Kap 7: **5G-sikkerhet: Norge mellom stormaktene**

Karsten Friis

Olav Lysne

6.1. **Introduksjon**[1]

I dette kapittelet tar vi for oss en digital sårbarhet som har dannet grunnlag for en opphetet sikkerhetspolitisk debatt både nasjonalt og internasjonalt. Denne sårbarheten er relatert til utbyggingen av femte generasjons mobilnett – 5G-nett – og det faktum at den største leverandøren av utstyr til slike nett kommer fra Kina. De senere par årene har vi sett en omfattende internasjonal debatt knyttet til de sikkerhetsmessige risikoer som er knyttet til dette forholdet. Fra vestlig side har man uttrykt bekymring for at kinesisk-produserte mobilnett kan misbrukes av Kina til spionasje eller sabotasje. Fra kinesisk hold blir det gjerne

Dette er en fagfellevurdert, akseptert postprint-versjon av følgende publiserte bokkapittel: Friis, Karsten; Lysne, Olav (2022). 5G-sikkerhet: Norge mellom stormaktene. Friis, Karsten; Bergsjø, Håkon (Red.). Digitalisering og internasjonal politikk. Kapittel 8. s. 147-169. Universitetsforlaget. URL: https://www.universitetsforlaget.no/digitalisering-og-internasjonal-politikk

hevdet at det er handelspolitiske forhold og global maktkamp som driver denne debatten fra vestlig side snarere enn en reell bekymring for systemenes sikkerhet.[2]

Det har vært krevende for mindre land, slik som Norge, å navigere i dette krysspresset fra stormaktene. I dette kapitlet spør vi hvordan Norge har håndtert dette. Før vi kommer dit vil vi imidlertid diskutere de teknologiske og sikkerhetspolitiske rammene som denne debatten utspiller seg i. Vi vil argumentere at det er visse teknologiske realiteter som springer ut av 5G-nettenes forventede sentrale plass i fremtidig digital infrastruktur, samt av at en teknologisk løsning på hvordan man kan beskytte seg mot digitale angrep fra de som har bygget utstyret i infrastrukturen ikke synes å være i sikte. Vi vil også diskutere den internasjonale maktkampen mellom USA og Kina samt noen ulike internasjonale initiativ knyttet til 5G som har påvirket prosessen i Norge. Til slutt vil vi se på den norske politiske debatten og hvordan norske myndigheter har manøvrert mellom teknologiske krav og politisk press. Vi vil konkludere at norske myndigheter ser ut til å ha balansert dette ganske bra og funnet løsninger uten å skape for mye politisk kontrovers.

6.2. **Hva er 5G, og hvorfor er det viktig?**

Den intense og plutselige debatten som kombinasjonen av 5G og kinesiske leverandører har avstedkommet etterlater et inntrykk av at utrullingen av 5G fører til et avhengighetsbilde mellom nasjoner og leverandører av IKT-utstyr som vi tidligere ikke har sett. Dette inntrykket er unøyaktig. Det er sant at 5G muliggjør en rekke nye anvendelser for kommuniserende systemer. Det forventes at den vil være instrumentell for utviklingen av tingenes internett, for styring av roboter over lange avstander og for autonome kjøretøyer for å nevne noe. Det er likevel grunnlag for å hevde at 5G representerer et naturlig neste skritt i en digitalisering av samfunnet, mer enn at det er en disrupsjon som åpner nye og hittil ukjente sårbarhetsflater.

En mer presis beskrivelse vil være at alle moderne samfunn de siste to tiår gradvis har migrert mange sentrale samfunnsfunksjoner over på en grunnmur bestående av en digital infrastruktur. Denne endringen har vært drevet av teknologiske nyvinninger, av økonomiske krefter og av et ønske om bedrede tjenesteleveranser til samfunnet som helhet. Parallelt med denne utviklingen har nye sårbarhetsflater kommet til, og disse blir debattert og adressert etter hvert som man blir oppmerksomme på den. Sårbarheter knyttet til leveransekjeden bak digitalt utstyr er et tema som kun forholdsvis nylig har fått politiske konsekvenser. Realitetene bak sårbarhetene har imidlertid vært tilstede over lengre tid.

6.2.1. Utviklingen av mobil kommunikasjonsteknologi

Mobil kommunikasjonsteknologi for forbrukermarkedet hadde sin spede begynnelse på 70-tallet. I flere land ble det bygget infrastruktur for bruk av analoge mobiltelefoner, og med NMT-standarden var Skandinavia langt fremme på dette området.[3] Digitale mobiltelefoner og tilhørende infrastrukturer kom med GSM-standarden, og utover 1990-tallet gjorde den mobiltelefoner til allemannseie. Den neste runden med standarder for mobil kommunikasjon ble rullet ut tidlig på 2000-tallet, og fikk navnet 3G. Dette navnet pekte på at dette var den tredje generasjonen av standarder for mobil telefoni, og det førte til at de to tidligere standardene begynte å bli omtalt som 1G for den første analoge standarden, og 2G for GSM.

Det nye som 3G brakte på banen var en kapasitet for dataoverføring som gjorde at mobilteknologien kunne benyttes til krevende internettoppkoblinger[4]. Det ble mulig å strømme både lyd og film over mobilnettene, noe som hadde en disruptiv effekt på både musikk-, TV- og filmbransje, og den la et muliggjørende grunnlag for den brede interaksjonen over sosiale medier som vi i dag anser som hverdagslig[5]. 4G ble rullet ut fra omlag 2010, og brakte med seg en kraftig kapasitetsmessig forbedring i forhold til 3G[6]. Der hvor alle de tre første generasjonene hadde markert startskuddet for betydelige endringer i måten folk kommuniserte med hverandre på vil effekten av 4G heller kunne beskrives som en videreføring og forsterkning av endringer som allerede var påbegynt.

Forventningene til samfunnsendringer som følger av 5G er på nivå med eller høyere de vi har sett for 2G og 3G. Spekulasjonene er mange, men spesielt tre anvendelsesområder peker seg ut ved å både være teknologisk sannsynlige og å ha en samfunnsmessig endringskraft.

1. 5G er laget for å være den ene teknologien som kan dekke alle infrastrukturbehov for mobil og trådløs kommunikasjon. En vanlig situasjon i mange land er at vi finner én infrastruktur for mobiltelefoni, én for distribusjon av radiokanaler, én for distribusjon av TV-signaler, én for kommunikasjon mellom nødetatene, én for forsvaret for å nevne noe. Vi har allerede sett at kommunikasjonsinfrastrukturer i noen grad har blitt slått sammen, ved at TV-signalene har blitt erstattet av kabler som også er bærer for Internett. 5G er laget for å kunne understøtte en stor teknologikonvergens, ved at en og samme infrastruktur kan fremstå som forskjellige nett med forskjellige egenskaper. Dette er realisert gjennom en funksjonalitet som kalles *network slicing **[7]**.* VI kan derfor se for oss en fremtid hvor spesialnett for nødetatene, for forsvaret, for strømming av radio og TV og for distribusjon av Internett er erstattet av hver sin «slice» i et 5G-nett.

