SOFF
Säkerhets- och försvarsföretagen

Till
Post- och Telestyrelse
Box 5398
102 49 Stockholm

**Yttrande med anledning av pågående riskanalys av IT-säkerhet i svenska 5G-nät**

## Inledning

Kommunikation, inklusive datakommunikation, är avgörande för att vårt moderna digitala samhälle ska kunna fungera obehindrat. I den allmänna debatten benämns data (information) ibland som vår tids nya guld eller den moderna oljan. Data driver innovation och förändring i samhället med en otrolig hastighet. Fortsatt och utökad digitalisering[i] är en förutsättning för att klara stora samhällsutmaningar inom välfärd, miljö/energi, trygghet, säkerhet och ett effektivt näringsliv, kort sagt ett fundament för fortsatt positiv samhällsutveckling. Här är effektiva och säkra kommunikationslösningar en av de viktigaste byggstenarna.

Existerande 3G/4G kommunikationssystem utgör även de en, kanske inte tillräckligt uppmärksammad, säkerhetsrisk. Även om kommande 5G-nät i sig innehåller fler säkerhetsmekanismer är den stora utmaningen det kraftigt ökade beroendet av datakommunikation i samhället. 5G-systemens roll för digitalisering och uppkoppling av allt – från samhällstjänster, kritisk infrastruktur till industri 4.0 – gör att de erbjuder en enorm möjlighet men medför också en ökad sårbarhet.

## Ny hotbild

I takt med att digitaliseringen ökar, tilltar även hotbilden[1] och det s.k. säkerhetsgapet[ii] ökar. Såväl icke antagonistisk påverkan såsom naturkatastrofer och bristande tillförlitlighet som antagonistisk påverkan från organiserad brottslighet, främmande makt[2] eller ”vanliga” hackers riskerar att leda till betydande konsekvenser för hela samhället.

Moderna kommunikationssystem är komplexa system av system som det i praktiken är omöjligt att enbart genom tester och granskningar kontrollera så att de inte innehåller oavsiktliga eller avsiktliga säkerhetsrisker. För säkerhetskritiska system löses detta bland annat genom en strikt kontroll på alla led i tillverkningskedjan. Hårdvarudesign och tillverkning, programvaruutveckling och distribution underställs omfattande kontroll avseende allt från strukturerade processer till kontroll av inblandad personal. Även om det inte alltid är genomförbart att fullt ut tillämpa ett liknande förfarande måste man vid

[1] https://soff.se/vara-fragor/cyberforsvar/cyberhotet-och-dess-aktorer-lanksamling-till-rapporter/
[2] https://www.foi.se/rest-api/report/FOI%20MEMO%206698

kravställningen på säkerhetskritiska system göra en riskbedömning som inkluderar hur systemet utvecklats, tillverkats, driftas och skall underhållas.

Digitala system uppdateras löpande med ny programvara, s.k. patchar, för t.ex. åtgärdande av problem, säkerhetsrisker eller utökad funktionalitet. Detta medför att, även om systemet bedöms säkert vid leverans, en uppdatering av programvaran kan skapa nya risker och skulle även kunna utnyttjas av en extern aktör för att implementera säkerhetsluckor. Det finns även exempel på system som slutar fungera om de inte regelbundet är uppkopplade och får programvaruuppdateringar.

Såväl privata som statsunderstödda aktörer bedriver aktivt underrättelseinhämtning[iii] via kommunikationsnätverken. Avsiktliga eller oavsiktliga säkerhetsbrister i kommunikations-systemen ger här en möjlighet att komma åt känslig information och utgör ett högst påtagligt hot för både samhälle och näringsliv.

- Digitaliseringen medför att samhället blir mer beroende av kommunikationssystemen.
- Störningar i kommunikationssystemet riskerar att få allvarliga konsekvenser – samhällets sårbarhet ökar.
- Ökad digitalisering och uppkoppling gör att datanäten i än högre grad kan utnyttjas för olovlig informationsinhämtning
- Den inbyggda säkerheten i moderna kommunikationssystem är hög, däremot kan man inte genom granskning eller test garantera att det inte finns säkerhetsrisker. Här måste man kunna lita på att leverantören inte själv, eller möjliggjort för andra att, avsiktligt implementera bakdörrar, eller nedstängnings-mekanismer.

Nya kommunikationslösningar, nu närmast 5G, kommer att utgöra en av de viktigaste infrastrukturella resurserna för samhället. Sammantaget gör detta att frågan om säkerhet i kommunikationsnäten ytterst blir en nationell säkerhetspolitisk fråga. Svårigheten att säkerhetsgranska systemen i sig medför att det blir högst väsentligt att göra en samlad säkerhetsbedömning av en tilltänkt leverantör inklusive dennes ägarstruktur och eventuella koppling till främmande makt.

