP adressene til både avsender og mottaker i hver nettverkstransaksjon. Data blir sendt gjennom en vilkårlig valgt og med hensikt villedende rute i et peer-to-peer nettverk, altså et nettverk som eksisterer på servere som er stilt til disposisjon av frivillige bidragsytere.

Som så mange internetteknologier ble Tor utviklet ved det amerikanske instituttet for forsvarsforskning Defense Advanced Research Projects Agency (DARPA) i 1990 årene. Formålet med Tor-porosjektet var å beskytte militær kommunikasjon. I dag er Tor en frittstående non-profit organisasjon som etter eget sigende arbeider for å fremme personvern og anonymitet online.

5.1.2.1 Modenhet

Tor-nettverket er som nevnt et peer-to-peer nettverk. Pr. i dag består nettverket av ca. 5000 dedikerte servere, noe som ikke er mye. Tallet er langt lavere enn antallet Tor-klienter. Dette misforholdet er såpass stort at det går merkbart ut over overføringshastigheten. Tor-nettverket oppleves derfor per i dag ikke som like responsiv som det ordinære nettet.

Tor-nettverket er allikevel stort nok til å støtte små- til mellomskala foretak og kan også tilby anonymitet til *servere*, ikke bare til brukere eller klienter. Servere som er konfigurert til å svare på forespørsel kun fra Tor-nettverket kalles gjerne *skjulte* servere og kontaktes vanligvis gjennom spesialdesignede Tor-browsere.

5.1.3 Dark Web og kriminalitetsbekjempelse

Mørknettet har både blitt applaudert som et fyrtån for demokratiske idealer slik som ytringsfrihet og personvern, og kritisert som et redskap som først og fremst tjener interessene til kriminelle. Selv om disse ikke nødvendigvis er motstridende, bekrefter den første seriøse studien av mørknettet [8] at det siste er mer dekkende. Ifølge denne studien var 57 prosent av alle nettstedene designet for Tor—kjent som .onion-steder—opprettet i kriminell hensikt, typisk for narkotikahandel, ekstrempornografi eller ulovlig pengeoverføring. Det finnes så langt nærmest ikke noe nærvær av islamsk ekstremisme.

Hva gjelder bekjempelse, så er det klart at anonyme og alternative nettverk samt anonym og kyptert telefoni og chat, gjør tradisjonelle IP-baserte metoder for digital etterforskning langt på vei foreldede.

Andre metoder er under utprøving. F. eks. har DARPA utvikler en søkemotor kalt *Memex* som et støttesystem for å avdekke og bekjempe menneskehandel og annen illegal adferd på mørknettet (se [9]). Memex er i bunn og grunn en indekseringsteknologi sammenliknbar med Google, men spesielt innrettet på mørknettet og med forsterket funksjonalitet for analyse av innhold. Memex traverser millioner av nettsider på mørknettet, og forsøker å analysere innholdet underveis. Den kan ikke avmaskere IP-adresser, men forsøker i stedet å identifisere personer på bakgrunn av mønstre og relasjoner som er implisitt i innhold på mørknettet (dette er ikke ulikt stordataanalyse (jamfør avsnitt 5.3.3)).

I tillegg til dette har FBI med hell anvendt en metode de kaller Network Investigative Technique (NIT) (se [9]) for å avmaskere IP-adresser til konsumenter av barnepornografi. Metoden ble prøvd ut i 2012 i en etterforskning kalt "Operation Torpedo" som startet i det Nederlandske politiet. Det nederlandske politiet benyttet en søkemotor (eller *web crawler*) for å identifisere Tor-servere som sprer barneporno. I ett tilfelle greide de å avsløre den virkelige IP-addressen bak et nettsted kalt "Pedoboard". Dette førte til at FBI kunne ta beslag i serveren og installer programvare som til slutt avslørte IP-adressene også til de besøkende. Lovlighetern av denne fremgangsmåten ble senere bestridt [9, s. 115].

5.2 Blockchain

Selv om de ofte nevnes i samme åndedrag, og ofte også brukes i kombinasjon (jf. avsnitt 5.2.2.3), er Blockchain-teknologien på mange måter den diametrale motsetningen til Tor. Tor-teknologien søker å maskere IP-adresser og online-aktivitet mens blockchain-teknologien tvert om er grunnlagt på fullstendig åpenhet og fullstendig etterettelighet i alle økonomiske mellomværender.

Abstrakt betraktet er blockchain simplethen et system for formidling av tillit i økonomiske transaksjoner uten bruk av tiltrodde mellommenn. Stort sett alle prosesser mellom institusjoner og individer i det moderne samfunnet er avhengig av tillit. Dette gjelder selvsagt spesielt kontrakter og økonomiske transaksjoner, men også interaksjon mellom institusjoner mer generelt. Det er f.eks. banken som garanterer gyldigheten av en pengeoverføring, attesterer at det finnes midler, at midlene ikke brukes mer enn én gang etc. Dersom bankene ikke hadde hatt allmenn tillit, ville de ikke ha kunnet spille denne rollen, og konvensjonelle monetære systemer ville derfor ha brutt sammen.

Tradisjonelt har formidling av tillitt vært monopolisert av institusjonelt definerte mellommenn slik som advokater, myndigheter og banker. Blockchain-teknologien er utviklet for å bryte dette monopolet ved å gjøre tillit til en egenskap ved selve transaksjonsformen. Det fungerer i grove trekk på denne måten:

Et blockchain-nettverk kan betraktes som en distribuert database for å loggføre økonomiske transaksjoner. Disse loggene dupliseres over tusenvis av maskiner og holdes oppdatert med hverandre. Logger kan videre lenkes sammen i kryptografisk validerte regnskapskjeder som representerer suksessive transaksjoner knyttet til en konto eller blockchain-adresse. Dersom man f.

eks. gjør et kjøp med en digital valuta slik som bitcoin, så vil det foregående leddet i regnskapskjeden loggføre saldo før kjøpet, mens detaljer om kjøpet samt saldo etter kjøpet noteres på et nytt "kort" (les *block*) som hektes til det foregående, og slik forlenger regnskapskjeden for denne kontoen. Disse transaksjonskjedene kringkastes i blockchain-nettverket, og utgjør tilsammen en *åpen regnskapsbok* som deles av hver maskin i nettverket.

Det faktum at regnskapskjeder er kryptografisk validert innebærer at ingen av dem kan endres retrospektivt uten at endringen avsløres og avvises av de andre maskinene i nettverket. Denne egenskapen gjør at nettverket som sådan kan opprettholde og forvalte tillit i økonomiske transaksjoner uten bruk av en tiltrodd tredjepart slik som for eksempel en bank. Ingen enkelt person, algoritme, eller maskin har autoritet eller mulighet til å endre en transaksjon i ettertid.

Hensikten med blockchain-teknologien er derfor i bunn og grunn å avmonopolisere formidlingen av tillit ved å regnskapsføre transaksjoner i en kryptografisk validert, allment åpen, desentralisert database som ingen eier. Idéen er at kryptografisk validering alene er tilstrekkelig til å borge for ektheten av en transaksjon, og derfor at tiltrodde mellommen som banker og meklere strengt tatt er overflødige.

5.2.1 Blockchain og vareflyt

Selv om blockchain-teknologien muligens er mest kjent som en muliggjører for alternative, digitale former for valuta slik som Bitcoin, så er det i prinsippet mulig å tenke seg anvendelser innenfor alle verdioverføringsystemer, også fysisk vareflyt.

Globale varekjeder kan være svært komplekse, og involverer genrelt sett aktører som ikke kan forutsettes å ha sammenfallende interesser. Veien en vare tar fra en produsent til forbruker, er lovregulert gjennom eksport og importdeklarasjon, og går via tilrodde mellommenn som import- og eksportmeklere, tollagenturer, spedisjonsselskap, finansielle institusjoner og revisjonsinstitusjoner.

Det er mulig å se for se at denne prosessen både kan gjøres mer effektiv og sikrere ved hjelp av blockhain: mer effektiv ved at man unngår overflødig datavalidering og revisjon, og sikrere ved at dokumentkjeden er lagret og validert i en åpen og distribuert regnskapsbok som f.eks. kan utelukke feilaktige tariffsatser for en vare dersom den opprinnelige transaksjonen allerede er bokført.