2. Vi ser allerede nå starten på en trend der dagligdagse gjenstander blir utstyrt med kommunikasjonsteknologi. Det er allerede mulig å kjøpe både lamper, kjøleskap og

panelovner som kan styres fra en mobiltelefon, og både trafikklys og de fleste nye biler er tilkoblet nettet. Dette fenomenet går under navnet Internet of Things (IoT). 5G er laget slik at praktiske begrensninger på antallet gjenstander som kan tilkobles nettet formål er fjernet. Dette åpner for en eksplosjon i anvendelser, hvor alt du eier er tilkoblet nettet og kan kommunisere med deg. Eksempelvis vil emballasje kanskje kommunisere med nettet om hvor mye melk det er igjen, og om kartongen har blitt resirkulert korrekt. De aller fleste gjenstander du eier kan fortelle deg hvor de befinner seg. Veiene vil kunne fortelle hvor trafikkbelastede de er, bygningene vil kunne fortelle om de er utsatt for fukt, sopp eller råte, og vannrør vil kunne fortelle om de er i ferd med å gå tette, eller om de er i ferd med å springe lekk. Noen av de anvendelsene man spekulerer i vil kreve ytterligere teknologiutvikling knyttet til miniatyrisering, men de nødvendige løsningene på de tekniske problemene for dette er i stor grad allerede å se i horisonten.

3. Automatisering, robotisering og fjernstyring vil kunne tas til et nytt nivå. Det i hovedsak tre teknologiforbedringer i 5G som gjør dette mulig. Først er forsinkelsen i kommunikasjonen over 5G drastisk redusert i forhold til 4G. Det betyr at tiden som går fra en beslutning er tatt i en sentral til en robot har reagert vil reduseres fra i mange tilfeller å kunne måles i tidels sekunder, til å bli målt i tusendels sekunder. Dette vil kunne åpne for automatisert trafikkavvikling med vesentlig bedre utnyttelse av infrastruktur, og vesentlig færre ulykker enn vi har i dag. De to andre teknologiforbedringene som er nødvendige for å muliggjøre dette er knyttet til robusthet og sikkerhet. 5G er laget for å være mer stabil, og den er laget for å være vesentlig vanskeligere å bryte seg inn i for å gjøre skade.

Når vi spekulerer i viktigheten av 5G-utrullingen er de utviklingstrendene som følger av disse anvendelsesområdene helt sentrale, og graden av spekulasjon stiger fra den første av disse tre til den siste. Det fremstår nå som opplagt at 5G vil føre til at den diversitet vi nå har i fysisk infrastruktur vil reduseres. Det vil være kraftige kostnadsbesparelser knyttet til eksempelvis å realisere fremtidens nødnett som en *slice* i et allerede eksisterende 5G-nett, fremfor å operere et stort antall spesialiserte basestasjoner spredt over lokasjoner i hele landet. Det samme argumentet kan benyttes hva gjelder mange av Forsvarets behov for mobil kommunikasjon, og det er grunn til å anta at kostnader knyttet både til bredbåndstilknytning, og distribusjon av radio og TV-signaler i fremtiden vil bli målt opp mot kostnader ved å oppnå det samme gjennom et 5G-nett. En utrulling av 5G vil derfor være et vesentlig bidrag til at alle våre måter å kommunisere på samles på én og samme plattform.

IoT-utviklingen er fremdeles i tidlig fase, men det anses ikke som en dristig påstand at IoT-anvendelser basert på mobilnett vil få stor samfunnsmessig betydning.

Selv om den siste av disse anvendelsesområdene – automatisering, robotisering og fjernstyring – gjerne eksemplifiseres ved selvkjørende biler som fremdeles har noe

spekulativt over seg, er det all grunn til å tro at utrullingen av 5G vil ha en betydelig endringskraft på samfunnet. Dersom forventningene til denne teknologien slår til – selv kun i begrenset grad – vil 5G starte en bevegelse som gjør mobilnettene til den mest kritiske infrastruktur vi noensinne har sett.

6.3. **Økende internasjonal politisering**

Betydningen av at sikkerheten ivaretas i 5G mobilnett er derfor stor. Når samfunnet blir så avhengig av én infrastruktur, blir det naturlig nok også mer sårbart for feil, ustabilitet eller misbruk av systemet. Gitt Kinas voksende teknologiske dominans på IKT systemer, inkludert 5G, er det derfor ikke overraskende at bekymringen har vokst i vestlige land, og særlig i USA.

USAs skjerpede tone overfor Kina i 5G-saken kom som en del av en større amerikansk reorientering i forhold til Kina og Russland de siste år. USA og Vesten for øvrig hadde siden 1990-tallet hatt som strategi å bringe disse landene, og andre, inn i den eksisterende verdensorden. Det betød i praksis at de ble invitert inn i de eksisterende regimer, slik som Verdens Handelsorganisasjon, og at man la opp til handel og dialog, med det håp at autoritære regimer skulle åpne seg og gradvis demokratiseres. For Russlands del ga man opp denne linjen etter invasjonen av Krim og øst-Ukraina fra 2014.

For Kina kom endringen mer gradvis, men Trump-administrasjonen la seg tidligere på en mer konfronterende linje overfor Kina enn Obama hadde gjort. Dette hadde imidlertid bred politisk støtte i USA, også fra Demokratene. Man oppfattet at strategien om inkludering og endring hadde feilet, og at Kina hadde misbrukt vestlig åpenhet til å subsidiere egen industri, manipulere valutaen, stjele teknologi og posisjonere seg i markedene. En stadig mer autoritær politisk utvikling og voksende press på nabolandene bidro også til kursendringen. Selv om visse begrensninger på kinesisk telekomutstyr ble innført alt i 2010[8] og i 2012[9], ble tonen skjerpet av Trump-administrasjonen.[10] FBI, politikere og eksperter i USA pekte stadig oftere på at kinesiske selskap kunne utgjøre en sikkerhetstrussel mot USA. I 2018 forbød Pentagon det amerikanske forsvaret å bruke utstyr fra Huawei eller ZTE.[11] I løpet av 2018 og 2019 ble amerikanske myndigheter stadig tydeligere overfor allierte i sine advarsler mot å kjøpe kinesisk telekom-teknologi.[12] Land som Australia og Japan uttalte kort tid etter at de også ville forby Huawei i sine 5G-nett.[13] Saken nådde sitt foreløpige klimaks da USA i mai 2019 satte Huawei på sin *Entity List*, som er en liste over selskap som

ikke får lov til å kjøpe amerikanske produkter.[14] Det betød i praksis at Huawei ikke lenger kunne benytte amerikanskproduserte chips og andre komponenter i sine produkter.

I det internasjonale faglitteraturen sees denne utviklingen som en del av en større trend. Begreper som «weaponized interdependence» viser for eksempel til hvordan global gjensidig avhengighet kan gjøre som til våpen for stater til å fremme deres strategiske interesser[15]. Et eksempel er USAs advarsler om å sanksjonere det internasjonale betalingssystemet SWIFT dersom det fortsatte å tillate iranske selskap å bruke systemet. Bruken av sanksjoner og press er dermed ikke bare rettet mot selskap som er underlagt amerikansk lov, men også internasjonale aktører som handler med Iran, eller som i vårt tilfelle, som selger sensitive produkter til Kina.[16] Den integrerte globale økonomien muliggjør altså slike tiltak, men den underliggende årsaken er konkurranse, rivalisering og mistillit. Det gjelder også 5G-konflikten. Markedsandeler, arbeidsplasser, teknologiutvikling og andre økonomiske faktorer er viktige, samt politisk handlefrihet og innflytelse globalt.[17] Den voksende teknologi-riften mellom USA og Kina gjør at forskere nå bruker begrep som «splinternett»[18] og «the great decoupling»[19]. IKT-verden ser ut til å være i på vei til å deles i to, der henholdsvis Kina og Vesten har sine egne produksjonslinjer og forsyningskjeder. Det er altså ikke bare sikkerhetsbekymringer som fører til dette.

