FFI Forsvarets forskningsinstitutt

22/00631

FFI-RAPPORT

Utviklingen av nye IoT-baserte infrastrukturer i samfunnet

– utfordringer for nasjonal sikkerhet

(revidert rapport)

Bodil Hvesser Farsund
Torkjel Søndrol
Kjell Olav Nystuen
Lars Hornfelt
Stig Rune Sellevåg
Vinh Pham

Utviklingen av nye IoT-baserte infrastrukturer i samfunnet
– utfordringer for nasjonal sikkerhet

(revidert rapport)

Bodil Hvesser Farsund
Torkjel Søndrol
Kjell Olav Nystuen
Lars Hornfelt
Stig Rune Sellevåg
Vinh Pham

Forsvarets forskningsinstitutt (FFI) 7. mars 2022

Emneord
Tingenes internett (IoT)
Kritisk infrastruktur
Nasjonal sikkerhet

FFI-rapport
22/00631

Prosjektnummer
551801

Elektronisk ISBN
978-82-464-3398-1

Engelsk tittel
The evolution of new IoT-based infrastructures in the society – challenges for the national security

Godkjennere
Raymond Haakseth, *forskningsleder*
Ronny Windvik, *forskningssjef*

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur

Sammendrag

Bakgrunnen for denne studien er at man forventer en stor vekst i bruk av *Internet of Things* (IoT) i hele samfunnet, ikke minst i forbindelse med at 5G bygges ut. IoT vil i økende grad bli brukt til å underholde oss, gjøre hverdagen vår enklere, byer mer ressurseffektive, industribedrifter mer kostnadseffektive og til å gi oss bedre offentlige tjenester. Det kan også gi oss et bedre forsvar.

IoT er ofte komplekse systemer og omfatter som regel flere ulike teknologier som trådløs kommunikasjon, skytjenester, stordata og kunstig intelligens. Med økt bruk av IoT vil vi få helt nye infrastrukturer, infrastrukturene som allerede finnes vil få nye egenskaper, og det vil være vanskelig å vite hvilke infrastrukturer som er kritiske.

Økt bruk av IoT vil gi mange fordeler, men det vil også utfordre nasjonale sikkerhetsinteresser. Vi har gjennom arbeidet med denne rapporten identifisert tre grunnleggende utfordringer. Disse har vi kalt *økt innsamling av data, større angrepsflate* og *mer komplekse infrastrukturer.*

IoT-systemene samler ofte inn detaljerte data fra deres brukere og/eller miljø, og disse dataene havner ofte i utlandet. Tester vi har utført på noen tilfeldige IoT-produkter rettet mot forbrukermarkedet bekrefter dette. Det er vanskelig å beskytte seg mot denne datainnsamlingen, og det er en opplagt utfordring både når det gjelder etterretningstrusselen og personvern.

Siden IoT-systemene omfatter flere ulike teknologier og komponenter, som kan ligge i ulike geografiske områder, vil disse systemene ha en stor angrepsflate. Dette gir økt sårbarhet mot både konfidensialitets-, integritets- og tilgjengelighetsangrep.

Disse IoT-systemene vil inngå i infrastrukturer som vil være svært komplekse. Kompleksiteten er blant annet knyttet til at disse infrastrukturene ofte er svært dynamiske og at de innehar mange interne og eksterne avhengigheter. Dette vil gi en stor sårbarhet og er den største utfordringen vi ser med økt bruk av IoT.

Utviklingen vi ser her er drevet av globale kommersielle interesser det er vanskelig å begrense eller styre. For å kunne møte utfordringene økt bruk av IoT medfører, mener vi det er to områder som peker seg ut som spesielt viktig. Det første er å utvikle metoder for å kunne vurdere risiko av komplekse infrastrukturer. Hendelseshåndtering og vurdering av ulike forebyggende tiltak knyttet til kritiske infrastrukturer og nasjonal sikkerhet krever et oppdatert og helhetlig risikobilde. Et slikt bilde må evne å innlemme kompleksiteten og beskrive den usikkerheten som opplagt er tilstede. I dag mangler man tilstrekkelig kunnskap og metoder for å utvikle dette. Det andre området vi ser at er viktig omhandler kontinuerlig kunnskapsutvikling og -forvaltning, og dette innenfor mange fagfelt. Her vil det være helt essensielt med en metode for å kunne sette denne kunnskapen i system.

Summary

This study was initiated because of the expected increase of Internet of Things (IoT) in our society, which will accelerate with the 5G deployment. IoT will be used to entertain us, make our everyday life more simple, cities more resource efficient, industries more cost efficient, and give us better public services. It may also give us an improved national defense.

IoT are often complex systems consisting of multiple different technologies, such as wireless protocols, cloud services, big data and artificial intelligence. The increased use of IoT will result in new infrastructures, provide new abilities and characteristics to existing infrastructures, and it will be difficult to tell which of the infrastructures are critical.

Increased IoT usage will provide many advantages, but it will also challenge our national security interests. We have through this research identified three basic challenges named *increased data collection, larger attack surfaces* and *more complex infrastructures.*

IoT systems often gather detailed data from their users and/or environment, and these data are often sent abroad. Tests performed by us on some arbitrary consumer IoT products confirm this. It is difficult for the end user to protect herself from this data gathering, and it is an obvious challenge regarding both foreign intelligence and privacy.

As IoT systems consists of multiple technologies and components, which may be located at different geographical areas, they will have a large attack surface. This increases its vulnerability regarding attacks on confidentiality, integrity and availability.

IoT systems will be part of very complex infrastructures. This complexity is because of all the dependencies between the infrastructures, and the fact that they are dynamic. This makes them vulnerable, and is what we consider the greatest challenge with the increased IoT usage.

As we see it, the development is driven by global commercial interests that are difficult to control. We have identified two important areas when it comes to meeting the challenges caused by the increased IoT usage. First is establishing methods for risk assessment of complex infrastructures. It is necessary to have an updated and correct risk picture when doing event handling and assessing various preventing measures for critical infrastructure and national safety. This must include the complexity and describe the uncertainty that obviously will be present. We do lack the necessary methods and knowledge to perform such risk pictures today. The second area relates to continuously develop and maintain knowledge within multiple disciplines. It will be essential to have methods for converting this knowledge into practice.

Innhold

1 Innledning

"*The internet is no longer a web that we connect to. Instead, it's a computerized, networked, and interconnected world that we live in. This is the future, and what we're calling the Internet of Things.*

Broadly speaking, the Internet of Things has three parts. There are the sensors that collect data about us and our environment: smart thermostats, street and highway sensors, and those ubiquitous smartphones with their motion sensors and GPS location receivers. Then there are the "smarts" that figure out what the data means and what to do about it. This includes all the computer processors on these devices and - increasingly - in the cloud, as well as the memory that stores all of this information. And finally, there are the actuators that affect our environment. The point of a smart thermostat isn't to record the temperature; it's to control the furnace and the air conditioner. Driverless cars collect data about the road and the environment to steer themselves safely to their destinations.

You can think of the sensors as the eyes and ears of the internet. You can think of the actuators as the hands and feet of the internet. And you can think of the stuff in the middle as the brain. We are building an internet that senses, thinks, and act."

Bruce Schneier (2017)[1]

Internet of Things (IoT) refererer til fysiske enheter som er koblet til internett. Disse «tingene» kan være alt fra industrielle roboter, private og offentlige overvåkningskameraer og biler til barneleker og lyspærer.

Bakgrunnen for denne rapporten er at man forventer en stor vekst i bruk av IoT i hele samfunnet, ikke minst i forbindelse med at 5G bygges ut. For eksempel omhandler nesten alle trendene som beskrives i *Gartner Top 10 Strategic Technology Trends for 2020*[2] IoT enten direkte eller indirekte. IoT vil i økende grad bli brukt til å underholde oss, gjøre hverdagen vår enklere (smarthjem), byer mer ressurseffektive (smartbyer), industribedrifter mer kostnadseffektive (Industri 4.0), og til å gi oss bedre offentlige tjenester som for eksempel helsetjenester (e-helse). Det kan også gi oss et bedre forsvar.

Disse IoT-systemene består egentlig av mange ulike teknologier. De består av sensorer og/eller aktuatorer, trådløs kommunikasjon, brukergrensesnitt, og som regel også skytjenester, stordata og kunstig intelligens. Dette gir oss «smarte» produkter som gir rask respons i den fysiske verden, og som gjør gapet mellom den fysiske og den logiske verden mindre. Sistnevnte er ofte hensiktsmessig i forhold til tiltenkt bruk, men gjør at tilsiktede og utilsiktede hendelser i

[1] https://www.schneier.com/blog/archives/2017/02/security_and_th.html [sist besøkt 27.04.20].
[2] https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2020/ [sist besøkt 07.05.20].

cyberdomenet kan få store konsekvenser i den fysiske verden. IoT gjør det mulig for en angriper å gjøre umiddelbar fysisk skade i en annen del av verden enn der han befinner seg.

Hensikten med dette arbeidet har vært å utvikle et fundament for forståelse av utviklingen av nye IoT-baserte infrastrukturer i samfunnet og hvordan denne utviklingen vil kunne påvirke nasjonal sikkerhet. Hensikten med arbeidet er dermed å etablere et kunnskapsgrunnlag for fremtidig forvaltning av nasjonal sikkerhet på området, og også gi innspill til strategigrunnlag for hvordan samfunnet skal kunne møte potensielle sikkerhetsutfordringer. IoT-baserte infrastrukturer er et omfattende tema. Denne rapporten dekker de områdene vi mener er viktige når det gjelder denne utviklingens betydning for nasjonal sikkerhet.

Rapporten starter i kapittel 2 med å beskrive hva vi mener med IoT, deretter blir de grunnleggende IoT-teknologiene beskrevet i kapittel 3, mens kapittel 4 beskriver noen av sårbarhetene som kan finnes i IoT-systemer. De nye IoT-baserte infrastrukturene har noen egenskaper som blir skissert i kapittel 5, mens vi beskriver noen utvalgte infrastrukturer og bruk av IoT i kapittel 6. I kapittel 7 gjengis noen observasjoner basert på tester vi har gjort på vanlig forbruker-IoT, mens vi i kapittel 8 oppsummerer hvilke muligheter og utfordringer økt bruk av IoT vil ha for nasjonal sikkerhet. Tilslutt i rapporten diskuteres hvordan utviklingen med økt bruk av IoT kan møtes av forvaltningen.

Dette er en revidert utgave av en tidligere rapport[3].

2 Hva er IoT?

Det finnes ikke noen omforent definisjon av IoT, men et eksempel på en definisjon er følgende: «Samhandling via internett mellom datamaskiner som er innebygd i dagligdagse enheter, som gjør dem i stand til å sende og motta data».[4]

Som nevnt innledningsvis er det imidlertid flere teknologier som er sentrale i det vi i dag omtaler som IoT. Siden IoT består av flere ulike komponenter og teknologier, har vi i dette arbeidet valgt å bruke begrepet «IoT-system». I dette kapitelet beskriver vi hva et slikt IoT-system kan bestå av, og det vil da være dette vi refererer til senere i rapporten.

Et IoT-system kan bestå av følgende komponenter:

[3] Farsund, B. H.; Søndrol, T.; Nystuen, K. O.; Hornfelt, L.; Sellevåg, S. R.; Pham, V.; *Utviklingen av nye IoT-baserte infrastrukturer i samfunnet – utfordringer for nasjonal sikkerhet* (FFI-rapport 20/01745 [UNNTATT OFFENTLIGHET]), Forsvarets forskningsinstitutt (2020).
[4] https://www.lexico.com/definition/internet_of_things [sist besøkt 07.05.20].

- Én eller flere **sensorer** – dette kan for eksempel være temperaturmålere, avstandsmålere eller kameraer.

- Én eller flere **aktuatorer** – dette kan for eksempel være døråpnere, brytere/releer eller varsellys.

- **Lokal styringsenhet/hub** – her ligger det logikk knyttet til sensoren(e) og/eller aktuatoren(e). Den kan være bygd inn i sensoren, og hvis det foregår kryptering vil dette typisk gjøres her. Vi ser en trend i at funksjonalitet flyttes herfra til et sentralt grense-snitt i skyen.

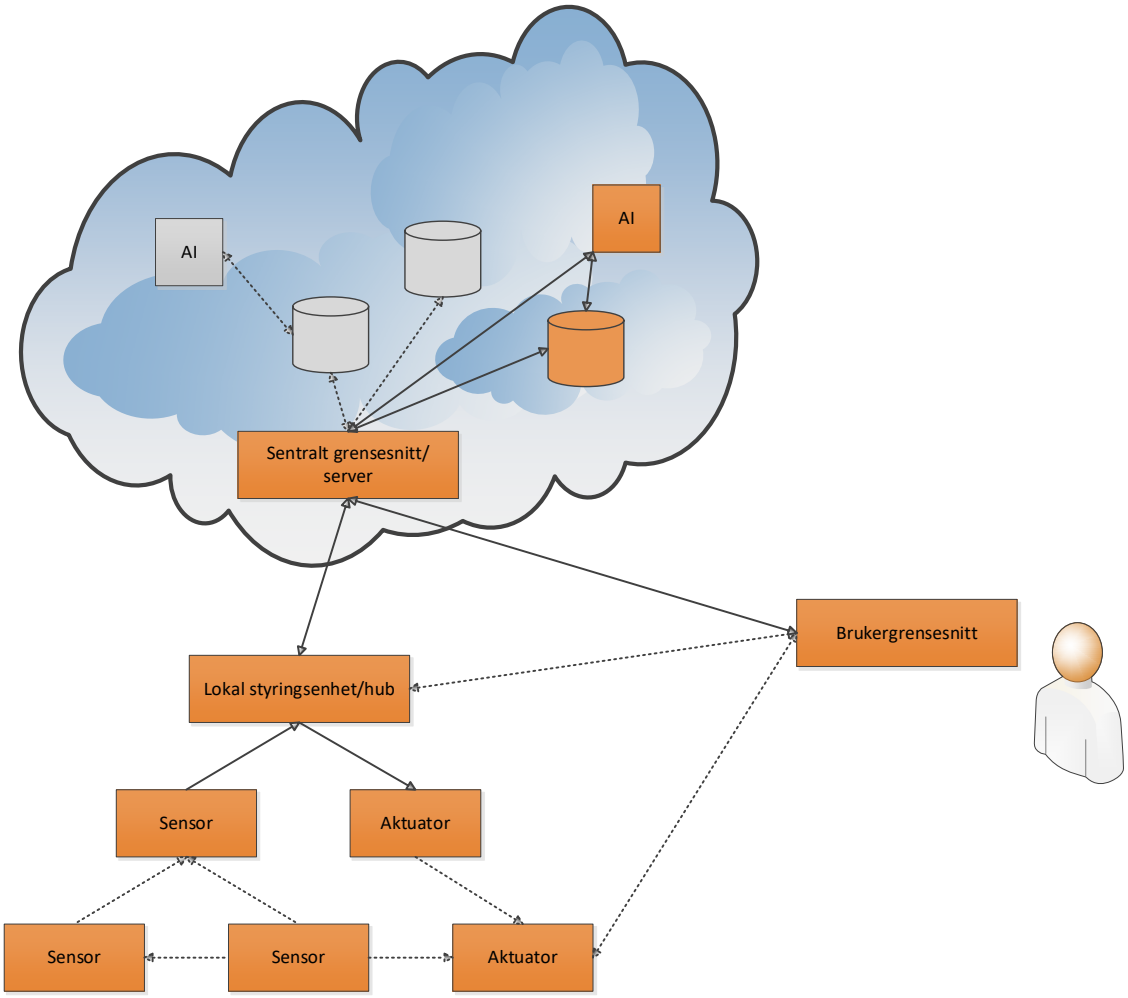
- **Brukergrensesnitt** – gjør det mulig for brukerne å samhandle med IoT-systemet. Her kan sensorinformasjon vises og/eller kommandoer gis til aktuatoren(e). Grensesnittet kan for eksempel være en app på en mobiltelefon eller en terminal på et større Supervisory Control and Data Acquisition (SCADA)-system. Dette kommuniserer i utgangspunktet med lokal styringsenhet, men vi ser en økende grad av integrasjon mot sentralt grensesnitt i skyen.

- **Sentralt grensesnitt** – styrer kommunikasjonen mellom bruker(e), sensor(er) og/eller aktuator(er) og tilhørende skytjenester. Dette ligger nå stort sett i skyen, og utenfor brukers kontroll.

- **Skytjenester** – dette er knyttet til IoT-systemets funksjonalitet. For mange IoT-systemer er det her data samles og lagres, og det er her kontrollen til systemet ligger. Innsamlede data kan imidlertid også brukes i nye tjenester knyttet til eventuelle 3. parter.

- **Kommunikasjon** – sørger for konnektivitet mellom sensor(er) og/eller aktuator(er) og den lokale styringsenheten/huben, dersom disse ikke ligger integrert i IoT-enheten. Videre vil det være behov for kommunikasjon mellom lokal styringsenhet og sentralt grensesnitt/server, og mellom sentralt grensesnitt/server og brukergrensesnittet.

Et IoT-system er illustrert i Figur 2.1.



Figur 2.1 Ulike komponenter i et IoT-system.