Regnskapsboken i et blockchain-nettverk er digital og kan programmeres. Det er derfor teknologisk fullt mulig å implementere "smarte" kontrakter/transaksjoner, for eksempel applikasjoner som implementerer dokumentflyten som ledsager en vare på tvers av tollgrenser. Slike "smarte" kontrakter vil eksekvere nøyaktig slik de er programmert, uten forsinkelse eller nedetid, og uten mulighet for svindel eller forfalskning av tredjeparter.

5.2.1.1 Korporative blockchain-nettverk.

Gjennomsiktighet er en grunnleggende byggekloss i blockhain-teknologien, og en nødvendig forutsetning for at regnskapsboken og revisjonskjedene skal kunne valideres av 'peers' i nettverket. Alle historiske transaksjoner i nettverket kan inspiseres av alle aktører til enhver tid.

Det er allikevel ingenting ved dette som fordrer at nettverket som sådan er allment tilgjengelig. Det finnes allerede komersielle applikasjonsplatformer som kjører spesialbygde, private eller korporative blockchain-nettverk (to eksempler er IBM Blockchain og Ethereum).

En slik plattform har mange potensielt interessante anvendelser innenfor regulering av vareflyt. Selv om man riktignok må forutsette et betydelig internasjonalt standardiseringsarbeide før noe slik kan realiseres, er det ikke utenkelig å se for seg et korporativt blockchain-nettverk som er delt og driftet av tollmyndighetene i f.eks. det felleseuropeiske tollområdet.

En slik overnasjonal infrastruktur vil kunne gjøre det mulig å flytte verdier over landegrensene uten at eierskapsinformasjon, tariffsatser, gjeld, rapporteringsforpliktelser o.a. misligholdes.

5.2.2 Modenhet

Blockchain er en potensielt transformativ teknologi med stor økonomisk og kulturell betydning. Det er allikevel velkjente problemer med den som foreløpig mangler allment aksepterte løsninger og løsninsgstrategier. Dette gjelder spesielt områdene skalérbarhet, personvern og sikkerhet.

5.2.2.1 Skalérbarhet

En velkjent begrensning ved blockchain-teknologien er det maskimale antallet transaksjoner pr. sekund. Dette antallet er lik størrelsen som i henhold til blockchain-protokollen er avsatt til registreringen av en enkelt transaksjon (dvs. størrelsen på en *block*) delt på den gjennomsnittlige størrelsen på faktiske transaksjoner. På grunn av det totale antallet bytes som kreves for å lenke en blockchain-registrering sammen med foregående transaksjon, sammen med annet nødvendig bokholderi, så gir dette en maksimumsrate på mellom ti og tyve transaksjoner pr. sekund.

Til sammenlikning håndterer VISA gjennomsnittlig 2000 transaksjoner pr. sekund, og har en maksimumskapasitet på rundt 56 000.

5.2.2.2 Sikkerhet

Enhver node i et blockchain nettverk lagrer en komplett kopi av regnskapsboken som nettverket som sådan fører. Dette gjør at et blockchain-nettverk vil kunne bevege seg mot sentralisering etterhvert som det eldes: jo større regnskapsboken blir desto mer regnekraft må til for å validere nye transaksjoner. I ytterste konsekvens betyr dette at nettverket vil kunne begynne å konvergere mot noen få aktører som er store nok til å levere tilstrekkelig med regnekraft.

Allerede i dag er det slik at ca. fem til ti aktører leverer over 50% av den regnekraften som driver valideringsprosessene i det globale internettbaserte blockchain-nettverket. Dette er få nok til å utgjøre et reelt sårbarhetspunkt og derfor en reell sikkerhetsrisko.

5.2.2.3 Personvern

Når ny informasjon lagres i et blockchain nettverk kan alle maskiner i nettverket sjekke at informasjon representerer en gyldig transaksjon—dette er et grunnleggende premiss i den kryptografiske

valideringsmodellen i blockchain. For at en maskin skal kunne validere en transaksjon så må den imidlertid ha adgang til å slå opp alle tidligere transaksjoner som er knyttet til den samme blockchain-adressen. Dette er nødvendig for at nettverket skal kunne validere at den som ønsker å kjøpe en vare faktisk har midler til å kjøpe den. Det må, med andre ord være mulig for en hvilken som helst maskin i nettverket å rekonstruere en komplett finansiell historie for enhver aktør i nettverket.

Bitcoins brukes ofte for å illustrere hva dette innebærer. For at en person skal kunne betale med Bitcoin må han eller hun disponere en blockchain-adresse. Det må videre finnes informasjon åpent tilgjengelig i nettverket som sier nøyaktig hvor mange Bitcoins som er knyttet til denne adressen, hvor disse pengene kommer fra, hva de har blitt brukt til osv.

Dette er selvsagt svært sensitiv informasjon dersom den skulle kunne knyttes til en person, og det er ikke vanskelig å se for se hvordan det skulle kunne skje. Det skal som kjent ikke mange variabler til for å identifisere en person fra anonymiserte data, spesielt ikke dersom man, som i tilfellet er med blockchain, allerede vet hvilke informasjonfragmenter som kan knyttes til samme person.

5.2.3 Blockchain kombinert med Tor-teknologi

Det er ikke mulig å kryptere eller skjule informasjonen i den åpne regnskapsboken i et blockchain-nettverk. Enhver transaksjon kan inspiseres av hvem som helst.

Det er imidlertid mulig å adressere dette personvernsproblemet ved å maskere identiteten til *partene* i en transaksjon. En vanlig måte å gjøre dette på er å kombinere blockchain med Tor-teknologi.

Det også vanlig at kombinasjonen av blockchain og Tor ledsages av en praksis der man oppretter én ny blockchain-adresse for hver nye transaksjon man utfører. På denne måten akkumulerer man ingen økonomisk historie i nettverket som kan brukes til å avsløre ens identitet, eller som man kan holdes til ansvar for dersom ens identitet blir kjent.

5.3 Lagringsløsninger, analyseverktøy, infrastrukturkonsepter

Gitt Tolletatens informasjonsbehov spesielt på områdene etteretning, objektutvelgelse og kontroll, må man se for seg at Tolletatens fremtidige informasjonsinfrastruktur ikke bare består av arkiveringsløsninger og forvaltningssystemer. Den vil også ha en yttergrense bestående av et stort og varierende antall sammenkoplete sensorsystemer som besørger en stor del av informasjonsfangsten.

Mange sensorer er i dag allerede integrert i Tolletatens virksomhetsmodell, om enn ikke direkte i en overgripende informasjonsinfrastruktur. Eksempler er ANPR-kameraer, laserdetektorer og konvensjonelle kameraer, men listen av mulige utvidelser kan forlenges nesten uten ende med droner, sniffere, scannere, satelitter, biometriske kameraer, radiofrekvensidentifikasjon m. m.

Alt dette sett under ett innebærer at man må se for seg Tolletatens fremtidige informasjonsinfrastruktur som et system for multi-sensoral datafangst og sammenstilling, med avansert analysekapabilitet og vilkårlig skalerbar datalagring. Det er spesielt fire trender innenfor IKT det er viktig å følge med på i dette perspektivet:

Alt dette sett under ett innebærer at man må se for seg Tolletatens fremtidige informasjonsinfrastruktur som en sensorplatform, forstått som et system for multi-sensoral datafangst og sammenstilling, med avansert analysekapabilitet og vilkårlig skalérbar datalagring. Det er spesielt fire trender innenfor IKT det er viktig å følge med på i dette perspektivet:

- *Internet of Things*, eller *Tingenes internett*.
- *Stordata*.
- *Semantic Web*-teknologier.
- *Cloud computing* eller *skytjenester*.

En kort beskrivelse av hver av disse følger.

5.3.1 Tingenes internett

Tingenes internett (IoT) er en teknologitrend og et konsept basert på en idé om å koble sammen fysiske ting gjennom en virtuell representasjon av dem på internett. Hensikten er å gjøre det mulig for objekter som er fremstilt helt uavhengig av hverandre, og for ulike formål, å koordineres over verdensveven og å utveksle informasjon. Når flere og flere fysiske gjenstander slik som bygninger, biler, armbåndsur, kjøkkenapparater m. m. produseres med innebygget elektronikk og nettverkskapabiliteter, er dette en nærliggende tanke.