Globalt har ulike land inntatt forskjellige posisjoner med hensyn til denne dragkampen. Mange forsøker nok en balanse, men på 5G er dette krevende. Vestlige land har kanskje ikke overraskende landet nærmere USAs posisjon enn mange andre, men også her er det forskjeller. Enkelte land har som nevnt fulgt USA i å forby navngitte kinesiske selskap, gjerne Huawei og ZTE, i sine 5G-nett. Andre har oppnådd det samme ved å innføre sikkerhetskrav som umuliggjør bruk av kinesisk infrastruktur i hele eller deler av nettet – men uten å nevne Huawei eller Kina eksplisitt. Flere land har ikke bestemt seg, mens andre allerede har gjort avtaler med Huawei og har begynt å rulle ut deres 5G-løsninger. Vi skal se nærmere på europeiske responser nedenfor. Men først må vi spørre om de sikkerhetsmessige utfordringene knyttet til 5G-teknologien kunne vært løst på måter der man unngikk stormaktsrivalisering og geopolitikk. Finnes det teknologiske løsninger som kan sikre at 5G-nettet vil være er sikkert og trygt?

6.4. Tillit og teknologileverandører

Sikkerhetsvurderinger knyttet til innkjøp av kritisk teknisk utstyr har blitt gjennomført til alle tider. Kjøp av våpen til forsvaret og innkjøp av elkraftutstyr til kraftnettene har blitt gjennomført kun etter en grundig teknisk gjennomgang av det utstyret som skulle kjøpes inn. Når vi nå ser en bred internasjonal bekymring over innkjøp av elektronikk til

telekom-operatører, er det knyttet til en egenskap ved elektronikk som tidligere tiders teknologi ikke har. Elektronisk utstyr lar seg ikke fullt ut analysere, og den sikkerheten som følger av å gjennomføre en teknisk revisjon av utstyret vil derfor langt på vei være illusorisk. La oss i det følgende kort diskutere hvorfor.[20]

6.4.1. Kan vi oppdage uønsket funksjonalitet?

Svaret på dette spørsmålet er sammensatt. Analyse av både hardware og software er i noen grad mulig, og slik analyse gjennomføres rutinemessig i sikkerhetsmiljøer. Vanskeligheten med slik analyse er imidlertid den at den kun kan gjennomføres på svært små kodesegmenter. En full analyse av et komplett produkt som inneholder hardware, operativsystem og applikasjonssoftware ligger milevidt utenfor det praktisk mulige. En enkel illustrasjon av dette kan være følgende regnestykke. Det anslås at en erfaren kodeanalytiker kan analysere mellom 100 og 1000 linjer kode på én dag[21]. En helt enkel PC vil være et resultat av opp til 100 millioner kodelinjer dersom man tar med både hardware og software. Det indikerer at det krever opp til 1 million feilfrie arbeidsdager til for å analysere en enkelt PC. Dette eksemplet representerer ikke en full diskusjon av temaet, da kodeanalyse kun er én av flere måter å analysere en maskin på. Det gir imidlertid en indikasjon på den kompleksiteten som umuliggjør en full analyse av elektronisk utstyr.

6.4.2. Tidspunkt for plassering av uønsket funksjonalitet

En komponent i et telekommunikasjonsnettverk vil typisk bestå av to deler. Den ene delen er den hardwaren som kan betraktes, og berøres. Denne er statisk, og er levert fra leverandøren en gang for alle. Den andre delen består av software – programvare – som kjører på komponenten. Denne delen leveres gjerne sammen med komponenten selv, men i motsetning til hardwaren vil den byttes ut og modifiseres flere ganger gjennom produktets levetid.

Det er flere grunner til slike softwaremodifiseringer. Den ene er at det kommer nye standarder og ny funksjonalitet som gjør at det stilles nye krav til hva det integrerte produktet skal være i stand til å gjøre. En annen grunn er at man har avdekket feil eller sikkerhetshull som må rettes eller tettes. I alle disse tilfellene vil leverandøren av utstyret ta initiativ til at softwaren som kjører på boksen skal byttes ut. Det er sjelden et alternativ å ikke installere slike softwareoppdateringer, da disse oppdateringene er et helt sentralt virkemiddel mot cyberangrep fra en tredjepart.

Dette har konsekvenser for hvordan et forsvar mot en potensielt uærlig leverandør må arte seg. Uønsket funksjonalitet vil nemlig lett kunne installeres gjennom en slik

softwareoppdatering. Av dette følger at man selv om man hadde kunnet analysere den elektroniske komponenten til bunns da komponenten ble kjøpt, ville ikke det gitt noen garanti for at uønsket funksjonalitet ble lagt inn i komponenten ved et senere tidspunkt. Det har også den konsekvensen at når man kjøper elektronisk utstyr fra en leverandør er det ikke tilstrekkelig at man kunne stole på leverandøren på kjøpstidspunktet. Man må kunne stole på leverandøren gjennom hele produktets levetid.

6.4.3. Kan vi oppdage faktisk utnyttelse av uønsket funksjonalitet?

Spørsmålet om deteksjon av at utstyr i infrastrukturen opererer mot våre avhenger i stor grad av hvilken operasjonsmodus man snakker om. En kort diskusjon av våre muligheter til å oppdage henholdsvis spionasje og sabotasje følger under.

Å oppdage at utstyret benyttes til spionasje består langt på vei i å detektere at det lekker informasjon ut av utstyret på irregulære måter. Det er en lang rekke måter informasjon kan lekke på, og en full diskusjon av dette temaet vil ikke få plass i dette kapittelet. Hovedbildet er imidlertid at muligheten til å oppdage informasjonslekkasje vil avhenge av hvor mye data som lekker. Det er mulig å gjennomføre en informasjonslekkasje på en slik måte at det er teoretisk umulig å oppdage lekkasjen[22]. Disse metodene gir imidlertid lav kapasitet, slik at det er lite informasjon som kan lekke om gangen. Generelt kan man si at jo høyere båndbredde lekkasjen har, jo lettere er den å oppdage. Det er imidlertid klart at fra et spionasjeståsted kan svært mye skade skje allerede ved svært lav båndbredde.

Sabotasje vil ofte være langt lettere å oppdage. Til gjengjeld vil det i noen tilfeller – spesielt i internasjonalt tilspissede situasjoner – være for sent når skaden faktisk har skjedd. I andre scenarier vil det være slik at sabotasjen er ment å detekteres, enten fordi den inngår i et avskrekkingsstrategi eller en utpressingsstrategi.

6.4.4. Sannsynlighet for misbruk

Det har ofte blitt anført at det er lite sannsynlig at en leverandør av telekom-utstyr vil bruke utstyret til spionasje eller sabotasje. De markedsmessige konsekvensene av at slik virksomhet blir avslørt ville være for alvorlige til at noen ville tatt sjansen[23]. Dette argumentet har mye for seg, og det er all grunn til å tro at en leverandør av utsyr ville være svært forsiktig med slike aktiviteter. Det er imidlertid noen observasjoner som det er verdt å merke seg.