De oransje boksene illustrerer de komponentene av IoT-systemet som ofte er kjent for bruker, og som er en del av tjenesten som brukes. For å illustrere at dataene som samles inn fra sensorer og brukergrensesnitt kan brukes videre i andre tjenester, har vi vist dette som grå bokser. Dette er ikke nødvendigvis kjent for bruker.

Noen ganger brukes også begrepet Industriell IoT (IIoT). IIoT brukes der fokuset er på å koble sammen sensorer og aktuatorer i industrier som for eksempel olje og gass, kraftproduksjon og helsevesen. Det er ventet at disse også vil bruke skytjenester og kunstig intelligens, men at risikotenkningen vil være annerledes. Her vil systemfeil kunne få større følger enn ved feil med forbruker-IoT.

3 Grunnleggende IoT-teknologier

Som nevnt i innledningen er flere teknologier sentrale i det vi i dag ser på som et IoT-system. Spesielt gjelder dette trådløs kommunikasjon, skyteknologi, stordata og kunstig intelligens. Her har vi kort beskrevet disse teknologiene.

3.1 Trådløs kommunikasjonsteknologi

For å realisere smarte hjem, byer og industri ser man for seg høy tetthet av sensorer og aktuatorer som kommuniserer trådløst. Denne kommunikasjonen mellom sensorene/aktuatorene og styringsenheten i et IoT-system må være tilpasset disse sensorenes/aktuatorenes behov. Dette er preget av at enhetene gjerne har begrenset med batteri, lite minne og lite prosessorkraft, samt at infrastrukturene må kunne håndtere svært mange enheter av denne typen. Det eksisterer i dag flere ulike trådløse kommunikasjonsteknologier tilpasset dette formålet, samt at 5G utvikles spesielt for dette. Vi beskriver noen utvalgte protokoller for slik kommunikasjon nedenfor.

I dette arbeidet fokuserer vi på protokoller for trådløs kommunikasjon, i tillegg benyttes det gjerne også meldingsprotokoller for å fasilitere kommunikasjonen mellom IoT-enhetene. Et populært eksempel på dette er Message Queuing Telemetry Transport (MQTT) som følger en *publish-subscribe*-metodikk. Enheter som ønsker å motta gitte typer meldinger vil registrere seg som *subscribers* hos en *broker*, og blir så informert når denne type meldinger blir publisert av en *publisher.* Extensible Messaging and Presence Protocol (XMPP) er en alternativ IP-basert meldingsprotokoll med støtte for autentisering og aksesskontroll.

3.1.1 Eksisterende kommunikasjonsteknologier

Når man ser på protokollene som benyttes for trådløs kommunikasjon mellom sensorene/aktuatorene og styringsenheten i et IoT-system er det hensiktsmessig å dele IoT-systemene inn i tre ulike kategorier avhengig av om sensorene/aktuatorene benytter eksisterende kommunikasjonsinfrastruktur, om de kommuniserer direkte med en mobiltelefon eller om de kommuniserer via en hub eller gateway.

Konfidensialitets- og integritetsbeskyttelse skjer typisk også gjennom disse protokollene, men den begrensede kapasiteten til IoT-komponentene legger føringer på de kryptografiske protokollene. Et tilstrekkelig sikret IoT-system kan man allikevel forvente legger til rette for en registrering og autorisering av IoT-sensorene og aktuatorene før de kan begynne å kommunisere. Dette kan gjøres ved hjelp av sertifikater, eller en form for gjensidig autentisering og nøkkelutveksling. Advanced Encryption Standard (AES) er en svært utbredt protokoll for symmetrisk kryptering – også innenfor IoT. For å sikre konfidensialiteten kan trafikken krypteres med AES i Counter mode (AES-CTR), og den kan integritetsbeskyttes ved å bruke

AES i Cipher Block Chaining mode (AES-CBC). Ved å kombinere AES-CTR og AES-CBC kan man dermed oppnå både konfidensialitets- og integritetsbeskyttelse.[5]

3.1.1.1 Protokoller som benytter eksisterende infrastruktur

Protokoller som benytter eksisterende infrastruktur brukes typisk av mobile enheter og ting som trenger lang rekkevidde, som biler eller målestasjoner for vær og flom. Disse kan ha et SIM-kort eller en hel mobiltelefon innebygd, og dermed bruke mobilnettet direkte. Eksempelvis har Onstar[6] et eget mobilabonnement for bilene utstyret deres sitter i, mens Veivesenet bruker Telenor sitt NB-IoT nett (se under) for sitt nye flomvarslingssystem.

Fellestrekket for disse protokollene er gjerne at de er LPWAN-baserte (Low-Power Wide Area Network), som vil si at de har lavt strømforbruk og båndbredde for å operere over avstander på flere kilometer. 5G er også et eksempel på en egnet infrastruktur for IoT, og grunnet den store betydningen som vi antar at den får i fremtiden, er den beskrevet mer detaljert i kapittel 3.1.2.

Sigfox er en fransk tjenestetilbyder som ruller ut et globalt 0G-nettverk for IoT-enheter. Den benytter en ultra-narrowband LPWAN-protokoll som opererer på 868MHz i Europa, og er optimalisert for lang rekkevidde (inntil 30 km) og lav båndbredde. Siden sensorene som benytter protokollen må lisensieres av Sigfox ser vi ikke at protokollen er svært utbredt i dag sammenlignet med alternativene.

Wirepas er en ren programvarepesifikasjon som lisensieres for bruk på standard SoC-enheter (System on a Chip). Dette brukes blant annet i Aidon sine AMS-strømmålere (Avansert Måle- og Styringssystemer) som benyttes av Hafslund Energi i Oslo-området. Her danner de et maskenettverk (*mesh network*) med en node koblet til internett.

NB-IoT (NarrowBand-IoT) og **LTE-M** (LTE Cat M1) er eksempler på LPWAN-protokoller som er avhengig av en eksisterende 4G-mobilinfrastruktur. LTE-M har høyere båndbredde og mindre rekkevidde enn NB-IoT.

3.1.1.2 Protokoller for kommunikasjon direkte med en mobiltelefon

Protokoller som kommuniserer direkte med en mobiltelefon blir brukt av enheter som hodetelefoner, smartklokker og mikrofoner som bruker kortholdsradio. Disse enhetene kommuniserer primært med mobiltelefon, og en eventuell kobling mot internett skjer via denne. Bluetooth er en populær protokoll til dette formålet.

Bluetooth opererer på 2,4GHz og har en rekkevidde på 1 – 20 meter. Bluetooth Low Energy er en versjon av protokollen med mindre effekt, og er designet spesielt for IoT-produkter.

[5] Raja, S. P.; Sampradeepraj, T.; *Internet of Things: a research-oriented introductory* (2018).
[6] https://www.onstar.com/us/en/home/ [sist besøkt 02.06.20].

Wi-Fi opererer på 2,4GHz og 5GHz. Denne protokollen brukes mye til videooverføring fra droner, og vi har sett den i ringeklokker.

3.1.1.3 Protokoller for kommunikasjon via en hub eller WiFi-gateway.

Små billige IoT-enheter som smarthjemprodukter bruker WiFi og rimelige nær-kommunikasjonsprotokoller av økonomiske og administrative årsaker. Dette innebærer gjerne at IoT-utstyret kommuniserer med en lokal hub, og derfor ikke er direkte avhengig av en eksisterende infrastruktur, som tilfellet er med mobiltelefoniprotokollene. Det finnes leverandører av hub-er som benytter veldokumenterte grensesnitt og støtter mange ulike protokoller, slik at man ikke må ha én hub for hver IoT-leverandør. Typiske eksempler er *Samsung Smart Hub* eller *Google Home Nest*. Disse er utstyrt med Ethernet-tilkopling og mikrofon, og støtter tilleggstjenester som *Amazon Alexa* eller *Google Assistant*.

Zigbee opererer på 2,4GHz og har en rekkevidde på opptil 100 meter frisikt. Protokollen er ment å være et enklere og billigere alternativ til Bluetooth, og benyttes ofte av enheter som inngår i smarthussystemer. Protokollen støtter også at IoT-enhetene kommuniserer i maskenettverk for å oppnå økt rekkevidde.

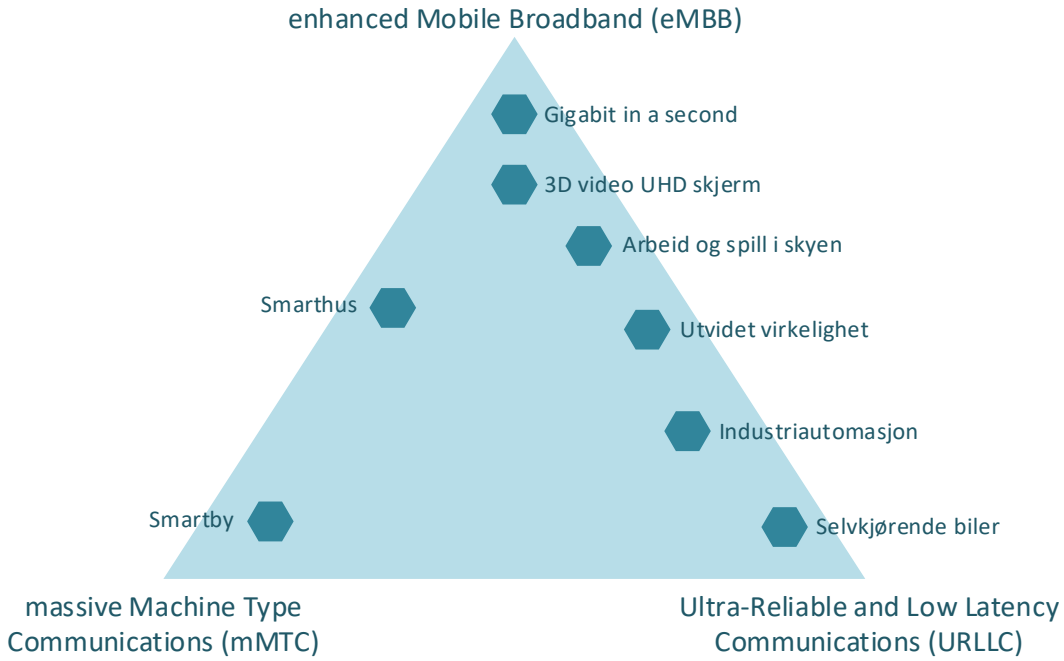
Z-Wave opererer på 800 – 900MHz og har en rekkevidde på opptil 100 meter. Den benyttes i smarthussystemer av utstyr som for eksempel lysbrytere, termostater, dørlåser og garasjeport-åpnere. Den støtter også maskenettverk.

LoRaWAN (Long Range Wide Area Network) er et eksempel på en LPWAN-protokoll designet for lange rekkevidder og lave båndbredder. Den benytter seg av Semtec sin proprietære LoRa-protokoll og opererer på 868MHz i Europa. Den benyttes gjerne av utstyr som inngår i smartbysatsninger. I tillegg til at bruker kan sette opp en egen gateway, finnes det også globale og regionale LoRaWAN-nettverk.[7, 8, 9]

3.1.2 5G

5G er neste generasjons mobilnettverk. Mens fokuset ved utviklingen av 3G og 4G var på å gi brukerne høyere båndbredde, har det ved utviklingen av 5G også vært stort fokus på infra-struktur og tjenester som skal kunne støtte det hypertilkoblede «smarte» samfunnet og nye industrielle behov. Her trenger man foruten det klassiske behovet for høyere båndbredde (enhanced Mobile Broadband, eMBB), også å kunne støtte høy tetthet av oppkoblede enheter (massive Machine Type Communications, mMTC), samt oppkoblede enheter som krever høy pålitelighet og svært lav forsinkelse (Ultra-Reliable and Low Latency Communications, URLLC). Den fysiske infrastrukturen i 5G skal derfor kunne støtte tjenester med svært ulike behov for tjenestekvalitet, som vist i Figur 3.1.

[7] https://www.thethingsnetwork.org/ [sist besøkt 02.06.20].
[8] https://www.stavanger.kommune.no/samfunnsutvikling/smartbyen-stavanger/lorawan---sensornettverk/ [sist besøkt 02.06.20].
[9] https://www.altibox.no/IOT/ [sist besøkt 17.06.20].



Figur 3.1 Ulike bruksområder for 5G.

mMTC fokuserer på å tilby kommunikasjon til enheter med høy tetthet, og vil derfor være en viktig teknologi for utviklingen av IoT. Kravene som settes til 5G er at teknologien skal støtte 1 million enheter per kvadratkilometer, og at enhetene skal ha en batterilevetid på ti år. Det er her snakk om enkle enheter med et begrenset kommunikasjonsbehov. Eksempler på anvendelsesområder vil være innen logistikk, landbruk og smartby.

URLLC har andre krav til tjenestekvalitet enn mMTC. Her er fokuset høy pålitelighet, det vil si veldig lavt pakketap og lav forsinkelse, ned mot 1 ms, mens relativt høy båndbredde og god sikkerhet også vil være viktig. Viktige applikasjoner innen URLLC inkluderer autonomi, slik som selvkjørende biler, helsetjenester, mange industrielle prosesser, samt at teknologien antakelig også vil omfatte mange samfunnskritiske funksjoner.

Både mMTC og URLLC vil være viktige teknologier for utviklingen av IoT, men hverken mMTC eller URLLC er ferdig standardisert. Krav til lavt energiforbruk i mMTC og lav forsinkelse i URLLC vil imidlertid påvirke valget av sikkerhetsalgoritmer og prosedyrer.

5G vil benytte flere frekvenser, fra noen hundre MHz til noen titalls GHz.

Selv om den fysiske infrastrukturen i 5G-nettverket skal kunne støtte tjenester med svært ulike krav, vil nettverket ikke kunne tilby dette til alle tjenestene samtidig. For å håndtere at ulik trafikk skal tilbys ulik tjenestekvalitet trenger man helt nye måter å skru sammen nettverkene på. Nettverksfunksjonene vil bli virtualiserte, og kan så bli kombinert for å lage ulike

virtuelle/logiske nettverk, også kalt «skivedelte nett» (*network slicing*). Her vil hver enkelt «skive» dekke ulike behov for tjenestekvalitet som forsinkelse, tetthet av enheter og så videre. Virtualiserte nettverksfunksjoner og skivedelte nett gjør det enklere for operatørene å gjøre oppdateringer og tilpasse nettverkene til løpende behov, samt at dette vil gjøre det enklere ved utrulling av nye tjenester.

Det er ventet at enkelte, for eksempel store bedrifter, vil benytte egne private 5G-nettverk[10, 11]. Slike private nettverk kan enten være helt frittstående eller de kan være koblet til en offentlig 5G-tilbyder. Motivasjonen for dette kan være at de ønsker sine egne sikkerhetsløsninger, som å ha kontroll på egne data, mens en annen grunn kan være at de er avhengig av svært lave forsinkelser.

3.2 Skytjenester

Med skytjenester mener vi i denne rapporten ulike datatjenester en kan få tilgang til ved hjelp av internett og eksterne datasentre. Disse datatjenestene kan inkludere alt fra datalagring og –prosessering til ulike former for programvare. En sky er egentlig et stort og sammenkoblet nettverk av kraftfulle servere, plassert i ulike datasentre, som utfører tjenester for personer og virksomheter. Noen av de største aktørene i verden i dag er Amazon Web Services, Microsoft Azure og Google Cloud.[12]

En klar fordel ved bruk av skytjenester er at de er utviklet med tanke på dynamisk skalering. Det betyr at kundene hele tiden kan få dekket sitt behov, selv når dette endres, og at de i utgangspunktet ikke trenger betale for mer enn de bruker. En annen fordel er mobilitet – det vil si at kundene alltid kan få tilgang til skytjenestene så lenge de har internettforbindelse. Ved å bruke skytjenester slipper også kundene mye av drifts- og vedlikeholdsoppgavene på systemene som brukes. Det å sette dette bort til en profesjonell skytjenesteleverandør, vil som regel føre til økt sikkerhet.

Det er vanlig å dele skytjenester opp i tre ulike tjenestemodeller:

- **Programvare som tjeneste** (*Software as a Service – SaaS*) er en modell hvor skyleverandøren leverer programvareapplikasjonen(e) og den underliggende infrastrukturen. Skyleverandøren håndterer også vedlikehold som sikkerhets- og programvareoppdateringer. Kunden får tilgang til applikasjonen(e) over internett, vanligvis via et web-grensesnitt på telefonen eller en PC. Typisk eksempel på en slik tjeneste er Microsoft Office 365.

[10] https://www.networkworld.com/article/3319176/private-5g-networks-are-coming.html [sist besøkt 13.05.20].
[11] https://www.insidetelecom.no/artikler/snart-klart-for-nye-tjenester-pa-5g/492108?utm_source=newsletter-insidedaily&utm_medium=email&utm_campaign=newsletter-2020-05-14 [sist besøkt 14.05.200].
[12] https://www.zdnet.com/article/the-top-cloud-providers-of-2020-aws-microsoft-azure-google-cloud-hybrid-saas/ [sist besøkt 08.05.20].