Tingenes internett antas å skape muligheter for en mer direkte integrasjon av vår fysiske omverden i computersystemer. Dette anats i sin tur å kunne øke effektiviteten, nøyaktigheten og det økonomisk utbytte av forskjellige private og offentlige forvaltningsoppgaver og -forretningsprosesser (samt redusere behovet for menneskelig inngripen og -feil). Noen eksempler på anvendelsesområder er:

- IoT-enheter kan integreres i all typer av enheter som bruker eller leder strøm (brytere, stikkontakter, lyspærer, fjernsyn o.a.) og kommunisere direkte med strømselskapet for å balansere kraftproduksjon mot forbruk.
- Personlige enheter kan utstyres med sensorer som overvåker helse. Det finnes armbåndsur som måler puls og blodtrykk, og det forskes på mer avanserte og spesialiserte enheter, f. eks. implantater som måler glukosenivå hos diabetikere eller “smart beds” som overåker kroppstemperatur og døgnrytme, f. eks. til bruk i forbindelse med problematiske svangerskap.

IoT-teknologier har potensielt stor betydning for vareflyt og transport. Nettilkoblede enheter kan enkelt installeres i de aller fleste ting som inngår i et transportsystem, inkludert ruten eller farleden selv (kjøretøy, vare, konteiner, overgang o.a). En dynamisk interaksjon mellom slike komponenter vil kunne brukes til å støtte logistikk og flåtestyring, men også mer direkte til kontrollrelaterte oppgaver som for eksempel forsegling og/eller sporing av konteinere.

5.3.1.1 IoT i blockchain-nettverk.

Det er i dag en del interesse knyttet til kombinasjonen av IoT og blockchain-teknologier. Det er da heller ikke vanskelig å se for seg synergieffekter her: En adresse i et blockchain-nettverk

representerer typisk en person eller institusjon, men det er ingenting i veien for at den også kan representere en gjenstand.

Siden den åpne regnskapsboken i et blockchain-nettverk er digital og kan programmeres, er det derfor teknologisk fullt mulig å se for seg at også transaksjoner mellom gjenstander kan automatiseres og arkiveres i et blockchain-nettverk. Mengden av mulige transksjonskjeder kan programmeres på forhånd, og hver transaksjon vil være åpen for inspeksjon og validering av alle involverte parter. Det vil ikke være mulig for en tredjepart å forfalskse noen av leddene i en slik kjede.

Med fremveksten av sensorteknologi som gjør det enkelt og billig å oversette fysisk bevegelse til data, kan man tenke seg at gjenstander på en adresse på f.eks. et felleseuropeisk korporativt blockchain-nettverk vil kunne interagere direkte. Dette vil sannsynligvis i første omgang innebære at slike ting som avgift, tariffering og deklarering kan gjøres automatisk ved grensepassering av objektene selv.

Det er selvsagt mange ikke-teknologiske forutsetninger som må være tilstede før noe slikt som dette vil kunne realiseres i stor skala, for eksempel et adekvat overnasjonalt regelverk. Å implementere konvensjonell lovgivining om sjøfart, farleder, nasjonsgrenser og vareflyt i et digitalt og overnasjonalt nettverk er, som det er unødvendig å si, ikke trivielt.

5.3.1.2 Modenhet

Tingenes internett er å betrakte mer som et konsept enn en teknologi. Det er foreløpig liten grad av konvergens mot en bestemt applikasjonssuite eller protokoll.

Dersom man med, “tingenes internett” forstår “sensorintegrasjonsplatform”, er det imidlertid riktig å si at IoT har nådd et slags produktivitetsplatå, da det allerede finnes mange utviklere som tilbyr sensorer og intergrasjonssystemer under den generelle rubrikken ‘IoT’. Det finnes mange variasjoner over dette temaet.

Noen systemer baserer seg på bruken av SIM-kort og virtuelle mobiloperatører. Alle enheter med et slikt SIM-kort kan administreres og koordineres av systemet. Virtualiseringen av mobiloperatøren gjør at slike systemer også kan brukes til korporative og private IoT-nettverk.

Andre IoT-systemer bygger på blockchain-teknologi. Typisk for disse er at all interaksjon med- og mellom ting loggføres i regnskapskjeder, og at gjenstander kan utveksle verdier seg i mellom. Verdier kan her bety Bitcoins, men det kan også mer generelt dreie seg om ressurser slik som prosessorkraft og båndbredde.

5.3.2 Semantic Web-teknologier

Internett, eller mer spesifikt verdensveven, er i utgangspunktet designet som et globalt informasjonsrom for *tekstdokumenter* som peker til hverandres nettadresser, såkalt *hypertekst*. Rådata derimot, dvs. ubehandlede data som ikke er bearbeidet eller manipulert, var ikke opprinnelig tiltenkt en plass i denne arkitekturen.

Data er derfor typisk noe som pipler inn på nettet fra bakenforliggende databaser, regneark, tekstfiler etc. De er som oftest presentert i behandlet form i HTML-tabeller eller liknende. Til forskjell fra dokumentene som inneholder dem, er ikke disse dataene en del av nettverkstrukturen selv: de har ingen nettverksadresse og kan ikke peke til hverandre.

Internett er en stadig mer gjennomgripende del av våre daglige liv, og det er et økende behov for å gjøre nettet mere datadrevet og mer intelligent. Men for at dette skal kunne skje, må rådataene, beregningsgrunnlagene, være direkte tilgjengelige og ikke bundet opp i hypertekstdokumenter på denne måten.

Slike betraktninger har gitt opphav til idéen om *lenkede data*. Akkurat som nettadresser på det klassiske internettet lenker dokumenter sammen i et globalt informasjonsrom, så er tanken at dataene selv skal kunne lenkes på samme måte, slik at nettet utvikler seg fra et arkiv til en global database. Bruken av standarder og en felles datamodell vil gjøre det mulig å utvikle genériske nettapplikasjoner som er i stand til å navigere i- og utnytte data ved å følge lenkene. På denne måten ser man for seg at nettet skal bli mer datadrevet, informert og betydningsorientert.

Denne strategien er nedfelt i standarden *The Resource Description Framework (RDF)*, som er en av de grunnleggende Semantic Web-standardene. RDF er en datamodell for å uttrykke relasjoner mellom dataelementer. Den kan sammeliknes med relasjonsmodellen i som underligger klassiske relasjonsdatabaser, men med noen avgjørende forskjeller:

- For det første så identifiseres alle objekter *og* relasjoner i RDF som nettadresser. For eksempel, dersom man ønsker å uttrykke at et bestemt lastemanifest er knyttet til en konvoi av biler, så navngir man manisfestet med én nettadresse, hver av bilene med en annen, og relasjonen mellom dem med en tredje. Disse nettadressene vil selvsagt abstraheres vekk klientapplikasjoner og er derfor å betrakte simpelthen som en standard for å indeksere *objekter* (ikke bare dokumenter) som omtales på internett.
- For det andre er RDF lenker typede: Vanlige hypertekst lenker indikerer at to dokumenter er relatert på en eller annen måte, men overlater til brukeren å slutte seg til hvilken relasjon det er snakk om. RDF, derimot, gjør det mulig for den som utgir et datasett å være eksplisitt mhp. hva slags forbindelse det er snakk om. I eksempelet over vil man f.eks. kunne si at hver av bilene i konvoien *tilhører* samme konvoi, at hver av dem utgjør et *subset* av manifestet etc.

Dette nettverket av lenkede data, mer kjent som *The Semantic Web*, er designet for å gjøre det mulig for RDF-bevisste applikasjoner å følge lenker fra et datasett til et annet. Slike applikasjoner vil typisk kunne forsterke et datasett med annen relevant informasjon ved å bruke informasjon om lenkene, de vil kunne bevege seg sømløst fra ett datasett til et annet uansett hvor på internett de er publisert, og de vil kunne sammenstille og utveksle informasjon fra- og med helt uavhengige dataeiere for, si, statistisk analyse eller etterforskningsformål.