Først er det slik at flere land har lovgivning som pålegger sine selskaper å følge instrukser fra landets myndigheter. Det er derfor ikke opplagt at det vil være selskapet selv som fatter beslutning om slik virksomhet. Det mest omtalte eksempelet er den kinesiske etterretningsloven fra 2017, som pålegger kinesiske selskap å støtte og samarbeide med de nasjonale etterretningstjenestene.[24] Men Kina er ikke alene om slik lovgivning. Gitt diskusjonen over om vanskelighetene med å oppdage slik virksomhet, er det derfor ikke opplagt at alle selskap har kunnet, eller vil kunne stå imot press fra egne myndigheter. Dernest finnes det et dokumentert eksempel der de økonomiske konsekvensene av overtramp synes å ha vært moderate. Etter at Edward Snowden lekket informasjon om at utstyr laget av Cisco ble manipulert av amerikanske sikkerhetstjenester, hevdet Cisco selv at deres økonomiske tap som resultat av lekkasjen kun var moderate[25]. Vi har derfor begrenset grunnlag for en antagelse at en stormakt vil la en så stor og lettvint metode for maktutøvelse ligge uprøvd.

Vi kan derfor konkludere at teknisk revisjon av digitalt utstyr ikke i seg selv vil være tilstrekkelig for å sikre det. Det er rett og slett ikke mulig. Det er ikke rom for å diskutere internasjonal rett her, men vi kan stadfeste at det ikke finnes folkerettslige eller andre internasjonale juridiske regimer som kan sikre tilfredsstillende sikkerhet i digitale systemer som 5G.[26] Dermed er *tillit* til leverandør fortsatt en avgjørende faktor. Tillit er subjektivt og politisk, i motsetning til tekniske og juridiske forordninger.[27] Imidlertid kan ikke utfordringen knyttet til 5G-sikkerhet reduseres kun til tillit. Vestlige land, som har en stor grad av tillit til hverandre, har likevel måttet navigere presset fra både Kina og USA. En viktig del av det arbeidet har vært å utvikle felles posisjoner og prinsipper som kunne bistå statene i deres regulering av 5G-sikkerheten. La oss se kort på noe av det som har blitt gjort i Europa.

6.5. Internasjonale prosesser på 5G-sikkerhet

6.5.1. Prague proposals

En viktig milepæl i det internasjonale samarbeidet om 5G-sikkerhet var en konferanse som fant sted i Praha mai 2019. Foruten en rekke europeiske land, deltok USA, Israel, Australia, New Zealand, Japan og South Korea, til sammen 32 land. Formålet med konferansen var å komme frem til et sett anbefalinger om hvordan man kan introdusere 5G nettverk på en sikker måte. Resultatet ble dokumentet «Prague proposals».[28] Her listes 20 prinsipper landene skal leve opp til når de ruller ut 5G-nettverkene. Verken Kina eller Huawei nevnes, men det står for eksempel at man må ta hensyn til risikoen for at tredjeland kan påvirke en leverandør. Det står også at fraværet av sikkerhetssamarbeid eller at tredjelandet ikke er en del av internasjonalt samarbeid om cybersikkerhet, kriminalitet og personvern, er noe som

bør vurderes. Mange vil nok lese dette som Kina og andre ikke-demokratiske og ikke-vestlige land uten at det sies eksplisitt. Det at både USA og de fleste vestlige land ble enige om «Prague proposals», var viktig fordi man da fikk brakt diskusjonen ned på konkrete sikkerhetsløsninger og bort fra den handelspolitiske dimensjonen som Kina hevdet var USA egentlige motivasjon.

6.5.2. EU 5G Toolbox

En annen viktig milepæl er EUs såkalte «verktøykasse». De ulike medlemslandene i EU har hatt en ganske ulik tilnærming til Huawei-spørsmålet. I utgangspunktet var de fleste relativt åpne og positive, og hadde gode erfaringer fra 3G og 4G-nett levert av Huawei. EU-kommisjonen utformet i 2016 en «Action plan» for 5G, men sikkerhet er knapt vurdert i dokumentet. I stedet legges det vekt på den strategiske muligheten 5G representerer, og at Europa må være beredt.[29] Imidlertid, i takt med voksende bekymring knyttet til sikkerhet og sårbarhet, samt ulike grader av press fra USA, begynte også EU å behandle dette. Det begynte med at Europaparlamentet skrev en rapport i mars 2019 om «*sikkerhetstrusler knyttet til den voksende kinesiske teknologiske tilstedeværelsen i EU*».[30] EU-kommisjonen fulgte så opp like etterpå med en henstilling til medlemsstatene om å gjøre konkrete grep for å vurdere cybersikkerhetsrisiko ved 5G-nett og til at styrke risikobegrensende tiltak.[31] Like etter dette kom altså «Prague-proposals».

I oktober 2019 publiserte EU en rapport som vurderte risikoen knyttet til den digitale sikkerheten i 5G-nettverk.[32] Her skriver de at statlige aktører representerer den største trusselen, og at flere EU-medlemmer har identifisert «visse ikke-EU land» som en spesiell trussel mot deres nasjonale interesser. Kina nevnes altså ikke med ord, men ganske tydelig mellom linjene. Videre legger rapporten vekt på diversifisering, ved at man ikke bør gjøre seg avhengig av kun en leverandør – for å gjøre seg motstandsdyktig mot feil og forstyrrelser.

Deretter, i januar 2020 publiserte EU-kommisjonen en såkalt «verktøykasse» («5G toolbox») der formålet var å identifisere noen felles grep som kan redusere de mest alvorlige digitale truslene mot 5G-nettverk.[33] Heller ikke her er Kina nevnt, og verktøykassen omfatter alle slags risikoer, ikke bare statlig inntrengning. Likevel står det at man både kan pålegge restriksjoner og ekskludere leverandører man anser å være en risiko for nøkkelfunksjoner.

Imidlertid er dette altså kun anbefalinger, og selv om medlemslandene skal rapportere implementeringen av anbefalingene i verktøykassen, er det likevel frivillig hva de velger å

gjøre. De ulike EU-initiativene hjelper altså landene i å implementere god sikkerhet i de nye 5G-nettene, men overlater til hvert enkelt land hvordan de vil håndtere Kina og Huawei. De fleste ser imidlertid ut til å ha valgt en tilnærming som ligner EUs; altså at verken land eller leverandører nevnes eksplisitt i 5G-reguleringene, men at kinesiske selskap likevel kan ekskluderes helt eller delvis på bakgrunn av sikkerhetsvurderinger og behov for diversifisering.

6.5.3. Clean Network

Fra amerikansk side fortsatte den mer eksplisitte kampanjen for å stenge kinesiske selskap ute fra verdens 5G-nett. I april 2020 annonserte utenriksministrer Mike Pompeo at de ville innførte et eget «5G Clean Path» system som skulle sørge for at ingen korrespondanse fra amerikanske ambassader skulle gå via kinesiske nett eller systemer. Senere ble dette utvidet til «Clean Network», der formålet var å «sikre nasjonale ressurser, inkludert borgernes datasikkerhet og selskaps mest sensitive informasjon, fra aggressive innbrudd fra ondsinnede aktører, slik som det kinesiske kommunistpartiet».[34] «Clean Network» inkluderte “Clean Apps”, “Clean Carrier”, “Clean Store”, “Clean Cable” og “Clean Cloud” I tillegg til “Clean Path”.