- **Plattform som tjeneste** (*Platform as a Service – PaaS*), er en modell hvor skytjenesteleverandøren tilbyr et miljø for å utvikle, teste, levere og vedlikeholde programvareapplikasjoner. Denne tjenesten brukes typisk av utviklere for å kunne lage web- eller mobile applikasjoner raskt, uten å måtte tenke på den underliggende infrastrukturen som servere, lagring, nettverk og databaser. Et eksempel på en skyleverandør som tilbyr en slik tjeneste er Oracle Cloud.

- **Infrastruktur som tjeneste** (*Infrastructure as a Service – IaaS*), er en modell hvor kunden leier IT-infrastruktur som servere, virtuelle maskiner, lagringsmuligheter, nettverk og operativsystem. Eksempler på skyleverandører som leverer en slik tjeneste er Microsoft Azure og Amazon Web Services.

Skytjenester kan i tillegg deles inn i følgende ulike leveransemodeller:

- **Allmenn sky** (*public cloud*) hvor skytjenesteleverandøren gjør tjenestene tilgjengelig for alle.

- **Privat sky** (*private cloud*) hvor skytjenesteleverandøren gjør tjenestene tilgjengelige kun for en gitt kunde eller kundegruppe. Denne leveransemodellen åpner for å kunne tilpasse tjenesten mer til kundens/kundegruppens behov enn tilfellet er med en allmenn tilgjengelig sky.

- **Hybrid sky** (*hybrid cloud*) hvor man kombinerer modellene over. Dette kan for eksempel gjøres ved at man primært bruker en privat sky, men bruker en offentlig sky i perioder når arbeidsmengden er spesielt stor.

Skytjenester blir ofte brukt av IoT-systemer. Dette gjør det mulig å samle og analysere store datamengder. Her lagres og prosesseseres typisk dataene som registreres av IoT-sensorene, samt at det er ofte er herfra aktuatorene styres, enten direkte av brukeren via brukergrensesnittet, utfra forhåndsbestemte kriterier, eller ut fra de innsamlede dataene, eller en kombinasjon av disse. En slik løsning gir gode skaleringsmuligheter, siden det ville være svært kostbart å utstyre hver sensor eller aktuator med tilsvarende prosesseringskapasitet. Det vil også redusere energi-forbruket, noe som er hensiktsmessig for IoT-enheter med begrenset batterikapasitet.

Flere leverandører tilbyr spesifikke skytjenester for IoT-systemer. For eksempel tilbyr Google Cloud verktøy for å sette opp forbindelser og prosessere, lagre og analysere – med maskinlæring – data både i kanten av nettverket og i sentrale datasentre. Det tilbys også verktøy for å visualisere dataene, og tjenester som viser geografisk lokasjon på enhetene.[13] Oracle tilbyr også skytjenester for IoT-systemer hvor brukere/virksomheter kan lage sine egne applikasjoner til IoT-enhetene.[14]

[13] https://cloud.google.com/solutions/iot/ [sist besøkt 08.05.20].
[14] https://docs.oracle.com/en/cloud/paas/iot-cloud/index.html [sist besøkt 08.05.20].

3.3 Stordata

Teknologiutviklingen har redusert kostnadene ved å lagre data, noe som har gjort at det lagres stadig mer data i verden. Med økt bruk av IoT, er det ventet at denne trenden forsterkes ytterligere. Begrepet *stordata* (*Big Data*) brukes om ulike analytiske metoder for å analysere eller ekstrahere informasjon ut fra disse store datasettene. I praksis er det snakk om så store og komplekse datasett, spesielt fra nye datakilder, at tradisjonell dataprosesseringsprogramvare ikke håndterer dem.

Gartner/MetaGroup's definisjon fra 2001[15] brukes fremdeles av mange, og den sier at «Stordata er data som inneholder stor variasjon (*variety*), ankommer i store volumer (*volume*) og med høye hastigheter (*velocity*)». *Variety*, *volume* og *velocity* er kjent som «de 3 V'ene» i stordata, og mer spesifikt mener man følgende med begrepene:

- Volume: Med stordata må man ofte prosessere høye volumer av ustrukturerte data med ofte ukjent verdi, som klikkmønstre på nettsider og data fra ulike sensorer på utstyr. Det kan være snakk om størrelser opp mot flere titalls terabytes[16].

- Velocity: Dataene mottas ofte med høy hastighet og de må ofte kunne behandles svært raskt. Noen smarte produkter koblet til internett opererer i sanntid og krever også at analyse og handling utføres i sanntid.

- Variety: Det er mange typer av data som er tilgjengelig. Tidligere var dataene strukturerte og passet inn i en database. I dag kan dataene være i form av både tekst, lyd og bilde. Disse ustrukturerte dataene krever ofte preprosessering for å kunne brukes videre.

Disse store mengdene med data kan bli brukt til å løse helt nye utfordringer, ikke minst ved hjelp av kunstig intelligens. Anvendelsesområdene er mange, fra finans til helse.

3.4 Kunstig intelligens

Kunstig intelligens (*artificial intelligence*, AI) er en samlebetegnelse på teknikker som blir brukt for å få programvaresystemer til å løse oppgaver som normalt krever menneskelig intelligens. Én av flere definisjoner på kunstig intelligens er «en gren innen feltet informatikk som omhandler simulering av intelligent oppførsel i datamaskiner».[17]

Kunstig intelligens bruker data fra IoT og andre datakilder som inndata for å identifisere underliggende mønstre. Til dette brukes i dag ofte maskinlæringsteknikker som forenklet kan beskrives som metoder som hjelper datamaskiner i å ta avgjørelser eller utføre prediksjoner uten

[15] https://blogs.gartner.com/doug-laney/deja-vvvue-others-claiming-gartners-volume-velocity-variety-construct-for-big-data/ [sist besøkt 26.05.20].
[16] https://www.oracle.com/big-data/guide/what-is-big-data.html [sist besøkt 15.01.20].
[17] https://www.merriam-webster.com/dictionary/artificial%20intelligence [sist besøkt 19.05.20].

eksplisitt å bli programmert. Det vil si at det brukes algoritmer som forbedrer seg selv gjennom erfaring. Det er en fordel å ha store og gode datasett å trene algoritmene på.

Maskinlæring er en viktig del av kunstig intelligens, men kunstig intelligens omfatter mer siden det også omfatter evnen til å tolke data, for eksempel språk og bilder, og til å kontrollere objekter, for eksempel en robot.

I dag utnyttes kunstig intelligens innenfor mange områder fra utviklingen av selvkjørende biler (transport), innen aksjehandel (finans) og til medisinering (helse). Det egner seg for eksempel godt til å overvåke ulike prosesser, og melde fra om avvik, eventuelt også håndtere dette. Her vil algoritmene kunne få mye data og dermed vite hva som er normaltilstand, og vil kunne reagere om sensordata avviker fra dette.[18, 19]

Stadig flere IoT-systemer inkluderer nå kunstig intelligens, og disse systemene blir da ofte omtalt som «smarte». Men, ikke alle systemer som blir markedsført som «smarte» inneholder kunstig intelligens.[20]

4 Mulige sårbarheter i IoT

Når man skal vurdere sårbarheten til et system, er det vanlig å finne hvilke faktorer som truer de grunnleggende sikkerhetsegenskapene konfidensialitet, integritet og tilgjengelighet til selve systemet og den informasjonen systemet behandler. Siden et IoT-produkt består av flere ulike komponenter og teknologier som vist i de to foregående kapitlene, vil det kunne være flere ulike faktorer som kan true disse grunnleggende sikkerhetsegenskapene.

Dette kapittelet gir eksempler på sårbarheter man kan finne i de ulike delene av rammeverket som ble beskrevet i kapittel 2, men det er ikke sett på sårbarheter knyttet til alle avhengighetene IoT-systemene har til andre systemer. Dette kommer vi tilbake til i kapittel 5. Kapittelet er ikke ment å gi en uttømmende liste, men for å vise hvor vanskelig det kan være å sikre et helt IoT-system på en tilfredsstillende måte.

Dette kapittelet gir en noe teknisk beskrivelse av de ulike sårbarhetene som presenteres.

[18] https://gcn.com/articles/2020/04/15/ai-intrusion-detection.aspx [sist besøkt 26.05.20].
[19] https://www.smartcitiesworld.net/news/news/-ai-fault-detection-for-hvac-2921 [sist besøkt 29.05.20].
[20] https://www.dinside.no/bolig/endelig-en-smart-robotklipper/70714570 [sist besøkt 19.05.20].

4.1 Brukergrensesnittet

Et brukergrensesnitt er en lokal styringsenhet for å lese av data fra sensoren(e) eller styre aktuatoren(e). Dette er gjerne en mobiltelefon med en tilhørende app installert, eller det kan være en PC eller tablet.

Apper kan inneholde hardkodet sensitiv informasjon som brukernavn, passord, eller IP-adresser. Dette kan hjelpe en angriper til å skape et bilde av den bakenforliggende infrastrukturen hvor data lagres og prosesseres. For en angriper kan det også være mulig å bruke informasjonen til å logge seg inn på servere og tjenester som om han var en legitim bruker og derfra få et fotfeste videre inn i systemet. Videre kan nettverkstrafikk gå ukryptert, være feilkonfigurert, eller det kan benyttes usikre og/eller utdaterte protokoller. Denne typen sårbarheter vil kunne gjøre det mulig for en angriper enten passivt å overvåke trafikken som går mellom brukergrensesnittet og IoT-enheten eller skytjenesten, eller angriper vil kunne være aktiv og injisere egen nettverkstrafikk inn i systemet.

Det kan også eksistere programvaresårbarheter som gir angriper mulighet for å kjøre egen kode på selve enheten (det vil si mobiltelefonen eller datamaskinen som kjører brukergrensesnittet). Dette kan gjøre det mulig for angriper å ta full kontroll over denne enheten, og dermed også gi han tilgang til annen sensitiv informasjon som ligger lagret på denne. Appene kan også bruke tredjeparts biblioteker som igjen kan samle inn sensitiv informasjon uten at bruker er klar over dette. NRK viste nylig hvordan de fikk tilgang til sensitive posisjonsdata som selskapet Tamoco hadde samlet inn fra apper. Dette kan ha skjedd via biblioteker som ble integrert i appene.[21] Informasjon kan også lekke via andre sidekanaler fra enheten som kan utnyttes av angriper, for eksempel i form av elektromagnetisk stråling (TEMPEST).

4.2 Skytjenesten og sentralt grensesnitt

Skytjenester benyttes til lagring og distribuert prosessering av dataene som registreres av IoT-sensorene, samt styring av aktuatorene enten av brukeren direkte via brukergrensesnittet, utfra forhåndsbestemte kriterier, eller ut fra de innsamlede dataene, eller en kombinasjon av disse. Det kan gjerne også eksistere et sentralt web-grensesnitt som gir bruker tilgang til disse dataene.

Potensielle sårbarheter i skytjenesten og webgrensesnittet inkluderer bruk av usikre protokoller og APIer (Application Programming Interface) som gir uvedkommende tilgang til dataene som lagres eller prosesseres. De lagrede dataene kan være dårlig beskyttet, eller være lagret ukryptert. Disse sårbarhetene kan gjøre det mulig for en angriper å injisere egne data inn i systemet, eller stjele sensitiv informasjon. Web-baserte tjenester er gjerne også sårbare for DoS (Denial of Service) og DDoS-angrep (Distributed Denial of Service).

Dersom skytjenesten har et eksponert webgrensesnitt kan dette være en mulig kanal for å utføre angrep som SQL-injection (Structured Query Language) eller cross-site scripting. Daniel

[21] https://www.nrk.no/norge/xl/avslort-av-mobilen-1.14911685 [sist besøkt 14.05.20].

Crowley et al. fant i 2018 sårbarheter i flere sensorsystemer som benyttes av smartbyer. Dette inkluderte sårbarheter i Echelon sine i.Lon-gatewayer hvor de kunne settes opp med standard brukernavn og passord for webgrensesnittet og FTP-serveren (File Transfer Protocol); de hadde en autentiseringsprotokoll som gikk i klartekst, og det var sårbarheter i selve autentiserings-APIet[22]. Videre fant de sårbarheter i webgrensesnittet til Libelium Meshlium, som benyttes av ulike industrikontrollsystemer blant annet for å detektere stråling fra kjernekraftverk, og for flomdeteksjon. Open Web Application Security Project (OWASP) har en oppdatert liste over de vanligste web-sårbarhetene, som alle er relevante i denne sammenheng.[23]

Det er også mulig at leverandøren av IoT-produktet deler sine data med tredjeparter både med og uten brukers samtykke. Dette gjør at sensitive brukerdata kan bli enda mer eksponert. Datainnbrudd hvor brukernavn og passord kommer på avveie skjer jevnlig, og noen eksempler er Adobe[24], Canva[25] og LinkedIn[26].

4.3 Sensorene og aktuatorene

IoT-enheter i form av sensorer og aktuatorer, i tillegg til hub-ene som de benytter for kommunikasjon må beskyttes mot konsekvensene av at en angriper får fysisk tilgang til utstyret.

Kretskortene til sensorene og aktuatorene kan ha tilgjengelige porter eller debug-grensesnitt som angriper kan koble seg til for å lese data, eller overstyre hva som foregår på enheten. Dette er tilgangspunkter som gjerne benyttes under produksjonsprosessen, men som noen ganger forblir tilgjengelige også på det ferdige produktet. Med fysisk tilgang til en sensor (eller hub) kan en angriper koble seg til disse portene. Denne typen tilgang kan gi mulighet for å lese eller manipulere de dataene som går mellom de fysiske kretsene (JTAG). Det kan også eksistere kontaktpunkter som gir tilgang til et kommando-shell (Universal Asynchronous Receiver/Transmitter, UART), hvor det både vil være mulig å få tilgang til statusinformasjon, og å kjøre egne kommandoer. Dersom dette kjører med root-rettigheter vil en angriper få ytterligere tilgang til sensoren.

Begge disse teknikkene (JTAG og UART) kan gi mulighet til å lese ut firmware fra sensoren, noe som er svært nyttig for en angriper. Det kan også være mulig å få tilgang til firmware eller annen informasjon ved å lodde av og dumpe FLASH-chiper. Firmware kan inneholde hardkodet sensitiv informasjon, som brukernavn, passord, krypteringsnøkler og sertifikater. Den kan også inneholde versjonsstrenger som gjør det mulig for angriper å slå fast om det finnes eksisterende upatchede sårbarheter. Det kan også være mulig for angriper å modifisere firmwaren og installere egne bakdører på systemet. Dette kan skje gjennom usikrede oppdateringsmekanismer i tillegg til fysisk tilgang.

[22] https://securityintelligence.com/outsmarting-the-smart-city/ [sist besøkt 14.05.20].
[23] https://owasp.org/www-project-top-ten/ [sist besøkt 14.05.20].
[24] https://www.csoonline.com/article/3268035/adobe-s-cso-talks-security-the-2013-breach-and-how-he-sets-priorities.html [sist besøkt 14.05.20].
[25] https://support.canva.com/contact/customer-support/may-24-security-incident-faqs/ [sist besøkt 14.05.20].
[26] https://blog.linkedin.com/2016/05/18/protecting-our-members [sist besøkt 14.05.20].

Da Charlie Miller og Chris Valasec i 2015 klarte å overta kontrollen over en Jeep Cherokee var muligheten for å installere egen firmware én av sårbarhetene de utnyttet[27]. Billy Rios fant i 2015 at det var mulig å installere egen firmware på Hospira sine medisinske infusjonspumper, og på denne måten få kontroll over dosene som ble gitt.[28] Mirai-botnetet fra 2016 infiserte sensorer av typen IP-kameraer og luftmålere, i tillegg til rutere, som var satt opp med standard brukernavn og passord. Disse ble brukt til å utføre det som fortsatt anses som et av tidenes største DDoS-angrep.[29]

4.4 Trådløs kommunikasjon

IoT-enheter i form av sensorer og aktuatorer er som regel tilkoblet internett gjennom en dedikert hub, eller de kan være direkte tilkoblet mobilinfrastrukturen. De kan også snakke direkte med en lokal styringsenhet. Mobiltelefonen og hub benytter enten mobilnettet, WiFi eller Ethernet for å kommunisere med den tilhørende skytjenesten. Et IoT-system benytter seg derfor ofte av flere av disse protokollene i kombinasjon – enten det er mellom IoT-enheter og hub, eller det er mellom hub og skytjenester.

Felles for alle disse protokollene er at de kan utsettes for klassiske nettverksangrep. Ved å avlytte kommunikasjonen mellom IoT-enheter og hub kan det være mulig å utlede nøkkel-informasjon, eller utgi seg for å være én av partene, og på denne måten kunne utføre Man in the Middle (MitM)-angrep. Det kan også være mulig å avlytte trafikken og på et senere tidspunkt utføre replay-angrep. Til slutt kan det også være mulig for angriper å gjøre IoT-produkter utilgjengelige via jamming.

Deler av kommunikasjonen vil i de aller fleste protokoller være ukryptert. Ved å avlytte dette kan det være mulig for en angriper å få informasjon om identiteten til de kommuniserende partene. Denne informasjonen kan senere benyttes til å utgi seg for å være en av partene.

