FFI-RAPPORT

17/17047

Sikkerhetsutfordringer i fremtidens EKOM-tjenester

–
Ole Ingar Bentstuen
Bodil Hvesser Farsund
Lasse Øverlier
Geir Køien

Sikkerhetsutfordringer i fremtidens EKOM-tjenester

Ole Ingar Bentstuen
Bodil Hvesser Farsund
Lasse Øverlier
Geir Køien

Forsvarets forskningsinstitutt (FFI) 1. februar 2018

Emneord

Trendanalyser
Trusler
Teknologisk utvikling
IKT

FFI-rapport
FFI-RAPPORT 17/17047

Prosjektnummer
5032

ISBN
P: 978-82-464-3036-2
E: 978-82-464-3037-9

Godkjent av
Ronny Windvik, *forskningsleder*
Tor-Odd Høydal, *assisterende forskningsdirektør*
Espen Skjelland, *forskningsdirektør*

Sammendrag

Denne rapporten beskriver viktige trender innen digitale verdikjeder og sikkerhetsmessige konsekvenser for virksomheter og samfunnet. Tidsrammen er satt til fem år. Bakgrunnen for rapporten er at Nasjonal sikkerhetsmyndighet (NSM) har bedt Forsvarets forskningsinstitutt (FFI) om å utarbeide en slik trendanalyse.

Utvalget er basert på hvilke trender vi mener vil medføre større endringer i hvordan samfunnet, virksomheter eller tjenesteleverandører kan eller må tenke sikkerhet og robusthet på. Disse trendene vil ikke nødvendigvis få størst kommersiell utbredelse. Rapporten beskriver fem hovedtrender:

Virtualisering medfører at funksjonalitet flyttes fra maskinvare til programvare, noe som blant annet gjør det enklere å rulle ut nye tjenester og funksjonalitet. Virtualisering er allerede mye brukt innenfor skytjenester, men i de kommende årene vil virtualisering av nettverksfunksjoner bli et nytt anvendelsesområde. Dette vil føre til at bedrifter og forvaltning må tenke annerledes om sikkerhet i sine nettverk. Virtualisering vil også muliggjøre helt nye konsepter og løsninger for helhetlig drift og vedlikehold av IKT-infrastrukturen.

Neste generasjon mobiltelefoni, **5G**, vil ikke bare gi høyere datakapasitet til brukerne, men også tilby tjenester for maskin-til-maskin-kommunikasjon (Machine-Type Communications, MTC). MTC inneholder de to hovedretningene massiv MTC, også kjent som "Internet of Things", og kritisk MTC, som tilbyr robuste tjenester for bruk innen blant annet autonome systemer og helse. Relativt til dagens mobiltelefoni er det ventet at sikkerheten generelt vil blir bedre for kritisk MTC, men dårligere for massiv MTC.

Kunstig intelligens og autonomi vil også innta datasentre og EKOM-sektoren. Virtualisering av nettverksfunksjoner er med på å gjøre dette mulig, i tillegg til at kompleksiteten i nettene vil bli så stor at det vil være nødvendig. Kunstig intelligens vil blant annet medføre ikke-verifiserbare systemer, som vil utfordre dagens regime for sikkerhetsgodkjenning innen IKT.

Komplekse digitale verdikjeder og markedsutvikling vil gjøre det enda vanskeligere å holde oversikt over avhengighetene mellom de tjenestene som brukerne ser, og de underliggende infrastrukturene som støtter opp under disse tjenestene. Dette vil blant annet gjøre det vanskelig å ha kontroll med hvor personlig informasjon havner. I tillegg vil stadig flere brukere benytte tjenester fra store internasjonale selskaper, som ikke nødvendigvis er regulert av norsk lovverk.

Tillitsskapende teknologier som blockchain og automatiserte sikkerhetsoppdateringer sammen med økt fokus på personvern vil redusere utilsiktet spredning av personlig informasjon og gjøre det enklere å oppnå tillit under transaksjoner. Samtidig ser vi at store aktører som Google og Facebook sitter på svært mye informasjon, og at denne informasjonsinnsamlingen vil øke.

Mange av de nye teknologiene vi ser komme, kan kobles til flere ulike trender og motsatt. Det har derfor vært en utfordring å sortere og strukturere innholdet.

Summary

This report describes important trends related to digital chains of values related to electronic communications and the security impact of these trends, with a time horizon of five years.

The choice of trends is based on which trends we expect to change how the society, business sector and service providers need to think about security, and not necessarily on which trends will have the most commercial prevalence. The report describes five trends.

Virtualization is the enabling technology of cloud services. In the near future, virtualization will also change how communications services and networks are implemented. This will change how service providers need to design and implement security within communications networks. Virtualization will enable new concepts for management and orchestration of communication networks.

Next generation mobile technology - **5G** - will, in addition to higher data capacity, also offer service for Machine-Type Communications (MTC). MTC covers the two areas Massive MTC, also known as the Internet of Things, and Critical MTC, which offers robust services for e.g. autonomous systems and within heath care. We expect that security for critical MTC will be on the same level or higher than the current 4G security mechanisms. Massive MTC will have lower security than existing technologies.

Artificial intelligence and autonomous system will enter the domains of data centers and communications service providers. Virtualization of network functions is the key enabler for these technologies. In addition, the complexity of modern IT infrastructures is so high that utilizing artificial intelligence is necessary. Artificial intelligence will lead to non-verifiable systems, which will challenge the current regime for security approval.

The market situation and complex digital value chains will make it even more difficult to understand and know the dependencies between the user-facing services and underlying IT infrastructures. It is difficult to keep control over personal information. In addition, users will use services from large international service providers that are not regulated by Norwegian law.

Trust-enabling technologies like blockchain and automatic security updates, together with higher focus on protection of personal information, will reduce the chance of unwillingly spreading personal information. At the same time, large companies like Google and Facebook will continue to gather large amount of personal information.

There were great challenges in sorting and structuring the content in this report since several of the emerging technologies drives different trends. There is not a one-to-one mapping between the underlying technology development and the usage of the technologies.

Innhold

Forord

Denne rapporten ble utarbeidet i løpet av juli og august 2017. En foreløpig utgave ble oversendt NSM i brevs form i august 2017. Forfatterne har i denne rapporten valgt ikke å utdype teknologier og trender utover det som ble oversendt NSM i august. Det er derfor kun gjort mindre endringer for å korrigere skrivefeil og rette opp potensielle misforståelser i denne rapporten.

1 Innledning

Nasjonal sikkerhetsmyndighet (NSM) ba i juni 2017 Forsvarets forskningsinstitutt (FFI) om å utarbeide en rapport om trender innen digitale verdikjeder og sikkerhetsmessige konsekvenser av disse trendene. Rapporten ble utarbeidet i juli og august 2017. Rapporten skulle dekke sikkerhetsmessige konsekvenser både for virksomheter og samfunnet, og omhandle både utilsiktede og tilsiktede uønskede hendelser. Tidsaspektet for trendanalysen ble satt til fem år. Vi har i enkelte tilfeller tatt med teknologiutvikling som vil komme etter denne perioden, men som virksomheter og samfunnet må ta hensyn til innenfor den kommende femårsperioden. Vi har også hatt noe fokus på endringer i kompetansebehov da sikkerhet og robusthet er avhengig av tilgang til riktig kompetanse.