5.3.2.1 Modenhet og nytte

Semantic Web er et teoretisk svært velstudert konsept, noe som reflekteres av standardene der det er beskrevet. Disse standardene har lenge vært stabile og promoteres aktivt av *The World Wide Web Consortium*. Det finnes i dag gode, velprøvde publiseringsverktøy for lenkede data, både komersielle

produkter og gratisvare. De fleste av de vanligste programmeringspråkene har støtte for RDF, f.eks. Java, Python, Scala, C#, Javascript og PHP.

Det har allikevel ikke utskrystallisert seg noen allment utbredt programvaresuite for å *konsumere* RDF data. Det finnes riktignok en god del "content mangament systemer"—f. eks. semantiske Wikier og webpubliseringsverktøy—som både er velutviklede og stabile, men få, hvis noen, har fått noen bredere komersiell eller industriell anvendelse.

Én av grunnene til dette er sannsynligvis at Semantic Web-teknologier er svært kunnskapsintensive teknologier. En effektiv utnyttelse som gir en reell merverdi sammenliknet med mer tradisjonelle forvaltningssystemer forutsetter høyt kvalifiserte ingeniører med spesialistkompetanse. Denne terskelen er såpass høy, at det muligens ikke er rimelig å forvente at disse teknologien noensinne blir standard verktøy.

Når det er sagt, er Semantic Web allikevel en teknologi Tolletaten kan ha nytte av å ha en viss kompetanse på, for selv om klientapplikasjonene muligens har et stykke igjen å gå, så blir det mer og mer vanlig å *publisere* lenkede data. Her er noen eksempler:

- Eurostat publiserer alle sine datasett som lenkede data (ikke *bare* som lenkedde data, vel og merke). Deres målsetning med dette arbeidet er etter sigende å tilby statistikk på europeisk nivå som er kontekstrik, assosiativ og selvbeskrivende.
- Offentlige lenkede dataportaler er mer og mer vanlig. Spydspissen i dette arbeidet er det britiske data.gov.uk-initiativet som er ledet av ingen ringere enn oppfinneren av *The World Wide Web* Tim Berners-Lee. Data.gov.uk publiserer lenkede data fra stort sett alle sektorer i samfunnet: skoler, veiarbeid, vann og kloakk, lover, vedtak etc. Slike .gov portaler har senere sprunget opp mange andre steder, bl. a. i USA (data.gov) og her hjemme (data.norge.no).
- Mange nyhetsmedier publiserer nyheter som live RDF strømmer. Dette gjelder f.eks. New York Times, BBC og The Guardian.
- Det finnes mye åpen geoinfromasjon tilgjengelig som RDF f.eks. datasettet LinkedGeoData. Dette er en stor stedsnavnsdatabase som utnytter lenkene i RDF til å berike geokoordinatene med informasjon fra andre uavhengige kunnskapbaser. En av disse er DBPedia, en åpen kollaborativ RDF-database som destillere strukturert informasjon fra Wikipedia. LinkedGeoData bygger i sin tur på OpenStreeMap som også er kollborativ. OpenStreetMap samler informasjon om alt fra kaféer til togstasjoner og trafikk gjennom en interaktiv kartappliaksjon (sammeliknbart med Google maps) som kjøres på lokasjonsbevisste enheter slik som mobiltelefoner og nettbrett. Databasen vokser og oppdateres etterhvert som brukere legger inn geolokalisert informasjon, f.eks. tekst, terningkast, lenker, telfonnummere, etc.

Konklusjonen man kan trekke fra dette er at det finnes en stadig økende mengde *Open Source Intelligence* der ute i form av lenkede data. I motsetning til mye av det som kan skrapes av nettsider andre steder, er dette er svært velstrukturerte og informasjonsrike data som på grunn av at de deler et felles format, kan utnyttes og analyseres av genérisk programvare. Det vil si at denne informasjonen kan analyseres, gjenbrukes, deles og utveksles uten at man trenger nye skreddersydde skript for hver oppgave.

Det er sannsynlig at det er mye informasjon her—noe av den sanntidsinformasjon—som ville kunne benyttes av Tolletaten for, digital etterforskning, statistikkproduksjon, risikoanalyse, analyse av bevegelser etc.

5.3.3 Stordatateknologier (*Big Data*)

Det finnes ingen autoritativ definisjon av hva stordata er, men som et minste felles multiplum kan man si at stordata, i den tekniske forstanden dette begrepet brukes i dag, betegner datasett som er for store til effektivt å kunne behandles av en enkelt maskin. Enten fordi en enkelt maskin ikke kan tilby nok prosessorkraft til å analysere datasettet innenfor rimelig tid, eller fordi en enkelt maskin ikke kan tilby lagringsplass som skalerer i takt med datasettets vekstrate.

En vanlig, og mer prosessorientert definisjon lyder: “Big data is high volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization”.

Variasjon i type, format, mengde og innhold kjennetegner spesielt stordatasystemer som er designet for slike ting som å sammenstille situasjonsbilder, eller for å støtte etteretning og overvåking. Slike systemer er ofte bygget opp som store distribuerte datavarehus som samler data fra mange uavhengige kilder for å besvare spørsmål som ingen av kildene alene dekker.

Et slikt stordatasystem utnytter vanligvis sensordata fra mobile enheter mobile enheter—telefoner, kameraer, mikrofoner, RFID-lesere, GPS-trackere og annet. I et stordatasystem vil dette imidlertid kun være én av en større mengde datakilder som inkluderer konvensjonelle dokumenter, f.eks. regneark, Websider og ren tekst, samt datastrømmer fra sosiale nettverk slik som Facebook og Twitter. Et stordatarammeverk vil tilby funksjonalitet for å traversere disse forskjellige kildene på jakt etter meningsfulle sammenhenger. Som et grovt omriss, kan man si at en typisk stordatadistribusjon, forstått som et programvarerammeverk for å lagre og bearbeide store mengder heterogene data, består av tre ting:

1. Et distribuert filsystem som skalerer *horisontalt*, hvilket vil si at dataene spres og lagres i en *serverklynge* som ekspanderer ved behov.
2. En programmeringsmodell (eller application programming interface (API) for å interagere med filsystemet gjennom programkode).
3. Et sett av algoritmer for prediktiv analyse, klassifisering, anbefaling o.a.

Basert på lagringsløsning og/eller programmeringsmodell er det mulig å sondre mellom noen ulike typer. Det må dog understrekes at disse kategoriene ikke er gjensidig utelukkende, og bør betraktes som tommelfingerregler.

- NoSQL-systemer: En NoSQL-database kan betraktes som en stor distribuert opplagstabell. Den skiller seg fra en tradisjonell relasjonell (SQL-) database ved at en NoSQL-database stiller færre krav til datastruktur, og at den gjerne spesialisere seg på bestemte typer operasjoner snarere enn å støtte et generelt spørrespråk slik som SQL. Likhetene stopper her. Det finnes svært mange forskjellige NoSQL-databaser i dag. De har alle forskjellig funksjonsmåte og er utviklet for forskjellige, ofte helt spesifikke formål (for eksempel for å lagre ‘posts’ og ‘tweets’ på Facebook eller Twitter). De er som regel *ikke* utviklet som genériske datavarehusløsninger. På mange måter kan det å velge en NoSQL database sammenliknes med det å velge en datastruktur—f.eks. en liste, vektor, mengde eller tabell—i et programmeringsspråk. Man vet på forhånd nøyaktig hva man trenger å gjøre, og man velger en databaseløsning som er optimalisert for akkurat dette.

- Batch-prosesseringssystemer: Det mest kjente eksempelet er Hadoop som er bygget over en programmeringsmodell som kalles Map/Reduce. Disse systemene kjennetegnes av enorm regnekraft og lav responsivitet/lang ventetid. De er bygget for store beregningsoppgaver som lar seg parallellisere, slik at deler av beregningen kan utføres samtidig på ulike fragmenter av et datasett på forskjellige maskiner. Typiske anvendelser vil være indeksering av nettsider for en søkemotor eller statistikkproduksjon.
- Distribuerte grafdatabaser: En grafdatabase representerer forholdet mellom dataelementer vha. en semantisk graf. Noder i grafen representerer objekter (i en vid forstand;mennesker, maskiner, steder, hendelser etc.), mens kantene representerer forholdene mellom dem. En distribuert grafdatabase er en virtualisering av denne datamodellen som støtter horisontal skalering over en serverklynge.