Formålet var eksplisitt å utestenge kinesiske selskap fra «app stores», fjerne amerikanske applikasjoner fra deres «app stores», ikke bruke kinesiske nettverk, skytjenester, kabler osv. «Clean Network»-initiativet ble også lansert som et internasjonalt samarbeid, der både land, telecom-selskap og leverandører har blitt listet som deltakere. Noen av disse har bekreftet deltakelse i nettverket, mens andre, som Norge, kom med på listen uten at norske myndigheter, eller teleselskapene, selv har bekreftet deltakelse. Det ser dermed ut til at amerikanske myndigheter listet aktører som har gjort sikkerhetsmessige grep som i praksis forhindrer kinesiske selskap sentrale roller i 5G-utbyggingen. Det er uklart om, eller i hvilken grad, Biden-administrasjonen akter å videreføre disse initiativene, men hovedelementene blir neppe reversert. Bekymringen for Kina er like stor som i forrige administrasjon.

La oss nå se mer spesifikt på hvordan disse utfordringene har blitt håndtert i Norge. Hvordan har politikere og myndigheter forholdt seg til kinesiske leverandører i forbindelse med utbyggingen av 5G-nettet?

6.6. Den norske håndteringen av 5G-sikkerhet

6.6.1. Politisk utvikling

Sikkerhet i telekommunikasjon var nesten utelukkende et teknisk spørsmål før 5G. Det handlet om å gjøre nettet driftsikkert og robust, slik at det var operativt også i kriser, at det kunne motstå naturkatastrofer, strømbrudd eller eventuell sabotasje. Det handlet altså ikke om politikk, men om å finne best mulige tekniske løsninger – til best mulig pris. Navn og nasjonalitet på leverandører og underleverandører av det tekniske utstyret var ikke et stort tema.[35]

Debatten i Norge knyttet telekommunikasjon, Kina og Huawei, var begrenset for ti år siden. Det handlet stort sett om Kinas raske vekst som en teknologisk og økonomisk stormakt. Da både Telenor og Netcom valgte Huawei til deres 4G-nett rundt 2010, var det knapt protester og offentlig debatt. Noen unntak var det, slik som Per-Morten Hoff i IKT-Norge som i desember 2009 sa at Telenor, med sitt samarbeid med Huawei, legger sitt mobilnett åpent for mulig industrispionasje og for tapping av sensitiv trafikk.[36] Han problematiserte også Huaweis tette bånd til Kinas militære styrker. I januar 2010 kom Fremskrittspartiets Bård Hoksrud på banen og refererte til amerikanske og britiske bekymringer knyttet til Huawei.[37] Han ba om at Post- og teletilsynet og Samferdselsdepartementet skulle gå grundigere inn i det, men Telenors teknologidirektør avviste bekymringene:

> *Huawei har allerede et hundretall ansatte på Fornebu. Jeg kjenner mange av dem, og våre undersøkelser tilsier at det ikke foreligger noen sikkerhetsrisiko. Jeg har også selv vært i Kina og møtt toppledelsen.**[38]***

I 2012 stilte Høyres Stortingsrepresentant Anders B. Werp flere spørsmål til regjeringen om valget av Huawei i 4G-nettet noen år tidligere. Han uttrykte stor bekymring for sikkerheten, men fikk litt vage svar. Samferdselsminister Marit Arnstad svarte for eksempel at myndighetene var klar de internasjonale bekymringene knyttet til Huawei, men la til: «Jeg har tillit til at tilbyderne gjør de nødvendige risiko- og sårbarhetsanalyser ved valg av leverandør».[39] Bekymringene Werp og andre uttrykte fikk større oppmerksomhet etter hvert. I 2014 nedsatte regjeringen et digitalt sårbarhetsutvalg (Lynse-utvalget) som presentere sin rapport i 2015.[40] Samme år ble sikkerhetsutvalget nedsatt (Traavik-utvalget), som leverte sin rapport i 2016.[41] Begge utvalgene påpekte den voksende betydningen av ekom-infrastrukturen og behovet for sikringen av denne. I kjølvannet av Traavik-utvalget utarbeidet så regjeringen en ny sikkerhetslov som ble lagt frem for Stortinget i 2017. Denne skjerpet sikkerhetskravene som alt lå inne i Lov om elektronisk kommunikasjon (ekomloven).[42]

Selv om mye skjedde i fagmiljøene og internt i ekom-sektoren, var det først rundt 2018 at den offentlige oppmerksomheten rundt 5G og Huawei virkelig tok av. Om vi ser på for eksempel antall avisopplag, var det i 2019 så mange som 4765 artikler der Huawei var nevnt i norske medier, mot bare 21 i 2003.[43] På Stortinget økte også oppmerksomheten, og fra 2018 av fikk regjeringen jevnlig spørsmål fra opposisjonspolitikere i Stortinget om Huawei, 5G-nettet og sikkerhet.[44] Den økte oppmerksomheten i Norge sammenfaller med den amerikanske opptrappingen av ordbruken mot Kina og Huawei. Fra rundt 2018 gjentok USA som sagt stadig oftere at 5G kan brukes til storstilt spionasje mot et lands borgere og institusjoner, og at de som leverer systemet også kan manipulere det, og i verste fall sabotere det.

Et tydelig signal om hvordan myndighetene tenkte kom da daværende samferdselsminister Ketil-Solsvik Olsen i august 2018 uttalte at departementet ville gjøre «vurderinger knyttet til utstyr i norske telenett fra land vi ikke har *sikkerhetspolitisk samarbeid med*» (vår utheving).[45] Han la til at en følger den løpende utviklingen internasjonalt, der blant annet USA har gitt tydelige signal om at en bør unngå Huawei og kinesiske leverandører.

Den mest tydelige politikeren var Justisminister Tor Mikkel Wara som i januar 2019 sa at «Vi deler Huawei-uroen i USA og Storbritannia, Norge vurderer tiltak mot Huawei».[46] Han fikk støtte kort tid etter fra PST-sjef Benedicte Bjørnland som også uttalte seg eksplisitt om Huawei for første gang: «Vi har sagt at man bør være oppmerksom på Huawei som aktør i forbindelse med 5G-nettet som skal bygges ut. Ikke fordi vi tror at det er noe galt med Huawei og menneskene som jobber i Norge, men Huawei som selskap har antagelig ganske tette bånd til kinesiske myndigheter».[47]

Den eksplisitte utpekingen av Huawei skapte en viss bekymring i andre deler av offentligheten. En ting er å vise til ekom-loven og sikkerhetsloven, noe annet er å offentlig gå politisk ut mot enkeltbedrifter som tross alt opererer lovlig i Norge. Når den samme virksomheten inntil nylig har blitt gitt tillit nok til å levere infrastrukturen til det eksiterende 4G-nettet, kunne det nok fremstå mer politisk enn sikkerhetsmessig begrunnet.