Begrepet digital verdikjede ble gjort allment kjent gjennom Lysne-utvalgets rapport «Digital sårbarhet – sikkert samfunn»[1]. Begrepet dekker alle de enkeltelementene som til sammen bygger opp en digital tjeneste som benyttes av en bruker, og strekker seg fra transport- og transmisjonsnett, via aksessnett til tale- og datatjenester. På toppen av datatjenestene er såkalte Over The Top-tjenester, som gjerne tilbys av aktører som ikke tradisjonelt er regnet som en del av EKOM-bransjen, og som derfor kan være utenfor direkte regulatorisk kontroll. En tjeneste, som for eksempel billettbestilling hos Ruter, benytter en lang rekke forskjellige underliggende tjenester innen både data- og EKOM-sektoren. Dette er både fysiske enheter og infrastrukturer, som datamaskiner og kommunikasjonsnettverk, og «logiske» tjenester som datalagring og dataprosessering. Lysne-utvalget peker på at de digitale verdikjedene ofte er ukjente for brukerne av tjenester, og at mange forskjellige tjenester er avhengig av de samme bygge-klossene. Et kjent eksempel som nevnes av Lysne-utvalget er den nasjonale avhengigheten til Telenors kommunikasjonsnettverk.

En stor utfordring for arbeidet med denne rapporten har vært sortering og strukturering av innholdet. Utfordringen er at det ikke er en en-til-en kopling mellom underliggende teknologiske drivere og de store trendene. En rapport som ikke klarer å sette de underliggende teknologiske driverne inn i en større samfunnsmessig sammenheng, vil ikke bli forstått av det generelle publikum.

Arbeidet startet med å definere og begrense antall teknologiområder som skulle omhandles. Analysen er begrenset til EKOM-tjenester, og høyere lags tjenester som på sikt kan erstatte dagens bruk av EKOM-tjenester. Det ble også tidlig gjort en beslutning om å fokusere på underliggende teknologiske utviklingstrekk uavhengig av hvordan teknologiutviklingen vil bli anvendt. Om lag 25 teknologiske utviklingstrekk ble listet opp i innledende fase. Disse ble kategorisert og gruppert slik at vi sto igjen med de fem teknologitrendene som omhandles i rapporten.

[1] NOU 2015:13, "Digital sårbarhet - sikkert samfunn -- Beskytte enkeltmenneske og samfunn i en digitalisert verden", 2017

Utvalget av trender vi trekker frem kan selvsagt diskuteres. Utvalget er gjort basert på trender vi mener vil medføre til dels store endringer i hvordan samfunnet, virksomheter og/eller tjeneste-leverandører kan eller må tenke sikkerhet og robusthet på, og muligens ikke de største trendene når det gjelder kommersiell utbredelse i samfunnet og hos enkeltindivider. Utvalget er også noe påvirket av tilgjengelig kompetanse på FFI innenfor forskjellige teknologiområder. Vi har valgt ikke å ta med andreordens effekter av feil i IKT-systemer. For eksempel vil da trafikksikkerhet ved selvkjørende biler falle utenfor studien, selv om kunstig intelligens, i seg selv, er inkludert.

Vi har også forsøkt å legge vekt på teknologiske utviklingstrekk som ikke er en ren videre-utvikling av dagens teknologi. For eksempel er mer bruk av datasenter og skytjenester, samt mer datarate innenfor mobilteknologi opplagte trender, men vi ser ingen fundamentale endringer i sikkerhetsbildet relatert til denne utviklingen. Vi har derfor vektlagt andre aspekter innenfor skytjenester og mobilteknologi. Vi har inkludert en del teknologiutvikling innenfor infra-strukturer som antagelig ikke vil være så synlig for sluttbrukere. Særlig EKOM-sektoren vil gjennomgå en stor endring i underliggende teknologi de neste fem til ti år, som ikke nødvendigvis er synlig for den generelle bruker.

FFI ser at noen teknologiske trender også vil påvirke NSM sitt ansvar, kompetansebehov og prosesser innenfor sikkerhetsgodkjenning av IKT-systemer, og dette er nevnt i rapporten. Noen av trendene kan også påvirke pågående nasjonal debatt innen frekvenser for nødnett og for nasjonal autonomi i EKOM-nett.

Risiko vil være avhengig av hvem du er og hvor du er. Sårbarheter som krever svært store ressurser å utnytte utgjør ofte en større trussel mot strategisk viktige aktører som Forsvaret og statsapparatet enn mot små- og mellomstore bedrifter og enkeltpersoner. Denne differensieringen er ikke eksplisitt nevnt i rapporten. Relatert til dette er det noen få trusler og sårbarheter vi mener kun vil få effekt for Forsvaret og utvalgte elementer av statsforvaltningen innenfor perioden på fem år, og disse er dermed utelatt. Et eksempel på dette er relasjonen mellom kvanteprosessering og kryptoalgoritmer.

2 De viktigste trendene

Arbeidet startet med å liste viktige teknologiske utviklingstrekk som deretter ble gruppert og satt sammen til fem hovedtrender som blir beskrevet her. De første tre er virtualisering, 5G, og kunstig intelligens og autonomi innenfor EKOM og IT. Sammen danner disse grunnlag for den kanskje største og mest betydningsfulle hovedtrenden som omhandler komplekse digitale verdikjeder og markedsutvikling. Den siste hovedtrenden beskriver tillitsskapende teknologier.

De to store trendene Internet of Things (IoT) og stordata (big data) er utelatt som overskrifter fra rapporten. Flere av sikkerhetsutfordringene ved disse trendene bør være kjente, og videre

utvikling av disse teknologiene vil inneholde mange av disse allerede kjente utfordringene. Sikkerhetsutfordringer og -muligheter som er nevnt i kapitlene om virtualisering, 5G og kunstig intelligens og autonomi vil i noe grad også gjelde for IoT. I tillegg kan anvendelse av IoT gi store utfordringer innen personvern. Mye av utviklingen innen kunstig intelligens og personvern krever stordata som en grunnleggende teknologi. Noen utfordringer knyttet til stordata kommer dermed til syne i disse kapitlene.

2.1 Virtualisering

Kort fortalt er målet med virtualisering[2] logisk å separere en tjeneste fra maskinvaren som kjører tjenesten. Virtualisering medfører at funksjonalitet flyttes fra maskinvare til programvare, noe som blant annet vil gi stor gevinst ved utrulling og realisering av nye tjenester. Dette fordi endringene kan gjøres i programvare istedenfor ved at fysiske komponenter må byttes ut.

Virtualiseringsteknologien i seg selv er ofte ikke synlig for sluttbrukerne, men effekten er synlig innen mange områder, og vi velger derfor å omtale virtualisering som eget punkt istedenfor en av anvendelsene av virtualisering. Virtualisering har en rekke konsekvenser innenfor sikkerhet som berører mer enn kun utvalgte anvendelsesområder for teknologien. Virtualisering er også en viktig byggekloss i de andre trendene som er nevnt i denne rapporten.