Disse typene av stordatasystemer har ganske forskjellige egenskaper som det gjelder å være oppmerksom på: NoSQL-systemer er designet for å støtte responsive brukergrensesnitt der flere små lese- og skriveoperasjoner må utføres i sanntid. Et typisk eksempel er statusoppdateringer i et sosialt nettverk. Batch-prosesseringssystemer har lav responisvitet men stor regnekraft, og egner seg derfor bedre for ressurskrevende oppgaver som ikke er tidskritiske, og som kan kjøres i bakgrunnen. Typiske eksempler er indeksering av nettsider og statistisk analyse for overvåking og/eller etteretning. Grafdatabaser, på sin side, er designet for å modellere assosiative semantiske nettverk der noder representer ting og kanter representerer forholdene mellom dem. En grafdatabase er spesialdesignet for for data med høy konnektivitet. Den er med andre ord optimalisert for nettverksanalyse og raske søk i komplekse hierarksiske og relasjonelle strukturer. Typiske eksempler er analyse av bekjentskapskretser og interessefellesskap, men anvendelsene er mange; analyse av genklynger i bioinformatikk, analyse av aksjeporteføljer i finans, m.m.

En interessant undergruppe av grafdatabaser er de som implementerer Semantic Web-standarder. På grunn av RDF-standardens tidligere omtalte spesielle egenskaper, egner disse seg spesielt godt for datasett som skal utveksles mellom systemer, og for datasett som skal arkiveres eller gjenbrukes. Å utnytte slike grafdatabaser til fulle vil kreve mer tid i form av datamodellering. Til gjengjeld vil dataene ofte kunne anlyseres dypere, presisjonen på resultatene heves, og gjenbruks- og arkiveringsverdien vil øke.

5.3.3.1 Modenhet

Alle de nevnte typene av stordatasystemer er velstudert, utprøvd og i industriell bruk: NoSQL-systemer drive sosiale nettsteder slik som Facebook og Twitter. Grafdatabaser av Semantic Web-typen driver spørregrensesnittet til Wikidata og publiseringsløsningen til Yahoo. Map/Reduce systemer brukes av Google til indeksering av nettsider, og er svært utbredt innenfor prediktiv analytikk og statistikkproduksjon.

Det finnes mye hyllevare som kan taes i bruk uten videre. Det er først og fremst et spørsmål om å plukke det rette redskapet for en oppgave.

5.3.4 Skytjenester (Cloud computing)

Cloud Computing, eller *skytjenester*, er en modell for å tilby programvareprodukter, båndbredde, lagringsplass og prosessorkraft som utleieprodukter over internett. Tanken er at en bedrift eller orga-

nisasjon ikke skal trenge å drifte sin egen maskinpark for å kjøre forretningsspesifikk programvare, men snarere at infrastrukturen bør kunne leies over internett og dimensjoneres etter behov.

Det er vanlig og skille mellom tre forskjellige *tjenestemodeller* innenfor Cloud Computing. Tjenestemodeller kan betraktes som en type produktporteføljer som grupperer varer og tjenester på forskjellige generiske nivåer. De tre vanligste nivåene er:

- Software as a Service (SaaS): På dette tjenestenivået kjøper kunden lisenser til programvare som driftes og kjøres av tilbyderen. Programvaren er tilgjengelig fra mange forskjellige tynne klienter som kan kjøres på ulike enheter slik som nettlesere, mobiltelefoner og nettbrett. Alt ansvar for å administrerte nettverk, servere, operativsystemer og lagringsplass tilfaller tilbyderen.
- Platform as a Service (PaaS): På dette tjenestenivået kjøper kunden et miljø bestående av programmeringsspråk, programvarebiblioteker, tjenester og verktøy som setter kunden i stand til å deployere egenutviklet programvare på tilbyderens infrastruktur. Alt ansvar for å administrerte nettverk, servere og operativsystemer tilfaller tilbyder, men kunden har kontroll over sine egne applikasjoner samt de konfigureringsinnstillingene som er nødvendige for å drifte dem.
- Infrastructure as a Service (IaaS): På dette tjenestnivået kjøper kunden kun rene maskinvareressurser, typisk prosessorkraft, nettverk og lagringsplass. Kunden betaler kun for den kapasiteten og de maskinressursene han eller hun bruker, og kan raskt skalere opp for å ta unna økninger i trafikk eller utføre spesielt prosessorintensive beregninger.

Det er mulig å se for seg tre områder hvor skytjenester vil kunne ha betydning for Tolletaten. Fra generelt til spesifikt:

1. Virtualisering av infrastruktur krever ingen ressurser til drift av maskinvare og ingen ressurser knyttet til oppdatering av programvare. Kostnadene vil være direkte proposjonale med behov til enhver tid.
2. Skytjenester er en svært viktig muliggjører for stordatatsystemer som trenger å skalere horisontalt, f.eks. i forbindelse med spesielt tunge beregningsoppgaver som trenger å øke den samlede tilgjengelige prosessorkraften for å fullføre innen rimelig tid. I den grad Tolletaten har behov for slike systemer, vil den derfor også kunne ha behov for skytjenester.
3. Man kunne tenke seg at Tolletaten kunne utvikle klienter tilpasset de ulike tollstasjonene og deres kontrollfunksjoner i et skybasert miljø. Data fra kontrollene ville da umiddlebart blitt lagret i skyen og derfor enkelt kunne redistribueres og gjenbrukes nærmest i sann tid. En slik løsning vil også gi Tolletaten en integrert informasjonsinfrastruktur hvor f.eks. oppdatering av programvare er svært mye enklere å rulle ut.

5.3.4.1 Sikkerhet

Når en organsisasjon velger å lagre data eller kjøre programvare over en skytjeneste så mister den selvsagt muligheten til å ha fysisk kontroll med de maskinene der denne informasjonen ligger lagret.

Dette innebærer en sårbarhet for innsideangrep. Anslag fra 2010 (som riktignok er noe gammelt i denne sammenhengen) tyder på at innsideangrep er en betydelig trussel for skybaserte tjenester, og at potensielt sensitive data løper en ikke uvesentlig risiko for å komme på avveie.

Det er derfor svært viktig å sette seg inn i hvilket sikkerhetsregime som praktiseres av tilbyder, og dette gjelder ikke kun de digitale ressursene, men også ansettelsesprosedyrer, servertilgang etc.

For å spare kostnader og utnytte maskinparken effektivt, er det videre ikke uvanlig at tilbyder lagrer data for mer enn én kunde på den samme serveren. Det er derfor i prinsippet en sjanse for at én kunde vil kunne skaffe seg tilgang til en annen kundes data. For å unngå en slik situasjon er det viktig å forsikre seg om at tjenestetilbyderen benytter en logisk partisjonering av diskplass med dokumenterte og etterprøvbare sikkerhetsegenskaper.

5.4 Web Processing Service

Foredling og distribusjon av geografisk, meteorologisk og oseanografisk informasjon (geografi, meteorologi og oseanografi (GEOMETOC)) kan med fordel gjøres i tjenesteorienterte distribuerte systemer, men dette gjelder også andre krevende prosesser som ikke nødvendigvis er stedfestet. Dataprosessering implementeres da som tjenester, dvs. selvstendige programmer som kan iverksettes gjennom plattformuavhengig meldingsutveksling, og som typisk er fordelt på ulike maskinnoder i et nettverk. Prosessering av stedfestet informasjon kan være svært regnekrevende. Dette gjelder særlig ved fjernmåling og observasjon av jordens overflate og havbunn, der ny sensorteknologi produserer store datamengder, og hvor mulighetene for nye statlige anvendelser langt fra er utnyttet. Tjenesteorienterte systemer er spesielt aktuelle for anvendelser innen datafusjon (sammenstilling av data fra flere kilder), analyser av store eller dynamiske datasett, tidkrevende eller vedlikeholdskrevende beregninger, og i situasjoner der ny funksjonalitet må realiseres på kort tid. Eksempler på dette finnes innen terrenganalyse, ruteplanlegging og mobilitetsanalyse, bildeanalyse og klassifisering, analyse av trafikkdata, hav- og atmosfæremodellering, fartøysporing og maritim overvåking, miljøavhengig simulering av sensorytelse, med mer [10].