For regjeringen og deler av næringslivets del kom også denne økte skepsisen mot Huawei også på et svært ubeleilig tidspunkt. Kina hadde innført politisk boikott av Norge 2010 som følge av fredsprisutdelingen til dissidenten Liu Xiaobo, men i 2016 ble Kina og Norge enige om en avtale som normaliserte relasjonene. Både politikere og næringsliv var opptatt av å ta igjen det tapte og raskest mulig åpne for mer handel, dialog og samarbeid med Kina. Den mer konfronterende linjen USA la seg på overfor Kina var derfor krevende for Norge.

6.6.2. **Nye sikkerhetskrav**

Av de norske teleselskapene var ICE først ute med å velge 5G-leverandør, og gikk for Nokia i begynnelsen av 2019. Telia fulgte etter i oktober 2019, og valgte Eriksson i stedet for Huawei som hadde vært deres leverandør på de tidligere nettverkene.[48] Digitaliseringsminister Nikolai Astrup ble da spurt om regjeringen hadde lagt noen føringer på om de ville ha Huawei som leverandør av 5G-nett i Norge eller ikke. Han svarte da: «Vi har god og løpende dialog med alle teleoperatørene om sikkerhet og beredskap, men vi har ikke utelukket noen enkeltleverandør».[49]

Noen måneder senere, da Telenor også annonserte at de valgte Eriksson som hovedleverandør til 5G-nettet[50], gikk imidlertid regjeringen ut med litt mer detaljer om hva «dialogen om sikkerhet og beredskap» hadde bestått i. Kommunal- og moderniseringsdepartementet (KMD) skrev i en pressemelding at:

> *Selskapene velger selv sine utstyrsleverandører i global konkurranse innenfor rammene av sikkerhetsloven. Norske myndigheter utelukker ingen leverandører fra det norske markedet, men har stilt krav til teleselskapene om at de må velge flere enn en leverandør dersom de velger 5G-leverandører fra land Norge ikke har sikkerhetsavtale med. Minst 50 prosent av basestasjonene skal være fra leverandører fra land Norge har sikkerhetsavtale med.**[51]***

Beslutningen var forankret i den nevnte nye sikkerhetsloven som trådte i kraft 1. januar samme år. Den pålegger departementene å identifisere «grunnleggende nasjonale funksjoner» som skal omfattes av loven og definere som skjermingsverdige. Også i den foregående sikkerhetsloven var deler av ekom-sektoren definert som skjermingsverdig og flere teleoperatører ble delvis underlagt sikkerhetslovens bestemmelser. Dette ble forsterket under den nye loven, der flere ekomtilbydere ble underlagt loven.

I et utdypende brev fra Kommunal og moderniseringsdepartementet (KMD) titulert «Sikkerhetsloven – krav om 'forsvarlig sikkerhet' for neste generasjons mobilnett, 5G», skrev departementet: «For private virksomheter som er underlagt loven etter sikkerhetsloven § 1-3, må kravet til forsvarlig sikkerhetsnivå ivaretas allerede fra ny infrastruktur planlegges».[52] Presiseringen av «forsvarlig sikkerhetsnivå» i sikkerhetslovens forstand måtte altså avklares allerede i planleggingsfasen. KMD skrev videre at «nærmere kartlegging av hva som vil utgjøre et forsvarlig sikkerhetsnivå for den enkelte virksomhet, og

på de enkelte fagfeltene loven dekker, vil måtte vurderes opp mot hva som anses som god faglig praksis på de enkelte fagområdene».

«God faglig praksis» med hensyn til «forsvarlig sikkerhetsnivå» ble dermed det avgjørende. Regjeringen definerte altså dette som at kun land man har sikkerhetsavtale med kan levere de viktigste komponentene i 5G-nettet, og minst 50% av basestasjonene. I den forrige sikkerhetsloven hadde teleselskapene også sikkerhetsbegrensninger når det gjelder kjernenettet, altså de mest sentrale funksjonene i mobilnettet. Her var ekstern tilgang ganske begrenset. Det er all grunn til å anta at dette er videreført for 5G, i tillegg til 50%-regelen på basestasjonene, samt mulige andre begrensninger knyttet til geografi eller annet. Dette er imidlertid ikke offentlig kjent. Uansett er dette skjønnsmessige sikkerhetsvurderinger som nok kunne vært spesifisert på andre måter også. Imidlertid har også andre land har stilt liknende prosentvise begrensninger på basestasjoner fra ikke-vestlige leverandører.[53]

Poenget for myndighetene var altså å gi føringer til telekomselskapene *før* de valgte leverandør til utrullingen av 5G. Sikkerhetsloven har en varslingsplikt for anskaffelser som uansett ville inntreffe etterpå. Da kunne man risikert at selskapenes vurdering av forsvarlig sikkerhet ikke stemte overens med departementets vurderinger – med de økonomiske konsekvensene det kunne gi for selskapene. Det kunne selvsagt også skapt mer krevende politiske situasjon for myndighetene.

Norske myndigheter hadde dermed i praksis bestemt seg for sikkerhetskravene lenge før Telia og Telenor hadde valgt sine leverandører og skrevet kontrakter, og dette ble gjort offentlig kjent. Trolig ble disse føringene lagt på operatørene alt på våren 2019. Norge var med andre ord ganske tidlig ute med å begrense eller utestenge kinesiske leverandører – uten å si det eksplisitt eller offentlig. Norge fulgte også de ulike EU-initiativene tett og deltok på Praha-møtet i mai 2019, men hadde trolig allerede konkludert da dette møtet fant sted. Men den norske tilnærmingen var uansett på linje med både «Prague proposals» og den gjennomgående linjen i EUs verktøykasse og andre dokument.

Selv om Norge hadde utstrakt dialog med flere land, både i Norden, Europa, samt med USA og Kina, var de også tydelige på å understreke at det var selskapene selv som valgte 5G-leverandør. Dermed var det nok primært disse som ble usatt for oppmerksomhet og press fra amerikanske myndigheter og fra Huawei rundt beslutningsprosessene. Samtidig reduserte dette trolig også de politiske ubehagelighetene knyttet til saken for Norge. Huawei har ikke offentlig klaget på verken norsk sikkerhetslov eller at Telia og Telenor ikke valgte dem som primærleverandør til 5G. I land der Huawei har blitt eksplisitt nevnt og forbudt, slik som i Australia, Storbritannia og Sverige, har den responsen vært sterk, både fra Huawei og fra kinesiske myndigheter.[54] Australia er klaget inn for WTO av Kina, mens saken ble bragt

inn for domstolene i Sverige.[55] Kinesiske myndigheter har også uttalt at de vil ta «alle nødvendige virkemidler» i bruk som svar på Sveriges Huawei-forbud.[56] Dette er nok norske myndigheter meget tilfredse med at de har unngått.

6.7. **Konklusjon**

IT-industrien har gjennom tiår utviklet seg til å være svært internasjonal i sin natur. Både software, hardware og tjenester har blitt utviklet og produsert som et samarbeid mellom mange land. Som et eksempel vil et produkt kunne designes i USA, designet vil bruke komponenter som er utviklet i Europa, disse komponentene kan produseres og settes sammen til et ferdig produkt i Kina før det ferdige produktet selges og tas i bruk i Oseania. Dette globale samarbeidet har virket fremmende på teknologiutviklingen, og det har vært økonomisk fordelaktig for alle parter.

Diskusjonen knyttet til Huawei og 5G har imidlertid ført til en oppvåkning knyttet til de sikkerhetsmessige aspektene av et slikt samarbeid. Ved kompleks elektronikk står vi for første gang overfor produkter som ikke lar seg fullt ut undersøke. Når vi skal vurdere de sikkerhetsmessige sidene av et elektronisk produkt er vi langt på vei avhengig av å kunne ha tillit til det leverandørene forteller oss. Spesielt må vi ha tillit til at leverandørene selv ikke vil handle på tvers av våre sikkerhetsinteresser.

VI ser nå tydelige tegn til at leverandørkjeder innad i IT-industrien og internasjonal sikkerhetspolitikk sees i sammenheng. Dette har fått flere internasjonale IT-selskaper til å forberede seg på en situasjon hvor samarbeid om utvikling og produksjon av utstyr ikke kan foregå på tvers av geopolitiske interessesfærer.[57] Vi går med andre ord mot en bipolar verden – i alle fall innen digitale verdikjeder.

Det er å vente at utviklingen i retning av en slik bipolar verden hva gjelder produksjon av IT-utstyr vil fortsette, i det minste for produkter som har sikkerhetskritiske anvendelsesområder. De kreftene som vil trekke i retning av en slik oppdeling er lett identifiserbare i form av teknologiske og sikkerhetspolitiske realiteter. De økonomiske konsekvenser dette vil ha er vanskelig å kvantifisere, men det synes ikke som om økonomiske besparelser vil kunne være tilstrekkelig til å motvirke en slik utvikling. Så lenge full tillit mellom verdens stormakter ikke er tilstede, og elektronikk ikke lar seg fullt ut undersøke, vil kreftene som drar i retning av en oppdeling av verden sannsynligvis virke sterkest.

Små land som Norge blir i økende grad tvunget til å velge side enten de vi eller ikke, da det både økonomisk og politisk vi bli krevende å ha et ben i begge leire. Bedrifter kan utsettes for sanksjoner og utestengelse fra markeder, mens politiske myndigheter utsettes for press og mulige represalier også utenfor det digitale domenet. Et spørsmål er om EU vil makte å seile opp som en slags tredje pol på sikt. Per i dag er det langt dit, ettersom mesteparten av digital utvikling foregår i USA og Kina. På telekom-siden er det imidlertid de europeiske Eriksson og Nokia som er Huaweis hovedkonkurrenter. Et styrket EU på både innovasjon og regulering og vil trolig være viktig også for Norge, særlig i situasjoner der våre og USAs interesser ikke er helt overlappende. I slike tilfeller kan et sterkere EU bidra til å gi oss mer handlingsrom enn i en helt to-delt verden. Uansett kommer sikkerhet i telekom og annen digital infrastruktur til å bli tillagt stadig større vekt, og da har vi sett i dette kapitlet at *tillit* til leverandørene en like avgjørende faktor som teknologiske standarder. Om verden endres raskt er det i alle fall noe som fortsatt står ved lag.

---

[1] Denne artikkelen er dels basert på tidligere forskning på denne tematikken, personlig involvering i enkelte av prosessene som omtales, samt møter og samtaler med sentralt plasserte personer. Takk til Erik Kursetgjerde for bistand, samt til de anonyme fagfellene for gode og kritiske bemerkninger.

[2] “China vows 'necessary' measures in response to UK's Huawei ban”, *Reuters*, 16. juli 2020. https://www.reuters.com/article/us-britain-huawei-china/china-vows-necessary-measures-in-response-to-uks-huawei-ban-idUSKCN24H0Z7

[3] Dunnewijk, T., Hultén, S., A brief history of mobile communication in Europe, *Telematics and Informatics* (2007)

[4] Ezhilarasan, E. and Dinakaran, M., (2017). A Review on mobile technologies: 3G, 4G and 5G. In *2017 second international conference on recent trends and challenges in computational models (ICRTCCM)* (pp. 369-373). IEEE.

[5] Vincent, J., Haddon, L. and Hamill, L., 2005. The influence of mobile phone users on the design of 3G products and services. *The Journal of the Communications Network*, *4*(4), pp.69-73.

[6] Patel, S., Shah, V. and Kansara, M., 2018. Comparative Study of 2G, 3G and 4G. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *3*(3), pp.1962-1964.

[7] Foukas, X., Patounas, G., Elmokashfi, A., & Marina, M. K. (2017). Network slicing in 5G: Survey and challenges. *IEEE Communications Magazine*, *55*(5), 94-100.

[8] "Huawei Bid for Sprint Contract Hits a Hurdle - The New York Times." 22 Aug. 2010, https://www.nytimes.com/2010/08/23/business/global/23telecom.html. Accessed 19 Jul. 2019.

[9] "Investigative Report on the U.S. National Security Issues Posed by ...." https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=96. Accessed 19 Jul. 2019.

[10] https://www.reuters.com/article/us-usa-china-huawei-tech-eu/u-s-warns-european-allies-not-to-use-chinese-gear-for-5g-networks-idUSKCN1PU1TG

[11] "John S. McCain National Defense Authorization Act for ... - Congress.gov." https://www.congress.gov/bill/115th-congress/house-bill/5515/text. Accessed 22 Jul. 2019.

[12] https://www.reuters.com/article/us-usa-china-huawei-tech-eu/u-s-warns-european-allies-not-to-use-chinese-gear-for-5g-networks-idUSKCN1PU1TG

[13] "New Zealand Blocks Huawei, in Blow to Chinese Telecom Giant - The ...." 28 Nov. 2018, https://www.nytimes.com/2018/11/28/business/huawei-new-zealand-papua-new-guinea.html. Accessed 19 Jul. 2019. "Japan effectively bans China's Huawei and ZTE from government ...." 10 Dec. 2018, https://www.washingtonpost.com/world/asia_pacific/japan-effectively-bans-chinas-huawei-zte-from-government-contracts-joining-us/2018/12/10/748fe98a-fc69-11e8-ba87-8c7facdf6739_story.html. Accessed 19 Jul. 2019.

[14] "Addition of Entities to the Entity List - Federal Register." 21 May. 2019, https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list. Accessed 19 Jul. 2019.

[15] Farrell, Henry and Abraham L. Newman (2019): "Weaponized Interdependence: How Global Economic Networks Shape State Coercion", *International Security* 44 (1): 42–79; Drezner, Daniel W., Henry Farrell and Abraham L. Newman (2021) *The Uses and Abuses of Weaponized Interdependence*. Washington DC: Brookings Institution Press. Se også Thomas J. Wright (2017), *All Measures Short of War: The Contest for the Twenty-First Century and the Future of American Power*, New Haven, CN: Yale University Press.

[16] "Trump administration pressed Dutch hard to cancel China chip-equipment sale: sources" Reuters, 6. Januar 2020.

https://www.reuters.com/article/us-asml-holding-usa-china-insight/trump-administration-pressed-dutch-hard-to-cancel-china-chip-equipment-sale-sources-idUSKBN1Z50HN

[17] Powers, Shawn M. og Michael Jablonski. *The Real Cyber War: The Political Economy of Internet Freedom*. Baltimore, Il: University of Illinois.

[18] Mueller, Milton (2017): *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace*. Oxford: Polity Press.

[19] Inkster, Nigel (2020): *The Great Decoupling: China, America and the Struggle for Technological Supremacy*. London: Hurst.

[20] For en grundigere teknisk diskusjon av dette spørsmålet, se Lysne, Olav (2018): *The Huawei and Snowden Questions*, London: SpringerNature 2018.

[21] Down, M., McDonald, J., Schuh, J. (2006): The art of software security assessment: Identifying and

preventing software vulnerabilities. Pearson Education.

[22] B.A. Bash, D. Goeckel and D. Towsley. Limits of reliable communication with low probability of detection on AWGN channels. *IEEE Journal on Selected Areas in Communications*, 11.9 (2013): 1921-1930.

[23] Se f. eks
https://www.nbcnews.com/politics/national-security/does-china-s-huawei-really-pose-threat-national-security-n1124746

[24] National Intelligence Law of the People's Republic,
http://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf

[25]
https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html

[26] For en grundig innføring i krigens folkerett, se Hellestveit, Cecilie og Gro Nystuen (2020), *Krigens folkerett – Norge og vår tids kriger*, Oslo: Universitetsforlaget. Når det gjelder folkerettens relevans for cyberoperasjoner i fredstid er Tallinn-manualen 2.0 et standardverk: Tallinn Manual 2.0 (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge: Cambridge University Press.

[27] Ruzicka, Jan, and Vincent Charles Keating (2015). "Going Global: Trust Research and International Relations." *Journal of Trust Research* 5 (1): 8–26.

[28] The Prague Proposals. The Chairman Statement on cyber security of communication networks

in a globally digitalized world. Prague 5G Security Conference, Prague, 2 May 2019.

[29] European Commission: *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee Of The Regions: 5G for Europe: An Action Plan*, Brussels, 14.9.2016, COM(2016) 588 final.

[30] European Parliament: *Security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them*, 12.3.2019, 2019/2575(RSP)

[31] European Commission: *Commission recommendation: Cybersecurity of 5G networks*. Strasbourg, 26.3.2019 C(2019) 2335 final

[32] NIS Cooperation Group: *EU coordinated risk assessment of the cybersecurity of 5G networks,* Report 9 October 2019.

[33] NIS Cooperation Group: *Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures*, CG Publication 01/2020

[34] Se https://www.state.gov/the-clean-network/

[35] Sikkerhetsmiljøer og etterretningstjenestenes graderte trusselvurderinger var trolig mer og tidligere fokusert på dette enn allmenheten.

[36] VG, *Spionfrykt mot kinesere i Norge,* 30. desember 2009.

[37] E24, *Krever mobilkontrakt gransket,* 2. januar 2010, https://e24.no/norsk-oekonomi/i/LAk5mV/krever-mobilkontrakt-gransket

[38] Ibid.

[39] Skriftlig spørsmål fra Anders B. Werp (H) til justis- og beredskapsministeren, https://www.stortinget.no/no/Saker-og-publikasjoner/Sporsmal/Skriftlige-sporsmal-og-svar/Skriftlig-sporsmal/?qid=54627

[40] NOU 2015: 13, *Digital sårbarhet – sikkert samfunn.*

[41] NOU 2016: 19, *Samhandling for sikkerhet.*

[42] Lov om elektronisk kommunikasjon (ekomloven), https://lovdata.no/dokument/NL/lov/2003-07-04-83

[43] Retriver-søk.

[44] Se for eksempel: *Skriftlig spørsmål fra Sigbjørn Gjelsvik (Sp) til justis-, beredskaps- og innvandringsministeren*, 03.08.2018, https://www.stortinget.no/no/Saker-og-publikasjoner/Sporsmal/Skriftlige-sporsmal-og-svar/Skriftlig-sporsmal/?qid=72936

[45] Tek.no, *Samferdselsdepartementet vurderer tiltak for å sikre norske mobilnett*, 27. august 2018, https://www.tek.no/nyheter/nyhet/i/RRE3Ja/samferdselsdepartementet-vurderer-tiltak-for-aa-sikre-norske-mobilnett

[46] E24*, Justisminister Tor Mikkel Wara: – Vi deler Huawei-uroen i USA og Storbritannia*, 9. januar 2019, https://e24.no/norsk-oekonomi/i/P3QEbX/justisminister-tor-mikkel-wara-vi-deler-huawei-uroen-i-usa-og-storbritannia

[47] DN*, PST ber myndighetene holde et øye med Huawei*, 4. februar 2019, https://www.dn.no/teknologi/huawei/benedicte-bjornland/politiets-sikkerhetstjeneste/pst-ber-myndighetene-holde-et-oye-med-huawei/2-1-535086

[48] E24, *Telia lanserer 5G-plan for Norge: Velger Ericsson over Huawei*, https://e24.no/teknologi/i/wP5vnd/telia-lanserer-5g-plan-for-norge-velger-ericsson-over-huawei.

[49] Ibid.

[50] E24, *Huawei har tapt for andre gang: Telenor velger Ericsson som 5G-leverandør*, https://e24.no/naeringsliv/i/MR2wVK/huawei-har-tapt-for-andre-gang-telenor-velger-ericsson-som-5g-leverandoer. Men merk at Telenor vil fortsatt bruke Huawei basestasjoner i noen deler av landet: Reuters, *Telenor says Huawei will still play role in 5G rollout*, 15. desember 2019, https://www.reuters.com/article/idUSKBN1YJ0BW.

[51] Kommunal- og moderniseringsdepartementet, – *Viktig steg for digitaliseringen av Norge*, Pressemelding 13. Desember 2019, https://www.regjeringen.no/no/aktuelt/-viktig-steg-for-digitaliseringen-av-norge/id2682654/

[52] Kommunal- og moderniseringsdepartementet*, Sikkerhetsloven – krav om "forsvarlig sikkerhet" for neste generasjons mobilnett, 5G,* 14. januar 2020.

[53] Storbritannia innførte for eksempel i januar 2020 et krav om at «høyrisikoleverandører» maks kunne levere 35% av de ikke-sensitive delene av 5G-nettet. I juli 2020 skjerpet de imidlertid kravene og forbød Huawei-utstyr i mobilnettverkene. Se *Press Release: New plans to safeguard country's telecoms network and pave way for fast, reliable and secure connectivity,* 28. januar 2020, https://www.gov.uk/government/news/new-plans-to-safeguard-countrys-telecoms-network-and-pave-way-for-fast-reliable-and-secure-connectivity og *Press release: Huawei to be removed from UK 5G networks by 2027*, 14. juli 2020, https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027.

[54] Xinhuanet, *Huawei says UK ban threatens to move UK into digital slow lane*, 14. juli 2020, http://www.xinhuanet.com/english/2020-07/14/c_139212268.htm

[55] Reuters, *China warns Australia at WTO about 5G restriction*, 12. april 2019, https://www.reuters.com/article/us-huawei-australia-china-wto-idUSKCN1RO20H; Reuters*, Sweden halts 5G auction after court grants relief to Huawei*, 9. November 2020,

https://uk.reuters.com/article/us-sweden-huawei-appeal/sweden-halts-5g-auction-after-court-grants-relief-to-huawei-idUKKBN27P2IA

[56] Politico, *Sweden faces Chinese blowback over Huawei ban,* 21. januar 2021, https://www.politico.eu/article/sweden-faces-chinese-blowback-over-huawei-ban/

[57] Isaac Anna Exclusive: Nokia and Ericsson plan emergency break-up over trade war and security fears, The Telegraph. – 2019; Bloomberg, *China could replace 20 million computers in 3 years as Beijing pushes to wean itself off foreign tech*, Fortune. - 2019