**Kommunikationssystemen säkerhetsmekanismer**

Riskerna avseende sekretess och integritet kan hanteras med hjälp av kända tekniska åtgärder, såsom virtuella privata nätverk (VPN) och end-to-end-kryptering. Sådana åtgärder används redan idag i stor utsträckning för att säkra konfidentiell kommunikation som sker över osäkra kanaler. Frågan om tillgänglighet är däremot svårare att ta itu med och har en större säkerhetspolitisk implikation. Idag förhindrar ingenting säljaren från att installera en funktionalitet som kommer att störa eller bryta ned nätverket vid en vald tidpunkt.

5G-systemen utformas med avancerade säkerhetsmekanismer som kraftigt ökar systemens tillgänglighet, integritet och autenticitet jämfört med tidigare generationers kommunikationssystem. Lösningarna följer i många fall universella standarder och skiljer sig inte markant åt mellan olika leverantörer. 5G-nätens säkerhetsmekanismer kan liknas med ett skal som skall skydda kommunikationsinnehållet. Så länge skalet är intakt är informationen säkrad.

Mycket fokus läggs idag på frågan hur vi kan säkerställa att systemen inte innehåller oavsiktliga eller avsiktliga sårbarheter och säkerhetsrisker. Ett initiativ rör certifiering som en viktig del för att uppnå högre säkerhet och det pågår nu ett arbete inom EU för att uppnå högre säkerhet genom certifiering. Certifiering når dock inte hela vägen fram när det gäller skydd mot alla hotnivåer. Ett annat initiativ som är gemensam för merparten av alla digitala system är metoder som Common Criteria (CC). För kommunikationsområdet finns NESAS[3] som bygger på att kontrollera processerna kring utveckling, tillverkning, distribution och underhåll. Metoderna bygger på strukturerat och kontrollerade processer med transparens och bidrar till en ökad tillförlitlighet och säkerhet i systemen. Metoderna klarar däremot inte att hantera en tillverkare/aktör som medvetet implementerar skadliga eller oönskade funktioner i hårdvara eller programvara.

Moderna kommunikationssystem utvecklas kontinuerligt och mjukvaran uppdateras ofta, till exempel för att skydda mot nya typer av attacker och för att förbättra övergripande systemskydd baserat på ny forskning. Det innebär att testresultat från en version av systemet inte speglar systembeteendet efter en programuppdatering. Att ha en insyn i värdekedjan innefattande både komponenter och underhåll är därmed av största vikt.

**Globala system kräver gränsöverskridande lösningar**

Genom 5G kan myndigheter, näringsliv och individer kommunicera i en hastighet anpassad efter vårt föränderliga och sammankopplade samhälle. Infrastrukturen är gränsöverskridande och därmed är frågan om 5G och säkra nät likaså. Sverige har traditionellt en god kunskap inom kommunikation och säkerhet. Vi har även en internationellt bra position för att ytterligare stärka denna. Här kan Sverige bidra till andra länders säkra kommunikationslösningar och också medverka till en positionering av europeiskt industriellt ledarskap.

Säkerhet är en nationell angelägenhet, EU ger ingen generell lösning, utan Sverige måste forma sina egna säkerhetsregler rörande framtida kommunikationsnät. Däremot stärks de facto säkerheten i kommunikationsnäten genom att fler länder antar liknande säkerhetskrav vid anskaffning av sina kommunikationssystem.

**Marknads- och leverantörs aspekter**

SOFF poängterar att vi som förening främjar fri och rättvis konkurrens och är av den övertygelsen att alla leverantörer ska bedömas likvärdigt, oavsett vilken leverantören är.

SOFF vill framhålla att frågan om 5G förvisso har ett flertal tekniska aspekter, men att de säkerhetspolitiska aspekterna är desto viktigare. Sverige har en tradition av öppenhet och tillgänglighet. Vi är ett av världens mest digitaliserade länder och har en politisk plan att fortsätta i samma riktning. Vidare är det ett av världens mest innovativa länder och särskilt

[3] The NESAS (network equipment security assurance scheme) is an initiative from 3GPP and GSMA to create a security assurance scheme suitable to the telecom equipment lifecycle

gällande tekniska innovationer. Vitalt blir därmed att göra en grundlig säkerhetspolitisk analys kring vilka effekter val av olika leverantörer kan få.

Säkerhet skapas inte enbart genom att ha ett förtroende för ett system. Säkerhet löses inte heller enbart med frågan om tillit, huruvida vi kan lita på att en leverantör agerar oberoende av det land där säljaren har sitt huvudkontor eller sitt ägande.

Säkerhet handlar i grunden om att möta tekniska, operativa och strategiska krav för att öka motståndskraften mot cyberattacker. Men säkerhet är ingenting som står separerat från resterande funktioner och när det rör så vitala funktionaliteter som kommunikation och datakommunikation så krävs en säkerhetspolitisk avvägning innefattande både tekniska och politiska parametrar samt tillit till alla aktörer i värdekedjan.

Även om säkerheten i en produkts utrustning eller installationer av dess utrustning, kan eller inte kan äventyras kvarstår det otvetydiga faktum att exempelvis kinesiska produkter är föremål för kinesisk lag som kräver att kinesiska organisationer eller medborgare ska stödja, bistå och samarbeta med den kinesiska statens underrättelsemyndigheter. I grunden faller således frågan tillbaka på om kinesisk teknik kan bli betrodd med tanke på den kinesiska regeringens inflytande och styrning av kinesiska företag. I praktiken kan inkrementella kostnader för riskreducering vara tillräckligt hög för att göra kinesiska tekniska produkter oacceptabla, dock av ekonomiska skäl snarare än politiska skäl. Det ska samtidigt understrykas att Kina inte är det enda landet för vilket detta är en risk. Det gäller även exempelvis Ryssland och Iran.

**Frågan om tillit och förtroende**

Principen om en rättsstat är en av de grundläggande princip som fastställs i artikel 2 i Fördraget om Europeiska unionen. Det innefattar gemensamma värden såsom en transparent och demokratisk process för att anta lagar. Rättssäkerheten bygger på objektivitet och opartiskt rättsväsen med respekt för de grundläggande rättigheterna och lika värde inför lagen. Det är viktigt att förstå skillnaden mellan rättsstat och kinesiska regelverket ”rule of law”, som bl.a. i rättsprocesserna legitimerar partiets ledarskap[4]. Den konstitutionella rättsmodellen är av betydelse för att bedöma tilltron till en leverantör till samhällsviktig verksamhet, i synnerhet 5G-tjänster.[5] Eftersom program- eller hårdvara kan påverkas av utländsk lag, inte minst när det finns uttryckliga underrättelselagar som företag och individer har att följa även utanför hemlandets jurisdiktion så kan dessa lagar vara i strid mot Sveriges rättssäkerhet.

Många länder har underrättelselagar, inte minst tillåter de flesta länder inhämtning för de brottsbekämpande myndigheternas underrättelseverksamhet, genom vilka myndigheter kan begära samarbete från exempelvis operatörer. När det gäller extraterritoriell lagstiftning, såsom den kinesiska, måste en värdering ske utifrån rättsstaten principer och vilket skydd som finns för de grundläggande rättigheterna. Fattas beslut om att exempelvis utelämna

[4] ”Understanding the Chinese Communist Party’s Approach to Cyber-Enabled Economic Warfare”, Zack Cooper, https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/documents/REPORT_China_CEEW.pdf
[5] How the Track Record of the CCP Should Play into the Due Diligence of Huawei’s Partners and Customers, https://www.rwradvisory.com/wp-content/uploads/2019/05/Assessing-Huawei-Risk.pdf

information av operatörerna av ett oberoende rättsväsen eller är beslut påverkade av politiska motiv? För att bättre förstå vilket rättsskydd som aktörer har kan ett antal faktorer vara av betydelse: a) Har lagen ett definierat syfte såsom brottsbekämpning eller nationell säkerhet (t.ex. terrorism), b) finns där ett oberoende rättsväsen, samt c) är rättsväsendet oberoende i förhållande till styrande regering eller den myndigheten som begär beslutet.

Det är naturligt att stater värderar förtroendet för leverantören vid anskaffning av produkter och tjänster, inte minst under höjd beredskap och ytterst vid krig.[6] Dock är gråzonen idag betydligt mer komplicerad och krav, utifrån trygghet, innebär att staten ser behov av att ställa krav på försörjningstrygghet vid upphandlingar där förtroende till leverantören krävs som en följd av utformningen av försvarsplaneringen. Mot bakgrund av vissa kritiska teknologiers betydelse för skyddet av samhället är det för SOFF lika naturligt att vissa produkter och tjänster som levereras inom samhällsviktig verksamhet och totalförsvaret, såsom telenät och datacenter, bör värderas utifrån motsvarande förtroende. Det är naturligt, inte minst för att begränsa risken för statsunderstött spionage och stora förluster.

Givet den säkerhetskritiska roll kommunikationssystemen har i dagens och morgondagens samhälle behöver de värderas utifrån utrikes-, försvars-, och säkerhetspolitiskt perspektiv.

**SOFF:s rekommendationer**

- Se över möjligheterna att i enlighet med säkerhetsskyddslagstiftningen tydligare föreskriva att leverantörer av it- och kommunikationstjänster, utöver tekniska riskbedömningar, även i sin analys beaktar exempelvis beroendeställning hos underleverantörer och risker i värdekedjan.
- Se över kraven vid upphandling av IT-produkter till kritisk infrastruktur, inte minst relaterat till samhällsviktig verksamhet och av betydelse för civilt försvar.
- De ändringar som föreslås för lagen om elektronisk kommunikation (LEK) riskerar att endast träffa en del av 5G-infrastrukturen, nämligen en begränsad del av verksamheter som sänder radio. Föreningen har i yttrande till regeringen föreslagit att lagstiftaren bör förlita sig på unionsrätten för att kunna införa villkor eller skyldigheter på operatörer och för att kunna säkerställa ett mer ändamålsenligt säkerhetsskydd för hela 5G-infrastrukturen.
- Se över hur dagens rådgivning i enlighet med säkerhetsskyddslagstiftningen ska utövas och av vem. SOFF anser att den främsta åtgärden för att höja nivån på säkerhetsskyddet i Sverige är just rådgivning och att en effektiv rådgivning skulle höja nivån på säkerhetsskyddet i Sverige på ett betydligt bättre sätt än vad ett hot om sanktioner kan göra. SOFF anser därför att rådgivningen bör utvecklas från dagens nivå och att en eller flera myndigheter utpekas särskilt för denna uppgift och även får resurser för att genomföra uppdraget. Exempel på områden där rådgivningen behöver förbättras är kring aktuell och verksamhetsanpassad hotbild, metodstöd för säkerhetsskyddsarbete samt i den viktiga diskussionen om vad som är – och inte är – säkerhetskänslig verksamhet inom olika sektorer. Även hur säkerhetsprövning av personal för utveckling och tillverkning av säkerhetskritiska system kan hanteras inom ramen för säkerhetsskyddslagen bör prövas.

[6] The 5G Fight Is Bigger Than Huawei, https://foreignpolicy.com/2019/05/22/the-5g-fight-is-bigger-than-huawei/

- Utöver säkerhetsskyddslagstiftningen, även se över hur staten bistår företag som bedömer att de bedriver skyddsvärd verksamhet eller företag som har en särskild roll inom totalförsvaret. Det handlar om att bistå företagen med preventiva verktyg och åtgärder att minska risken för spionerі, cyberattacker, oönskade underleverantörsberoenden/ risker, granskning av utländska förvärv eller personal verksam i för företagen känslig verksamhet såsom vid innovationsmiljöer, etc.
- I Sverige finns ingen övergripande lagstiftning som syftar till genomlysning och kontroll av utländska investeringar. Verksamheter som enligt säkerhetsskyddslagen är säkerhetskänsliga är underställda krav på att en säljare av sådan verksamhet ska anmäla en överlåtelse till myndigheten. Anmälan tar inte sikte på om köparen är en utländsk eller svensk köpare. Nya regler, inklusive kontrollprocesser, har föreslagits. Dock skulle sådana kontroller även fortsättningsvis endast gälla säkerhetskänslig verksamhet. Verksamheter med kritisk teknologi, men som inte är säkerhetskänsliga, skulle fortfarande inte träffas. Detta behöver tydligare hanteras och relationen mellan teknik och infrastruktur beaktas.

Yttrandet har beretts av medlemsgruppen för samhällssäkerhet tillsammans med medlemsgrupperna för säkerhetsskydd samt cyberförsvar.

Föreningen vill även uppmärksamma myndigheten över det yttrande föreningen lämnat på promemorian om ”Kompletterande förslag till betänkandet Frekvenser i samhällets tjänst (SOU 2018:92)”.

Stockholm den 10 juni 2019.

Robert Limmergård

Generalsekreterare

[i] Värnkraft Inriktningen av säkerhetspolitiken och utformningen av det militära försvaret 2021–2025, kap 3.2 https://www.regeringen.se/49b29c/globalassets/regeringen/dokument/forsvarsdepartementet/forsvarsberedningen/slutrapport-14-maj/ds-2019_8-varnkraft---inriktningen-av-sakerhetspolitiken-och-utformningen-av-det-militara-forsvaret-2021-2025.pdf

[ii] Nationell risk- och förmågebedömning 2019**,** Myndigheten för samhällsskydd och beredskap (MSB), https://www.msb.se/RibData/Filer/pdf/28836.pdf

[iii] FRA Årsrapport 2018, https://www.fra.se/download/18.69cf97cd167832fc038250/1548773731405/FRA-arsrapport-2018.pdf