Skytjenester, ofte omtalt som «Cloud computing», er antagelig den mest kjente anvendelsen av virtualiseringsteknologi. Kommersielle skytjenester, som dataprosessering og datalagring, vil fortsette å øke i omfang og tilby nye sett med tjenester, og teknologien vil bli tatt i bruk på stadig flere områder. Skyteknologi er ikke låst til de store offentlige leverandørene som Google og Amazon. Teknologi som tillater virksomheter å mikse leverandører av skytjenester, og også tillater en miks av internt implementert datasenter og offentlige skytjenester, er allerede på markedet. Denne teknologien[3] forventes å øke sterkt i omfang de neste årene, sammen med verktøy som tillater virksomheter å ha større kontroll på hvordan virksomheten bruker forskjellige skytjenester, inkludert kontroll på plassering av datalagring. En økning i bruk av virtuelle arbeidsflater (Virtual Desktop Infrastructure) vil generelt øke datasikkerheten i virksomheter ved at mulige angrepsflater blir redusert. Liten til ingen datalagring på lokale datamaskiner reduserer sårbarheten for datalekkasje. Flytting av dataprosessering og -lagring fra lokale datamaskiner til sentrale lokasjoner vil også påvirke implementering av eksisterende sikkerhetsmekanismer samt gi noe økt sårbarhet grunnet avhengighet til sentrale tjenester. Vi forventer utover dette ingen store endringer innen risiko og sårbarhet tilknyttet skyteknologi i nær fremtid.

I tillegg til en naturlig videreutvikling av dagens bruk av virtualiseringsteknologier forventer vi to store endringer de neste årene relatert til virtualisering: Virtualisering av nettverksfunksjoner og helt nye konsepter og løsninger for helhetlig drift og vedlikehold av IKT-infrastrukturen.

[2] Store norske leksikon: https://snl.no/virtualisering_-_IT
[3] http://www.zdnet.com/article/hybrid-cloud-what-it-is-why-it-matters/

2.1.1 Virtualisering av nettverksfunksjoner

Virtualisering av nettverksfunksjoner (Network function virtualization (NFV)) er som nevnt i neste kapittel en viktig bestanddel av 5G, og vil komme for fullt innen fem år. NFV er allerede i bruk i noen datasentra[4], og det foregår pilottester hos flere store EKOM-leverandører på global basis[5]. NFV vil gjøre det samme for kommunikasjonsnettverk som skyteknologi og virtualisering har gjort for dataprosessering og datasentre. Istedenfor å ha dedikert maskinvare for hver enkelt nettverksfunksjon, blir nettverksfunksjoner applikasjoner som kjører på standard maskinvare. Et eksempel er at rutere fra firmaer som Cisco og Juniper blir erstattet av virtuelle «appliances» som kjører på standard dataservere[6]. Virtualisering av nettverksfunksjoner vil også medføre en utvidelse av hvilke funksjoner og tjenester som dekkes av begrepet nettverksfunksjon. Med denne teknologien vil det ikke lenger være forskjell på for eksempel sikkerhetsfunksjonalitet og ren nettverksfunksjonalitet som ruting. En brannmur eller tilsvarende teknologi vil også bli virtualisert på samme måte som andre nettverksfunksjoner.

Nettverksprodukter, både profesjonelt utstyr som står sentralt i EKOM-infrastrukturene og forbrukerutstyr som rutere, vil bli NFV-baserte. Oppgraderinger og vedlikehold av et stort antall forskjellig utstyr fra et stort antall forskjellige leverandører er vanskelig. Innholdet i mange av disse spesialiserte produktene er skjult for brukerne, og det kan være vanskelig og ta lang tid å implementere en sikkerhetsoppdatering. En flytting over til standard dataservere vil redusere både kompetansebehovet og sårbarheten i disse spesialiserte produktene. Tjenesteleveranser blir også uavhengige av dedikerte fysiske produkter og mer robust mot feil som oppstår i disse, ved at en tjeneste enkelt kan flyttes til en annen dataserver. Samtidig vil man møte de samme sikkerhetsutfordringene som andre IT-systemer kan rammes av. Dette kan være utilsiktede feil i programvare, feil under implementasjon og konfigurasjon, men også tilsiktede hendelser som for eksempel sabotasje eller spionasje gjennom cyberoperasjoner. Sentraliseringen kan føre til økt skadepotensiale ved at for eksempel feil kan ramme mange kritiske nettverksfunksjoner samtidig, men virtualiseringen gjør også at det blir enklere å rette opp feil. Det vil imidlertid kreve en annen kompetanse enn tidligere. Teknikere og ingeniører innen kommunikasjons-nettverk og nettverksutstyr må erstattes med programvareutviklere med spesialisert kompetanse innenfor virtualisering og kommunikasjonsnettverk.

Innføring av NFV vil også medføre endringer i hvordan virksomheter må tenke sikkerhet i sine nettverk. Eksisterende teknologier som «Intrusion Detection Systems» og «Deep Packet Inspection», vil bli kraftig berørt av innføring av NFV og programmerbare nettverk. Noen av disse teknologiene kan bli overflødige ved at det blir enklere å kontrollere trafikken i et nettverk, og noen av disse teknologiene vil konvergere sammen med annen nettverksteknologi.

[4] Se for eksempel: http://octo.vmvare.com/software-defined-telco-nfv og https://www.emc.com/about/news/press/2017/200170912-02.htm
[5] https://insight.nokia.com/nfv-mano-solutions-poc-production
[6] Google annonserte i april 2017 at de har begynt denne omleggingen på sine grensesnitt til de store Internett-leverandørene. Se https://www.blog.google.com/topics/google-cloud/making-google-cloud-faster-more-available-and-cost-effective-extending-sdn-public-internet-espresso/

2.1.2 Virtualisering av drift og vedlikehold av EKOM

Tjenesteleverandørene innen EKOM vil bruke virtualiserings- og skyteknologier til å virtualisere sine egne interne IKT-systemer, inkludert drift og vedlikehold. Sammen med den økte fleksibiliteten som kommer av virtualisering av nettverksfunksjoner, vil dette ha store konsekvenser for hele konseptet rundt drift av store infrastrukturer. Når slike interne IKT-systemer kan kjøres i et vilkårlig datasenter vil pris på strøm, prosesseringskapasitet med mere spille en større rolle i vurderingene av hvor disse tjenestene skal plasseres enn hvor den fysiske infrastrukturen er. Samtidig er stordriftsfordelene så store at det vil tvinge seg frem global eller regional konsolidering av driftssentre.

De store internasjonale selskapene vil på sikt samle sin kompetanse og sine driftsmiljøer på et fåtall steder på global basis. På lang sikt vil antagelig drift av en stor internasjonal EKOM-infrastruktur utføres fra et lite antall lokasjoner på verdensbasis, som roterer med døgnet. Selv norske selskaper kan finne det lønnsomt å ha disse miljøene lokalisert utenfor Norge. Den samme teknologien kan også tillate flytting av drift hjem til Norge ved behov. Dette er omtalt under kapittel 2.3 om kunstig intelligens og autonomi.

2.1.3 Dynamisk plassering av tjenesteproduksjon

Det er enda et aspekt av virtualisering som er viktig å nevne. Teknologien tillater dynamisk å flytte produksjon av enkelttjenester til det til enhver tid mest hensiktsmessige stedet. Dette kan utnyttes til alltid å ha de riktige tjenestene tilgjengelig på de riktige stedene til riktig tid. 5G-teknologi, som omtalt i neste kapittel, vil få denne egenskapen og dermed tillate dynamisk sammensetting og plassering av tjenester fra forskjellige aktører. En viktig forutsetning er nok dataprosesseringskraft lokalt og at tjenestene er virtualiserte. Denne utviklingen bør påvirke fremtidig design og implementering av kommunikasjonsnettverk for Nødnett og Forsvaret.