Open Geospatial Consortium (OGC) [11] er et internasjonalt industrikonsortium av bedrifter, offentlige etater og høyskoler som sammen utvikler offentlig tilgjengelige standarder for stedfestet informasjon. OGC standarden styrker interoperabiliteten i løsninger som benytter stedfestet informasjon på internett eller over lokale eller trådløse nettverk. Standardene forenkler teknologiutvikleres arbeid i å gjøre komplisert romlig informasjon tilgjengelig med forholdsvis enkle tjenester. Disse tjenestene kan benyttes direkte av brukere eller inkluderes i mange forskjellige typer applikasjoner.

OGC-standarden Web Processing Service (WPS) er en spesifikasjon for vevtjenester som opererer på stedfestede data [12], og er altså en åpen standard for beregningskrevende tjenester. En WPS-tjeneste tilbyr en eller flere *operasjoner* (delprogram som kjøres på tjenermaskinen) som gjør beregninger med gitte parametere fra klienten (inndata), og returnerer et resultat på en spesifisert form (utdata). WPS definerer mekanismer for å beskrive tjenestene, overføre inndata, iverksette operasjoner og returnere resultatet.

WPS spesifiserer ikke hvordan operasjoner skal implementeres, eller hva inndata og utdata skal være. En følge av dette er at WPS også er egnet for prosessering av andre typer data enn stedfestet informasjon. WPS spesifiserer i stedet et felles sett metadata for WPS-transaksjoner, og hvordan inndata og utdata kan transporteres og omsluttes av metadata i Extended Markup Language (XML)-format [12], [13]. Det kreves mindre kode for å ta i bruk og kombinere data fra flere tjenester når alle tjenestene har et felles grensesnitt. Dette er et viktig formål med standardisering.

5.4.1 Anvendelser og muligheter

Et eksempel er deteksjon av endringer i en scene som blir videofilmet flere ganger [14]. Denne WPS-tjenesten sammenligner en innspilt video med en ny videostrøm av samme scene og sender hvert bilde hvor endringer detekteres til en OGC Sensor Observation Service (SOS). Felles for disse eksemplene er at de integrerer flere datakilder og proseseringstjenester via OGC-tjenester, og demonstrerer nytten av standardisering og interoperabilitet.

I et nettverk der det er mange datakilder tilknyttet, og den viktige/nyttige informasjonen må trekkes ut av rådatamaterialet og videreformidles etter behov. Her er noen typer situasjoner og anvendelser der prosesseringstjenester er aktuelle:

1. anvendelse på Tolletatens mobile enheter hvor man ikke har anledning til å prosessere informasjonen/data lokalt;
2. fusjon/integrasjon av data fra mange kilder (innsamling, forbehandling, sammenstilling og foredling av informasjon);
3. analyser av datasett som er for store til å distribueres til alle brukere;
4. anvendelser som krever stor grad av kontroll over grunnlagsdataene, mens avledete produkter kan distribueres videre;
5. beregninger som tar lang tid, krever spesiell maskinvare eller kode med særlig vedlikeholdsbehov, f.eks store simuleringer eller analyse av store fjernmålingsdatasett;
6. analyser av datasett som oppdateres ofte (f.eks vær- og havmodeller fra Meteorologisk institutt);
7. situasjoner der ny funksjonalitet må realiseres på kort tid (f.eks. foran en øvelse);
8. anvendelser hvor det er vanskelig å installere ny programvare på etatens plattformer, eller når det er komplisert å holde programvaren oppdatert hos mange brukere til enhver tid.

5.4.2 Klassifikasjon generelt

Statistisk klassifikasjonsteori og mønstergjenkjenning [15, 7] beskriver metoder som brukes i datasystemer som "lærer" å ta beslutninger automatisk ved å klassifisere signaler. Begrepet *signal* brukes her i vid forstand, og kan være en tidsserie (som i talegjenkjenning), en tekst (som i søppelpostfiltre), et bilde (som i diagnostisering av mikroskopibilder), en DNA-mikromatrise, etc. "Data mining" er et beslektet felt som benytter noen av de samme teknikkene, der formålet er å oppdage mønstre eller sammenhenger i et stort, mangedimensjonalt datasett [15]. Maskinlæring anvendes typisk for automatisk klassifikasjon av signaler (i vid forstand), f.eks. for tekstgjenkjenning i skannede boksider, medisinsk diagnostikk (om et mikroskopibilde viser kreft eller ikke), eller filtrering av e-post (søppelpost eller ikke). Statistisk klassifikasjon anvendes også mye innen fjernmåling, overvåkning og annen geografisk databehandling. Avviksdeteksjon kan formuleres som et klassifikasjonsproblem [16, 6]. Et annet eksempel er deteksjon av oljesøl på havet ved hjelp av fly- eller satellittbilder [17].

Det er andre grunner til å implementere klassifikasjonsalgoritmer som WPS-tjenester. Beslutningsregler blir beregnet på grunnlag av treningsdata der innholdet i signalene er kjent. Jo mer treningsdata, jo mer robuste (generaliserbare) blir beslutningsreglene. Løpende innsamling av

treningsdata (kan hende fra forskjellige kilder) og oppdatering av beslutningsreglene er en form for datafusjon som det er naturlig å gjøre på en tjenermaskin. I noen tilfeller kan det også være grunner til å skjerme beslutningsreglene istedenfor å dele dem med mange brukere.

6 Konklusjon og anbefalinger

I dette avsluttende kapitlet vil vi trekke fram de viktigste temaene som er berørt i de foregående kapitlene.

Mennesker bruker tilegnet kunnskap og sanser til å forstå virkeligheten og planlegge handlinger for å oppnå mål i en kontinuerlig gjentakende prosess. Å ta vare på kunnskap og gjøre den tilgjengelig er grunnleggende for intelligent handling og læring. En tilsvarende prosess ligger til grunn for aktuelle former for kunstig intelligens som maskinlæring. Hvis det fins tilgjengelig verifisert informasjon som kan sammenholdes med løpende sensordata gir dette mulighet for en datamaskin automatisk og sukessivt å læres opp til bedre utførelse.

6.1 Sensorer

Sensorer er både en kilde til å lagre informasjon som mennesker kan sanse, men også egenskaper som ligger utenfor menneskers oppfattelse. Utover de sensorer som Tolletaten allerede har tatt i bruk kan (nye) kjemiske detektorer, muultispektral og terrahertz bildedanning, akustiske sensorer, radar og ulike rombaserte sensorer være aktuelle. Fornyelse av egne sensorer og supplering med nye sensortyper bør holde takt med utviklingen.

Fremtidig varetransport over grensene med droner vil være utfordrende å få kontroll med. Det vil kreve både overvåkningskapasitet og mer aktive tiltak for å avskjære transporten. Vi har pekt på at sensorteknologien for deteksjon av droner, både akustisk og vha. radar, har kommet langt og vil sannsynligvis kunne addressere overvåkningsproblemet.

Innenfor BarentsWatch-samarbeidet vil flere nye sensorer etter hvert bli implementert som vil gi Tolletaten bedre oversikt over det maritime domenet og således være til hjelp ved utvelgelse av interessante fartøy for nærmere inspeksjon.

Sammenstilling av informasjon fra ulike sensorsystemer vil gi et bredere og mer presist informasjonssett (bilde) av objekter og bedre grunnlag for utvelgelse for nærmere kontroll. Teknologiområdet "utvidet virkelighet" muliggjør presentasjon av sensorinformasjon fra flere kilder uten å hindre egne sanser eller manuelle operasjoner. Dette vil kunne være et godt hjelpemiddel for tollerne for å kunne undersøke objekter som tungtransport eller konteinere.

6.2 Maskinlæring

Tolleaten vil kunne utnytte metoder fra maskinlæring i en rekke ulike anvendelser. I et helhetlig automatisert system for kontroll kan et opplært maskinsystem overta analysen av bilder fra røntgenskanningen (eventult supplert med annen sensorinformasjon) av pakkene. Dette kan frigi tid for tollerne til å fokusere på inspeksjonsoppdrag der det foreligger konkret mistanke. I noen situasjoner vil det kunne øke treffprosenten for objektutvelgelse ettersom maskinlæring i noen sammenhenger vil kunne integrere informasjon som mennesker ikke klarer å forholde seg til.

For å lykkes med maskinlæring er det en forutsetning at man har data som kan danne grunnlaget for trening av selve mønstergjenkjenningen. Data må kunne lagres som rådata kombinert med metadata som beskriver hva bildene viser. Et eksempel her kunne være å samle røntgenbilder tatt under inspeksjon av postpakker og sortere disse bildene i "positive" og "negative" funn av for eksempel piller. Metainformasjonen vil ganske enkelt være ulike kataloger for bilder med positive og negative funn. Man kan også tenke seg at å lagre mer kompleks metainformasjon så som pakkens vekt, pakkens volum, avsenderland, speditør osv. for å gi grunnlag for bedre utvelgelse.

Denne typen bilder og øvrig metainformasjon utgjør et verdifullt datasett som så vil kunne benyttes i trening av metoder basert på dyp læring. Datasettet bør lagres på et slikt format at det kan deles med andre lands tollmyndigheter og på en slik måte at data hentet fra andre etater og myndigheter lett kan integreres.

Gitt at slike datasett foreligger, er det neste skrittet å foreta trening og testing av maskinlæringssystemet. Dette er en prosess som krever spesialisert hardware og kompetanse, men denne typen ressurser er lett tilgjengelige i dag. Vi vurderer det som en enkel sak å gjennomføre treningen dersom data foreligger. Avhengig av kvalitet og mengde av data vil ytelsen for det endelige systemet variere og det er generelt vanskelig å forutsi hvordan den endelige ytelsen vil være. Vår anbefaling er å gjennomføre pilotprosjekter som kan gi en pekepinn om forventet endelige ytelse før store investeringer av tid og ressurser foretas.

Det siste trinnet i prosessen er naturligvis å ta de nye metodene i praktisk bruk. Dette fordrer at resultatene fra den automatiske analysen integreres i tollbetjentenes arbeidsflyt, noe som i seg selv kan være krevende.

6.3 Automatisering

Hvis ambisjonen er å opprettholde dagens kontrollvolum og arbeidsflyt er det begrenset hva automatisering kan tilføre. En viktig forutsetning for automatisering av en prosess (arbeidsflyt) er å strømlinjeforme den som en rekkefølge av enkle, avgrensede deloperasjoner på en optimalisert måte. Ved bygging av nye grensestasjoner og postmottak bør en slik strømlinjeforming av varestrømmen ligge til grunn, samt en ambisjon om å skanne alle transporter/pakker som passerer. Informasjon fra ulike sensorer i en systematisk rekkefølge, og særlig i kombinasjon med maskinlæring, kan gjøre utvelgelse av objekter for kontroll mer presis.

Roboter vil i fremtiden kunne utføre de fleste manuelle operasjoner. For Tolletaten vil utpakking (og pakking) av konteinere og lastebiler være en viktig forenkling og muliggjøre automatisering av kontrollprosessen og en vesentlig økning av kontrollvolumet. Med autonome farkoster vil sporing av mistenkelige transporter kunne gjennomføres.

6.4 IKT-trender

Nye nettverksprotokoller Det mørke nettet (dark web) er den del av internett som ikke er tilgjengelig uten spesiell programvare, konfigurering og autorisering. Det bidrar til styrking av demokratiske

idealer som ytringsfrihet og personvern. Legal bruk griper om seg, men også kriminell aktivitet beveger seg over på det mørke nettet fordi klassiske (IP-baserte) metoder for digital overvåkning og etterforskning er ubrukelige. Ifølge en undersøkelse er over halvparten av nettstedene på det mørke nettet opprettet for kriminell virksomhet; narkotikasmugling, ekstrempornografi og ulovlig pengeoverføring. Det er svært krevende for myndighetene å utvikle ny teknologi som kan identifisere nettsteder som er knyttet kriminalitet, men det satses betydelige ressurser. Denne utviklingen vil kunne få stor betydning for Tolletaten.

Nye metoder for kryptering og anonymisering av virksomhet på nettet er under utprøving. Blockchain-teknologien (utviklet for å skape tillit ved økonomiske transaksjoner) kan ha mange interessante anvendelser for vareflyt. Teknologien kan benyttes til å effektivisere globale varestrømmer, og hindre forfalskning av f.eks. tariffsatser.

Hvis blockchain-teknologien kombineres med sensorer som gjør det enkelt og billig å oversette fysisk bevegelse til data, kan avgift, tariffering og deklarering gjøres automatisk av objektene selv ved grensepassering. Dette ligger dog langt frem i tid og fordrer standardisering både av teknologi og lovverk.

Lagringsløsninger, analyseverktøy, infrastrukturkonsepter. I mange sammenhenger har man tilgang på store og komplekse datamengder (Big data) som ikke lar seg prosessere på en enkelt maskin til f.eks. et godt situasjonsbilde. Stadig mer data er tilgjengelig på nettet for å bygge slike situasjonsbilder. Det finnes mange typer stordatarammeverk, utviklet for ulike formål. De har som regel svært forskjellige egenskaper. Dette gjelder ikke minst hvordan de lagrer data. Stordatasystemer er ofte designet for å støtte en ganske spesifikk oppgave, f.eks. statistikk¬produksjon for prediktiv analyse.

Det er viktig å være oppmerksom på at disse systemene ikke er ment som arkiver, og vanligvis ikke er gode til å ta vare på metainformasjon. Man bør være forberedt på at et stordatasystem vil kunne redusere både gjenbruks- og arkiveringsverdien av de dataene man putter inn. Det vil derfor kunne være hensiktsmessig å tenke seg et annet regime for grunnlagsregistre.

Lenkede data. Internett er bygget opp av nettsider som lenker til hverandre og inneholder data. Dataene selv har imidlertid ingen nettadresse, og kan ikke lenke til hverandre. Idéen om lenkede data er at dataene selv skal kunne lenkes sammen. Det foreligger i dag ikke noen bred kommersiell eller industriell anvendelse, men mengden av open source-baserte lenkede data er økende. Et eksempel er geo- og kartinformasjon som ligger åpent tilgjengelig på internett. En GPS-posisjon kan lenke til et stedsnavn som igjen kan lenke til nyheter, historisk informasjon etc.

6.5 Anbefalinger

Det anbefales å se nærmere på om teknologier for utvidet virkelighet kan bidra til å gjøre operatøren mer effektiv i sitt arbeid. Dette innebærer i første omgang å foreslå egnet teknologi, herunder sensortype (optisk kamera, røntgen eller terahertz). I neste omgang bør det være en reell utprøving av teknologien som både ser på tekniske begrensninger til systemet og om det faktisk gjør arbeidet lettere og mer effektivt for operatøren.

Maskinlæring er en moden teknologi som vil kunne være nyttig for Tolletaten. Både ANPR og røntgen gir verdifull informasjon til operatøren. Ved å benytte maskinlæring kan sensorinformasjonen suppleres med annen tilgjengelig informasjon slik at treffsikkerheten blir større, trolig uten behov for mer personell. Det anbefales at slike muligheter studeres nærmere.

Systematisk lagring av data er en forutsetning for maskinlæring. Det bør derfor ses nærmere på hva behovet for lagring, prosessering og tilgjengeliggjøring av data vil være for at systemet skal kunne virke optimalt.

A Bidragsytere til rapporten

I tillegg til forfatterne av denne rapporten har vi fått bidrag og innspill fra andre forskere ved FFI. Stor takk til:

- Arthur van Rheenen for informasjon om TerraHertz,
- Robert MacDonald for informasjon om LINE ESM/NRD,
- Richard Olsen for innspill til kapittelet om satellitt,
- John Tørnes, som har skrevet om kjemiske detektorer og
- Børge Torvik, som har skrevet om radar.