Det finnes flere eksempler på produkter som har benyttet usikre eller åpne protokoller for kommunikasjon. I 2016 ble det oppdaget at Owlet sine babymonitorer sendte ukryptert trafikk mellom babymonitorene og hub-ene, og at det heller ikke var nødvendig å autentisere seg for å få tilgang til WiFi nettverket som hub-en opprettet.[30] I 2012 fant man at TRENDnet sine webkameraer sendte brukernavn og passord i klartekst under innlogging.[31] En sårbarhet i protokollen til St. Jude Hospital sine pacemakere gjorde det i 2017 mulig å utføre MitM angrep mellom pacemakeren og monitoren som den kommuniserte med.[32] En rekke sårbarheter i Smiths Medical sine medisinske infusjonspumper, som hardkodet brukernavn og passord,

[27] https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/ [sist besøkt 14.05.20].
[28] https://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps/ [sist besøkt 14.05.20].
[29] https://elie.net/blog/security/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/ [sist besøkt 14.05.20].
[30] https://www.theregister.co.uk/2016/10/13/possibly_worst_iot_security_failure_yet [sist besøkt 14.05.20].
[31] https://www.technewsworld.com/story/78891.html [sist besøkt 14.05.20].
[32] https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-identified-st-jude-medicals-implantable-cardiac-devices-and-merlinhome [sist besøkt 14.05.20].

mangel på autentisering og sertifikatverifisering gjorde det i 2017 mulig å overta kommandoen over pumpene.[33]

5 Egenskaper ved de nye IoT-baserte infrastrukturene

Hittil har vi snakket om IoT-system enkeltvis. Disse IoT-systemene kan hver for seg danne infrastrukturer, som for eksempel bilparken til en elbilprodusent. Denne infrastrukturen vil da også kunne inkludere andre infrastrukturer som skytjenester, internett og flere ekom-infrastrukturer i ulike land.

Slike infrastrukturer av IoT-systemer kobles gjerne sammen. En kan tenke seg at denne elbilprodusenten og Statnett kunne ha nytte av å koble sine infrastrukturer sammen, slik at elbilene fortrinnsvis lader når det er overskudd av kraft, mens det også går an å tenke seg løsninger der elbilene kan selge kraft tilbake til strømnettet når det er stor etterspørsel etter kraft. En kan også tenke seg at infrastrukturen til denne elbilprodusenten kunne ha nytte av informasjon fra Statens Vegvesen, for eksempel hvor er det veiarbeid, mens Statens Vegvesen kunne ha nytte av data som elbilene samler inn, for eksempel på hvilke strekninger det er mange kraftige nedbremsinger, noe som kan tyde på at strekningen er ulykkesutsatt og bør utbedres.

På denne måten ser en at det er mulig å oppnå økt funksjonalitet ved å koble ulike infra-strukturer sammen, og infrastrukturene vil da få avhengigheter til hverandre. En kan anta at disse avhengighetene vil øke med økende bruk av IoT.

Økt bruk av IoT vil endre bildet av infrastrukturer, og i dette kapittelet prøver vi å beskrive denne endringen på en enkel måte. Først beskriver vi hva vi mener med infrastrukturer, og hvilke generelle utviklingstrekk vi ser her. Deretter beskriver vi ulike former for kompleksitet som oppstår i disse nye infrastrukturene. Disse nye egenskapene blir så diskutert opp mot tradisjonelle risikoanalyser. En viktig driver i disse nye infrastrukturene er data og datainn-samling. Dette beskrives tilslutt i kapittelet.

5.1 Hva menes med infrastruktur?

Infrastruktur beskrives som et nett av faste anlegg som er grunnlaget for en virksomhet. Begrepet brukes ofte om systemet av veier, havner, flyplasser, ledningsnett med mer, som betjener næringslivet og husholdningene i et land eller område.[34]

[33] https://thehackernews.com/2017/09/hacking-infusion-pumps.html [sist besøkt 14.05.20].
[34] Store norske leksikon.

Samtidig kan infrastruktur, i sin mest generelle form, betraktes som et konsept som formes av teknologiene som samfunnet har tilgjengelig og som følgelig er i konstant endring.[35] Et eksempel på dette er skiftet fra romerske akvedukter til dagens vann- og avløpssystemer.

I Norges offentlige utredninger «Når sikkerheten er viktigst»[36], er kritisk infrastruktur beskrevet som «de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnets grunnleggende behov og befolkningens trygghets-følelse.»

Det er karakteristisk at veldig mange typer infrastrukturer viser seg å være kritiske i en eller annen sammenheng. De fleste infrastrukturene innehar økende kritikalitet, fordi de har økende direkte betydning for samfunnet, men også for Forsvarets evne.

Utviklingen de senere årene har medført at infrastrukturene nå i stadig mindre grad dreier seg om fysiske lineære strukturer, men i stedet om fysiske strukturer som i stadig og sterkt økende grad benytter IKT-baserte kontroll- og styringssystemer. De er også i økende grad avhengig av ulike former for IKT-systemer og -infrastrukturer for tjenesteproduksjon. Det hører også med at både infrastrukturene selv, og ikke minst IKT-systemene som inngår som integrert del av infrastrukturene, er svært kompetansekrevende og at behovet for ulike former for ekstern kompetanse og eksterne tjenester øker. Dette er kompetanse som ikke nødvendigvis finnes i Norge.

Det ser også ut til å være en økende tendens til at utvikling og operasjon av de viktigste tekniske infrastrukturene blir overlatt til private eller offentlig eide selskaper med begrenset mulighet for offentlig styring. Muligheten for samfunnets styring av utviklingen innen mange av disse infrastrukturene blir også gradvis redusert fordi kompetansen innen offentlig forvaltning reduseres.

Disse beskrivelsene av infrastruktur og kritisk infrastruktur reiser flere betraktninger. For det første er ikke infrastruktur noe som er statisk over tid, men noe som vil oppstå og endre seg etter hvert som nye teknologier utvikles og tas i bruk. I tillegg gjør den teknologiske utviklingen at kritiske infrastrukturer blir mer komplekse med et intrikat nettverk av vekselvirkninger mellom de ulike komponentene eller delsystemene som utgjør infrastrukturen.

5.2 Økte avhengigheter og kompleksitet

Som vi har vært inne på tidligere i rapporten, så eksisterer det en del avhengigheter mellom IoT-baserte infrastrukturer og andre infrastrukturer. Dette er noe av det som bidrar til at kompleksiteten til de nye IoT-baserte infrastrukturene er høy. Det er imidlertid andre egenskaper som også bidrar til å øke kompleksiteten. Nedenfor har vi forsøkt å beskrive noen

[35] Lesniewska, F. & McCann, J. A. (2019). *The Little Book of Critical Infrastructure and the Internet of Things*. ImaginationLancaster, Lancaster University. ISBN 978-1-86220-359-4. https://s3-eu-west-1.amazonaws.com/uclpetras/wp-content/uploads/2019/10/28145653/Little_Book_of_Critical_Infrastructure.pdf.
[36] Norges offentlige utredninger (NOU) 2006:6 side 32, *Når sikkerheten er viktigst*.

egenskaper som vi mener er viktige når man skal vurdere kompleksiteten til et system. Valget av egenskaper er inspirert av arbeider gjort av Nancy Leveson[37] og Charles Perrow[38]. Egenskapene er ikke direkte knyttet til bruk av IoT, men økt bruk av IoT-systemer vil i de fleste tilfeller forsterke disse egenskapene.

- **Samspillkompleksitet:** Med samspill (*interactions)* mener vi

    - Interne avhengigheter i en infrastruktur, som kan betraktes som et sett med aktiviteter mellom elementer eller funksjoner i et system eller en infrastruktur. Et eksempel på dette kan være at en intern pumpe er avhengig av en intern sensor.

    - Eksterne avhengigheter til andre (komplekse) infrastrukturer, der man er avhengig av ressurser eller tjenester fra disse andre infrastrukturene. Dette kan typisk være ekom, kraft, skytjenester og tidstjenester. En feil i disse infrastrukturene kan gjøre at mange ulike infrastrukturer kan gå ned samtidig.

    - Eksterne avhengigheter mellom infrastrukturer fordi de trenger data fra hverandre. For eksempel vil det kunne være en avhengighet mellom en infrastruktur som skal styre varmekabler i gater og meteorologisk institutt sin sensorinfrastruktur, fordi førstnevnte vil ha god nytte av værdata.

    - Eksterne avhengigheter mellom infrastrukturer fordi de bruker samme maskinvare, for eksempel antenner eller sensorer, og/eller programvare hentet fra samme programvarebibliotek. En sårbarhet som utnyttes her kan fort ramme mange ulike infrastrukturer.

  Samspillkompleksitet er en egenskap knyttet til kompleksitet som mange IoT-systemer vil score høyt på. Avhengighetene kan medføre at en tilsiktet eller utilsiktet hendelse ett sted, vil kunne føre til en eller flere feil andre steder, og disse kan gjerne være vanskelig å forutse. I noen tilfeller vil konsekvensene kunne eskalere. Bruk av kunstig intelligens vil gjøre det vanskeligere å ha oversikt over avhengighetene i og mellom infrastrukturene. Dette fordi enkelte algoritmer som brukes ved kunstig intelligens kan sammenlignes med «sorte bokser» der man ikke har oversikt over hvordan inndata brukes.

- **Koblingskompleksitet:** Sammenkoblinger mellom elementer og funksjoner i infrastrukturene kan være tette eller løse. Ved tette koblinger vil en handling ett sted ha umiddelbare og gitte effekter et annet sted. Dette kan være fordi det er bestemt hvordan handlingen skal håndteres på forhånd, eller fordi det ikke er rom for fleksibilitet når handlingen skal håndteres. Tette koblinger tolererer ikke forsinkelser og tillater ikke slakk. Dette er i motsetning til løse koblinger, som responderer saktere. Løse koblinger er dermed mer robuste med tanke på feilhåndtering, fordi de tolererer mer slakk og vil fremstå som en

[37] Leveson, Nancy G; *Engineering a Safer World – Systems Thinking Applied to Safety*, The MIT Press (2011).
[38] Perrow, Charles; *Normal Accidents – Living with High-Risk Technologies*, Princeton University Press (1984).

slags buffer. Tette koblinger vil bidra til høy kompleksitet, mens løse koblinger vil bidra til det motsatte.

- **Organisatorisk kompleksitet:** For å levere en tjeneste kan det være mange involverte aktører. Det kan være private virksomheter, offentlige instanser og utenlandske virksomheter, og ofte en kombinasjon av disse. Det er i dag mange eksempler på at virksomheter splittes opp og/eller at deler av virksomheten tjenesteutsettes. Dette kan gjøre det vanskelig å ha oversikt over hvor data havner og gi uklare ansvarsforhold. Jo flere aktører som er involvert jo større vil den organisatoriske kompleksiteten bli.

- **Verdikompleksitet:** Verdi kan for eksempel være velvære for individer eller stor produksjonskapasitet for en produksjonsbedrift. Hvis man har en god oversikt over hvilke verdier infrastrukturen bidrar til, vil verdikompleksiteten være lav. Har man derimot liten oversikt over dette, fordi infrastrukturen for eksempel blir brukt av mange, både indirekte og direkte, vil verdikompleksiteten være høy.

- **Dynamisk kompleksitet:** Infrastrukturer kan også ha kompleksitet knyttet til hvordan hele eller deler av systemet endrer seg over tid. Disse endringene kan være knyttet til alt fra hvor ofte det skjer programvareoppdateringer, hvor ofte den fysiske infrastrukturen endres, hvor ofte det skjer endringer i hva infrastrukturen brukes til, til hvor ofte det skjer organisatoriske endringer.

IoT-baserte infrastrukturer vil generelt score høyt på mange av disse egenskapene. Det vil si at kompleksiteten ofte vil være høy, og dette er en stor utfordring når man skal tenke sikkerhet. Bruce Schneier, en kjent forfatter og foredragsholder innen kryptografi og informasjons-sikkerhet, mener at «complexity is the worst enemy of security»[39].

5.3 Risikobaserte vurderinger vil bli mer krevende

De nye IoT-baserte infrastrukturene har en del egenskaper som vanskeliggjør risikobaserte vurderinger. Dette er spesielt knyttet til kompleksiteten som er beskrevet over.

Når man skal gjøre risikobaserte vurderinger er det viktig å beskrive hva man ønsker å beskytte. Det vil si hva man regner som «verdi». I kapittel 5.2 er verdikompleksiteten beskrevet som en av flere former for kompleksitet som vi mener må legges til grunn for sårbarhets- og risikobaserte vurderinger, uansett om det gjelder tradisjonelle eller nye former for samfunns-infrastrukturer.

Som vi har vært inne på tidligere dreier infrastrukturer, som konsept, seg ofte om sammen-stillingen av mange systemer og systemer av systemer. Disse består også ofte av svært tett integrerte fysiske og IKT-baserte systemer som samlet står for viktige prosesser og funksjoner for samfunnet. I motsetning til for systemer som normalt inngår i oversiktlige verdikjeder, kan

[39] Schneier, Bruce; *Click here to kill everybody*, W.W. Norton & Company (2018).

infrastrukturer inngå i mer komplekse og uoversiktlige verdikjeder. Den som leverer en infrastrukturbasert tjeneste, som for eksempel en mobildatatjeneste, vil ofte ikke vite hvilken verdi denne tjenesten eller funksjonen har for brukeren som har kjøpt tjenesten. Samtidig er det ofte svært vanskelig for brukeren av en slik tjeneste både å forstå og å ha innsikt i hvilken sårbarhet tjenesten egentlig har, hvordan trusselbildet er, og dermed hvilken risiko brukeren tar. Dette har tidligere til dels vært håndterbart siden infrastrukturene har vært under en viss nasjonal kontroll når det gjelder eierskap, og at strukturene og delfunksjonene i infrastrukturene i stor grad har vært mulig å ha en viss oversikt over.

Ved tradisjonelle sikringsrisikoanalyser, som ved bruk av Norsk Standard 5832[40], er det ofte hensiktsmessig å avgrense systemet man ser på og vurdere verdiene, truslene og sårbarhetene til dette avgrensede systemet. En slik avgrensning vil i mange tilfeller ikke være mulig å finne for IoT-baserte infrastrukturer siden disse blant annet innehar svært mange eksterne avhengigheter, som det vil være svært krevende å få oversikt over. Samtidig er det også mange andre forhold, som skissert i kapittel 5.2 om kompleksitet, som det vil være til dels svært krevende å skaffe seg innsikt i gjennom en tradisjonell risikoanalyse etter denne standarden. I tillegg til dette vil en slik vurdering ha begrenset gyldighet i tid, siden disse infrastrukturene er i stadig endring.

Det er derfor mange utfordringer knyttet til det å utføre risikobaserte vurderinger av moderne IoT-baserte infrastrukturer, men å utelate noen av disse forholdene vil kunne gi et feilaktig bilde av risikoen.

5.4 Dataforhandlere og overvåkningskapitalisme

I løpet av de senere årene har utviklingen av teknologier som internett, økt prosesseringskraft i datamaskiner og reduserte kostnader for datalagring gjort at det har blitt enklere for virksomheter å overføre, samle, lagre og analysere data. Dette har gjort at vi har fått en ny «industri» som kalles *dataforhandlere* (*Data Brokers*). Med IoT vil mulighetene for datainnsamling øke ytterligere.

En dataforhandler er en virksomhet som aggregerer informasjon fra ulike kilder, og så prosesserer dataene for å berike, rense og/eller analysere dataene. Deretter lisensierer de resultatet til andre virksomheter. Dataforhandlere kan også lisensiere andre selskapers data direkte, eller prosessere en annens organisasjons data for deretter å tilby dem et ekstrahert resultat. Data blir typisk ikke «solgt», det vil si at eierskapet ikke overføres, men blir heller lisensiert for en spesiell eller begrenset bruk.[41]

Det hevdes å være over 4000 slike selskaper i verden, som omsetter for om lag 200 milliarder dollar årlig. Acxiom som er en av de største har 23 000 servere som samler og analyserer

[40] Norsk Standard 5832; *Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikoanalyse* (2014).
[41] https://www.gartner.com/en/information-technology/glossary/data-broker [sist besøkt 08.05.20].

forbrukerdata. De har data på 500 millioner forbrukere i verden og opp til 3000 datapunkter per person.[42]

Mange selskaper har i dag også hele eller deler av sin verdi knyttet til dataene/informasjonen de besitter. Velkjente eksempler på dette er Facebook og Google. Selv om data ikke i så stor grad «selges», er det ikke uvanlig at selskaper kjøper andre selskaper fordi man er interessert i informasjonen eller informasjonsinfrastrukturen som dette selskapet besitter. Eksempler på dette er Facebook som har kjøpt Instagram (2012) og WhatsApp (2014), Alphabet som har kjøpt Waze (2013) og IBM som har kjøpt The Weather Company (2015) og Truven Health Analytics (2016).