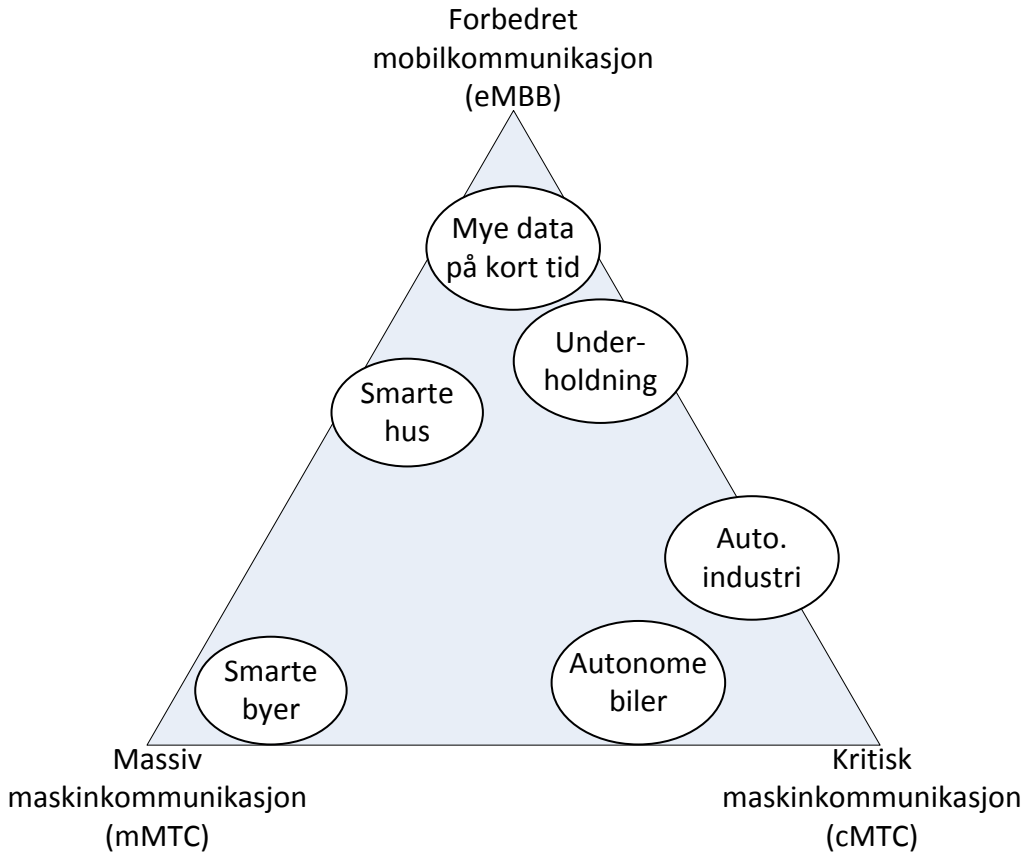
2.2 5G

Til forskjell fra tidligere generasjoner dreier ikke 5G (IMT2020[7]) seg bare om bedre datakapasitet, selv om dimensjonen «forbedret mobilkommunikasjon» (eMBB) utvilsomt gjør det. For eMBB er datakapasitet en svært viktig faktor, og det er denne dimensjonen som først og fremst blir frontet mot det kommersielle markedet for mobiltelefoni. De to andre dimensjonene, som er massiv og kritisk maskin-til-maskinkommunikasjon, vil mest sannsynlig få større konsekvenser for samfunnets sikkerhet og robusthet enn mer datakapasitet til konsumentmarkedet.

For operatørene vil det viktigste være trafikktetthet, det vil si flere enheter per flateareal og høyere datakapasitet per enhet. Mye av den økte datakapasiteten kommer ved å bruke vesentlig høyere frekvensbånd enn det en i dag gjør. Her skal en kunne nå overføringskapasitet på over 20 Gbit/s[8], men avstandene vil være korte og kapasiteten kan falle fort i miljøer som har ugunstige

[7] ITU utvikler teknologier og standarder for «5G» gjennom programmet IMT2020.
[8] https://www.itu.int/md/R15-SG05-C-0040/en

radiomessige forhold. Mye av denne hastighetsøkningen kommer av teknologi som kun fungerer i miljøer med mange basestasjoner og mulighet for utnyttelse av moderne antenneteknologier. De høyeste overføringskapasitetene vil for eksempel ikke være tilgjengelig utaskjærs eller i tynt befolkede områder.



Figur 2.1 Forskjellige tjenester som skal tilbys i 5G

2.2.1 Maskinkommunikasjon i 5G

Trekanten i figur 2.1 viser at mer datakapasitet kun er en liten andel av hele 5G-utviklingen. De to andre dimensjonene består av varianter av «Machine Type Communications» (MTC). MTC er i hovedsak kommunikasjon mellom maskiner, men vil også brukes innen tjenester for virtuell og utvidet virkelighet (VR/AR). Anvendelse av MTC vil drive utviklingen innen «Internet of Things» (IoT) i fremtiden, og IoT er derfor ikke omtalt spesifikt i denne rapporten.

"Massive MTC (mMTC)" fokuserer på å tilby dekning for et stort antall enheter. Disse vil være enkle IoT-enheter, og de vil ofte ha svært beskjedne kommunikasjonsbehov. Systemet må kunne støtte en million enheter per kvadratkilometer og enhetene skal kunne være operative i minst 10 år på kun batteridrift. Dette setter strenge krav til effektforbruk som vil begrense muligheten for

gode sikkerhetsalgoritmer[9] og prosedyrer. 5G-nettet kan derfor ikke pålegge energikrevende sikkerhetsprosedyrer for disse enhetene. Vi forventer derfor utvikling av nye lettvekts sikkerhetsprotokoller, spesielt innenfor autentisering, for å håndtere denne utfordringen. Inntil nye protokoller er utviklet vil mMTC være en stor sikkerhetsutfordring. Vi minner om at mMTC vil være en viktig teknologi innen IoT.

"Critical MTC (cMTC)" har helt andre krav enn mMTC. Her er høy pålitelighet (svært lavt pakketap), lav forsinkelse (ned mot 1 ms), til dels høy overføringshastighet og «sterk» sikkerhet viktige krav. Industriell automasjon og autonomi (selvstyrte kjøretøy med mere) er viktige bruksområder her, men dimensjonen skal også kunne håndtere nødetater og andre samfunns-viktige funksjoner. For å få virkelig lav forsinkelse vil såkalt «edge computing» eller «fog computing» tas i bruk. Disse konseptene er basert på virtualiserte funksjoner og tjenester, og innebærer at deler av nettverkslogikken flyttes utover i nettet, så nært brukeren som mulig, for å redusere forsinkelse. Her ser en også for seg å flytte tjenestelogikken («business logic») helt ut i operatørens infrastruktur, og en ser også muligheten for at funksjoner og tjenester er mobile og kan følge kunden uavhengig av brukerens fysiske tilkopling til infrastrukturen.

IMT-2020 skisserer altså forskjellige løsninger for forskjellig bruk. Det vil ikke være én enkelt teknologi som klarer å dekke alle funksjonene som er vist i figuren. 5G vil derfor inneholde mange forskjellige teknologier og løsninger, tilpasset ulike behov. Radioteknologi som oppfyller kravet til datakapasitet i bredbåndsmarkedet vil ikke være egnet for å gi robust kommunikasjon til kritisk viktige funksjoner.

5G- infrastrukturen vil bli bygget på virtualiseringsteknologier som omtalt i kapittel 2.1 og kunstig intelligens som blir omtalt i kapittel 2.3. 5G-infrastrukturen vil dermed få endret karakter innen sikkerhet og robusthet.

2.2.2 Sikkerhet i 5G

Det er rimelig å regne med at cMTC potensielt kan gi bedre robusthet for utvalgte kunder og tjenester enn dagens mobilnett da dimensjonen vil ha fokus på høy pålitelighet.. En usikkerhet innen cMTC er den markedsmessige situasjonen. Hvis EKOM-leverandørene selv får velge hvilke dimensjoner av 5G de vil levere, er det mulig at fokus stort sett blir på mer datakapasitet til forbrukermarkedet, særlig i starten av 5G-utrullingen.

Utover dette bør en anta at 5G vil ha samme eller lavere sikkerhet enn dagens systemer. Dette betyr at brukerne av 5G-tjenester selv må sørge for sin egen kommunikasjonssikkerhet. Slik sett er det ingen reell endring fra dagens situasjon. Ettersom mobilnettene nå er kritiske infrastrukturer for nesten alle virksomheter er det svært viktig at virksomhetene har et realistisk bilde av både svakhetene og mulighetene som 5G gir.

For 5G-infrastrukturen vil situasjonen bli helt ny. Introduksjonen av NFV og nye løsninger for drift og vedlikehold, vil åpne for både bedre og billigere nettverk. Dette er avgjørende for at en

[9] https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf

skal kunne klare å tilby nye tjenester til akseptable priser, men det åpner naturlig nok opp for helt nye trusler. Truslene mot programvarebaserte systemer inkludert NFV er dog ikke helt nye. De store datasentrene (cloud computing) har allerede tilsvarende teknologi, og skytjenester er jo basert på virtualisering. Trusler og dataangrep en har sett her vil i stor grad også angå 5G-infrastrukturen. Det samme vil gjelde mottiltak. Utstrakt bruk av maskinlæring og algoritmer for å operasjonalisere policy-håndtering vil kunne gi både langt bedre effektivitet, men også mindre kontroll. Totalt sett betyr dette at drift av den nye 5G-infrastrukturen blir langt mer spesialisert enn den hittil har vært, og mye rutinemessig administrasjon vil bli automatisert. Behovet for høy kompetanse vil øke. Tjenesteleverandørene vil i større grad anskaffe ferdig forvaltede teknologiløsninger istedenfor å kjøpe inn utstyr og integrere dette i sin infrastruktur selv. Dette betyr at leverandørene av utstyr også vil stå for driften av utstyret og de tjenestene utstyret implementerer. Dermed blir noe sikkerhetsfunksjonalitet også håndtert av ekstern leverandør.

Det er verdt å nevne at 5G-infrastrukturen ikke vil støtte 2G (GSM/EDGE) eller 3G (UMTS) aksessnett. Dette betyr ikke at 2G eller 3G vil forsvinne i 2020, men det betyr at disse nettene ikke blir en del av nyutviklingen, og at de fortsatt vil være egne infrastrukturer separert fra 5G-infrastrukturen, eventuelt implementert som en egen virtualisert funksjon. Det er derfor trolig at både 2G og 3G blir dyrere å drifte etter hvert, og de vil antagelig fases ut ganske raskt. 3G vil antagelig forsvinne før 2G grunnet støtten for tale i 2G. Virksomheter som har basert seg på 2G- eller 3G-teknologier bør derfor snarest utarbeide planer for overgang til 4G eller 5G. Et eksempel er at mye velferdsteknologi i helsesektoren fortsatt bruker 2G og til dels 3G. Kommuner, og andre aktører, må derfor forberede kommende bortfall av først 3G og så 2G mobilteknologi.

2.3 Kunstig intelligens og autonomi innenfor EKOM og IT

Kunstig intelligens og autonomi vil innta flere og flere områder i samfunnet. Selvkjørende biler er ett eksempel. Kunstig intelligens vil også innta datasenter- og EKOM-sektoren innenfor femårsperioden, men muligens ikke i full skala før nærmere 2025.

Videre i rapporten bruker vi uttrykket «kunstig intelligens» som et samlebegrep for mange relaterte teknologier, inkludert begreper som maskinlæring[10], «deep learning» og autonomi.

Det er i hovedsak to utviklingstrekk som driver frem bruk av kunstig intelligens innenfor EKOM og databehandling: 1) Programvaredefinerte nettverk (SDN) og virtualisering, og 2) kompleksitet i moderne EKOM- og datasystemer.

Behovet for økt skalerbarhet i store datasentre kom med fremveksten av skytjenester og selskaper som Google og Facebook på 2000-tallet. Dette krevde nye metoder for drift og vedlikehold av både datasystemene i datasenteret og datanettverkene i og mellom datasentre. Mange prosesser som tidligere krevde menneskelig interaksjon er nå fullstendig automatisert. Samtidig ser vi at fremtidens EKOM, og særlig utviklingen mot 5G med «Machine Type

[10] Samuel, A.L. (1959) "Some studies in Mashine Learning Using the Game of Checkers", *IBM J. Res. Dev.*, 3(3):210-219

Communications», får en kompleksitet og skala som gjør det nær umulig å bruke manuelle prosesser i drift og vedlikehold. Nettverkstrafikken vil måtte styres både etter hvilken type trafikk det er, for eksempel streaming av en film, kritisk sensorinformasjon eller twitter-meldinger, men også etter hvilke kommunikasjonsløsninger som er tilgjengelige. Fremveksten av programvarebasert nettverk og virtualisering muliggjør bruk av dataalgoritmer som kontrollerer datasystemer og kommunikasjonsnettverk. De nye kommunikasjonsnettverkene krever derfor avansert nettverksstyring i stor skala, som blir muliggjort ved hjelp av virtualisering av nettverksfunksjoner og kunstig intelligens.

Innenfor EKOM har det den senere tid vokst frem helt nye løsninger for «Management and Network Orchestration» (MANO) fra både Metro Ethernet Forum[11] og kommersielle selskaper som AT&T og China Mobile gjennom initiativ som Open Network Automation Platform[12]. Disse nye konseptene og løsningene for MANO er alle basert på policydrevet arkitektur som tillater kunstig intelligens og automatisering av alle standardprosesser i et EKOM-nett. Tilsvarende løsninger eksisterer allerede for datasentre.

Kunstig intelligens har også gjort sitt inntog i manipulasjon av opinionen gjennom spredning av falske nyheter og annen propagandainformasjon. Dette skjedde svært aktivt under 2016-presidentvalget i USA og under 2017-valget i Storbritannia[13]. Se også avsnittet «Personvern» i kapittel 2.5.1.

2.3.1 Sikkerhetsmessige konsekvenser ved kunstig intelligens i EKOM og IT

Når kunstig intelligens styrer nettverk og datasystemer vil dette medføre ikke-verifiserbare systemer. Systemeiere kan ikke til enhver tid ha full oversikt over oppførselen til sine data- og EKOM-systemer. Dette er også en utfordring innen sikkerhetsgodkjenning av systemer. Dagens regime for sikkerhetsgodkjenning blir utfordret når et systems oppførsel kan endres basert på automatiserte algoritmer. Merk at kompleksiteten i moderne og kommende EKOM- og datasystemer er så høy at det heller ikke er mulig for menneskebaserte prosesser å ha full kontroll over systemet til enhver tid, så alternativet til kunstig intelligens vil heller ikke være lett å håndtere.

Innføring av kunstig intelligens vil også utfordre kompetanseprofilen til systemeiere. Utvikling av algoritmer for kunstig intelligens krever meget høy kompetanse, samtidig som behovet for dagens driftsingeniører blir kraftig redusert. Det er liten garanti for at denne spesialiserte kompetansen vil eksistere i Norge. Det er mulig at slik kompetanse kun vil være tilgjengelig hos et fåtall spesialiserte firmaer på global basis. Det er initiativ, blant annet hos Telenor i samarbeid med NTNU[14], som har som mål å utvikle nasjonal kompetanse innenfor feltet.

Kunstig intelligens sammen med virtualisering, som nevnt tidligere, vil antagelig gjøre det lettere konseptuelt for EKOM-leverandørene å opprette nasjonal autonomi i sine EKOM-nett.

[11] https://wiki.mef.net/display/CESG/MEF+55+-+LSO+Reference+Architecture
[12] https://www.onap.org/
[13] http://comprop.oii.ox.ac.uk/2017/05/31/junk-news-and-bots-during-the-2017-uk-general-election/
[14] https://www.ntnu.no/aktuelt/pressemeldinger/2017/ai-lab

Så lenge de systemene bygget på kunstig intelligens klarer å håndtere de forskjellige situasjonene det er satt krav om, vil det være mulig å drifte og forvalte EKOM-nett nasjonalt. Kunstig intelligens gjør det også mulig å utvikle scenario-basert oppførsel i EKOM-nettene. Det kan etableres forskjellige policyer som dekker forskjellige beredskapssituasjoner, som for eksempel større naturkatastrofer, terror eller militære anslag. EKOM-nettene kan gjennom dette endre oppførsel automatisk basert på uventede hendelser i deler eller hele landet. Dette kan skje uten at det nødvendigvis finnes kompetent personell i Norge. En slik bruk av kunstig intelligens må være forhåndsplanlagt og det må eksistere nok dataprosesseringsressurser (datasentre) i Norge til å håndtere hendelsen i henhold til kravene.

Som tidligere nevnt er det så store stordriftsfordeler ved å ta i bruk denne teknologien at internasjonale firmaer, også muligens norske selskaper, vil samle all sin overordnete drift og forvaltning på regionalt (verdensdel) eller globalt nivå. Slik drift vil bli utført fra lokasjoner med billig og stabil datakraft, som ikke nødvendigvis befinner seg i Norge. Det er etter vår vurdering lite sannsynlig at selskaper med majoritetseiere utenfor Norge vil ha driftssenter og kompetanse i Norge hvis det ikke opprettes spesielle økonomiske og/eller regulatoriske forhold for å tilrettelegge for slik virksomhet.

2.4 Komplekse digitale verdikjeder og markedsutvikling

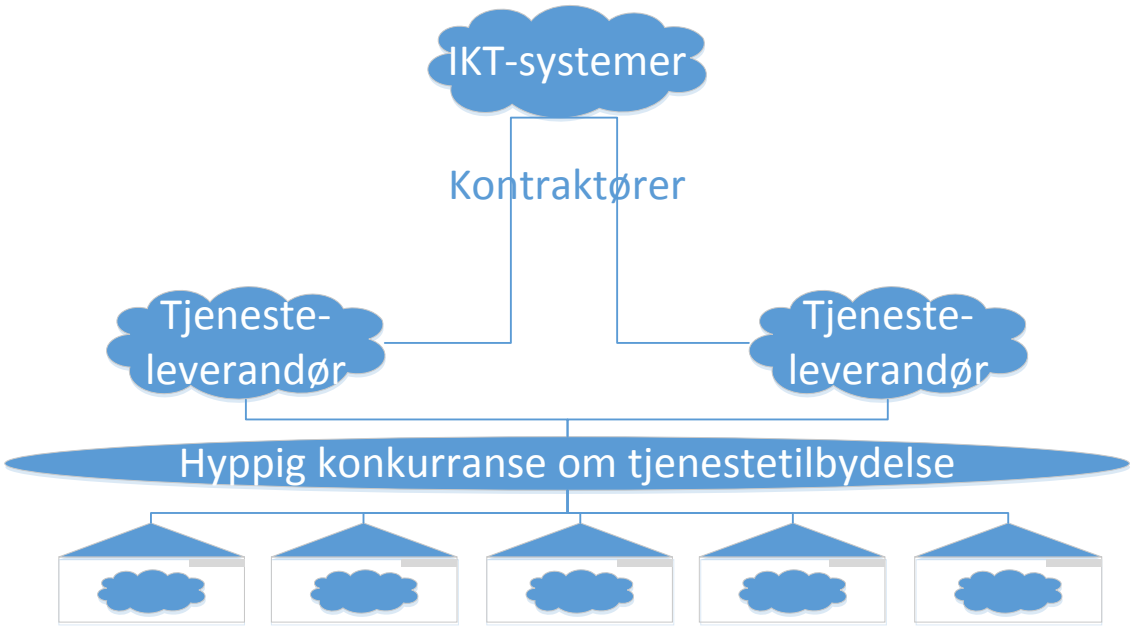
Vi støtter opp under Lysne-utvalgets konklusjoner om uoversiktlige digitale verdikjeder. Denne utviklingen vil fortsette, og kompleksiteten i avhengighetene mellom de tjenestene som brukerne ser og de underliggende infrastrukturene som støtter opp under disse tjenestene vil øke. Nye teknologier som programvaredefinerte nettverk (SDN) og nettverksvirtualisering (NFV), sammen med nye metoder for drift og forvaltning av både datasentre og EKOM-systemer, vil gjøre det enda vanskeligere for brukerne i fremtiden å kunne ha full kontroll over verdikjedene.

Virtualiseringen som kommer innen både datasentre og EKOM vil medføre konsolidering av teknologi på infrastruktursiden. Det vil oppstå en sammensmeltning av EKOM og datasentre, og EKOM-tjenestene vil stort sett bli usynlige for den jevne bruker. Brukerne vil i enda større grad benytte "Over The Top"-tjenester som Facetime, Snapchat, Google Hangouts og tilsvarende tjenester fra store leverandører som Google, Apple, Facebook og Amazon (GAFA) istedenfor de tradisjonelle tjenestene som telefoni og SMS. Denne utviklingen har pågått en del år, men med den kommende utbyggingen av 5G, med medfølgende teknologier, vil denne utviklingen mest sannsynlig skyte fart. Datasenter- og nettverksfunksjonalitet, inkludert tradisjonelle IT-tjenester, vil også etter hvert bli «app'er», som benyttes på samme måte som en app på en mobiltelefon i dag.

Som nevnt vil teknologiutviklingen innenfor styring og forvaltning av infrastrukturer, også tillate kunstig intelligens. Kunstig intelligens vil bli benyttet av de store aktørene til å håndtere all underliggende teknologi, det vil si de digitale verdikjedene. Dette har både positive og negative konsekvenser for sikkerhet og robusthet. De positive er mulighet for økt uavhengighet til de underliggende tjenestene. Kunstig intelligens vil tilpasse seg enhver tid gjeldende forhold,

og gjøre brukerfunksjonene uavhengig av hvilke EKOM-leverandører og teknologier som benyttes. For eksempel vil 5G-tjenester bli levert over et stort antall forskjellige teknologier fra trådløse lokalnett (Wi-Fi) og høyhastighets mobilteknologi til kablede forbindelser. Den negative siden er at det vil være vanskeligere å opprettholde oversikt over de digitale verdikjedene. Dette kan blant annet gjøre det vanskelig å ha oversikt over hvor informasjon lagres og hvordan den håndteres. Manglende mulighet til oversikt og kontroll av verdikjedene vil også gjøre det vanskeligere for trusselaktører å skaffe seg den samme oversikten.

En sannsynlig utvikling er at GAFA-leverandørene blir fullstendige tjenesteleverandører, og det er mulig at dette også vil gjelde selskaper som Netflix og HBO. Med den teknologiske utviklingen som kommer med 5G, basert på SDN og NFV, kan disse tjenesteleverandørene, som en del av sin abonnementskostnad, tilby brukerne tilknytning til internettbaserte tjenester nesten uavhengig av hvor brukeren befinner seg. Brukerne slipper dermed først å bestille tilgang til Internett fra en leverandør før han/hun bestiller tjenester fra GAFA eller Netflix/HBO. Høyere lags tjenesteleverandører vil i størst mulig grad benytte tredjepartsleverandører for EKOM-tjenester og kan bygge egne tjenester der hvor tredjepartsleverandører ikke er tilgjengelig. Denne utviklingen er allerede synlig gjennom diverse initiativ fra Google og Facebook, hvor Google og Facebook etablerer seg som EKOM-leverandører i områder med dårlig utbygd eller dårlig regulert infrastruktur. En fare med denne utviklingen er mulighet for segmentert Internett. Det er indikasjoner på at brukerne kan bli låst til den GAFA-leverandøren brukeren velger, og få dårligere tilgang til andre tjenester på Internett[15].



Figur 2.2 Verdikjeder

Figur 2.2 viser et hierarki av tjenesteleverandører. En bedrift, skissert på øverste linje, har som oftest langsiktige avtaler med et fåtall store tjenestetilbydere. Disse vil igjen benytte et stort

[15] https://www.wired.com/2016/01/facebook-zuckerberg-internet-org/

antall forskjellige underleverandører. Figuren inneholder kun 3 nivåer, men i realiteten vil det være flere nivåer. Kunstig intelligens vil brukes for å håndtere det store antallet underleverandører, og automatisk tilpasse seg forskjellige hendelser hos underleverandørene. Effekten vil mest sannsynlig være lavere avhengighet til en bestemt dominerende underleverandør. Denne teknologien vil også tillate at konkurransen om leveranser vil bli meget hyppig, antagelig flere ganger i døgnet. Konsekvensen er at virksomheter mister muligheten til å kontrollere sine digitale verdikjeder.

2.5 Tillitsskapende teknologier

Med tillitsskapende teknologier mener vi teknologier og teknologiutvikling som påvirker særlig personvern og samfunnets tillit til både teknologi og forskjellige aktører. Vi inkluderer også trender som påvirker datasikkerhet generelt.

2.5.1 Personvern

Snowden-avsløringene har bidratt til økt fokus på personvern, og dette vil få effekt i den kommende perioden, for eksempel gjennom nytt direktiv fra EU som trer i kraft i 2018[16].

Nytt EU-direktiv om personvern vil gi skjerpede krav til både behandling av personopplysninger og krav til varsling ved eventuelle brudd på direktivet. I tillegg vil det komme straff i form av bøter til firmaer som bryter personverndirektivet. Særlig det siste punktet vil føre til at sikring av interne data, inklusive personsensitiv informasjon, vil få større fokus i mange bedrifter.

Grunnet mer fokus på personvern og de skjerpede kravene for oppbevaring av personopplysninger forventer vi at særlig små og mellomstore bedrifter vil sette ut drift og forvaltning av sin datasikkerhet til tredjeparts spesialister. Dette vil mest sannsynlig få en positiv effekt på datasikkerhet generelt og personvern spesielt, da små og mellomstore bedrifter i dag ofte ikke vil evne å ha slik kompetanse i egen organisasjon.

Store nasjonale og internasjonale konserner, inkludert GAFA, har meget stort fokus på egen sikkerhet. Det vil si at de må sikre sin egen virksomhet både mot uheldig omtale og mot direkte påvirkning av egne datasystemer. Økt personvern er en bieffekt av dette, og den virkningen må ikke undervurderes. Store selskaper har ikke råd til å få dårlig omtale innen egen sikkerhet og vern av kundenes data. De er også indikasjoner på at de store selskapene sterkere vil regulere og kontrollere hvordan sine samarbeidspartnere bruker og utveksler sensitiv informasjon. Det er derfor vår vurdering at utilsiktet spredning av personinformasjon vil reduseres fremover.

Likevel er det slik at mange forbrukere ønsker tjenester som er personlig tilpassede og dermed mer eller mindre bevisst gir fra seg informasjon om seg selv til tjenestetilbydere og «app-er», for eksempel geografisk posisjon, interesser med mere. I andre tilfeller kan man bli «tvunget» til å gi fra seg informasjon til tredjeparter for å kunne benytte enkle tjenester på telefonen.

[16] https://www.eugdpr.org

Mengden informasjon vi frivillig gir fra oss vil mest sannsynlig fortsette å øke. Dette medfører at store selskaper besitter store menger informasjon om enkeltpersoner, som brukes for å tilpasse tjenester per bruker. Samtidig blir det mindre sannsynlig at informasjon blir spredt utilsiktet gjennom datainnbrudd og likende.

Valget i USA i 2016 synliggjorde en helt ny industri som spesialsyr informasjon mot forbrukere i hensikt å påvirke meninger. Underliggende teknologier er både stordata og forskjellige former for kunstig intelligens. I USA-valget ble dette brukt direkte for å påvirke velgere som med stor sannsynlighet lot seg påvirke av rettet informasjon, men teknologien kan også brukes for opinionspåvirkning innen andre områder enn politikk. Effekten av denne teknologien er sannsynligvis ikke fullt utforsket ennå, og vi forventer mer bruk av den i fremtiden. Denne teknologien er blitt mulig fordi personopplysninger har blitt en handelsvare på det åpne markedet.

2.5.2 Blockchain

Blockchain er en teknologi som muliggjør offentlig og distribuert godkjenning (sertifisering) av innhold. Bruken av blockchain er mest kjent gjennom den digitale valutaen Bitcoin hvor teknologien benyttes til å vedlikeholde en liste over alle transaksjoner som gjennomføres med valutaen. Listen («blockchain») kan senere benyttes til å verifisere at transaksjoner faktisk har funnet sted. Blockchains vurderes for tiden i en rekke protokoller til å verifisere integritet av data. Noen mulige eksempler er offentlige lister[17] med aksesshistorikk av sensitive data, som pasientjournaler og skattelister.

De store mulighetene i blockchain-teknologien ligger i at det er en distribuert modell som ikke er avhengig av sentrale noder, det vil si uten tiltrodde tredjeparter som for eksempel bankvesen og notarius publicus. Denne distribuerte tilliten som teknologien muliggjør vil gi oss nye samarbeidssystemer på alle nivåer, fra mindre grupper av mennesker til systemer som overholder integriteten i data utvekslet mellom (grupper av) nasjoner.

Det kan finnes grunnleggende svakheter i noen Blockchain-systemer hvor det oppstår en situasjon der tilliten kan misbrukes. Dette har for eksempel kommet til syne i Bitcoin, hvor et problem oppstår dersom en entitet/organisasjon som er med i den felles godkjenningen av transaksjonslisten kontrollerer over halvparten av ressursene benyttet til å generere denne blockchainen. I tillegg vil også offentlige transaksjonslister ha mange personvernutfordringer, for eksempel dersom koblinger til identiteter blir offentlig tilgjengelige.

2.5.3 Betalingstjenester

Digitale betalingstjenester har lenge vært under konstant utvikling og eksperimentering, men utviklingen, introduksjonen og den enkle tilgangen til bruk av digital valuta sammen med bruk av blockchain-teknologi, har skjøvet ytterligere fart i denne prosessen. World Economic Forum

[17] https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector

tror at kompleksiteten i internasjonale banktransaksjoner er noe av det første som kommer til å forenkles ved bruk av blockchain-teknologi[18].

Dersom internasjonale teknologiske løsninger som involverer forenklet bruk og lavere transaksjonskostnader blir etablert utenfor regulatoriske myndigheters kontroll, vil dette raskt skape et globalt marked med fullt legale transaksjoner. Dersom slike løsninger etablerer seg som en standard, vil den raskt også tas i bruk til illegal virksomhet og bli svært vanskelig å regulere i etterkant. Dette er omtrent situasjonen med de digitale valutaene Bitcoin og Ether i dag. Utbredelsen av digital valuta og ikke minst tilgang til anonyme (ikke-sporbare) digitale valutaer vil sette ytterligere press på myndigheter for å beholde mulighetene til å fange opp skatteunndragelser, illegale transaksjoner, finansiering av terror, med mere.

2.5.4 Automatisert og tvungen sikkerhet

Historisk har oppdateringer av operativsystemer, applikasjoner med mer vært overlatt til brukerne. I mange tilfeller er sikkerhet overlatt til tredjepartsleverandører som for eksempel antivirusprogramvare. I de nyeste operativsystemene er det en trend at leverandørene overtar dette ansvaret selv gjennom at sikkerhetsoppdateringer blir tvunget på brukerne. Dette gjelder både operativsystemer og applikasjoner. For leverandørene bidrar dette til mye enklere brukerstøtte da det blir færre varianter av systemer med oppdateringer å holde orden på.

De store leverandørene av IKT-produkter, inkludert leverandører av operativsystemer, er avhengig av brukernes tillit til sikkerhet i sine produkter, og tvungen sikkerhetsoppdatering av produkter vil fjerne mange eldre sårbarheter. Dette vil kunne forhindre vidtspredende forsøk på datainnbrudd som påvirker ikke-oppdaterte systemer som vi nylig har sett eksempler på [19]. Med innføring av NFV, se kapittel om virtualisering, vil det også være enklere for tjeneste-leverandører å gjennomføre oppdateringer i systemer og utstyr som er plassert ute hos kundene.

Ulempen for brukerne er at slike oppdateringer kan endre oppførselen til et system uten at brukerne får et forvarsel. Dette er spesielt gjeldende hvis brukerne benytter tredjeparts programvare hvor leverandørene av denne programvaren ikke forbereder seg til disse oppgraderingene.

Vår mening er at denne trenden i stor grad vil øke datasikkerheten i konsumentmarkedet og i små og mellomstore bedrifter.

2.5.5 Konsekvenser ved økt fokus på tillitsskapende teknologier

Regulering er et nødvendig verktøy for å håndtere ny teknologi. Det som er spesielt med de nevnte tillitsskapende teknologiene er at regulering bør etableres og tilpasses på et tidlig tidspunkt. Dette må reflektere den graden av åpenhet som er forventet og akseptert i samfunnet, samt forsøke å minimalisere de utfordringer som er nevnt i kapitlet.

[18] https://www.weforum.org/agenda/2017/11/the-rise-of-bitcoin-doesnt-mean-the-end-of-banks-heres-why/
[19] Eksemplifisert med WannaCry: http://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack

Mekanismer for å forsvare EKOM og IT-systemer vil alltid teknologisk kunne utnyttes for overvåking og kan medføre svakheter innen personvern. Innføring av slik teknologi uten åpenhet om bruken kan potensielt redusere samfunnets tillit til IT-teknologi.

Økt bruk av tredjeparts tjenester vil på sikt antagelig øke personvern og datasikkerhet for konsumentmarkedet og små- og mellomstore bedrifter. Dette vil derimot forsterke dagens situasjon, hvor noen store selskaper besitter store menger informasjon om mange mennesker. På en annen side vil utviklingen bidra til å redusere risiko for at ukjente aktører henter ut persondata fra mindre sikrede datasystemer.

3 Oppsummering

Målsetningen med denne rapporten har vært å undersøke trender innen digitale verdikjeder og påpeke mulige sikkerhetsmessige konsekvenser av disse trendene. Tidsaspektet for trend-analysen ble satt til fem år.

Det har vært en utfordring å sortere og strukturere innholdet da noen av de nye teknologiene vi ser komme kan kobles til flere ulike trender og motsatt. Vi har valgt å dele inn i følgende fem hovedtrender: virtualisering, 5G, kunstig intelligens og autonomi innenfor EKOM og IT, komplekse digitale verdikjeder og markedsutvikling, og tillitsskapende teknologier. Disse trendene vil gi både sikkerhetsmessige utfordringer og muligheter.

Den kanskje største utfordringen vil være at de digitale verdikjedene vil bli enda mer komplekse og uoversiktlige. Det vil være svært vanskelig å vite hvilke underliggende tjenester og teknologier som er involvert når man for eksempel bruker en «app» på telefonen. Det vil være kompliserte avhengigheter mellom tjenestene og teknologiene, og som igjen blir styrt av virtualisering og kunstig intelligens. Dette vil for eksempel vanskeliggjøre vurderinger knyttet til personvern.

Denne kompleksiteten gjør det også vanskeligere å ha kontroll med hvilken informasjon vi gir fra oss. Ved hjelp av stordata og kunstig intelligens kan denne informasjonen for eksempel brukes til å skreddersy nyhetsmeldinger til ulike befolkningsgrupper for å endre opinionen i samfunnet. I ytterste konsekvens vil dette være en trussel mot vårt demokratiske system.

En annen utfordring er at tjenesten «massiv MTC», som skal møte kravene fra IoT i 5G, antakelig vil få dårligere sikkerhet enn det vi ser i 4G i dag, da kravet til lavt effektforbruk vil begrense muligheten for gode sikkerhetsalgoritmer/prosedyrer.

Den teknologiske utviklingen kan gi oss nye muligheter når det gjelder sikkerhet. Spesielt gjelder dette innen blockchain-teknologien hvor en del tjenester som trenger en tiltrodd

tredjepart, vil kunne bli enklere og rimeligere. Et kjent eksempel her er digital valuta og bankvesenet. Videre vil virtualisering av nettverksfunksjoner og nye konsepter for drift og vedlikehold av IKT-infrastrukturen antakelig gi økte muligheter for nasjonal autonomi i EKOM-nett. En kan også anta at tjenesten "kritisk MTC" i 5G vil få bedre sikkerhet enn det 4G tilbyr i dag, fordi det vil være strenge krav til pålitelighet og robusthet. Virtualisering og kunstig intelligens vil også føre til økt robusthet fordi det vil være enklere å benytte ulike typer tjenester og teknologier. Samtidig vil vi antakelig se mer automatisert sikkerhet der en ikke blir avhengig av at alle husker å oppdatere programvaren sin.

En annen faktor er at mer fokus på personvern er i ferd med å gi sterkere regulering fra myndighetenes side på dette feltet.

About FFI

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

FFI's MISSION

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

FFI's VISION

FFI turns knowledge and ideas into an efficient defence.

FFI's CHARACTERISTICS

Creative, daring, broad-minded and responsible.

Om FFI

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

FFIs FORMÅL

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

FFIs VISJON

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs VERDIER

Skapende, drivende, vidsynt og ansvarlig.

FFI's organisation

Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

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

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

Office address:
Instituttveien 20
N-2007 Kjeller

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

FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment