FOI
Totalförsvarets forskningsinstitut

Vid korrespondens åberopa
FOI beteckning

Datum
2023-08-16

Nr FOI-2023-959

Finansdepartementet
Enheten för digital infrastruktur och säkerhet
103 33 Stockholm

Er referens
Fi2023/01693

Vår handläggare
Daniel Eidenskog

Svar gällande frågor om dagens och framtidens utmaningar på konnektivitetsområdet

Sammanfattning av FOI:s synpunkter

Totalförsvarets forskningsinstitut (FOI) har – från de utgångspunkter myndigheten har att beakta – följande kommentarer till de frågor som ges i frågeunderlaget. FOI:s kommentarer nedan avser huvudsakligen området *robusthet och säkerhet*.

Frågorna som ställts kring robusthet och säkerhet är mycket breda och det finns inga enkla svar. Följande text tar upp några få aspekter av robusthet och säkerhet, men i praktiken skrapar texten bara på ytan av den komplicerade struktur av hot, säkerhets-avväganden, skyddsåtgärder och styrmedel som är relevanta i sammanhanget. FOI välkomnar därför en fortsatt dialog med Finansdepartementet i dessa frågor.

Sverige har genomgått en mycket omfattande digitalisering inom i stort sett alla samhällsområden och digitaliseringen fortsätter med oförminskat tempo. Den höga graden av digitalisering innebär att Sverige numera är helt beroende av digital infrastruktur för att samhället ska fungera. En robust och säker digital infrastruktur är således *av mycket stor vikt* för såväl offentliga som privata verksamheter samt för privatpersoner i såväl fredstid som totalförsvarsperspektiv. Samhällsviktig verksamhet såsom Försvarsmakten, bankväsendet samt hälso- och sjukvården är kraftigt beroende av digitala system, samtidigt som privatpersoner snart är helt beroende av digital infrastruktur för att exempelvis hantera sin ekonomi i dagens huvudsakligen kontantlösa samhälle.

För att kunna upprätthålla samhällets funktion i allmänhet och totalförsvarets funktion i synnerhet även i kris, gråzon och krig behöver den digitala infrastrukturen byggas och förvaltas med tillräcklig nivå av robusthet, redundans och cybersäkerhet utifrån de faktiska behov som föreligger. De antagonistiska hoten i gråzon och krig går långt bortom de hot som föreligger i fredstida normalläge, vilket således ställer

Postadress
FOI
164 90 STOCKHOLM

Besöksadress
Gullfossgatan 6, Kista
Leveransadress
Gullfossgatan 12, Kista

Telefon
08-55 50 30 00

Fax

registrator@foi.se

Orgnr: 202100-5182
www.foi.se

mycket höga krav på säkerhetsarbetet om infrastrukturens funktion ska kunna upprätthållas även i sådana situationer.

Digital infrastruktur utgör – precis som alla andra digitala system – sociotekniska system bestående av samhälle, organisationer, människor och teknik. Tekniken kan inte ses i ett vakuum, utan måste hanteras utifrån dess roll i det omkringliggande sammanhanget. Därigenom blir bland annat tillräckliga förutsättningar för säkerhetsarbetet; sammanhållen styrning och stöd utifrån faktiska säkerhetsbehov; försörjningsberedskap; kompetensförsörjning och spektrumallokering[1] vitala för att nå lämplig nivå av säkerhet som resulterar i tolerabel kvarstående risk i infrastrukturen sett ur ett samhällsperspektiv.

Följande avsnitt fördjupar och utvecklar resonemangen som ligger bakom de ovanstående kommentarerna.

Förutsättningar och hotbild

Den digitala infrastruktur som finns idag ägs och förvaltas av ett stort antal olika aktörer, allt från internationella bolag till stadsnät och små fiberföreningar, ägda såväl offentligt som privat. De olika aktörerna har mycket olika förutsättningar för och behov av att arbeta med tillgänglighet och robusthet i sina kommunikationsnät. De större aktörerna har generellt sett bättre förutsättningar för strategiskt, strukturerat säkerhetsarbete och bättre tillgång till personal som snabbt kan utföra åtgärder vid olika händelser, speciellt jämfört med de minsta aktörerna såsom små stadsnät och fiberföreningar.

De digitala hoten mot infrastrukturen är mångfacetterade och inkluderar allt från fredstida misstag av systemadministratörer till riktade, välplanerade angrepp från främmande makt. Andelen riktade, välplanerade angrepp kan överlag antas öka i en gråzon, med en topp som troligtvis kommer i samband med ett krigsutbrott.

De fysiska hoten som infrastrukturen har att hantera varierar också stort. I fredstid och kris är det sannolikt främst misstag och olyckshändelser i form av avgrävningar, bränder, översvämningar och väderhändelser (inklusive sekundäreffekter såsom långa elavbrott) som kan påverka infrastrukturen. I gråzon och krig tillkommer ökande antagonistiska hot såsom sabotage, bombningar och fientligt övertagande.

De antagonistiska hot som tillkommer i gråzon och krig ställer signifikant högre krav på skyddsåtgärder än de fredstida hoten om samma nivå av risk och tillgänglighet ska vidmakthållas. Exempelvis är det mycket svårt att skydda alla de fysiska delarna av infrastrukturen mot sabotage vilket har illustrerats bland annat vid fällningen av Häglaredsmasten utanför Borås 2016, fällningen av en mobilmast i Bygdeå 2013 och

[1] Spektrumallokering innebär tilldelning av radiofrekvenser till olika typer av ändamål och aktörer, såsom kommersiella TV-sändningar och militär radiokommunikation.

sabotagen mot transformatorstationer i Moore County, North Carolina, USA, 2022. Skyddsåtgärderna för gråzon och krig kan också kräva en betydligt högre grad av autonomi i organisationen gällande personal, kunskap och material, då tillgången till externa parter och externa leveranser potentiellt kan begränsas kraftigt. Det försämrade omvärldsläget, med exempelvis kriget i Ukraina och ökade handelshinder mellan Kina och USA, leder bland annat till påverkan på försörjningskedjor inom exempelvis elektronik där det potentiellt kan leda till kraftiga begränsningar i tillgången på utrustning och reservdelar.

En bred beskrivning av gråzonsproblematik återfinns i rapporten *Civilt försvar i gråzon* (Jonsson, 2019). Fördjupningar inom digitaliseringens problematik återfinns i rapporterna *Vilse i lasagnen? – En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur* (Ingemarsdotter m.fl., 2020) och *Digitaliseringens risker i hälso- och sjukvård – Om påverkan på patienter, personal och verksamhet* (Eidenskog, 2023). Fördjupning om offentliga verksamheters beroenden av externa digitala kommunikationer återfinns i rapporten *IT när de externa anslutningarna går ner – Konsekvenser och reservalternativ i offentliga verksamheter* (Karlzén, 2022).

Tillgänglighetsbehov

För användarna är möjligheten att kommunicera rimligtvis den viktigaste förmågan som infrastrukturen har att upprätthålla. Tillgängligheten hos kommunikations–tjänsterna – det vill säga att information kan transporteras till den plats där den behövs när så behövs – är därmed central. Tillgänglighet är också den skyddsaspekt som infrastrukturen huvudsakligen har möjlighet att bidra till. Såväl privat som offentligt ägd civil digital infrastruktur används även av samhällsviktiga verksamheter inom exempelvis Försvarsmakten, hälso- och sjukvården, blåljusmyndigheter, bankväsendet, transporter och energiförsörjning.

Det krävs många olika former av skyddsåtgärder och robusthetshöjande åtgärder för att upprätthålla tillgängligheten över ett brett spektrum av såväl olyckshändelser som antagonistiska angrepp. Åtgärderna inkluderar bland annat tillräcklig cybersäkerhets-nivå inom infrastrukturen för att skydda infrastrukturens utrustning mot cyber-angrepp; tillräckliga skydd mot överbelastningsattacker; tillräckliga skydd för att upptäcka eller motverka störsändningar; god praxis vid förläggning av kabelstråk; adekvat fysiskt skydd av noder och basstationer; adekvat fysiskt skydd av centrala kopplingspunkter; skydd mot översvämningar, bränder och väderhändelser samt väl utformad diversitet och redundans i centrala infrastrukturdelar.

Vilka skyddsmekanismer och robusthetshöjande åtgärder som är lämpliga och tillräckliga beror på behoven inom respektive del av infrastrukturen. Behoven bör i sin tur utgå från användarnas faktiska behov av kommunikationstjänsternas tillgänglighet. Detta faktiska behov av tillgänglighet är dock ett komplicerat ämne, då behovet i många fall kan bli starkt beroende av hur användarorganisationerna

utformar sina digitala system och därigenom påverkar beroendena till infrastrukturen. Då behoven ska utgöra grunden för arbetet med säkerhet och robusthet är det viktigt att tillräckliga resurser och tid läggs på att identifiera dessa behov.

Dagens lagreglering av tillgänglighetsaspekter inom digital infrastruktur består huvudsakligen av lagen om elektronisk kommunikation (2022:482) med tillhörande förordning (2022:511) samt PTS föreskrifter (PTSFS 2022:11). I föreskrifterna utgår kraven från antalet användare som drabbas, snarare än på användarnas faktiska behov av tillgänglighet. För så kallad nummeroberoende interpersonell kommunikation, där bland annat vanliga fasta internetanslutningar ingår, är det endast relativt stora anläggningar som omfattas av krav på redundans eller reservkraftförsörjning enligt PTSFS 2022:11. Ett avbrott som drabbar en enstaka särskilt tillgänglighetskänslig verksamhet kan rimligen få långt större konsekvenser än ett avbrott som drabbar många användare som saknar specifika säkerhetsbehov. Samtidigt ser förutsättningarna för infrastrukturen mycket olika ut i olika delar av landet. Exempelvis återfinns akutsjukhuset i Gällivare i en glesbefolkad kommun med ca 17 000 innevånare på knappt 6 500 km^2, medan Södersjukhuset på Södermalm i Stockholm befinner sig i en mycket tätbefolkad stadsdel med ca 130 000 innevånare på 5,7 km^2.

Värt att observera är att EU-direktivet (2018/1972) som ligger bakom lagen om elektronisk kommunikation även tar upp andra parametrar utöver antalet användare som kan drabbas och hur länge en säkerhetsincident varar – däribland ”den utsträckning i vilken ekonomisk och samhällelig verksamhet påverkas” (EU 2018/1972, artikel 40). Dessa andra parametrar omnämns inte i den svenska regleringen. Den svenska regleringen är också vag gällande vilka krav som gäller på infrastrukturens tillhandahållare i händelse av höjd beredskap och krig.

Det är generellt sett mycket kostsamt att nå hög säkerhetsnivå avseende tillgänglighet, speciellt när hotbilden inkluderar kvalificerade antagonistiska angrepp, varför hög tillgänglighet rimligtvis inte ska kravställas i onödan. Olika aktörer inom digital infrastruktur har dessutom olika möjligheter och förutsättningar för att arbeta med denna typ av frågor.

Sett ur perspektivet att regleringens krav inte möter samhällsviktig verksamhets behov men att det samtidigt är orimligt att utforma infrastrukturen som helhet för att möta dessa behov, bör andra metoder användas för att nå en lämplig nivå på tillgänglighet och robusthet i berörda delar av infrastrukturen. För detta ändamål är det av stor vikt att tillse att tillhandahållare och användare har möjlighet till ömsesidig förståelse av varandras behov och förutsättningar. Exempelvis kan ett samordnat stöd vid behovsanalyser och kravställning av digital infrastruktur och kommunikationstjänster för samhällsviktiga verksamheter ge möjlighet såväl till rimliga, proportionella och enhetliga krav som till förståelse hos användarnas verksamheter för infrastrukturens och kommunikationstjänsternas begränsningar i

olika situationer. Därtill kan stöd för välgrundad aktörsöverskridande kontinuitetsplanering vara fördelaktigt för kris- och krigsberedskapen. Ytterligare en säkerhetshöjande åtgärd kan vara att underlätta samövningar mellan olika aktörer inom digital infrastruktur och samhällsviktiga verksamheter för att förbättra samarbetet och den ömsesidiga förståelsen mellan organisationerna.

Komplexitet och exponering

Dagens IT-system är extremt komplexa och utvecklas ofta under såväl ekonomisk press som tidspress samtidigt som kravbilden förändras under utvecklingens gång. Komplexiteten är ett av de största hindren för att skapa system som är fria från brister och sårbarheter. Utgångspunkten i allt cybersäkerhetsarbete måste därför vara att *systemen har sårbarheter* vilket i sin tur gör att säkerhetsarbetet i många avseenden är till för att hantera sårbarheter, undvika angrepp, avvärja angrepp samt minimera skadeverkningar. En fördjupning i den sociotekniska systemkomplexiteten och hur den påverkar cybersäkerheten återfinns i presentationen *Varför är cybersäkerhet så svårt?* (Eidenskog, 2022).

Sammankoppling av system medför större exponering mot potentiella antagonister. Användningen av internet utgör kanske den största exponeringen som går att uppnå, där i princip vem som helst i hela världen kan försöka sig på ett angrepp mot systemet. Digital infrastruktur är av nödvändighet exponerad, speciellt när det gäller internet-infrastruktur. Infrastrukturens självskydd i form av cybersäkerhetsåtgärder är därmed central för infrastrukturens funktion.

Trådlösa kommunikationer medför några specifika utmaningar som behöver hanteras. Trådlöshet innebär bland annat att externa parter ges större möjligheter att avlyssna och påverka kommunikationen, men exponerar även kommunikationsvägen mot intrångsförsök. Trådlös kommunikation kan också störas ut med mer eller mindre sofistikerade störsändare. Sofistikerade störsändare kan vara mycket svåra att lokalisera utan speciell utrustning och kompetens, något som i dagsläget huvudsakligen bara finns hos Försvarsmakten och FOI. Dessutom blir den fysiska exponeringen större för vissa trådlösa system. Exempelvis brukar basstationer för mobilkommunikation vara lätta att lokalisera då de ofta inkluderar synliga master eller antenner samt att de går att pejla genom att mäta utsända radiosignaler. Basstationerna utgör därmed tydliga mål för fysiska sabotage i gråzon eller krig.

Leverantörsberoenden

Digital infrastruktur drabbas av många olika typer av beroenden. Utrustning och reservdelar tillverkas i stor utsträckning utomlands, där exempelvis de funktionellt centrala halvledarkomponenterna nästan uteslutande tillverkas utanför Sverige och i mycket stor utsträckning utanför Europa. Även för IT-utrustning som slutmonteras i Sverige finns det således avgörande beroenden till utländska leverantörer.

Det är också relativt vanligt att driftsättning och underhåll av komplexa IT-system och IT-produkter kräver specialistkunskap som bara går att hitta hos leverantören eller specialiserade konsulter. Även om kompetensen teoretiskt sett skulle kunna upprätthållas i den egna organisationen kan det vara orimligt för en mindre organisation när för många olika IT-produkter kräver specialistkunskap.

Effekterna av beroenden i leveranskedjor har tydliggjorts under de senaste årens halvledarbrist som uppkom som en kombination av bland annat Corona-pandemin, en omfattande brand i en halvledarfabrik och torka i Taiwan. Sverige och EU bör ta fram strategiska planer för försörjningsberedskap där bland annat tillgången till utrustning och reservdelar säkras för samhällsviktig verksamhet och infrastruktur.

En fördjupning i leveranskedjeproblematiken för IT-system återfinns i rapporten *Säkra leveranskedjor för IT-system* (Eidenskog m.fl., 2019). Fördjupningar inom försörjningsberedskap återfinns i rapporterna *Nationell försörjningsberedskap - FOI:s analys av försörjningsberedskapen som svar på regeringsuppdrag Ju2020/02565/SSK, Ju2018/05358/SSK* (Stenerus & Ingemarsdotter, 2021) och *Strategisk autonomi: Om EU:s uppbyggnad av försörjningsberedskap ur ett svenskt totalförsvarsperspektiv* (Ingemarsdotter, 2022).

Inflytande över infrastrukturen

Samhällsviktig digital kommunikationsinfrastruktur bör ägas och kontrolleras av pålitliga och stabila aktörer, oavsett nationalitet, för att kunna upprätthålla en svensk rådighet över den svenska infrastrukturen även i försämrat omvärldsläge. Det kan finnas behov av att se över vilka utländska intressen som finns i samhällsviktig digital infrastruktur, inklusive intressen som kan utöva indirekt påverkan genom exempelvis påtryckningar eller finansiella maktmedel.

Kompetensförsörjning

Det är redan idag en brist på kompetent personal inom IT-området i stort och inom cybersäkerhetsområdet i synnerhet. Detsamma gäller för personal med kompetens inom informationssäkerhet och säkerhetsskydd. Kompetensbrist riskerar att begränsa förmågan att skydda systemen mot såväl fredstida hot som hot i gråzon och krig.

God tillgång på kompetent personal är central för att kunna bygga, driva, förvalta, underhålla och upphandla system med adekvat säkerhetsnivå. Brist på kompetent personal skadar även den autonomi som krävs i organisationerna för drift, förvaltning och underhåll av infrastrukturen och kommunikationstjänsterna i en långt gången gråzon eller i krig.

En bred översikt över kompetensförsörjningsproblematiken för totalförsvaret återfinns i rapporten *Växtvärk – Utmaningar med att personalförsörja det civila försvaret i fredstid* (Olsson & Reichel, 2021).

Totalförsvarets forskningsinstitut

Datum
2023-08-16

Nr FOI-2023-959

Spektrumallokering

Spektrumallokering är viktig för att säkerställa långsiktig tillgång till radiofrekvensutrymme för dagens och framtidens kommunikationsbehov. Det gäller att vidmakthålla en strategisk planering för allokering av frekvensband så att såväl civila som militära kommunikationsbehov kan tillgodoses även på längre sikt. Ett långsiktigt fokus är viktigt bland annat då det är svårt att återta frekvensband som tilldelats en viss funktion samt att spektrumallokering kräver internationell samordning. För att underlätta en kontinuitet och långsiktighet krävs tillräckliga resurser för Post- och telestyrelsens samt Försvarsmaktens arbete inom området.

Referenser

Eidenskog, Bildsten & Endres (2019). *Säkra leveranskedjor för IT-system*. FOI-R--4851--SE.

Eidenskog (2022). *Varför är cybersäkerhet så svårt?* Presentation på IT-försvarsdagen. https://www.youtube.com/watch?v=QRRdY5J-hkI

Eidenskog, Eckersand & Mittermaier (2023). *Digitaliseringens risker i hälso- och sjukvård – Om påverkan på patienter, personal och verksamhet*. FOI-R--5367--SE.

Ingemarsdotter, Eidenskog & Hedtjärn Swaling (2020). *Vilse i lasagnen? – En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur*. FOI-R--4814--SE.

Ingemarsdotter (2022). Strategisk autonomi: Om EU:s uppbyggnad av försörjningsberedskap ur ett svenskt totalförsvarsperspektiv. FOI-R--5338--SE.

Jonsson, Ingemarsdotter, Johansson, Rossbach, Wedebrand & Eriksson (2019). *Civilt försvar i gråzon*. FOI-R--4769--SE.

Karlzén (2022). *IT när de externa anslutningarna går ner – Konsekvenser och reservalternativ i offentliga verksamheter*. FOI-R--5260--SE.

Olsson & Reichel (2021). *Växtvärk – Utmaningar med att personalförsörja det civila försvaret i fredstid*. FOI-R--5230--SE.

Stenerus & Ingemarsdotter (2021). *Nationell försörjningsberedskap - FOI:s analys av försörjningsberedskapen som svar på regeringsuppdrag Ju2020/02565/SSK, Ju2018/05358/SSK*. FOI-R--5174--SE.

FOI-rapporterna går att ladda ner på https://foi.se/rapporter.html.

FOI
Totalförsvarets forskningsinstitut

Datum
2023-08-16

Nr FOI-2023-959

Detta svar har beslutats av generaldirektör Jens Mattsson efter föredragning av förste forskare Daniel Eidenskog. I den slutliga handläggningen har även enhetschef Jonas Hallberg, chefsjurist Eva Liljefors samt särskild rådgivare Mikael Wiklund deltagit.

……..
Jens Mattsson

……..
Daniel Eidenskog

Sändlista

Finansdepartementet (fi.registrator@regeringskansliet.se och david.troeng@regeringskansliet.se)

För kännedom

Försvarsdepartementet

Internt FOI

Registrator

GD-sekreterare

Chefsjurist

AC