> *«Data are to this century what oil was to the last one: a driver of growth and change. Flows of data have created new infrastructure, new businesses, new monopolies, new politics and—crucially—new economics. Digital information is unlike any previous resource; it is extracted, refined, valued, bought and sold in different ways. It changes the rules for markets and it demands new approaches from regulators. Many a battle will be fought over who should own, and benefit from, data.»*[43]

Surveillance capitalism er et begrep som ble innført av Shoshana Zuboff, professor i bedriftsøkonomi, ved Harvard Business School.[44] Selv om den generelle modus operandi til selskaper som Google, Facebook og Amazon har vært kjent en stund, så forsøker hun å sette dem inn i en bredere kontekst. Hun påpeker at mens de fleste av oss tror at vi bare har å gjøre med uforståelige algoritmer som prøver gi oss tilpasset reklame, så mener hun dette er en ny type kapitalisme. Råvaren i denne kapitalismen er prediksjoner om fremtidig adferd basert på innsamlet data. Hun mener denne nye formen for kapitalisme er årsaken til at det samles inn så store mengder informasjon om oss og samfunnet vi lever i. Hun mener denne overvåknings-kapitalismen har spredt seg fra Silicon Valley og til veldig mange andre sektorer som helse, forsikring, utdannelse, finans og transport.

Hun mener også at disse selskapene helt bevisst prøver å tåkelegge det de driver med. De store selskapene svarer sjeldent på henvendelser, og argumenterer som regel bare med at dataene de samler inn brukes til å forbedre deres tjenester. For eksempel vil ikke Ring svare på om de deler informasjon med morselskapet Amazon.[45]

[42] https://www.webfx.com/blog/internet/what-are-data-brokers-and-what-is-your-data-worth-infographic/ [sist besøkt 08.05.20].
[43] https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy [sist besøkt 08.05.20].
[44] Zuboff, Shoshana; *The Age of Surveillance Capitalism*, Profile Books Ltd, 2019.
[45] https://www.bbc.com/news/technology-51709247 [sist besøkt 02.06.20].

6 Noen infrastrukturer og bruk av IoT

Noen infrastrukturer er spesielt kritiske. Dette gjelder spesielt ekom og kraft, som også vil bli enda mer kritiske etterhvert som bruken av IoT øker. Men disse infrastrukturene vil også selv bruke avanserte driftskontrollsystemer. I dette kapittelet har vi beskrevet ekom- og kraftinfrastrukturene og hvordan disse vil utvikle seg fremover. Vi har også sett litt på infrastrukturer i smartbyer, og på ulike smartbyinitiativ i Norge og resten av verden. Tilslutt har vi beskrevet et fiktivt scenario knyttet til tjenesteutsetting av kritisk infrastruktur.

6.1 Ekom

Her har vi valgt å beskrive infrastrukturen til 5G, siden operatørene nå er i gang med å bygge ut 5G-nettverk i Norge. Mye av kommunikasjonen i Norge vil etterhvert gå over 5G-nettet, som vil inkludere ulike aksessteknologier som fastnett, wifi, 4G, SATCOM og så videre. Hvilke tjenester 5G tilbyr er nærmere beskrevet i kapittel 3.1.2.

5G er en nettverksteknologi som blir utviklet med tanke på å kunne tilby samtidig forbindelse til svært mange systemer med ulike krav til tjenestekvalitet. I 5G vil Management and Orchestration (MANO), som dreier seg om overordnet styring og koordinering av nettverksressursene, bli helt nytt og svært komplekst. Orkestreringen vil bestå i å sette sammen virtuelle nettverksfunksjoner til logiske nett som tilbyr ulik tjenestekvalitet. Disse skal settes sammen slik at de fysiske ressursene utnyttes best mulig. Management vil bli utfordrende, fordi det hele tiden vil være endringer i nettverket. Eksempler på dette er:

- enheter som skal kobles til og fra ulike nettverksskiver
- handover, også mellom ulike aksessnett
- variasjoner i trafikk på grunn av hendelser som store ulykker og arrangementer
- utilsiktede hendelser som rammer nettverket som fiberbrudd, konfigurasjonsfeil og naturkatastrofer
- tilsiktede handlinger som DoS-angrep og kutting av strømforsyning
- feil hos andre operatører

Operatørene vil ha et begrenset sett fysiske ressurser for å håndtere dette:

- Ulike fysiske forbindelser i både kjerne- og aksessnettet – disse består i hovedsak av fiber og ulike radioforbindelser.
- Ulike frekvenser – disse benyttes på radiogrensesnittet, har ulike egenskaper og er en begrenset ressurs.

- Prosessor- og lagringskapasitet i form av servere i datasentre – her ligger nettverksfunksjonaliteten. Det vil finnes mange små datasentre i kanten av 5G-nettverket og noen store sentralt i nettverket.

Disse fysiske ressursene sammen med virtuelle nettverksfunksjoner som kan flyttes, skaleres opp og ned, oppdateres og utvikles, gjør det mulig å kontinuerlig skreddersy nettverket etter løpende behov.

Nettverkene må hele tiden optimaliseres med tanke på kravene til tjenestekvalitet de ulike nettverksskivene har, og de gitte fysiske ressursene man har til rådighet. Optimal ressursutnyttelse krever overvåkning av hele nettverkets protokollstruktur og kompleks beslutningstaking basert på løpende og historiske data. Dette omfatter avgjørelser og håndtering av alt fra hvordan trafikk kan rutes mest hensiktsmessig, til oppdateringer av brannmurer. Nettene vil derfor ha ulike former for sensorer, og de trenger å være proaktive for å kunne tilby tjenester tidsnok og å kunne forutse ulike hendelser slik at ikke tjenestekvaliteten og sikkerheten forringes. Det er også ønskelig at det skal kunne «reparere seg selv» hvis det blir degradert. Kunstig intelligens blir helt sentralt for å få til alt dette, og mange mener at menneskelige ressurser ikke lenger er tilstrekkelig for å kunne drifte mobilnettverkene.[46]

Management trenger ikke legges der den fysiske infrastrukturen er. Den kan legges i et vilkårlig datasenter.

MANO er ikke ferdig standardisert, og det er uvisst når løsninger for dette kommer. De to standardiseringsinitiativene som har fått mest oppmerksomhet er Open Source MANO (OSM) som European Telecommunication Standards Institute (ETSI) står bak[47], og Open Network Automation Platform (ONAP) som utvikles av blant annet China Mobile og AT&T.[48] MANO vil kreve kompetanse som det er usikkert i hvilken grad Norge vil besitte.[49]

Kommunikasjonsinfrastrukturen i 5G vil bli mer kompleks enn dagens kommunikasjonssystemer. Det blir flere avhengigheter både innad i infrastrukturen og med andre komplekse infrastrukturer som skytjenester, og med bruk av kunstig intelligens til å kontrollere nettverket blir det vanskelig å vurdere disse avhengighetene. Samspillkompleksiteten vil derfor være høy, og koblingene vil være tette, ikke minst fordi det meste av dette må foregå svært raskt. Den dynamiske kompleksiteten vil bli høyere først og fremst på grunn av alle faktorene nevnt over som nettverket hele tiden må tilpasse seg. Verdikompleksiteten i ekom er allerede veldig stor, men vil bli enda høyere fordi det vil bli enda vanskeligere å ha oversikt over alt 5G brukes til, ikke minst på grunn av økt bruk av IoT. Det samme gjelder den organisatoriske kompleksiteten. Den vil nå bli enda høyere på grunn av alle de nye virksomhetene som vil være involvert. Tidligere har mobiloperatørene selv vært involvert, samt virtuelle mobiloperatører, produsenter

[46] https://www.insidetelecom.no/artikler/umulig-a-drifte-5g-uten-kunstig-intelligens/479331?utm_source=newsletter_2019-11-20 [sist besøkt 29.01.20].
[47] https://osm.etsi.org/ [sist besøkt 03.02.20].
[48] https://www.onap.org/ [sist besøkt 03.02.20].
[49] Bentstuen, O. I.; Farsund, B. H.; Øverlier, L.; Køien, G.; *Sikkerhetsutfordringer i fremtidens EKOM-tjenester* (FFI-rapport 17/17047), Forsvarets forskningsinstitutt (2017).

av nettverksutstyr som Huawei og Nokia, leverandører til produsentene av nettverksutsyr, mobiltelefonprodusenter, regulatører som Nkom og så videre. Nå inkluderes i tillegg blant annet skyleverandører og produsenter av IoT-utstyr som bilprodusenter.

6.2 Kraftforsyning

I 2020 gjennomførte Proactima en kartlegging av bruk av IoT og IIoT i kraftforsyningen på oppdrag av NVE.[50] Typiske produkter som benyttes i dag, foruten avanserte målesystem (AMS), er IoT-løsninger knyttet til drift, vedlikehold og overvåking av kraftforsyningsnettet, eksempelvis for jordfeilovervåking.[51] Imidlertid har disse sensordataene frem til nå ikke blitt overført direkte til driftskontrollsystemet (SCADA[52]). Når det gjelder utviklingen fremover, ønsker nettselskapene å benytte sensorteknologier for å innhente mest mulig informasjon om tilstanden til anleggene, eksempelvis sensorkuler til overvåking av kraftlinjer.[53]

På oppdrag fra NVE gjennomførte SINTEF Digital en risikoanalyse av økt integrasjon mellom AMS, prosesskontrollsystemer (DMS[54]) og driftskontrollsystemer (SCADA) i 2018. Analysen var avgrenset til risiko relatert til informasjonssikkerhet. I dagens system har DMS som hovedoppgave å representere topologien i strømnettet slik at man bedre kan forstå konsekvensen av endringer i nettet. DMS mottar i så måte tilstandsinformasjon fra SCADA, men det går ikke kommandoer fra DMS til SCADA for å unngå at DMS defineres som et driftskontrollsystem i henhold til kraftberedskapsforskriften.[55] Dagens integrasjon av AMS, DMS og SCADA er derfor basert på at DMS skal benyttes for økt situasjonsforståelse, mens AMS og SCADA benyttes for direkte effektuering av endringer i kraftnettet.[56] Sterkere kobling mellom AMS, DMS og SCADA medfører at DMS kommer tettere på operativ styring av kraftnettet utover å være et segregert system for økt situasjonsforståelse. Dersom integrasjonen økes dithen at et system både kan dekke oppgavene til DMS og sende kontrollsignaler til SCADA og AMS, vil dette være et driftskontrollsystem som må tilfredsstille kravene i kraftberedskapsforskriften.[57] I følge rapporten til SINTEF Digital, ser det ut som det allerede er en tettere kobling mellom DMS og SCADA i resten av Europa ved at DMS kan effektuere endringer i kraftnettet direkte. Det må derfor forventes at dette også vil skje i Norge siden de store utstyrsleverandørene leverer løsninger både til europeiske og norske kraftselskaper.[58]

Rapporten til SINTEF Digital påpekte at økt integrasjon av SCADA, DMS og AMS medfører at systemer som opprinnelig ble designet for å være selvstendige, kobles sammen og blir

[50] Røyksund, M. & Valdal, A.-K. (2020). *Kartlegging av bruk av tingenes internett (IoT/IIoT) i norsk kraftforsyning* (Eksternrapport nr. 2/2020). Norges vassdrags- og energidirektorat. ISBN: 978-82-410-2003-2.
[51] *Ibid.*, s. 8.
[52] SCADA er en forkortelse for «Supervisory Control and Data Acquisition» og er et driftskontrollsystem.
[53] Røyksund, M. & Valdal, A.-K. (2020). *Kartlegging av bruk av tingenes internett (IoT/IIoT) i norsk kraftforsyning* (Eksternrapport nr. 2/2020). Norges vassdrags- og energidirektorat. ISBN: 978-82-410-2003-2, s. 11.
[54] DMS er en forkortelse for «Distribution Management System» og er et prosesskontrollsystem.
[55] Frøystad, C., Jaatun, M. G., Bernsmed, K. & Moe, M. (2018). *Risiko- og sårbarhetsanalyse for økt integrasjon av AMS-DMS-SCADA* (Eksternrapport nr. 15/2018). Norges vassdrags- og energidirektorat. ISBN: 978-82-410-1789-6.
[56] *Ibid*.
[57] *Ibid*.
[58] *Ibid*.

avhengige av hverandre. Dette kan medføre risiko når systemer som tidligere ble konstruert for å unngå kravene til driftskontrollsystemer i henhold til kraftberedskapsforskriften, kobles sammen med eksisterende driftskontrollsystemer.[59] Spesielt ble følgende uønskede hendelser vurdert til å ha høy risiko:[60]

- Uvedkommende sender falske kommandoer med SCADA-bryteroperasjoner til fjernstyrte brytere i distribusjonsnettet.

- Uvedkommende utfører endring i DMS-delen av det integrerte DMS-AMS-SCADA-systemet (IDAS) som medfører at uhensiktsmessige SCADA-bryteroperasjoner effektueres.

Begge hendelsene kan føre til at hele eller deler av strømnettet kobles ut, samt utøve skade på utstyr og nett som medfører større og langvarige strømbrudd. I verste fall kan hendelsene føre til utkobling av store områder, inkludert sykehus og annen kritisk infrastruktur.[61]

I følge undersøkelsen til Proactima, erkjenner kraftbransjen at innføring av nye IoT-baserte løsninger kan gi større angrepsflater i form av flere angrepsvektorer for trusselaktører. Bransjeaktørene har derfor stort fokus på å beskytte SCADA.[62] Imidlertid vil ikke logiske sikkerhetsbarrierer gi samme grad av beskyttelse som systemer som er fysisk adskilte.

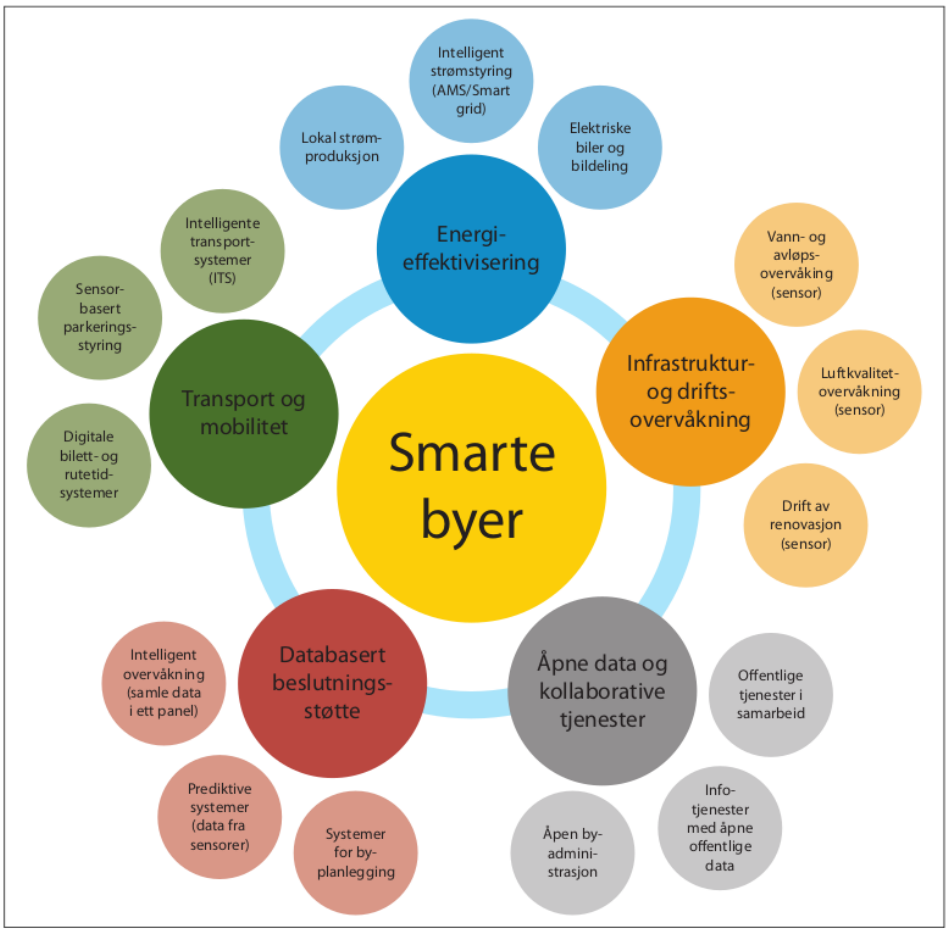
Tettere kobling mellom AMS, DMS og SCADA vil medføre økt samspillkompleksitet. En kan også forvente at den dynamiske kompleksiteten vil øke, fordi det vil medføre flere og hyppigere endringer i infrastrukturen.

Det er derfor nødvendig slik Røyksund & Valdal[63] anbefaler, å videreutvikle kunnskap om hvilke implikasjoner innføring av IoT-løsninger kan gi for sikker forsyning av kraft. Dette vil spesielt være tilfelle etter hvert som kraftforsyningen får større innslag av distribuert og variabel kraftproduksjon fra fornybare energikilder som vind- og solkraft. Det vil også være behov for mer forskning knyttet til resilient systemdesign når omfanget av IoT i kraftforsyningen øker, herunder hvilke kriterier som skal legges til grunn for å evaluere resiliens.[64]

[59] *Ibid*.
[60] *Ibid.*
[61] *Ibid.*
[62] Røyksund, M. & Valdal, A.-K. (2020). *Kartlegging av bruk av tingenes internett (IoT/IIoT) i norsk kraftforsyning* (Eksternrapport nr. 2/2020). Norges vassdrags- og energidirektorat. ISBN: 978-82-410-2003-2.
[63] *Ibid.*
[64] Sellevåg, S. R., Brattekås, K., Bruvoll, J. A., Buvarp, P. M. H., Fardal, H., Farsund, B., Fykse, E.-M., Gisnås, H., Hellesø-Knutsen, K., Kirkhorn, S., Nystuen, K. O., Olsen, R. & Seehuus, R. A.; *Samfunnssikkerhet mot 2030 – utviklingstrekk* (FFI-rapport 20/00530), Forsvarets forskningsinstitutt (2020).

6.3 Smarte byer

Begrepet *smartby* (*smart city*) har ikke noen entydig definisjon, men brukes gjerne for å illustrere ulike sider av teknologiutviklingen i byer. Begrepet omfatter på denne måten en økt bruk av IoT i kombinasjon med konvensjonell IKT for datainnsamling med det formål å lette forvaltning, ressurshåndtering og tjenester i et bymiljø som preges av et voksende innbyggertall og økt miljøfokus. Stortingsmelding 27 «Digital agenda for Norge»[65] legger til grunn for sin definisjon at en smartby «bruker digital teknologi for å gjøre byen til et bedre sted å leve, bo og arbeide i. Smartbyinitiativer har som mål å forbedre offentlige tjenester og innbyggernes livskvalitet, utnytte felles ressurser optimalt, øke byens produktivitet, og å redusere klima- og miljøproblemene i byene». Eksempler på dette er vist i Figur 6.1.



Figur 6.1 Eksempler på anvendelsesområder og tjenester for smartby, som vist i Stortingsmelding 27.

[65] Meld. St. 27; *Digital agenda for Norge – IKT for en enklere hverdag og økt produktivitet* (2015).

6.3.1 Smartbysatsninger i verden

I mange tilfeller går smartbyinitiativene ut på å oppgradere eksisterende bygninger og infrastruktur for å tilfredsstille nye teknologikrav. Barcelona er et eksempel på dette, hvor de fornyet infrastrukturen sin i form av Barcelona Smart City Program[66]. Dette innebar å innføre en rekke nye teknologier: gatelys med sensorer som detekterer forurensning, fuktighet, temperatur, støy og nærvær av personer; søppelkasser hvor avfallet oppbevares under bakken med sensorer som detekterer nivå; og et kollektivnett hvor busskurenes informasjonstavler er solcelledrevne. Barcelona var også blant de første byene i verden til å innføre en bysykkelordning. Det ble utviklet en *open source*-plattform for å samle inn og presentere data fra de ulike sensorene i byen, som værdata, støymålinger, ladestasjoner, bysykler, WiFi aksesspunkter, solcelleinstallasjoner, ledige parkeringsplasser og luftkvalitet.[67]

Til forskjell fra Barcelona, er Songdo i Sør Korea et eksempel på en smartby som er blitt bygget fra bunnen av. Byen består av et 600 hektar stort finansdistrikt hvor sensorer overvåker trafikkflyt og energiforbruk. Dataene brukes for avansert ruteinformasjon for kollektivtilbudene, samt å varsle myndighetene om lovbrudd.

Også store teknologiaktører involverer seg i smartbysatsninger. Det Alphabet-eide selskapet Sidewalk Labs er involvert i å digitalisere en bydel av Toronto og gjøre byen mer sensordrevet. Dette inkluderer sensorer for overvåking av trafikk, støy, vær, klima, energi og avfall, og initiativet har blitt kritisert på grunn av de store datamengdene som ett selskap vil kunne samle inn fra byens innbyggere.[68]

6.3.2 Smartbysatsinger i Norge

Stortingsmelding 27 «Digital agenda for Norge» skriver at «de fleste norske byer er for små til å investere i smartbykompetanse og -teknologi på samme nivå som store byer i Europa, USA og Asia. Norske byer kan likevel bruke teknologi til å utnytte ressursene bedre.» Noen av hoved-trekkene man ser under utvikling av norske smartbyer er:

- bruk av stordata fra en rekke ulike kilder og sensorer
- involvering i internasjonale samarbeidsprosjekter
- fokus fra regjeringen på at byutbygging er bærekraftig
- smarte energiløsninger for utnyttelse av eksisterende bygninger
- bruk av intelligente transportsystemer med tanke på kapasitet, transportsikkerhet, miljø og klima

[66] Harmom, Robert R. et.al.; *Smart cities and the Internet of Things* (2015).
[67] https://www.sentilo.io/wordpress/ [sist besøkt 02.06.20].
[68] https://www.bbc.com/news/technology-51658116 [sist besøkt 14.05.20].

Bergen, Trondheim, Oslo, Stavanger, Tromsø og Kristiansand er alle med i nettverket *Nordic Smart City Network* som er et samarbeidsprosjekt mellom 14 byer i de 5 nordiske landene. Målet er å dele erfaringer og lære av de andre byene.

Stavanger er deltaker i Trianglum, som er et EU-finansiert prosjekt under Horizon 2020-rammeprogrammet. Kommunen skal gjennom dette programmet utvikle løsninger for energioppfølging i smartbygg i samarbeid med Lysne Energi. Det kjøres også et prøveprosjekt på batteridrevne busser, og Universitetet i Stavanger utvikler en løsning for å samle data og kunnskap. Eksempler på tiltak utført i Stavanger er bruk av AV1-roboter i undervisning for langtidssyke barn som ikke har mulighet til å være til stede på skolen; et LoRaWAN-transportnett for sensorer som kan måle luftkvalitet, temperatur, støynivå, forbipasseringer, vannstand, CO2-nivå, ledige parkeringsplasser etc.; gatesluker som forutser og varsler når de overfylles; og lyktestolper med ladepunkt for elbiler. Deler av den innsamlede informasjonen som ikke er personsensitiv gjøres åpen for andre brukere gjennom portalen Opencom[69].

Oslo som smartby har et høyt fokus på miljø og klima. Det utvikles i denne forbindelse en portal for å presentere klimastatistikk og historiske data på en engasjerende måte. Det er også etablert et program kalt FutureBuilt i samarbeid med Bærum, Asker og Drammen som skal vise hvordan det er mulig å etablere klimanøytrale urbane områder.

Kristiansand har installert varmekabler i gatene som automatisk styres basert på temperatur-data de får fra yr.no. Det er også investert i avanserte klimasystemer, som ventilasjon, varme-pumper, lys og liknende for å redusere strømforbruk. De har også lagt vekt på offentliggjøring av informasjon og dokumenter.

Bergen har gjennom Smart Care som formål å modernisere helse- og omsorgstjenestene med teknologiske verktøy. De har etablert bildelingstjenester som en del av styringen av parkerings-plasser, og egne hub-er kombinerer bildelingsstasjoner, kollektivtransport, gangveier, sykkelstier, sykkelparkeringer og sanntid-transportinformasjon.

Trondheim er medlem i programmet +CityxChange i samarbeid med Limerick, Alba Iulia, Pisek, Sestao, Smolyan og Voru, og deres industri- og forskningspartnere.

Bodø oppgir til Agenda Kaupang at en viktig motivasjon til deres smartbysatsing er flyttingen av Bodø lufthavn og utviklingen av en ny bydel for nærmere 20 000 innbyggere.[70] I tillegg til byutvikling ser de på smart byplanlegging, helse og samferdsel og integrering av data på tvers av sektorer.

6.3.3 Smartbyer og kompleksitet

Siden det ikke finnes noen enhetlig definisjon av begrepet «smartby» eksisterer det en rekke svært ulike smartbyinitiativer over hele verden. Noen av disse er meget avanserte og integrerer sensorer og infrastrukturer fra en rekke ulike leverandører, som er tilfellet for Barcelona og

[69] https://opencom.no/ [sist besøkt 27.05.20].
[70] Agenda Kaupang; *Smarte byer og kommuner i Norge – en kartlegging* (2018).

Songdo. Norske initiativer har foreløpig ikke ressursene til å kunne investere i den samme skalaen, og har heller et fokus på deltakelse i ulike fora, og samarbeid med en håndfull leverandører. Dette påvirker kompleksiteten til de ulike initiativene.

I en avansert smartby vil det inngå mange IoT-baserte infrastrukturer. De IoT-baserte infrastrukturene er avhengig av både ekom og kraft og vil følgelig erverve kompleksiteten fra disse infrastrukturene, i tillegg til at de kan være svært komplekse i seg selv. De er kjennetegnet av mange avhengigheter både internt og eksternt, og vil dermed ha høy samspillkompleksitet. Siden systemene som inngår i infrastrukturene ofte vil ha kort responstid, vil koblingene her kunne være tette, og om det brukes kunstig intelligens vil avhengighetene kunne være vanskelig å få oversikt over. Verdikompleksiteten vil kunne være varierende. Noen systemer vil det være lett å vurdere verdien av, mens andre vil være vanskeligere. Organisatorisk kompleksitet vil kunne være høy, siden infrastrukturene kan involvere aktører fra mange ulike virksomheter, både offentlige og private. Dette vil gjelde innenfor mange områder som helse, transport, renovasjon og så videre. Den dynamiske kompleksiteten vil også kunne være høy, siden man må anta at disse nye systemene jevnlig vil oppdateres, eierforholdene vil kunne endres, hvilke systemer som henter data fra hverandre vil kunne endes, og så videre.

6.4 Scenario knyttet til tjenesteutsetting av kritisk infrastruktur

Her beskriver vi et scenario knyttet til tjenesteutsetting av kritisk infrastruktur som tidligere er brukt ved FFI. Selv om scenarioet ikke er reelt, vil det ikke være utenkelig.

Scenarioet går ut på at et veiselskap i Norge legger ut anskaffelse og drift av ladeinfrastruktur for elektriske kjøretøyer i Østerdalen ut på anbud. Et tysk firma, AutoEl Gmbh, vinner anbudsrunden og blir kontraktør. De leverer avanserte ladere, og ett av de viktigste kriteriene ved valg av kontraktør var å minimere kostnadene.

AutoEl Gmbh er et selskap som er eid av flere aktører i Asia og Midtøsten, og det benytter mange aktører for å produsere tjenestene de leverer. Når det gjelder ekom har de kontrakter med seks internasjonale ekom-selskaper, mens skytjenester kjøper de av to ulike leverandører. Operasjon av ladestasjonene utføres av fem aktører fordelt over Ukraina, Bulgaria, India og Vietnam, mens den tekniske operasjonen av ladestasjonene foretas av lokale aktører i Østerdalen. Strømleveranser får de fra en latvisk bedrift med sammensatt eierskap, mens den fysiske strømleveransen kommer fra en lokal nettleverandør.

En slik infrastruktur vil ha høy kompleksitet. Når det gjelder samspillkompleksitet, vil denne infrastrukturen av ladestasjoner ha avhengigheter til mange datasentre, driftssentre, kommunikasjonsnoder og kommunikasjonsveier i form av kjernenett, spredd over hele verden. Det vil være deling av data med andre tjenester og infrastrukturer. Samspillkompleksiteten vil derfor være høy, og koblingene vil i stor grad være tette. Verdikompleksiteten vil være noe høy, fordi det vil være vanskelig å ha oversikt over hvilke verdikjeder disse elkjøretøyene, som bruker ladestasjonene, inngår i. Den organisatoriske kompleksiteten vil også være høy. En kan tenke

seg at firmaet bygger ut nye ladestasjoner andre steder i verden, at selskaper blir kjøpt opp, og deler blir solgt ut. Infrastrukturen vil derfor også kunne inneha høy dynamisk kompleksitet.

Dette er som nevnt et fiktivt scenario, men vil ikke kunne være utenkelig slik virksomheter opererer i dag. Det er også å anta at ladeinfrastrukturer langs Norges hovedfartsveier vil være av betydning for nasjonal sikkerhet, siden bortfall av disse vil påvirke transportsektoren i alle fall på sikt.

7 Test av noen av dagens vanlige forbruker-IoT

Vi har som en del av oppdraget testet noen vanlige IoT-produkter for å få et bedre inntrykk både av hvordan de virker og hvordan de formidler informasjon, og ikke minst for å forstå noe av kompleksiteten i de enkelte produktenes verdikjeder.

Dette kapittelet beskriver laboppsettet vi benyttet under testing samt en oppsummering av resultatene. Vi hadde ikke ressurser til å gjøre en utfyllende test av alle sikkerhetsaspektene som er beskrevet i kapittel 4, men valgte å konsentrere oss om en trafikkanalyse for å avdekke hvor utstyret sender data, og hvorvidt de er avhengig av en aktiv internettforbindelse for å fungere. Dette mener vi bidrar til å vise at det antakelig foregår mye datainnsamling ved bruk av IoT, og at spesielt samspillkompleksiteten i infrastrukturene til de ulike produktene er høy.

En beskrivelse av testene knyttet til de konkrete produktene er gitt i den opprinnelige rapporten.[71]

7.1 Utvalg av produkter for testing

Utvalget av produkter var tilfeldig uten noen forutgående screening. Likevel representerer utvalget ulike former for produkter. Disse kan deles inn i ulike typer sensorer fra enkle brytere til bilde- og videobaserte sensorer, også med bevegelsesdeteksjon. Produktene innehar også ulike former for aktuatorer, som for eksempel å slå av eller på en fysisk gjenstand eller å regulere lys i en lampe. Forsøkene omfattet også to ulike typer IoT-huber tilknyttet internett, med innebygd mulighet for å programmere oppførsel gjennom brukergrensesnittet på de tilhørende appene. Vi hadde derfor også fokus på de appene som inngikk som del av produktene.

Markedet disse produktene inngår i er under sterk utvikling både med hensyn til produktene selv og den underliggende teknologien. Et begrenset utvalg av produkter, valgt uten noen form for

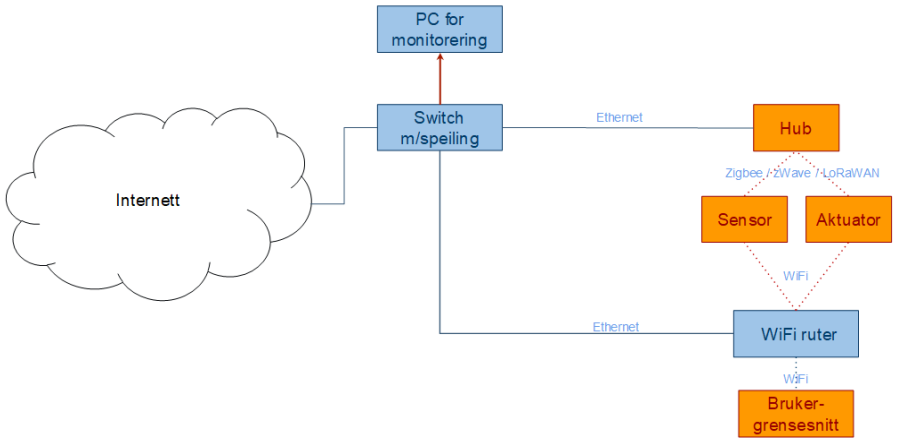
[71] Farsund, B. H.; Søndrol, T.; Nystuen, K. O.; Hornfelt, L.; Sellevåg, S. R.; Pham, V.; *Utviklingen av nye IoT-baserte infrastrukturer i samfunnet – utfordringer for nasjonal sikkerhet* (FFI-rapport 20/01745 [UNNTATT OFFENTLIGHET]), Forsvarets forskningsinstitutt (2020).

screening, kan gi usikkerhet om hvorvidt våre funn er representative. Vi brukte imidlertid tid på å gå gjennom ulike former for informasjon på internett om de ulike produktene og deres plass i forbrukermarkedet. Vi mener derfor at utvalget er representativt for vår test.

Vi har fokus på produktenes funksjonalitet fremfor hvilket selskap som produserer dem, fordi vi mener dette har mindre betydning for den faglige nytten av arbeidet. Opplysninger om de ulike produktenes varemerke vil også kunne skape uheldig og unødvendig fokusering på produkter fremfor problemstillingen.

7.2 Laboppsett

Vi har satt opp et lokalt labnett med lokale IP-adresser som er illustrert i figur 7.1. En ruter som er plassert mellom internett og labnettet sørger for brannmur, NAT (Network Address Translation) og DHCP (Dynamic Host Configuration Protocol).

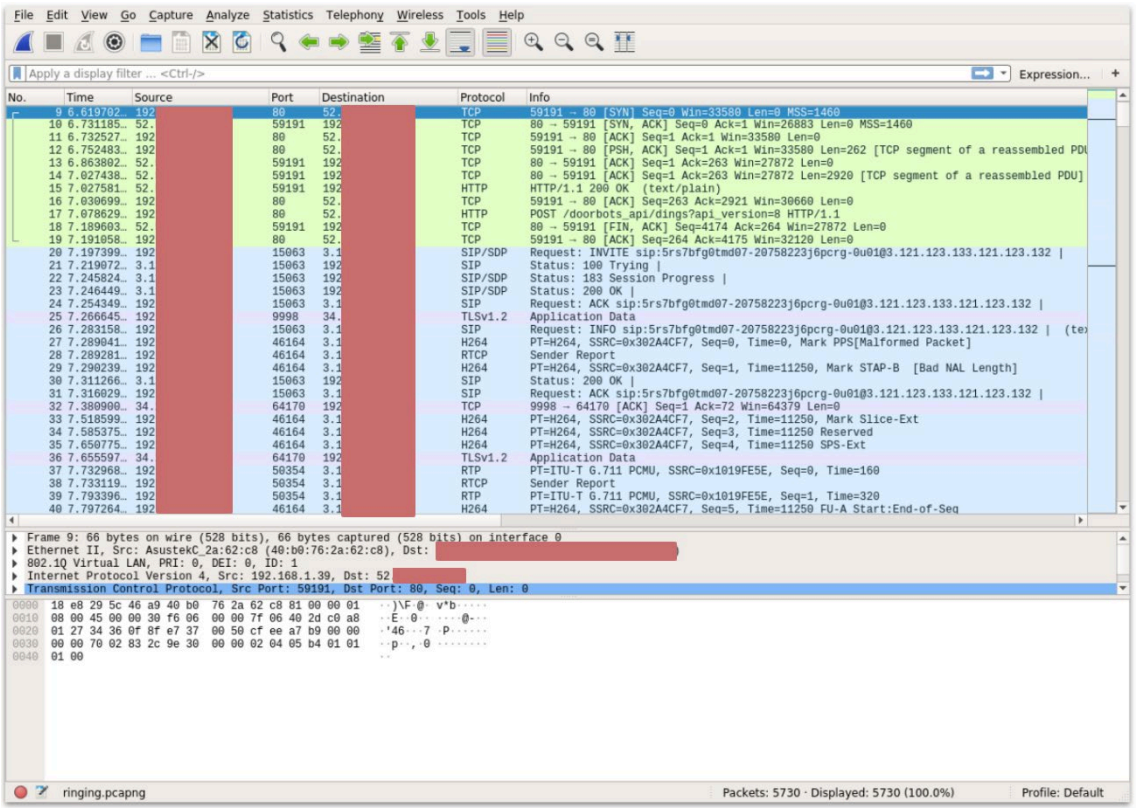


Figur 7.1 Laboppsett.

Til denne ruteren koplet vi en switch som ble satt opp til å speile all trafikken fra én valgt port til en annen speilingsport uten at enheter på den valgte porten ble påvirket av dette. Dette gjorde det mulig å selektivt få tilgang til nettverkstrafikken fra hub eller WiFi-ruter basert på hva som var tilkoblet den speilede porten. WiFi-ruteren sørget for trådløs oppkopling til IoT-enheter som ikke hadde kablet nettverksforbindelse.

En laptop med Wireshark[72], et verktøy for å analysere nettverksprotokoller, monitorerte all trafikk på speilingsporten og lagret trafikk for dokumentasjon og senere analyse. Figur 7.2 viser nettverkstrafikk som fanges med denne metoden.

[72] https://www.wireshark.org/ [sist besøkt 31.08.20].



Figur 7.2 Eksempel på nettverkstrafikk fanget opp av Wireshark.

Med dette oppsettet kunne vi se trafikken mellom de forskjellige IoT-enhetene ved trådbundet kommunikasjon, og vi kunne analysere WiFi-trafikk mellom IoT-enheter som benyttet den trådløse ruteren. Vi konsentrerte oss om hvordan IoT-enhetene kommuniserte mot internett med denne oppstillingen.

7.3 Noen generelle observasjoner

Vi har i forsøket testet fire ulike kommersielle og rimelige forbrukerrettede IoT-produkter. Dette ga oss et bilde på hvordan disse enhetene kommuniserer. Resultatet viste først og fremst at mye kryptert trafikk gikk mellom sensorer/hub og internett, spesielt til USA og Kina. Mye av trafikken var kryptert, slik at vi ikke hadde mulighet til å se innholdet i trafikken. En annen observasjon var at flere av produktene krevde en aktiv internettforbindelse for å fungere.

Det var imidlertid ikke bare selve IoT-produktene som syntes å formidle betydelig med informasjon til servere andre steder i verden. Vi registrerte også at de tilhørende appene krevde mange rettigheter på mobiltelefonen. Alle de tilhørende appene ville ha tilgang til lokasjon, tre av appene krevde tilgang til kamera, kontaktliste og lydopptak, mens to av appene ville ha tilgang til samtaleinformasjon og til å kunne installere apper på mobiltelefonen.

7.4 Mulig videre utvikling

Produktene innehar i første rekke betydelig funksjonalitet for å støtte og forenkle privatpersoners liv. I første omgang utgjør dette i stor grad en personvernsutfordring. Ved avansert bruk av produktene, for eksempel i ventilasjonsanlegg, varmeanlegg, brann- og vannalarmering, lysstyring, styring av dørlåser og så videre, kan andre sårbarheter knyttet til integritet og tilgjengelighet også bli en utfordring, når bruken av denne typen produkter og teknologier blir mer vanlig. Produktene, og særlig teknologiene. har også potensiale for å bli tatt i bruk i mer profesjonell sammenheng. For eksempel vil noen funksjoner kunne være svært nyttig for overvåking av pleietrengende i hjemmet. En slik bruk vil kreve en bedre oversikt over sårbarheter.

En særlig bekymring er knyttet til hvordan informasjonen, som vi har registret blir overført til land utenfor vår kontroll, blir brukt. Til et bilde eller en videostrøm kan det eksempelvis knyttes avanserte biometriske sensorer som kan kjenne igjen personer, uten at vi får kjennskap til det. Med tiden vil det kunne utvikles avanserte infrastrukturer basert på disse typene produkter og teknologiene som disse bygger på, og denne typen overvåkning vil kunne utgjøre en utfordring for nasjonal sikkerhet.

Avhengigheten av tjenester i samfunnet vil kunne bli så stor og altomfattende at bortfall eller andre former for manipulasjon med tjenestene også vil kunne påvirke funksjoner innen totalforsvaret, for eksempel evnen til effektiv sivil og militær logistikk. Det vil også være svært krevende å utøve myndighetskontroll med denne typen nye infrastrukturer, og det kan i stedet bli globale næringslivsaktører som fullt og helt har kontrollen med verdikjedene knyttet til disse. Dette vil være infrastrukturer som vil være flyktige og omfattet av stadige endringer, der for eksempel egnede juridiske styringsmekanismer vil kunne være krevende å finne.

8 Muligheter og utfordringer med økt bruk av IoT

Hva kan billige sensorer og aktuatorer, konnektivitet overalt, skytjenester, stordata og kunstig intelligens gi oss av nye funksjoner og infrastrukturer? Og hvilke sårbarheter vil disse nye funksjonene og infrastrukturene gi oss?

IoT-systemene gir ofte mye funksjonalitet i forhold til kostnader, men disse systemene har også noen karakteristikker som gir noen utfordringer. Basert på funnene i det foregående, vil dette kapittelet identifisere noen sentrale muligheter og utfordringer IoT kan gi for nasjonal sikkerhet.

Vi har konsentrert oss om utfordringene, fordi det er dette som har vært oppdragets fokus. Vi synes det allikevel er hensiktsmessig å peke på at økt bruk av IoT også vil kunne gi mange muligheter.

En begrensning for å vurdere hvilken betydning denne teknologiutviklingen vil ha for nasjonal sikkerhet er manglende fantasi til å se hele bildet av muligheter og utfordringer. Likevel forsøker vi i dette kapittelet å gi en oversikt, selv om dette ikke vil være uttømmende. Vi begynner med å forsøke å gi en innsikt i hvilke muligheter teknologiutviklingen vil ha for samfunn og forsvar, deretter forsøker vi å beskrive hvilke utfordringer denne utviklingen kan ha for nasjonale sikkerhetsinteresser.

En viktig rammebetingelse for dette er en forventning om at utviklingen av ulike former for funksjonalitet vil ha fortrinn for de sikkerhetsutfordringer som måtte komme som følge av funksjonen eller produktet.

I kapittel 8.1 og 8.2 beskriver vi de store mulighetene bruken av IoT åpenbart har for fremtidens samfunn, samtidig som vi beskriver de viktigste utfordringene ved denne utviklingen konkretisert til tre områder. I kapittel 8.3 beskrives noen faktorer som vi anser også å ha betydning for nasjonal sikkerhet og behov for utvikling av forvaltning.

8.1 Muligheter for styrket nasjonal sikkerhet med økt bruk av IoT

Som vi var inne på i innledningen vil økt bruk av IoT-systemer blant annet kunne gi oss et mer effektivt forsvar, mer ressurseffektive byer og mer konkurransedyktig industri.

Ved økt bruk av for eksempel kameraer og andre typer sensorer vil Forsvaret kunne få en bedre situasjonsforståelse, og dermed kunne ta raskere og mer presise beslutninger. Andre eksempler er automatiserte logistikksystemer og autonome enheter der sistnevnte kan utføre oppgaver der risikoen for skade eller tap av liv tradisjonelt har vært høy. Det at Forsvaret tar i bruk IoT-baserte systemer vil derfor kunne øke Forsvarets evne og dermed den nasjonale sikkerheten.

Den nasjonale krisehåndteringen vil også kunne bli bedre. Eksempelvis vil medisinske eksperter som sitter andre steder enn der krisen har oppstått kunne bidra med kunnskap til de som er på stedet ved å bruke ulike former for sensorer som kan settes på pasientene. Krisestaber vil raskere kunne få en bedre situasjonsoversikt ved hjelp av kameraer og andre typer sensorer, og på samme måte vil autonome enheter kunne utføre oppgaver som kan medføre skade eller tap av liv.

Industrien vil også bli mer effektiv og konkurransedyktig. Ved å automatisere prosesser vil for eksempel produksjonsbedrifter kunne produsere døgnkontinuerlig, og ved prosesser som innbefatter fare for skade eller tap av liv, vil man kunne redusere risiko for dette.

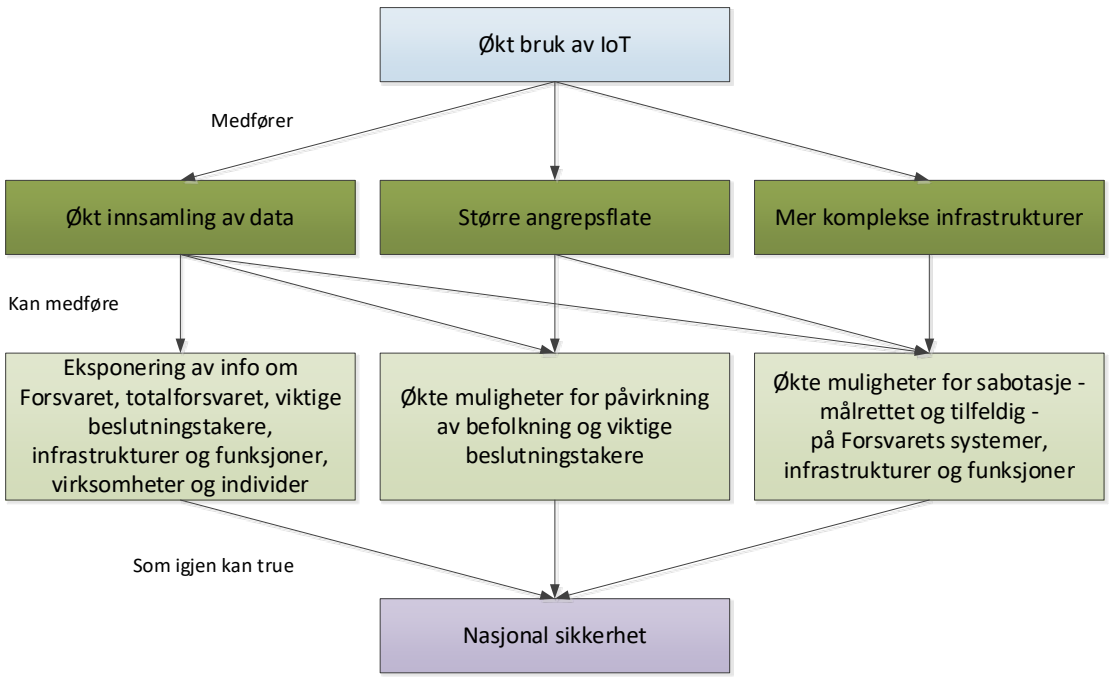
Som vi var inne på i kapittel 6.3 vil økt bruk av IoT kunne gi oss mer ressurseffektive byer, ikke minst i forhold til bedre og mer effektive funksjoner og tjenester. Mer ressurseffektive byer og bedre infrastrukturer vil først og fremst øke samfunnssikkerheten, men at viktige samfunns-funksjoner blir bedre, vil også bidra til økt nasjonal sikkerhet.

Om de nye IoT-systemene ikke erstatter noen tidligere systemer, men bare kommer i tillegg til de vi har i dag, vil effekten av systemene i stor grad være positiv. Dette vil for eksempel gjelde for flomvarslingssystemet som Statens Vegvesen har satt opp langs E6 i Innlandet.[73]

8.2 Utfordringer for nasjonal sikkerhet med økt bruk av IoT

Økt bruk av IoT særlig i nye samfunnsinfrastrukturer vil imidlertid endre risikobildet knyttet til nasjonal sikkerhet. Ved vurdering av risiko er det vanlig å benytte risikotrekanten (NS 5832) som består av «verdi», «sårbarhet» og «trussel». Vi mener at økt bruk av IoT-systemer vil kunne øke sårbarheten i samfunnet og også utfordre nasjonale sikkerhetsinteresser betydelig. Etter hvert som flere funksjoner digitaliseres vil også tradisjonelle grunnleggende infrastrukturer som ekom og kraft bli enda viktigere infrastrukturer i samfunnet. Trusselen og hvordan sårbarheter vil kunne utnyttes for å ramme verdiene våre vil imidlertid i stadig større grad bli sammensatt og være scenarioavhengig.

Vi har gjennom arbeidet identifisert tre grunnleggende utfordringer som blir særlig viktig å forvalte i et større og mer sammensatt risikobilde. Disse har vi kalt *økt innsamling av data, større angrepsflate* og *mer komplekse infrastrukturer.* Betydningen disse vil ha på nasjonal sikkerhet er oppsummert i Figur 8.1 og blir nærmere beskrevet i de neste delkapitlene.



Figur 8.1 Skisse av hvilke utfordringer økt bruk av IoT vil kunne gi.

[73] https://www.vegvesen.no/hovedside/nyheter/nytt-smart-tiltak-mot-varflommen [sist besøkt 09.05.20].

8.2.1 Økt innsamling av data

IoT-systemene samler inn detaljerte data fra deres brukere og/eller miljø. Disse dataene er ofte nødvendige for at IoT-systemet skal fungere hensiktsmessig, eller for å forbedre eller utvikle nye tjenester. Men noen ganger kan det være vanskelig å se hvorfor det gjøres, og innsamlingen kan også ofte være skjult for brukerne. En del av verdikjeden for en IoT-virksomhet kan være å selge disse dataene videre i en eller annen form.

Det er veldig vanskelig å beskytte seg mot denne innsamlingen av data. Det er ikke lenger nok «å legge fra seg telefonen». Et eksempel på dette er alle kameraene som nå inkluderes i IoT-produktene vi omgir oss med som ringeklokker, biler, støvsugere, etc. Det vil så og si bli umulig å ikke bli filmet av noen av disse kameraene vi omgir oss med.

Mange er bekymret over at så mye data og dermed kunnskap om samfunnet vårt havner hos store private selskaper. I tillegg vil mye av dataene lagres i utlandet og dermed utenfor nasjonal kontroll. Det er en utfordring å ha lovverk som håndterer dette, spesielt siden teknologi-utviklingen går så raskt.

Denne datainnsamlingen er en utfordring både når det gjelder personvern og etterretnings-trusselen mot personer, virksomheter, kritiske infrastrukturer, samfunnsfunksjoner samt Forsvaret. Dataene kan videre brukes som utgangspunkt ved ulike påvirkningsoperasjoner og til å utføre ulike angrep mot kritiske infrastrukturer og Forsvarets systemer. Dette er en opplagt utfordring for nasjonal sikkerhet.

8.2.2 Større angrepsflater

Frem til nå har «tingene» våre bestått av «det vi ser», og de har hatt få eller ingen avhengigheter. Avhengighetene har som oftest vært i form av behov for elektrisitet eller drivstofftilførsel. Eksempler på slike «ting» er varmeovner, biler og industrimaskiner.

Som tidligere nevnt består et IoT-system av flere ulike komponenter som sensorer og/eller aktuatorer, brukergrensesnitt og kommunikasjon. Det blir også stadig oftere benyttet skytjenester og kunstig intelligens. Dette medfører at systemene består av maskinvare og programvare som kan ligge i ulike geografiske områder, potensielt over hele verden, og med kommunikasjon dem imellom. Dette gir mange angrepspunkter, hvor mange kan nås fra internett, og da også i praksis fra hele verden.

Disse komponentene har igjen avhengigheter til andre systemer. Det er derfor mulig å angripe et gitt IoT-system via andre systemer som dette systemet har avhengigheter til. Det vil si at et IoT-system som i seg selv er sikkert, kan ha sårbarheter fordi det har koblinger til andre systemer som ikke er like sikre. Systemene kan også hver for seg være sikre, men hvor sammenkoblingen dem imellom ikke er like sikker. Til sammen gjør dette at IoT-systemene har en stor angreps-flate i form av mange mulige angrepsvektorer.

Dette representerer en stor endring fra «tingene» vi hittil har omgitt oss med, og vil gi en økt sårbarhet med fare for både konfidensialitets-, integritets- og tilgjengelighetsangrep. Spesielt vil integritets- og tilgjengelighetsangrep kunne få stadig større konsekvenser i den fysiske verden ettersom flere aktuatorer kobles til systemene. Sammen med den økte innsamlingen av data omtalt i forrige delkapittel vil dette øke faren for påvirkning av befolkningen og viktige beslutningstakere og for sabotasjehandlinger mot virksomheter, kritiske infrastrukturer, viktige samfunnsfunksjoner og Forsvaret.

8.2.3 Mer komplekse infrastrukturer

IoT-systemene er komplekse i seg selv siden de omfatter mange ulike komponenter og teknologier, samtidig som de har mange avhengigheter til andre komplekse systemer. I tillegg er de dynamiske og de inngår i svært komplekse verdikjeder. Et eksempel på sistnevnte er vist i kapittel 6.4 der et scenario knyttet til tjenesteutsetting av kritisk infrastruktur beskrives. Vi ser at en kompleks infrastruktur som IoT, kan bruke flere andre komplekse infrastrukturer som for eksempel skytjenester, 5G og internett. Ingen av disse infrastrukturene er statiske.

Fokus på rask utvikling og lave utviklingskostnader fører til mye bruk av programvare-biblioteker for å slippe å skrive all kode fra bunnen av. Av samme grunn er det også vanlig at ulike produkter kan bruke de samme maskinvarekomponentene som for eksempel trådløse sendere og ulike sensorer. Dette gjør at mange IoT-systemer potensielt kan ha de samme sårbarhetene. Det bør imidlertid nevnes at bruk av programvarebiblioteker og gjenbruk av maskinvarekomponenter også kan gi sikrere systemer. Disse blir ofte godt testet, gjennom å bli brukt av flere, og videreutviklet.

Uansett vil det være mange ulike IoT-systemer som bruker de samme infratrukturene, program-varebibliotekene og/eller maskinvarekomponentene. Dette gjør at tilsiktede og utilsiktede hendelser som rammer noe av dette potensielt kan ramme mange IoT-systemer. Det er i praksis umulig å ha oversikt over alle disse avhengighetene.

At systemene involvert i infrastrukturene blir stadig mer komplekse og kompetansekrevende er en viktig årsak til at systemene blir tjenesteutsatt, som igjen øker kompleksiteten til infra-strukturene ytterligere.

Siden IoT-systemene danner svært komplekse og dynamiske infrastrukturer, vil det ikke være praktisk mulig å ha full oversikt over disse infrastrukturene og deres avhengigheter. Dette er den største utfordringen vi ser med stadig mer bruk av IoT, og vil gjøre det svært utfordrende å gjøre risikovurderinger. Dette vil imidlertid også gjelde for trusselaktørene, siden det også for disse vil være vanskelig å vurdere hva konsekvensene vil bli av et gitt angrep.

Den økte kompleksiteten vil først og fremst ha betydning for sårbarheten til systemene. Denne sårbarheten kan utnyttes til både konfidensialitets-, integritets- og tilgjengelighetsangrep. Som i forrige punkt vil integritets- og tilgjengelighetsangrep kunne få stadig større konsekvenser i den fysiske verden ettersom flere aktuatorer kobles til systemene. Sammen med den økte inn-samlingen av data og de store angrepsflatene kan denne sårbarheten utnyttes til sabotasje-

handlinger mot virksomheter, kritiske infrastrukturer, viktige samfunnsfunksjoner og Forsvaret. Dette er en utfordring for den nasjonale sikkerheten.

8.3 Andre forhold knyttet til nasjonal sikkerhet og samfunnssikkerhet

Utviklingen av IoT legger til rette for rask utvikling av nye funksjoner og infrastrukturer til beste for individer og samfunn. Denne vil etter vår vurdering få stor betydning for nasjonal sikkerhet, og ikke minst hvordan vi som samfunn må forvalte nasjonal sikkerhet. I bunn og grunn fører utviklingen til en stadig sterkere sammenstilling av til dels komplekse systemer og systemer av systemer som vil inngå i svært sammensatte verdikjeder i et globalt marked. Informasjonssystemer med anvendelse av IoT gror også raskt sammen med tradisjonelle fysiske funksjoner og individers levesett. Denne utviklingen utfordrer blant annet samspillet mellom mange former for profesjoner i alle faser av utvikling, idriftsetting, drift og sikkerhet av infrastrukturer.

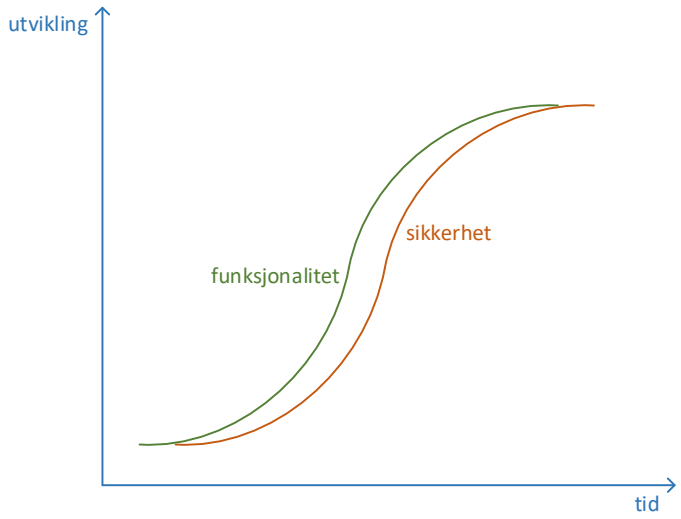
Dette har tidligere til dels vært håndterbart så lenge infrastrukturene har vært under en viss nasjonal kontroll på eierskap og at strukturene og delfunksjonene i infrastrukturene i stor grad har vært mulig å ha en viss oversikt over. Med den økte kompleksiteten og globaliseringen av både funksjoner og aktører innen særlig nye IoT-baserte infrastrukturer, vil det bli mye mer krevende å forvalte sikkerhet og særlig nasjonale sikkerhetshensyn ut fra en tradisjonell sikkerhetstenkning. Sikkerheten i disse funksjonene blir så god som markedet etterspør og er villige til å betale for. Dette til dels i kontrast til tradisjonelle grunnleggende sektorer som i dag er strengere regulert, som ekom, kraft og transport.

En annen faktor som i ytterligere grad gir utfordringer er en utvikling mot at Forsvaret og andre viktige forvaltninger ser store muligheter ved å inngå strategiske partnerskap med kommersielle aktører, særlig på funksjoner som i stor grad omfatter informasjonsteknologi. Dette er en utvikling som etter vårt syn i stor grad drives frem av et behov for effektivisering, samtidig med et åpenbart behov for kunnskapsforvaltning som det vil være svært krevende å utvikle som rene interne prosesser. Det kan være viktig å merke seg at også denne utviklingen med strategisk partnerskap går svært raskt, slik at det i økende grad vil bli krevende å følge opp denne utviklingen med effektiv forvalting av nasjonal sikkerhet.

I ulike deler av verden brukes også nye IoT-type teknologier svært ulikt. I vår del av verden er vi svært restriktive med å bruke teknologien til overvåking og andre tiltak mot for eksempel egne innbyggere og egne innbyggeres virksomheter. Nasjoner og organisasjoner vi kan stå overfor i sikkerhetspolitisk krevende situasjoner kan derimot ha stor erfaring med å utvikle og bruke teknologi også for slike anvendelser. Slik teknologi vil også i form av tjenester fra internasjonale aktører være implementert i systemer vi til daglig omgir oss med, uten at denne typen av funksjonalitet nødvendigvis er tatt i bruk.

Zuboff beskriver i sin bok *The Age of Surveillance Capitalism*[74] spennet mellom det hun beskriver som samfunn basert på «Instrumental Power» og «Social Trust»[75]. Under førstnevnte begrep kommer samfunn med regimer som aktivt utvikler og bruker IoT-type teknologi til å samle inn og utnytte informasjon om innbyggere og virksomheter, og samtidig mer eller mindre automatisk iverksetter tiltak mot mennesker eller grupper av mennesker [76]. Dette i sterk motsetning til regimer som vårt eget som bygger på ikke-totalitære verdier og er basert på høy grad av «Social Trust». At vårt samfunn bygger så vidt sterkt på prinsippet om «Social Trust», og en ikke-totalitær innretning, vil imidlertid også kunne utvikles som en sårbarhet når vi møter aktivitet fra andre typer regimer i det digitale rom, og som kan utnytte denne tilliten i samfunnet.

Et annet aspekt ved utviklingen med potensiell stor betydning for nasjonal sikkerhet og evne til å forvalte nasjonal sikkerhet er utviklingshastigheten av nye funksjoner og infrastrukturer. Nye og stadig mer avanserte funksjoner basert på ulike typer IoT utvikles med stadig større hastighet. Vi ser også gjennom våre forsøk vist i kapittel 7 at sikkerhet nødvendigvis ikke fremstår som like viktig i kappløpet med å få nye og mer funksjonelle IoT-produkter ut på markedet. I Figur 8.2 har vi skissert en erfaring som beskriver forholdet mellom funksjonalitet og sikkerhet ved ulike utviklingshastigheter. Stadig raskere utvikling av funksjonalitet vil erfaringsmessig skape et rom for sårbarhet som følge av et erfaringsmessig etterslep av sikkerhetsløsninger. Det oppstår derfor ofte et tidsvindu hvor funksjoner og infrastrukturer vil ha en større sårbarhet, og dette vinduet vil kunne utnyttes av trusselaktører til å utføre ulike angrep.



Figur 8.2 Illustrasjon som viser hvordan funksjonaliteten som regel utvikles raskere enn sikkerheten.

[74] Zuboff, Shoshana; *The Age of Surveillance Capitalism*, Profile Books Ltd (2019).
[75] http://essedunet.nsd.uib.no/cms/topics/2/ [sist besøkt 07.07.20].
[76] Buckley, Chris; Mozur, Paul; *How China Uses High-Tech Surveillance to Subdue Minorities,* New York Times 22. mai 2019.

9 Diskusjon og innspill til strategi

Gjennom arbeidet med denne rapporten har vi identifisert noen sentrale sikkerhetsutfordringer knyttet til utviklingen av IoT-baserte infrastrukturer i samfunnet. Disse er delt inn i tre hovedområder, som vist i kapittel 8:

- Større mulighetsrom til å angripe både infrastrukturenes funksjon og hvordan funksjonene anvendes.
- Potensial for å innhente dramatisk større mengde informasjon og metainformasjon i alle former for etterretnings- og overvåkingsvirksomhet, både med mål om å innhente informasjon om målobjekters virksomhet og som kan brukes videre til å angripe infrastrukturene.
- Mer komplekse infrastrukturer som øker sikkerhetsutfordringene i systemer og infrastrukturer i form av økt sårbarhet og dermed økt risiko.

Det er åpenbart at den delen av teknologiutviklingen vi har sett på i denne rapporten vil gi grunnlag for mange ulike former for funksjoner og tjenester som vil bli svært verdifulle for dagens og fremtidens samfunn. Dette er også en utvikling drevet av globale kommersielle interesser det i liten grad vil være mulig å begrense eller styre i særlig grad.

I fremtidens tjenestespekter vil det bli krevende å skille ut funksjoner av spesiell betydning for nasjonal sikkerhet. De funksjonene vi i dag definerer som kritiske samfunnsfunksjoner og -infrastrukturer, vil antakelig være i nært samspill med en potensiell stor mengde nye funksjoner og infrastrukturer vi i dag ikke har oversikt over. Alle disse nye og eksisterende infrastrukturene vil bli vevd sammen i komplekse verdikjeder som gjør det vanskelig å identifisere noen særskilte funksjoner og infrastrukturer som vil ha spesiell betydning for nasjonal sikkerhet. Dette i motsetning til tidligere da markedet var mer oversiktlig og det til en viss grad var mulig å identifisere og rette fokus mot funksjoner med særlig betydning for nasjonal sikkerhet.

Den raske teknologiutviklingen og samtidig hvordan teknologi raskt blir tatt i bruk i ulike deler av samfunnet er en krevende utfordring for forvaltningen av nasjonal sikkerhet. I kapittel 8.3 har vi beskrevet noen forhold knyttet til denne utviklingen vi mener er av sentral betydning.

De sentrale sikkerhetsutfordringene som har fremkommet i dette arbeidet viser at teknologi-utviklingen, hvor IoT vil inngå i stadig flere infrastrukturer, vil sette nye krav til hvordan vi som samfunn utvikler vår evne til å forvalte viktige samfunnsinteresser på en effektiv og robust måte. Vi mener at vi er kommet til et punkt i utviklingen der vi må utvikle nye måter å forvalte sikkerhet på. Et sitat fra en bok, som til tross for alder fremdeles utgjør et grunnleggende tenkesett for sikkerhet, illustrerer dette godt:

> *"Accidents and, thus, potential catastrophes are inevitable in complex, tightly coupled systems with lethal possibilities. We should try harder to reduce failures – and that will*

help a great deal – but for some systems it will not be enough… We must live and die with their risks, shut them down, or radically redesign them."

Charles Perrow (1984)[77]

Spesielt vil den økte kompleksiteten være en utfordring for dagens sikringsbaserte tilnærmingsmåte.

Denne rapporten har ikke som mål å utvikle noe konsept for hvordan vi kan gå frem for å møte denne utviklingen. Likevel er det gjennom arbeidet fremkommet noen områder som åpenbart bør være kandidat til å inngå i et slikt konsept.

For å kunne håndtere hendelser og kunne vurdere ulike forebyggende tiltak knyttet til kritiske infrastrukturer og nasjonal sikkerhet er det svært viktig å ha et oppdatert og helhetlig risikobilde. Et slikt bilde må evne å innlemme kompleksiteten og beskrive usikkerheten som opplagt er tilstede. I dag mangler man tilstrekkelig kunnskap og metoder for å gjøre dette. I motsetningen til dagens risikoanalyser som ofte er i form av øyeblikksbilder, og som ofte gjentas med lengre intervall, må fremtidens tilnærminger være tilpasset en mer dynamiske virkelighet og oppdateres kontinuerlig.

I et slikt helhetlig risikobilde er det viktig at også verdier og verdikjeder settes i fokus. En isolert trussel- og sårbarhetstilnærming, der man ikke gjør verdivurderinger vil i stadig mindre grad være relevante, fordi man ikke vil kunne vurdere hvilke konsekvenser ulike former for svikt vil kunne gi.

Kontinuerlig kunnskapsutvikling og -forvaltning vil også være viktig, og dette innenfor mange fagfelt. Disse fagfeltene spenner fra samfunnsvitenskap, samfunnets anvendelse av teknologi til hvordan teknologi realiseres i systemer og infrastrukturer. Dette gjelder da et bredt spekter av teknologier. I tillegg er det helt essensielt med en metode for å sette kunnskapen i system. Siden det dreier seg om en rask teknologiutvikling og dynamiske infrastrukturer er det viktig at også dette er en kontinuerlig prosess.

[77] Perrow, Charles; *Normal Accidents – Living with High-Risk Technologies*, Princeton University Press (1984).

Om FFI

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

FFIs formål

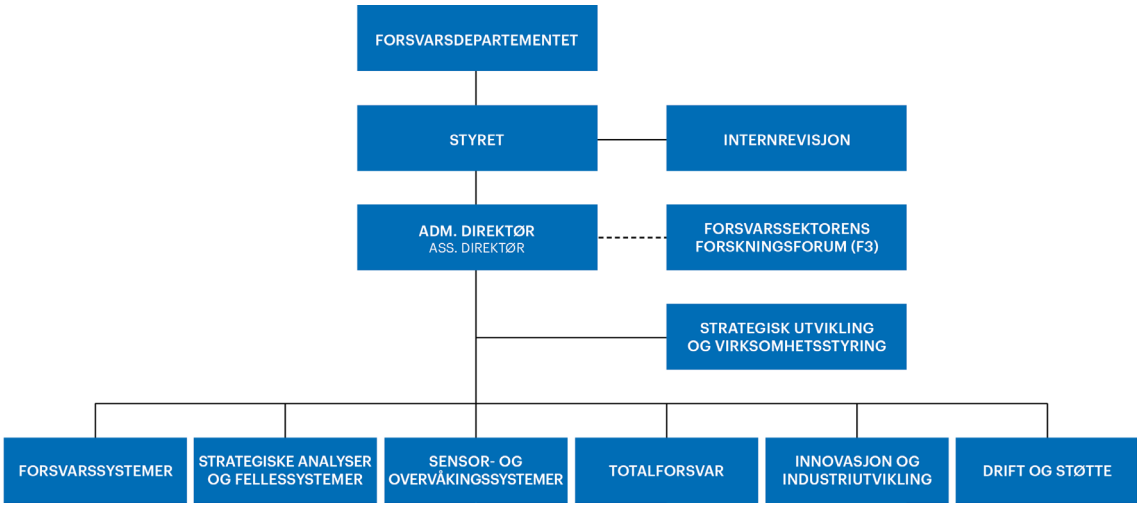
Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som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



Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

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