Referanser

[1] A. Y. Pawar, D. D. Sonawane, K. B. Erande, og D. V. Derle, "Terahertz technology and its applications," *Drug Invention Today*, bind 5, nr. 2, s. 157–163, 2013.

[2] R. Otnes. (2012, mai) NILUS – An underwater acoustic sensor network demonstrator system. in Proc. 10th Int. Mine Warfare Symp., Monterey, CA, USA. Forsvarets forskningsinstitutt. [Online]. Tilgjengelig: http://www.ffi.no/no/Publikasjoner/Documents/NILUS2012.pdf

[3] Forsvarets Forskningsinstitutt, "VITEN - Teknologien Forsvaret trenger." Forsvarets Forskningsinstitutt, 2016.

[4] B. Torvik, "Investigation of non-cooperative target recognition of small and slow moving air targets in modern air defence surveillance radar," Dr.-avhandling, 2016.

[5] M. Aronsen, E. Messel, og K. Landmark, "Smarte agenter i maritim overvåkning (BEGRENSET)," Forvarets forskningsinstitutt, Kjeller, FFI-rapport 2015/00054, mar. 2015.

[6] A. C. Jenssen, "Metoder for avviksdeteksjon i maritim overvåkning," Forvarets forskningsinstitutt, Kjeller, FFI-rapport 2014/xxxxx, jan. 2014.

[7] R. O. Duda, P. E. Hart, og D. G. Stork, *Pattern Classification*, 2. utg. New York: Wiley-Interscience, 2001.

[8] D. Moore og T. Rid, "Cryptopolitik and the darknet," *Survival*, bind 58, nr. 1, s. 7–38, 2016.

[9] S. D. Vogt, "The digital underworld: Combating crime on the dark web in the modern era," *Santa Clara Journal of Internatiojnal Law*, bind 115, nr. 1, 2017.

[10] K. Landmark, E. Messel, og A. Ommundsen, "Nettverkstjenester for prosessering av stedfestet informasjon –implementasjon og anvendelse," Forvarets forskningsinstitutt, Kjeller, FFI-rapport 2014/01075, sep. 2014.

[11] OGC. Open Geospatial Consortium. [Online]. Tilgjengelig: http://www.opengeospatial.org/

[12] P. Schut (ed.). (2007, jun.) OpenGIS Web Processing Service. Open Geospatial Consortium. [Online]. Tilgjengelig: http://www.opengeospatial.org/standards/wps

[13] A. Whiteside (ed.). (2007, feb.) OGC Web Services Common Specification. Open Geospatial Consortium. [Online]. Tilgjengelig: http://portal.opengeospatial.org/files/?artifact_id=20040

[14] S. Tillman (red.), "OGC OWS-7 Motion Video Change Detection," Open Geospatial Consortium, OGC Engineering Report OGC 10-036r2, aug. 2010.

[15] B. Clarke, E. Fokoue, og H. H. Zhang, *Principles and Theory for Data Mining and Machine Learning*. New York: Springer, 2009.

[16] V. Chandola, A. Banerjee, og V. Kumar, "Anomaly detection: A survey," *ACM Computing Surveys*, bind 41, nr. 3, s. 15:2–15:58, jul. 2009.

[17] A. H. S. Solberg, "Remote sensing of oil spill polution," *Proceedings of the IEEE*, bind 100, nr. 10, s. 2931–2945, okt. 2012.

Forkortelser

AIS Automatic Identification System
ANPR Automatic Number Plate Recognition
API application programming interface
AR Augmented Reality
CBR Chemical, biological and radiological
CD&E Concept Development and Experimentation
CT Computertomografi
DARPA Defense Advanced Research Projects Agency
EO Elektro-optisk
ESA European Space Agency
ESM Elektroniske Støttetiltak
EU European Union
FBI Federal Bureau of Investigation
FFI Forsvarets forskningsinstitutt
FOH Forsvarets operative hovedkvarter
GEOMETOC geografi, meteorologi og oseanografi
GHz GigaHertz
GPS Global Positioning System
HF High Frequency
IaaS Infrastructure as a Service
ICAO International Civil Aviation Organization
ID Identifikasjon
IKT Informasjons- og kommunikasjonsteknologi
IMO International Maritime Organization
IMS Ionemobilitetsspektrometri
IR Infrarød
IP Internettprotokoll
IoT Tingenes internett
IT Informasjonsteknologi
I2P The Invisible Internet Project
kHz kiloHertz
LF Low Frequency
LIBS Laser-Induced Breakdown Spectroscopy
LINE Liten navigasjonsradar ESM
NIR Near Infrared
MEMS Micro Eletro Mechanical Systems
MHz MegaHertz

MR Magnetisk Resonans
NATO North Atlantic Treaty Organization
NIT Network Investigative Technique
NGI Next Generation Identification System
NILUS Networked Intelligent Underwater Sensors
NRD Navigasjonsradardetektor
OGC Open Geospatial Consortium
OSTN Open Secure Telephony Network
OTR Off-the-Record Messaging
PaaS Platform as a Service
PFNA pulset høyenergi nøytronstråling
POL Pattern of life
RDF Resource Description Framework
RFID Radio Frequenecy IDentification
RCS Radar Cross Section
SAR synthetic aperture radar
SaaS Software as a Service
SIS Schengen Information System
SORS Spatially Offset Raman Spectroscopy
SOS Sensor Observation Service
SVM Support Vector maskiner
TIC Toxic industrial chemicals
TOR The onion router
UAV Unmanned aerial vehicle
UHF Ultra High Frequency
VIS Visa Information System
VR Virtual Reality
WPS Web Processing Service
XML Extended Markup Language
ZRTP Zimmermann Real-Time Transport Protocol

About FFI

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

FFI's MISSION

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

FFI's VISION

FFI turns knowledge and ideas into an efficient defence.

FFI's CHARACTERISTICS

Creative, daring, broad-minded and responsible.

Om FFI

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

FFIs FORMÅL

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

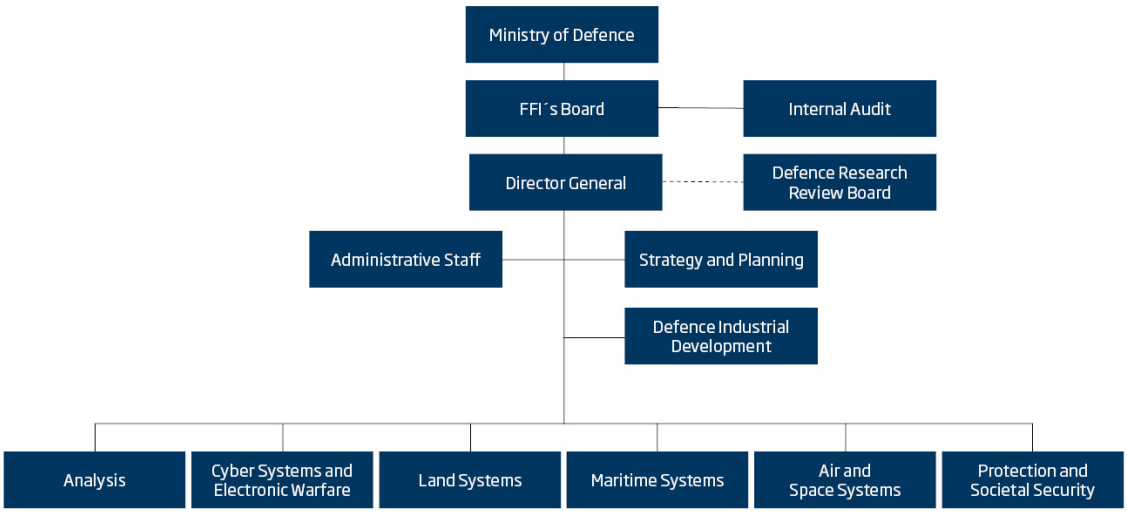
FFIs VISJON

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs VERDIER

Skapende, drivende, vidsynt og ansvarlig.

FFI's organisation



Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

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

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

Office address:
Instituttveien 20
N-2007 Kjeller

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

FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment