Vetenskapsrådet

Datum/Date
2018-12-07

Handläggare
Maria Häll/Börje Josefsson

Att motverka överbelastning av samhällsviktiga webbplatser

Slutrapport 2018 från projekt Särimner

VETENSKAPSRÅDET
SWEDISH RESEARCH COUNCIL

Box 1035
SE-101 38 Stockholm, Sweden

Tel: +46 (0)8 546 44 000
vetenskapsrådet@vr.se
www.vr.se

Sammanfattning

Post- och telestyrelsen (PTS) har som en del av myndighetens kontinuerliga arbete för ökad robusthet och beredskap identifierat ökade problem för medborgare att nå samhällsviktiga offentliga tjänster (till exempel krisinformation.se, valmyndigheten.se och regeringen.se). Dessa problem har även identifierats t.ex. vid övningen TELÖ17 som genomfördes med inriktning på utveckling och uppbyggnad av det civila försvaret inom totalförsvaret, samt de överbelastningsattacker som hade media som mål under våren 2016. PTS har med detta som grund fört diskussioner med Sunet, en enhet inom Vetenskapsrådet, om att genomföra ett pilotprojekt som syftar till att undersöka möjligheterna att bygga en robust internetinfrastruktur för distribution av webbaserat innehåll. Det primära syftet med pilotprojektet skulle vara att undersöka hur dessa tjänster ständigt ska kunna vara nåbara. Uppdraget gavs av PTS till Vetenskapsrådet 8 december 2017.

Detta pilotprojekt har haft som primärt mål att placera noder på ett distribuerat sätt inom och utanför Sverige för att uppnå det önskade målet. Dock visade det sig att lösningen inte hanterade vissa typer av hot, speciellt partitionering av Sverige, vilket i sin tur beror på en kombination av hur fiberutbyggnaden skett och operatörernas utformning av sina nät. Nätdesignen är idag centraliserad, vilket gör det i stort sett omöjligt att kommunicera inom en partitionerad del. Risken för partitionering vid t.ex. dammbrott, avgrävningar etc. är dessutom hög då det finns en stor brist på mötesplatser där ändpunkter på fiber som etablerats möts och kopplingspunkter skapas. Det är således både en risk för att partitionering sker och en risk att sådan partitionering får stor påverkan på samhället.

Detta är en fråga som lyfts i flera infrastrukturforum tidigare, där flera operatörer påpekade att för att övningarna skulle bli mer korrekta samt om tjänster skulle bli mer robusta måste moderna metoder och aktuella situationer användas. Beskrivningen av hur det såg ut i Sverige för att kunna genomföra övningarna stämde inte med det faktiska tillståndet (“kartan skiljer från verkligheten”).

Noderna i sig, kallade “Särimnernoder”, har konstruerats på sådant sätt att de fortsätter leverera innehåll till besökarna, trots att de tappat kontakt med den riktiga servern. I en kris där originalkällan inte finns så ska det finnas en sparad version av senaste, eller alternativ, information.

Lösningen har visat sig skydda mot olika typer av hot. Exempelvis ger lösningen möjlighet att distribuera innehåll under mycket hög belastning, men hotet gällande partitionering kan inte hanteras fullt ut. Dagens svenska IT-infrastruktur har framförallt byggts ut där det funnits affärsmässiga skäl som talat för detta, och bristande koordinering har medfört att det finns för få mötesplatser för fiber, vilket i sin tur leder till bristande redundans. Några få operatörer har etablerat redundanta vägar, men långt ifrån i den utsträckning samhället behöver.

För att öka robustheten gällande kommunikation i Sverige måste därför fler mötesplatser speciellt för fiber men även kommunikation generellt etableras. Mötesplatserna behöver byggas ut under god samordning och med säkrad finansiering. En rimlig målbild kan vara 3-5 mötesplatser per geografiskt område, som ligger 50-70 km från varandra. Troligen behövs på sikt storleksordningen något hundratal mötesplatser utslaget över hela Sverige.

Om frågan finansiering kan lösas, exempelvis via uppdrag till PTS, finns goda förutsättningar till fortsatt implementering av projektets resultat. Det är möjligt att såväl etablera mötesplatser som att bygga Särimner, dvs ett gemensamt system för extremt distribuerade webbaserade tjänster för

samhällskritisk information. Dock bör noder för dessa (Särimnernoder) placeras ut i mycket nära samarbete med Internetoperatörerna, och framför allt inom deras nät.

På kort sikt, parallellt med initiering av arbete med att etablera mötesplatser, är förslaget att SUNET/Vetenskapsrådet, med stöd av Netnod, får uppdrag att tillhandahålla Särimnerlösningen till aktörer, i en enklare förvaltningsorganisation. På sikt kan det därefter skapas en gemensam förvaltningsorganisation där för varje samhällsviktig tjänst ansvarig myndighet själva tar större ansvar för tjänstens funktionalitet i en beställarroll.

SUNET vill rikta ett stort tack till Netnod, för mycket gott samarbete i detta projekt och framtagandet av denna slutrapport.

Stockholm 2018-12-07

Maria Häll
Avdelningschef
Sunet och anknutna tjänster

Börje Josefsson
Biträdande avd. chef och operativ chef.

Innehållsförteckning

1. Inledning

1.1. Bakgrund

Post- och telestyrelsen (PTS) har gett i uppdrag till Vetenskapsrådet/SUNET att i ett lärande pilotprojekt, projekt Särimner, undersöka hur samhällsviktiga webbplatser kan nås i krissituationer. Bakgrunden är att det bl.a. vid olika totalförsvarsövningar (TELÖ) presenterades scenarier som krävde att det skulle gå att kommunicera inom en partitionerad del av Sverige. Här visade det sig att det inte gick att genomföra vissa övningar, utifrån IT-infrastrukturens nuvarande konstruktion där fiber och kommunikation inte möts. Detta är en fråga som lyfts i flera infrastrukturforum tidigare, där flera operatörer påpekade att för att övningarna skulle bli mer korrekta samt om tjänster skulle bli mer robusta måste moderna metoder och aktuella situationer användas. Beskrivningen av hur det såg ut i Sverige för att kunna genomföra övningarna stämde inte med det faktiska tillståndet ("kartan skiljer från verkligheten").

Till saken hör också att antalet överbelastningsattacker ökat markant i Sverige de senaste åren, mot såväl offentliga aktörer som företag. Under våren 2016 skedde exempelvis. ett antal attacker mot den operatör som de stora dags- och kvällstidningarna nyttjade. Attackerna medförde att medborgare inte kunde nå informationen på dessa webbsidor, som låg nere under cirka 24 timmar. Det visade sig då att de miljöer som mediehusen nyttjade inte var tillräckligt robusta. Dessa diskussioner intensifierades under 2017, när liknande attacker även riktades mot offentliga myndigheter (t.ex. Trafikverket, Riksdagsförvaltningen och ett flertal universitet).

För att genomföra uppdraget har SUNET anlitat Netnod, som är en leverantör av bl.a. tid, frekvens, DNS och knutpunkter i den svenska delen av Internet. Netnod har i sin tur haft stöd av Governo AB för processledning samt framtagande av föreliggande slutrapport och Assured AB för viss utredning av kryptografiska lösningar.

1.2. Syfte och mål med projektet

Det övergripande syftet är att säkerställa att medborgare och andra aktörer kan nå samhällsviktig information i kris.

Målet med projektet är att ta fram och utvärdera en pilotlösning som syftar till att samhällsviktig information ska kunna nås i kriser.

1.3. Avgränsningar

Projektet har inte haft som syfte att undersöka hur IT-infrastrukturen i sig kan göras mer robust och redundant, samtidigt som detta självfallet är avgörande för om medborgare kan nå informationen i olika sorters kriser. Vi har dock valt att i några avsnitt i rapportens analys och slutsatser även belysa denna fråga då den är central för fortsatt robusthetsarbete på nationell nivå.

1.4. Viktiga frågeställningar och begrepp

För att genomföra uppdraget har ett antal viktiga frågeställningar identifierats:

- Vilka problem finns i den svenska internetinfrastrukturen som synliggörs i samband med kriser?
- Vilken samhällsviktig information är relevant i krissituationer och hur hanteras denna idag?
- Hur skulle en lösning kunna se ut som säkerställer åtkomst till samhällsviktig information i kris?
- Vilka konsekvenser skulle en sådan lösning få vid ett eventuellt införande på nationell nivå, inkl. kostnadsaspekter och förvaltningsmodell?
- Vilka andra förslag finns för att kunna stärka den svenska infrastrukturens robusthet och redundans i kris?
- Då pilotprojektet handlar om att bygga och löpande utvärdera tekniska lösningar används också en rad olika tekniska termer och begrepp. Dessa återfinns i bilaga 1, Projektets begreppsordlista.
- Projektets namn, ”Särimner”, kommer från nordiska mytologin och grisen Särimner som utgjorde föda för de fallna krigarna i Valhall. Särimner åts upp varje kväll och återuppstod dagen efter.

1.5. Projektupplägg

Projektet har bedrivits som ett pilotprojekt, så kallat Proof of Concept (PoC), där ett antal lösningar tidigt definierats på principiell nivå och därefter byggts upp. Arbetet har bedrivits i en agil process, där reflektioner och iakttagelser under vägen har kunnat leda till förbättringar i den slutliga lösningen.

Projektorganisationen har bestått av en styrgrupp med representanter från Vetenskapsrådet/SUNET och Netnod, samt en projektgrupp med projektdeltagare från Vetenskapsrådet/SUNET, Netnod, och Governo AB. Därtill har personer i lokala organisationer på de platser som installation skett medverkat, samt Assured AB m.fl. engagerats då det funnits behov av detta.

- Utöver dessa organisationer har ett stort antal personer från relevanta myndigheter, operatörer och olika organisationer medverkat. De av dessa som dessutom intervjuats av Governo återfinns i bilaga 2, Intervjupersoner.

1.6. Sekretess enligt OSL samt skydd för affärshemligheter

I projektet har information med olika slags säkerhetsklassning förekommit. Det kan handla om information som bör beläggas med sekretess enligt Offentlighet och Sekretesslagen (SFS 2009:400) och då speciellt Säkerhetsskyddslagen (1996:627), men också information som är att betrakta som affärshemligheter, exempelvis hos operatörer. Projektet har i samband med slutrapportering valt att hantera detta så att den information som återges i denna huvudrapport kan inlämnas som allmän offentlig handling från Vetenskapsrådet till Post- och telestyrelsen.

1.7. Disposition

Projektets slutrapport är disponerad enligt följande:

- I kapitel 2 beskrivs problembilden, som också utgör bakgrunden till uppdraget.
- I kapitel 3 beskrivs projektet i alla dess delar inklusive konsekvenser utifrån olika scenarier.
- Kapitel 4 behandlar projektets huvudsakliga resultat samt andra viktiga lärdomar.
- Slutligen, i kapitel 5, ges förslag på vägen framåt för projektet samt för andra närliggande områden där insatser behöver ske.
- I bilagor återfinns en begreppsordlista (bilaga 1) och medverkande intervjupersoner (bilaga 2).

2. Vad är problemet?

För att förstå problematiken kring möjligheterna att nå samhällsviktig information vid kriser så är det av vikt att beskriva uppbyggnaden av den svenska Internet-infrastrukturen med dess olika aktörer, roller och affärsmodeller. Avslutningsvis beskrivs problembilden utifrån denna kontext.

2.1. Dagens svenska Internetinfrastruktur

I Sverige har vi idag flera utbyggda infrastrukturer som berörs vid kommunikation i kriser. Några som kan nämnas är:

- Det publika Internet tillhandahålls av internetoperatörerna till medborgare, företag, offentlig sektor samt olika organisationer. Olika delar av detta tillhandahålls av olika aktörer, inklusive stadsnät och liknande aktörer där en kommun eller en lokal förening (byalag) valt att bygga ett nät.
- Rakel, som är det nationella ”Blåljusnätet” för ett antal myndigheter med samhällsviktiga uppdrag såsom polis, brandkår etc. Detta nät tillhandahålls av MSB.
- Swedish Government Secure Intranet (SGSI) som erbjuder möjlighet för myndigheter i Sverige att kommunicera säkert med EU S-TESTA[1]. Detta nät tillhandahålls av MSB.
- Försvarsmaktens IP-nät (FMIP) som byggts som ett landsomfattande nät baserat på IP-protokollet med krypterade förbindelser och som är fysiskt avskilt från resten av Internet utom vid ett fåtal punkter, som är skyddade med särskilda mekanismer.

Dessa olika nät delar ofta vissa komponenter, som t.ex. elförsörjning, fiber och annan transmission och likaså potentiellt komponenter högre upp i värdekedjan såsom informationshanteringssystem och gemensamma personalresurser.

I denna rapport kommer vi fokusera på det publika Internet, givet att det är detta som används av slutanvändaren (och andra aktörer i dialog med slutanvändaren) i kris.

Här nedan beskrivs de olika lagren i infrastrukturen som behövs för att slutanvändaren ska kunna nyttja olika tjänster.

[1] EU S-TESTA är EU:s privata, IP-baserade nätverk.

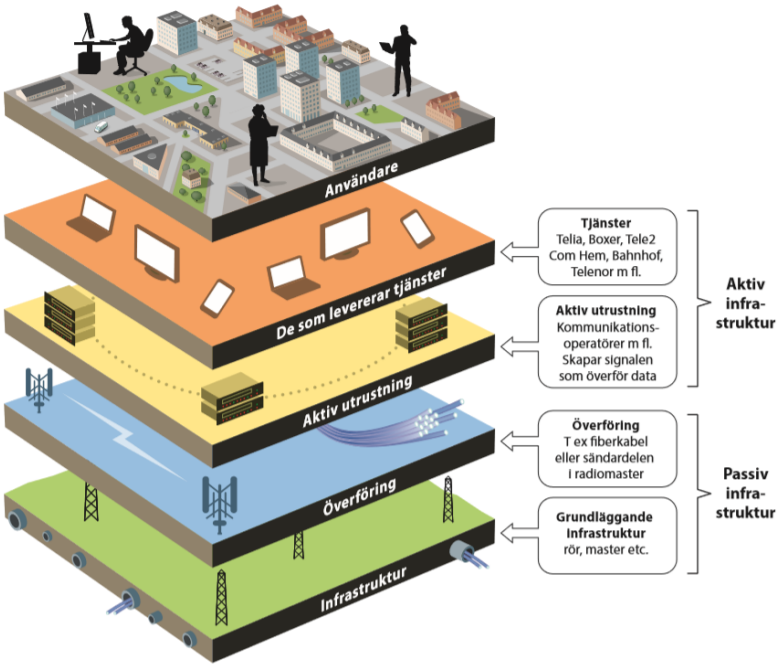

Bild 1: Infrastrukturens lager

På lägsta nivån återfinns den passiva infrastrukturen i form av master och rör som byggs, eller kan hyras, av operatörer. Operatörer kan också få tillträde till exempelvis nodhus genom att bygga, köpa eller hyra plats, för att kunna installera egen utrustning.

På nästa nivå, vilken också är passiv, återfinns själva fiberkabeln samt annan vidhängande utrustning (t.ex. kopplingspaneler). Här kan operatörer använda ledig svartfiber genom att hyra den eller bygga egen.

Den tredje nivån innehåller sådan aktiv utrustning som genererar signaler i nätet (bitström). Här återfinns t.ex. kommunikationsoperatörer och internetleverantörer (vilket i det fall båda används är två nivåer). Aktörerna i denna nivå är allt ifrån små kommunalt ägda nätbolag till stora landstäckande operatörer.

På den fjärde nivån återfinns tjänsteleverantörerna, som tillhandahåller internet till slutkunden. I vissa fall levereras även andra tjänster, som TV och telefoni, på denna nivå.

Det finns operatörer och bolag som är aktiva i samtliga fyra identifierbara lager och dom som är aktiva i bara en.

På den översta, femte, nivån återfinns slutanvändare som använder internet för att kommunicera. Här finns såväl privatpersoner och företag, men även leverantörer av tjänster över Internet som Spotify, Google och Facebook. Konsument och leverantör bör alltså anses vara på samma lager i värdekedjan.

Olika delar av Internet kopplas samman där det kan ske genom s.k. trafikutbyte. För att trafikutbyte ska kunna ske måste det först och främst finnas konnektivitet mellan de parter som utbyter trafik. Dessutom kan trafiken antingen vara direkt mellan parterna, gå via en s.k. knutpunkt, eller IX, eller lämnas över till annan operatör för vidarebefordran, så kallad “transit”. Trafiken går normalt via

närmaste plats där trafikutbyte sker utifrån var användaren nätverkstopologiskt (vilket kanske inte är samma som geografiskt) befinner sig.

För att Internet ska kunna nyttjas optimalt finns överenskommelser om hur samtrafik eller trafikutbyte ska ske. På Internet kallas detta peering, men en operatör kan också vara kund till en annan operatör (precis som en konsument är kund till en operatör). I detta fallet kallas trafikutbytet för transit.

Operatörerna använder sig ofta av en metod som kallas ”*hot potato routing*”, dvs. att de vill bli av med trafiken snarast möjligt för att inte belasta sitt eget nät.

2.2. Aktörer och roller i dagens infrastruktur

2.2.1. Leverantörer, affärsmodeller och investeringsvilja

För att fullt ut förstå dagens internetinfrastruktur är det också av vikt att förstå de olika aktörernas roller, ansvar och affärsmodeller.

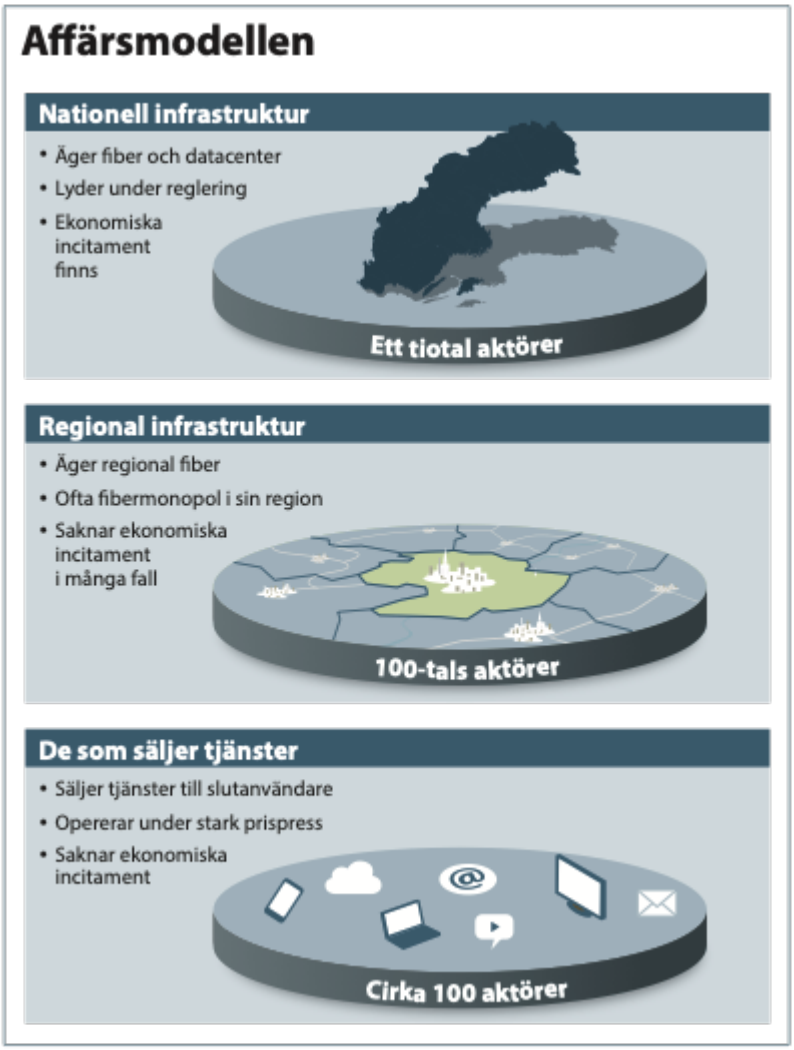

Bild 2: Affärsmodellen

Sammanfattningsvis kan de olika aktörerna delas in i tre grupper, där vissa aktörer förekommer i flera grupper beroende på roll:

- Ägare av den fysiska infrastrukturen (exv. nationellt fiber/stomnät och datacenter). Här finns enbart ett fåtal aktörer som samtliga förekommer på nationell nivå. Här finns typiskt en investeringsvilja hos aktörerna, eftersom de också har kunder som är beredda att betala för god tillgänglighet och driftsäkerhet. PTS har också bedömt att grossistmarknaden för svartfiber är nationell, varför denna kategori är speciell tillsynsmässigt.
- Ägare av regional infrastruktur, såsom kommuner/kommunala bolag/stadsnät. Här finns historiskt sett vissa teknikval gjorda, som försvårar kommunikation i händelse av kris. Merparten av lösningarna medför att trafiken tvingas gå via centraliserade serverhallar som företrädesvis är centralt placerade, t.ex. i Stockholm. Kunderna till dessa aktörer är inte heller villiga att betala för att klara den stress som en extraordinär händelse skapar.
- Tjänsteleverantörerna, som utgör ett stort antal. Dessa har tjänster till slutanvändare som affär. Betalningsviljan hos dessa slutkunder är generellt sett att betrakta som låg, vilket i sin tur påverkar leverantörernas investeringsvilja.

En viktig aspekt handlar således om affärsmodellen i dagens svenska Internet. Slutkunderna i form av konsumenter och företag har historiskt sett haft en låg betalningsvilja för en god internetuppkoppling. Detta har flera orsaker, bl.a. konkurrensen på marknaden, men också att många inte fullt ut är medvetna om robustheten i vald lösning (förrän då krissituationer uppstått). Sammantaget har detta lett till en situation med centraliserade nät, där operatörerna konkurrerar med låga marginaler mot slutkund vilket också leder till bristande investeringsvilja för sådant som kan beskrivas som samhällsviktiga uppdrag. Operatörernas vilja att rusta för extrema krislägen är också att betrakta som låg eftersom konsekvenserna om krisen inträffar inte ses som alltför kostsamma av operatörerna.

2.2.2. Möjligheter att påverka investeringsviljan

Det finns flera möjligheter att påverka investeringsviljan, där ett verktyg handlar om att ställa krav genom reglering.

Bild 3: Nätsäkerhetspyramiden

PTS använder sig av den s.k. Nätsäkerhetspyramiden som visar att viss grundläggande tålighet mot stress hanteras i kombination med kund- och författningskrav. Högre nivå kan fås genom att kund på egen hand t.ex. upphandlar redundanta lösningar. Men högsta nivå, som samhället kan ha intresse av, kan enbart uppnås genom extraordinära åtgärder som både koordineras och finansieras av staten.

PTS ställer idag krav på driftsäkerhet, huvudsakligen genom driftsäkerhetsföreskrifterna (PTSFS 2015:2). Föreskrifterna berör ett antal områden, exempelvis generella krav på driftsäkerhet, dokumentation, risk- och konsekvensanalys, incidenthantering, kontinuitetsplanering m.m.

Det finns även vissa grundläggande krav i PTS föreskrifter om fredstida planering för totalförsvarets behov av telekommunikation, som rör operatörernas fredstida förberedelser. Denna är för närvarande föremål för översyn.

Dessutom finns det möjlighet att förelägga operatörer att utföra åtgärder i enlighet med lagen om elektronisk kommunikation (2013:389).

PTS kan också bekosta robusthetshöjande åtgärder som går utöver vad som föreskrivs i författningar. På dessa åtgärder kan då ställas krav som gäller för den specifika åtgärden och vad som är kommersiellt motiverat.

2.3. Synen på kommunikation i kris – hos olika aktörer

I projektet har ett antal aktörer med samhällsuppdrag intervjuats, dels för att ge sin syn på projektet, dels för att beskriva hur de själva arbetar för att säkerställa att samhällsviktig information finns tillgänglig.

2.3.1. Offentliga aktörer med samhällsuppgifter

Post- och Telestyrelsen (PTS) är tillsynsmyndighet inom IT- och telekomområdet, med särskilt ansvar för krisberedskap och höjd beredskap. En del av ansvaret för nätsäkerhet handlar om att öka robustheten i nätet. Detta gör man bl.a. att utöva tillsyn och därigenom tillse att operatörer gör vad de ska enligt gällande avtal och lagstiftning. Enligt PTS föreskrifter ställs krav på operatörer kring robusthet och redundans, såväl generella krav som specifika krav utifrån olika slags operatörer. För exempelvis kommunikationsoperatörer som har aktiva anslutningar (kategori 2) finns krav på att klassificera sina tillgångar. För klass A och B (dvs. många aktiva anslutningar) ska operatörerna kunna säkerställa att tillgångarna i dessa klasser, om de upphör att fungera, inte orsakar störning eller avbrott i en kommunikationstjänst.

PTS bedriver också projekt för att öka kunskapen om nätsäkerhet. I detta projekt är PTS även mottagare av resultatet, samt finansiär av projektet som sådant. Som beskrivits ovan kan PTS också ställa krav på operatörerna på ett antal olika sätt.

Myndigheten för samhällsskydd och beredskap (MSB) har i uppgift att utveckla samhällets förmåga att förebygga och hantera olyckor och kriser. I detta ligger bl.a. att tillhandahålla och kvalitetssäkra informationen i tjänsten krisinformation.se. Informationen kommer vanligen från andra aktörer, exempelvis Polismyndigheten, då myndigheten själv inte äger informationen. Här är grunden för att kunna publicera information den informationssamordning som sker mellan olika parter med samhällsviktigt ansvar.

För att säkra att sidan alltid är tillgänglig har myndigheten upphandlat en lösning som innebär att en CDN-tjänst används för att kunna hantera distribution till olika delar av Sverige. Drift av tjänsten ses för närvarande över.

Vi har också intervjuat samhällsaktörer som bedriver såväl förebyggande som aktivt arbete i kriser: *Stockholms Läns Landsting* är ett av Sveriges största landsting. Krisarbetet styrs av krisberedskapsplan samt regional katastrofmedicinsk beredskapsplan. I en kris sker kommunikation till invånare i första hand via 1177.se, dvs. sjukvårdsrådgivningen som bedrivs av Inera, men kommunikation sker även via andra kanaler som t.ex. sll.se och media. Landstinget har formulerat krav på robusthet och redundans i det egna transportnätet, SLLnet. Till SLLnet ansluts vårdgivarnas lokala nät. I krissituationer samverkar man med andra, bl.a. i regional samverkan (Samverkan Stockholmsregionen).

Stockholms stads infrastruktur består av fibernätet som levereras av Stokab, samt kommunikationsnätet som levereras av St Erik Kommunikation. I centrala upphandlingar har krav ställts på internetleverantören gällande exempelvis robusthet och redundans. Vid kris sker kommunikation främst via stadens webbplats. Sociala medier används främst för att driva trafik till informationen på webbplatsen men också som förstahandsval om webbplatsen drabbas av tekniska problem. Krisinformation.se hämtar också information från staden, i de situationer där kommunen har ett ansvar i krisen.

2.3.2. Media – dagspress och TV

Tidningsutgivarna (TU) är branschorganisation för svensk dagspress, och bevakar trender och utveckling i sin bransch. Flera av dessa media drabbades hårt av den stora DDOS-attacken i mars 2016. TU beskriver att utvecklingen går mot en allt tuffare miljö – både vad gäller förekomsten av fler och allvarligare attacker, men också i form av "*fake news*" och hot mot journalister. TU har tillsammans med sina medlemmar adresserat frågan på flera sätt. Det finns bl.a. samarbeten mellan IT-avdelningarna på mediehusen – detta trots man konkurrerar om nyhetsförmedlingen i kriser.

Vid en kris är det traditionell media man vänder sig till i första hand. Trafiken har studerats i samband med flera kriser, nu senast kring sommarens skogsbränder. I den undersökning som SVT lät genomföra med stöd av Novus kunde konstateras att ”vanlig tv” och ”vanlig radio” var tillsammans med ”tidning i mobilen” de huvudsakliga källorna till information.

Sveriges television (SVT) ser sin nyhetsförmedling som samhällsviktig information. I broadcasting-nätet kravställer SVT robusthet och redundans gentemot Teracom. I sändningstillståndet finns idag inga specifika krav på detta, men SVT menar att detta skulle kunna förekomma i framtiden.

När det gäller distribution via Internet har SVT direkt peering mot många av leverantörerna. Man har även köpt en cachelösning som ska kunna garantera visst innehåll även i kris.

Man har också möjlighet att skala ner sajterna, dvs minska komplexiteten på innehållet, för SVT och SVT Play. Dock vill man helst kunna visa både text och rörlig bild. En viktig fråga framåt handlar om hur man ska hantera det faktum att allt mer av nyhetsförmedlingen sker genom Play-tjänsterna.

2.4. Utmaningar i dagens infrastruktur

Den stora utmaningen i Sverige är att vi är ett geografiskt utsträckt land med långa avstånd. Detta gör att en bredbandsutbyggnad som ska nå alla blir kostsam, och än mer om en parallell infrastruktur skulle etableras. Det nationella internet är idag byggt med fokus på serverplacering i Stockholm och med hög grad av centralisering, vilket gör att merparten av trafiken går denna väg. Ur ett säkerhetsperspektiv skapas därmed en stor sårbarhet.

På många ställen kan trafiken enbart gå en väg, vilket försvårar en alternativ routing i krissituationer. Delar av Sverige riskerar därmed att skäras av i ett krisläge.

Mycket pekar på att det idag inte går att garantera att viktiga samhällstjänster har fortsatt tillgänglighet och funktionalitet vid händelse av kris eller hot. Det finns idag också en stor sårbarhet där dataintrång och attacker med syfte att slå ut viktiga funktioner i samhället både är aktuella och möjliga.

Problembilden gör gällande att det finns ett stort och akut behov av en infrastruktur som uppfyller både försvarets och blåljusmyndigheternas krav samt kan säkerställa att slutanvändarens behov kan tillgodoses, vid en krissituation. Utifrån hur det svenska nätet är uppbyggt kan ansvariga myndigheter inte garantera detta idag. Utan ett redundant och diversifierat fibernät är det i framtiden inte möjligt att klara av krav på säkerhet vid en krissituation.

Denna problembild är inte ny utan har adresserats i flera utredningar, exempelvis i utredningen Generell vägledning till framtidssäker IT-infrastruktur från år 2000 där den dåvarande IT-kommissionen uppmärksammade en mängd faktorer de redan då såg som orosmoln för fortsatt utveckling av IT-infrastrukturen. En mängd åtgärder presenterades i utredningen, som nödvändiga att vidta för att säkerställa en framtidssäker IT-infrastruktur.

2.5. Andra länder

De utmaningar som Sverige möter är inte unika – även andra länder och många företag arbetar för att säkra åtkomst till samhällsviktig information under kriser. Det unika i Sveriges situation är just geografin och det sätt som vi successivt valt att bygga ut IT-infrastrukturen på.

I Tjeckien skedde 2013 en större överbelastningsattack, vilket lade grunden till Projekt Fenix. Syftet med projektet var att skapa redundanta anslutningar som bygger på att trafikutbyte ska vara möjligt på många platser i händelse av kris. Centralt i projektet var att ISP:erna lovat varandra att leva upp till vissa villkor, för att gemensamt möjliggöra tillgång till internet.

3. Beskrivning av projekt Särimner

Som beskrivits i inledningen har arbetet i projektets bedrivits agilt, vilket lett till att viktiga slutsatser kunnat införlivas i lösningen under arbetets gång. Nedan beskrivs projektet i form av den Proof of Concept (PoC) samt olika use cases (användningsfall) som lösningen testats mot. Avslutningsvis finns ett resonemang om konsekvenser och kostnadsaspekter av en ev. utrullning av Särimners resultat.

3.1. Beskrivning av projektets olika delar

Som beskrivits i kapitel 2 är stora delar av Internet centraliserat till Stockholm. Många aktörers servrar finns placerade här, och informationen behöver vandra viss väg i nätet för att nå sin mottagare i andra delar av landet. Dessutom är det s.k. kontrollplanet centraliserat till en enstaka plats och möjligen en alternativ reservplats. Med kontrollplan menar vi de funktioner som krävs för att nätet i sig skall fungera och inte bara driftledningscentral (NOC). Ett exempel på sådan funktion är den som tillser utdelning av IP-adresser till slutanvändare. Med jämna mellanrum, ungefär dagligen, krävs det för att slutanvändaren ska kunna kommunicera att denna funktion fungerar.

Dessa centrala funktioner är för de flesta operatörer placerad geografiskt i Stockholm. Detta medför att nätlösningen (och därmed informationen) blir sårbar för attacker av olika slag. Sammantaget kan två möjliga lösningar ses på detta problem:

- Förstärkning av kommunikationsinfrastrukturen och dess redundans så att information kan nå mottagaren på flera vägar.
- Etablera nya sätt att distribuera information till i krisen isolerade delar av Sverige som medför att mottagaren ändå kan nå informationen (alternativt se den senaste kopian).

Gällande kommunikationsinfrastrukturen krävs samordnade åtgärder från staten då den centraliserade driften gör att det i praktiken inte går att kommunicera inom en partitionerad (isolerad) del. Därför ger projektet rekommendationer gällande sådana åtgärder vilket inkluderar skapande av mångfaldigt fler mötesplatser för speciellt fiber.

För distribution av information, den s.k. Särimner-lösningen, så är målet att säkra att samhällskritisk information alltid finns tillgänglig på visst ställe (i projektets testfall en fiktiv sida såsom krisinformation.se), dvs. även vid krissituationer. Lösningen bygger på att flera noder levererar samma innehåll till besökare, detta för att alla slutanvändare ska få så kort väg som möjligt för att hämta innehållet.

Lösningen är uppbyggd av ett antal noder som ska kunna fungera autonomt, så att det alltid finns en nod som svarar, även vid stora mängder anrop. Noderna agerar även proxy till DNS (Domain Name System – dvs. det system som krävs för hopkoppling av domännamn med IP-adresser) och gör därmed att noden fortsätter att leverera trafik trots att den tappat kontakten med den riktiga servern. I en kris där originalkällan inte finns så ska det finnas en cachad (sparad) version av senaste informationen (med tidsangivelse). Detta kallas för scraping, dvs. en slags kopieringsmetod för att extrahera data från en webbsida.

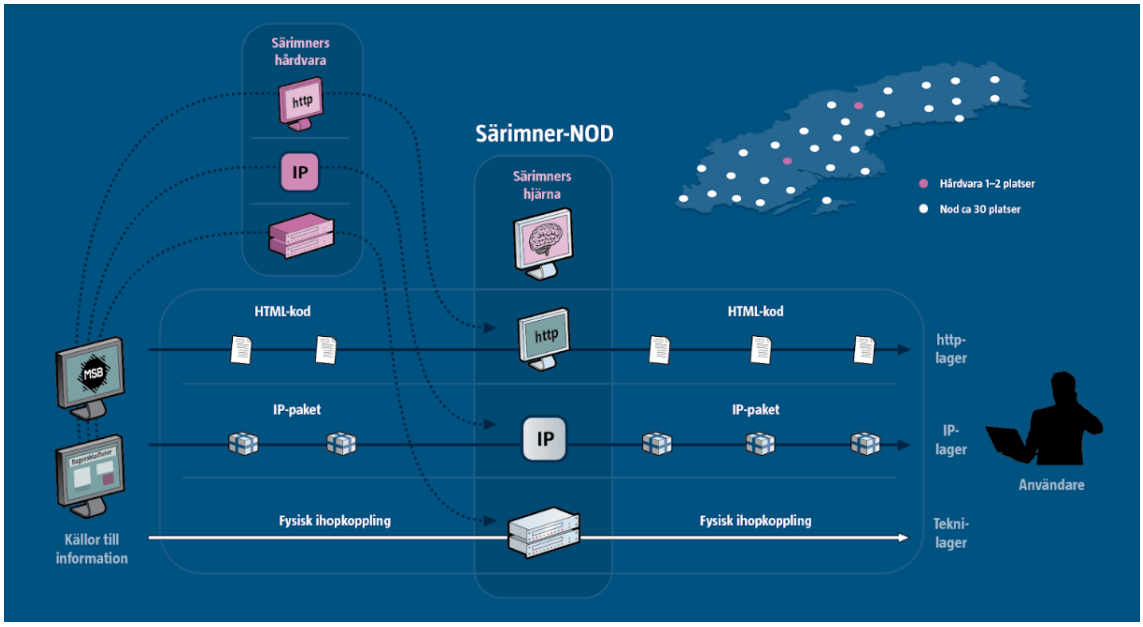

Bild 4: Särimner-lösningen

Noderna har i denna PoC placerats på platser som uppfyller höga krav på driftssäkerhet, fysiskt skydd, samt har bra nätverkskonnektivitet.

Sammantaget har tre Särimner-noder installerats och placerats ut på olika ställen i Sverige, och en utanför landet.

I projektet har SMHI medverkat för att tillhandahålla en potentiell sida med information (i testmiljö), https://www-tst.smhi.se/. SMHI har bl.a. viktiga väderdata som allmänhet, företag och myndigheter behöver få tillgång till vid vädermässiga kriser. Lärdomarna från arbetet med SMHI är att det varit tämligen enkelt och snabbt att ansluta en aktör till lösningen. Det enda som krävs är konfiguration av aktuell sida i Särimners provisioneringssystem samt omstyrning av DNS för tjänsten. Liknande tester planeras under 2019 med ytterligare några aktörer.

Utöver de fysiska placeringarna har projektet även studerat möjligheterna att hänvisa anrop vidare till servrar placerade utanför Sveriges gränser. Detta innebär att potentiella överbelastningsattacker får hanteras av de som tillhandahåller dessa servrar. Målet med dessa servrar utanför Sverige är primärt inte att ge korrekta svar utan att just attrahera trafik och därmed slippa denna vid servrar inom Sverige.

I projektet har också ingått att analysera hur certifikat/nycklar behöver hanteras för att åstadkomma tillit sinsemellan (TLS – *Transport Layer Security*). Varje nod måste ha rätt nyckel till respektive sajt för att få leverera informationen. I detta fall innebär det att den fiktiva krisinformation.se behöver lämna ifrån sig sitt certifikat/sin privata nyckel till Särimner-noder för att informationen ska kunna visas på ett säkert sätt (dvs. krypterat) för slutanvändaren. På detta sätt kan man garantera att informationen inte är att betrakta som falsk.

Det har visat sig att kostnaden för en komplett härdning av en nod är hög samtidigt som hanteringen i sig är synnerligen komplicerad. I projektet hittades därför en balans mellan absolut säker nod och säkerhet i inplacering, vilket resulterade i slutsatsen att noderna i sig håller en lägre säkerhet än ursprungligen planerat, och istället ställs högre krav på inplaceringen. Krav som fortfarande anses

rimliga. Lösningen har utformats och testats mot ett antal olika scenarier, för att iterativt generera kunskap som förbättrar lösningen.

En viktig lärdom handlar om de fysiska platser där såväl fiber som kommunikation möts (sk mötesplatser) och där noden kan placeras är idag ytterst få till antalet. Dock handlar det vanligen om korta avstånd som behöver överbryggas för dessa typer av infrastruktur ska kunna mötas även om det på vissa orter är synnerligen komplicerat att skapa denna typ av mötesplatser. Problemet är således inte att man inte dragit fiber till och på vissa orter, utan att olika aktörers fiber slutar (termineras) på olika ställen. Detta gör att platserna där Särimner kan placeras rent fysiskt är få till antalet, och att kabeldragning skulle behöva ske på de platser där en fullskalig Särimner-lösning skulle behöva finnas.

3.2. Möjliga problem vid kriser – utifrån scenarier

Det finns ett antal olika scenarier som projektet analyserat, där den eventuella eller inträffade krisen skiljer sig åt och där Särimner kan ha olika roller.
De fyra scenarierna är följande:

- Händelse inträffar som leder till stor uppmärksamhet från medborgare
- Händelse som innebär akut hotbild för medborgare på viss plats
- Händelse som innebär en överbelastningsattack på vissa webbsidor av företag, organisation eller annat land
- Händelse som orsakar fysiskt brott på infrastrukturen i form av naturkatastrof, större olycka eller krig

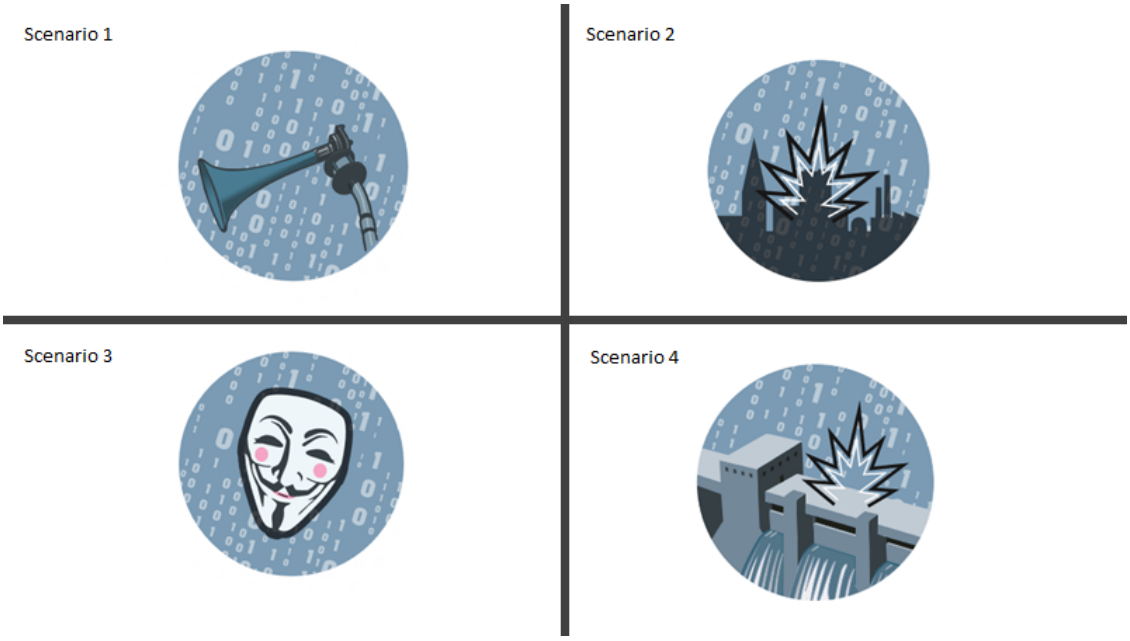

Bild 5: Fyra scenarier

3.2.1. Händelse inträffar som leder till stor uppmärksamhet från medborgare

En situation som studerats är vad som händer då en händelse inträffar som leder till stor uppmärksamhet och därmed mycket trafik från medborgare. Exempel på sådana händelser är om

”Hesa Fredrik” (VMA – viktigt meddelande till allmänheten) ljuder av misstag, en mindre skogsbrand uppstår eller om det skulle flyga militärplan på övning över visst område.

Det som händer är då att många medborgare samtidigt söker information. Troligen vänder sig merparten av dessa till kommersiella aktörer, som dags- och kvällstidningar samt sociala media såsom Twitter. Några kan väntas besöka krisinformation.se eller andra myndigheters sidor.

Särimners påverkan: I denna situation, som är att anse som en överbelastning orsakad av medborgarna själva, kan Särimner se till att informationen på vissa samhällsviktiga webbsidor alltid går att nå.

3.2.2. Händelse som innebär akut hotbild för medborgare på viss plats

Det finns också en situation som handlar om en lokal, akut hotbild för medborgare på viss plats. Här kan det exempelvis vara fråga om en terrorattack i likhet med den som ägde rum i Stockholm den 7 april 2017, eller en större olycka.

Även här söker många medborgare information på samma gång. De vill veta att närstående är utom fara, samt hela tiden hålla sig uppdaterade om utvecklingen. Även här är kvällstidningar, dagstidningar och sociala media de primära kanalerna, samtidigt som ev. förekomst av “*fake news*” kan leda till att myndighetssidor besöks. Här kan dagspress och offentliga aktörer ställa om till mer avskalade sajter, där mindre information laddas.

Särimners påverkan: I denna situation blir nätet snabbt överbelastat – många vill ha information som kontinuerligt uppdateras. Särimner kan även lösa denna situation, genom sin funktion att informationen på samhällsviktiga webbsidor speglas på flera ställen. Viktigt här är att det finns en funktion för att visa när informationen uppdaterades senast (tidsangivelse).

3.2.3. Händelse som innebär en överbelastningsattack på vissa webbsidor av företag, organisation eller annat land

Här handlar det om en riktad attack mot vissa webbsidor för att undvika att information når medborgare och/eller visa på svagheter i den svenska delen av Internet. Det kan handla om företag eller organisationer som utför sådana attacker, men också IT-krigföring av annat land för att försvaga Sverige genom att information inte kan nås eller att falsk information publiceras.

Särimners påverkan: Till skillnad från de två tidigare situationerna som orsakats av medborgarnas eget informationsbehov, så är det nu en tredje part vars beteende orsakar överbelastningen. Den här typen av attacker hanteras maskinellt, vilket gör att de kan bli mycket kraftfulla. Givet att Särimner dimensionerats för att klara ett tryck om minst 1 miljon uppslagningar per sekund, så kan lösningen även bidra i detta fall. Speciellt eftersom trafiken dirigeras på sådant sätt att noder inom Sverige inte drabbas av höga trafikflöden från utlandet. Systemet är designat i grund och botten för att kunna motstå de största identifierade versionerna av dessa attacker.

3.2.4. Händelse som orsakar fysiskt brott på infrastrukturen i form av naturkatastrof, större olycka eller krig

Detta är den allvarligaste av de situationer som beskrivits – nu handlar det om att en vital del av IT-infrastrukturen inte fungerar, genom en fysisk påverkan. Det kan handla om större brand i tunnlar i

Stockholm, en naturkatastrof i form av vattenkraftsdamm som brister i Norrland eller intrång av annat land med bomber på kritiska punkter i IT-infrastrukturen.

Särimners påverkan: I denna situation kan Särimner hålla informationen igång en viss tid genom att visa innehåll som temporärt sparats i noden alternativt att via logik byta över till en så kallad nödsite, om innehållets källa upphör att svara på förfrågningar. I ett katastrofläge där man inte har tillgång till uppdaterad information från centrala tjänster så vill man kunna visa ett förutbestämt innehåll som guidar slutanvändaren utan att vilseleda med potentiellt sett inaktuell information.

Särimnernoden kommer att vara tillgänglig för alla slutanvändare inom räckhåll, vars Internetaccess inte har påverkats eller avbrutits av händelsen. Anledningen till att enbart temporär information som sparats i noden kan distribueras är det stora problem som beskrivits i kapitel 2 med den centralt byggda IT-infrastrukturen med fokus på Stockholm – landet ”delas av” och stora delar kan inte ta del av informationen. För att förebygga den situationen behövs således andra åtgärder, vilka beskrivs i rapportens sista kapitel.

De slutanvändare som är kunder hos en operatör som nyttjar en redan sammanbyggd mötesplats kan dock fortsatt nå informationen.

3.3. Sammanfattning och slutsatser

Sammanfattningsvis kan Särimner lösa vissa problem när det gäller att säkra att information kan publiceras vid kriser som på något sätt leder till eller består av en överbelastningsattack. Däremot kan lösningen enbart ha en begränsad roll när det gäller fysiska avbrott på vitala delar av IT-infrastrukturen, pga. operatörernas centralisering av såväl nätdrift och hantering av tjänster.

4. Resultat och lärdomar

I detta kapitel redogörs för de huvudsakliga resultaten av projekt Särimner. Vidare beskrivs kostnadsaspekter och möjligt fortsatt arbete inom området, inkl. potentiell förvaltning av den framtagna lösningen.

4.1. Projektets resultat

Genom implementeringen av Särimner-lösningen har projektet kunnat visa att lösningen fungerar för att spegla information i scenario 1-3 i ovanstående kapitel. Noderna fungerar autonomt och fortsätter att leverera trafik trots att de tappat kontakten med den riktiga servern. Däremot fungerar inte lösningen fullt ut i scenario 4. Trots att Särimnernoden i sig fungerar så föreligger stor risk att slutanvändare inte kommer att kunna erhålla fullt fungerande Internetaccess som möjliggör tillgång till den fungerande noden. Anledningen till detta beskrivs i avsnitt 2.4.

Projektet har utfört ett antal tester som fullt ut kontrollerat funktionaliteten av Särimnernoder i ett flertal fall, specifikt:

- att slutanvändare automatiskt skickas till en annan Särimnernod om den närmaste blir utslagen.
- att lagrat innehåll visas om ursprungskällan blir otillgänglig.
- möjlighet att byta över till ett annat innehåll som visas för slutanvändaren vid krissituationer. Detta kan ske manuellt eller per automatik på tidsstyrning.

Lösningen som hänvisar anrop vidare till servrar placerade utanför Sveriges gränser har också visat sig fungera under belastning vid genomförda stresstester.

Som tidigare angivits så löser inte Särimner grundproblematiken den centraliserat byggda infrastrukturen. Lösningen fungerar under en viss tid för att tillhandahålla aktuell information, men möjligheten till robust kommunikation saknas då det inte finns alternativa transmissionsvägar genom landet. Det optimala vore om lokala mötesplatser kunde skapas för trafik i visst geografiskt område. Operatörernas trafik skulle då passera mötesplatsen, och trafik till samhällsviktiga tjänster skulle relativt enkelt kunna termineras vid noden. Olika operatörer skulle därigenom få möjlighet att transportera trafik till centrala delar av landet via flera fiberstråk. Detta förutsätter dock att mötesplatser existerar både gällande fysiskt lager (fiber) och IP-lager i värdekedjan på samma geografiska plats, vilket generellt inte är fallet idag.

Vi ser dessutom utifrån den analys som gjorts av befintlig reglering och intervjuernas resultat att detta inte kommer hända av sig själv. Därtill saknas investeringsviljan, eftersom slutanvändare inte efterfrågar och inte är villiga att betala för ökad robusthet till samma höga nivå som samhället kan anses kräva.

Mer specifikt ser vi således både avsaknad av mötesplatser för fiber samt avsaknad av möjlighet att utbyta trafik lokalt på IP-nivån. Som ett gott exempel kan Sunets upphandling av robust fiberinfrastruktur i hela landet användas. Genom att delvis definiera om vad en *region* är utifrån ett infrastrukturperspektiv lyckades man få trippelredundant fiberinfrastruktur till en plats i varje region, dvs knappt 20-talet platser i Sverige. Detta projekt drar slutsatsen att detta är alldeles för få, om hela Sverige ska kunna täckas. För att uppnå robusthet så behöver mötesplatser för fiber etableras på betydligt fler platser inom rimliga avstånd ifrån varandra.

En målbild bör vara 3-5 mötesplatser per kommun (eller annat likvärdigt stort geografiskt område). Mindre närliggande kommuner kan gå samman och dela på dessa mötesplatser, men i glest befolkade områden så bör man ändå eftersträva att inte ha allt för glest mellan mötesplatserna. Alla tillhandahållare av samhällsviktiga tjänster måste på ett relativt enkelt sätt kunna få motsvarande redundans och robusthet, och därmed inte bara de som råkar ligga i närheten av regionens centralort.

Samordning av fiberinfrastruktur behandlas delvis i utredningen Statens bredbandsinfrastruktur som resurs (SOU 2016:1). Utredningen menar att staten kan samordna den infrastruktur för fiber som redan finns inom verk och statliga bolag på ett mycket mer effektivt sätt. Detta förutsätter bland annat mer samarbete mellan de myndigheter och statliga bolag som idag sitter på underutnyttjad fiberinfrastruktur exempelvis Trafikverket, Svenska kraftnät och Vattenfall. I förlängningen skulle detta även kunna inkludera annan offentlig sektor (såsom kommuner) och naturligtvis även privat sektor. Om förslagen i utredningen genomförs skulle situationen bli bättre även om detta projekt anser att uppdraget måste vara ännu mer specifikt riktat till respektive organisation. Dessutom måste även lokala aktörer och privat sektor som innehar fiber och kanalisation inkluderas så att koordinering av etablering av kanalisation och fibernät kan ske. Därvid krävs samordning, en samordning som skulle kunna tolkas ingår i det uppdrag som lagts och åtagits av t.ex. länsstyrelser, kommuner, Bredbandsforum och Post- och Telestyrelsen.

Tyvärr har diskussionerna gällt *bredband* som ett mer allmänt och sammanfattande begrepp och inte specifikt fiber, kanalisation, master och annan passiv infrastruktur separat från aktiv utrustning, transmission och IP-nivån (se bild 1). Ett av många exempel på detta är PTS rapport *Kartläggning av hinder för utbyggnad av fast och mobilt bredband och förslag till hur processer kan effektiviseras* (PTS-ER-2018:13). Om målet är en stabil, robust och väl utbyggd fiberinfrastruktur, vilket är en förutsättning för robust elektronisk kommunikation, så behöver en kartläggning och utpekning ske av var mötesplatser behöver finnas, etablering av dessa samt undersökning av vad som krävs för att nätet ska byggas ihop. Efter dessa initiativ kan en robust grossistprodukt i form av svartfiber bli tillgänglig överallt i landet på ett helt annat sätt än idag. Alternativet är att varje aktör genomför parallell förläggning av t.ex. fiber, vilket för såväl för samhället som den enskilda aktören är ineffektivt och kostnadskrävande.

Gällande *IP-nivån* har som tidigare nämnts var och en av de större operatörerna ett eget nät som täcker hela Sverige, och i vissa fall ännu större geografiskt område. Varje förändring av routing inom detta nät, såsom utbyte av trafik vid en mötesplats för enbart vissa destinationer, skapar en ökad risk för instabilitet av routing inom nätet. Därför har projekt Särimner i ett sent skede diskuterat med operatörer placering av Särimner-noder inom operatörens nät istället för att trafikutbyte mellan operatör och Särimnernod ska ske vid en mötesplats som en del i en framtida Särimner-lösning. Det trafikutbyte som trots allt blir möjligt vid en mötesplats kan ske på många olika sätt, exempelvis genom hyra/swap av svartfiber eller transmission, eller explicit trafikutbyte på IP-nivå, men är alltså oberoende av placering av Särimnernod vid mötesplatsen.
Det är därför två olika mål som projektet anser bör uppnås framöver, och som delvis är oberoende av varandra:

- Skapa mötesplatser där först och främst fiber möts, vilket är en förutsättning för trafikutbyte, oavsett på vilken nivå i värdekedjan detta trafikutbyte sker.
- Placera ut Särimner-noder vid mötesplatser eller i operatörernas egna nät, där framför allt det senare är viktigt och i brist på lokalt trafikutbyte det som ger bäst effekt.

Riktade kravställningar och investeringar måste därför göras för dessa två mål ska uppnås. Då återstår frågan om vem som bör finansiera ett sådant arbete, där vi ser två vägar. Antagligen krävs en kombination av båda dessa:

- Reglering, där PTS i egenskap av tillsynsmyndighet ställer krav på fiberägare och operatörer att etablera mötesplatser samt placera ut noder och därmed kunna garantera att samhällsviktig information kan nå slutanvändaren.
- Finansiering i form av att regeringen, via lämplig myndighet, ger medel för att både genomföra kartläggningen av mötesplatser men också för att bygga ut en lösning där mötesplatser etableras samt Särimner-noder placeras ut och driftsätts.

4.2. **Kostnadsaspekter**

För att implementera Särimner-lösningen i PoC-format har vissa investeringar krävts. Kostnaderna har framförallt handlat om investeringar i teknik, tekniskt stöd samt konsultstöd för projektledning.

För att etablera mötesplatser och därmed få till en lösning på de riktiga problemen, är behovet primärt investeringar i fiber och i vissa fall lokaler för fysisk placering av nod. Dessutom måste denna föregås av en projektering och samordning mellan inblandade parter, såsom ägare av fiber, lokaler och mark i närområdet.

Om vi istället enbart ser på informationsspridningen är frågan vilken omfattning en mer permanent lösning skulle kunna ha? Den optimala lösningen består givet dagens situation med begränsat antal mötesplatser cirka 30 noder som finns vid större knutpunkter och i operatörers nät. Utplaceringen ska ske i nära samarbete med operatörer vars slutanvändare ska komma åt noderna på ett säkert och robust sätt.

Ett mindre mellanalternativ vore cirka 10-15 noder som framförallt placeras på befintliga mötesplatser. Noder bör framförallt placeras på orter som nätverkstopologiskt ligger långt från Stockholm, exempelvis i Norrland, Västsverige eller på Gotland. För att dessa skall fungera optimalt måste dock översyn av kontrollplanet (se avsnitt 3.1) för nätet i sig ses över.

För Särimner-noder är investeringskostnader 100 000-150 000 SEK per nod (två servrar med kringutrustning) och produktionskostnaden el- och lokalhyra för denna utrustning. Dessutom en kostnad för drift och support för systemet som helhet, vilken beräknas till 5-10 MSEK/år i personalkostnader (drift, utveckling och kontakt med leverantör av de tjänster som använder systemet etc.), i princip oberoende av antal noder.

En mer exakt kalkyl bör utarbetas utifrån det vägval som görs.

Projektet har funnit att den initiala grundinvesteringen samt drift och förvaltning bör bekostas med centrala medel under de första åren för att på så sätt få en bra lösning på plats. Detta ger också indirekt ekonomiskt incitament till medverkan av aktörer som tillhandahåller samhällsviktig information. Därefter bör en kostnadsallokeringsmodell tillämpas för att fördela kostnaderna för årlig drift och förvaltning, och samtidigt få till ett marknadsmässigt styrmedel för att utöka respektive minska (och slutligen möjligtvis lägga ner) tjänstens omfattning.

4.3. Möjlig förvaltning

Särimner-lösningen har hittills drivits som ett projekt, där ett viktigt syfte har handlat om att testa och löpande utveckla lösningen för att därigenom generera ökad kunskap. Denna PoC kommer fortsätta under 2019 för att ytterligare samla erfarenhet och ge möjlighet till förfining av systemet. Skulle lösningen sedan övergå i permanent drift och förvaltning, i befintligt eller utvecklat tillstånd inklusive utbyggnad av mötesplatser, så behöver en förvaltningsorganisation identifieras.

Vår rekommendation är att SUNET/Netnod efter initial uppbyggnad fortsätter att tillhandahålla tjänsten gällande informationsspridning enligt Särimner-konceptet, på uppdrag av PTS. Ett annat sätt kan vara att Vetenskapsrådet/SUNET får detta som ett uppdrag från regeringen, direkt eller genom regleringsbrev, för att kunna tillhandahålla detta utanför Sunets nuvarande mandat.

Vi förordar detta dels utifrån att det därmed snabbt blir möjligt att ansluta flera aktörer, dels att Netnod redan idag har möjlighet till nationell täckning, speciellt i samarbete med SUNET. Netnod kan också i detta avseende inta en neutral roll i förhållande till myndigheter och operatörer, samt utifrån sin organisationsform (ägs av en icke vinstdrivande stiftelse) och möjlighet att hantera skyddsvärd information, och Vetenskapsrådet/SUNET som statlig myndighet kan agera neutralt i förhållande till operatörerna.

I drift- och förvaltningsansvaret ligger också flera olika uppdrag som behöver fördelas, exempelvis:

- Utplacering och drift av noder
- Förvaltning av mjukvara för noder
- Anslutningar av nya samhällsviktiga tjänster
- Support

Ett nästa steg är här att ta fram en förvaltningsorganisation med tydliga roller och ansvar, liksom avtal för anslutande aktörer (inkl. SLAer).

4.4. Andra viktiga lärdomar och nästa steg

Som beskrivits i rapporten kan Särimner lösa flera av de utmaningar som finns rörande robusthet och redundans idag. Det som dock Särimner inte har kunnat lösa är de problem som uppstått genom den utbyggnad som skett av IT-infrastruktur i Sverige där t.ex. redundant fiber saknas till mötesplatser.

För att kunna ta nästa steg och bygga ut antalet noder för bättre nationell täckning behöver frågan om fler mötesplatser för fiber och kommunikation lösas. Om frågan om finansiering kan lösas, exempelvis via uppdrag till PTS, finns goda förutsättningar till fortsatt implementering av resultaten. Ett första steg är att kartlägga var dessa mötesplatser bör placeras samt hur situationen ser ut gällande fiber och kommunikationsinfrastruktur. Därefter kan mötesplatserna skapas och i samband med detta både förstärka operatörers nät samt Särimner-lösningen byggs ut.

I projektet har det inte varit möjligt att få till intervjuer med operatörer på alla nivåer i värdekedjan även om teknisk personal hos operatörer varit involverade, bl.a. genom samarbete med föreningen Sveriges Operatörers Forum (SOF). En av anledningarna till detta var den kursändring som projektet var tvungen att ta ungefär halvvägs då platser för inplacering hos operatörer av noder började planeras. Två operatörer är intresserade av att deltaga i den fortsatta testdriften under 2019. Vi ser det som viktigt att utredningens och testdriftens resultat även fortsättningsvis förankras bland

operatörerna och att deras kunskap tillvaratas i samband med fortsatt testverksamhet och eventuell uppbyggnad av lösningen. Det goda samarbete som uppnåtts mellan alla deltagare i projektet, vilket också inkluderar tjänstetillhandahållare, bör fortsätta.

5. Bilagor

5.1. Bilaga 1 Begreppsordlista

Aktiv infrastruktur – Infrastruktur som på något sätt kommunicerar med annan infrastruktur eller tjänster och därigenom sänder data.

Bitström – Dataöverföring i oavbruten ström och i fast takt utan start och stopp.

Certifikat – Elektroniskt intyg som styrker att en elektronisk identitetshandling är korrekt och giltig. Kan vara hård (lagrad i en krets) eller mjuk (lagrad som sifferserie i ett datorminne).

CDN – Content Delivery Network, nätverk av geografiskt spridda servrar som på ett samordnat sätt överför innehåll så snabbt som möjligt.

DDOS – Distributed Denial of Service attack, dvs. överbelastningsattack som genomförs av många samverkande datorer.

DNS – Domain Name System, dvs. den funktion på internet som översätter domännamn till sifferserier (IP-adresser).

Hot Potato Routing – Tidig vidaredirigering, dvs. att nätverk på internet lämnar över meddelanden till andra nätverk så snart som det är möjligt.

ISP – Internet Service Provider, dvs. internetoperatör.

IP-adress – Internet Protocol Adress, dvs nummer som identifierar en dator som är ansluten till internet.

IT-infrastruktur – I denna rapport används begreppet när vi syftar på den svenska delen av internet, dvs. inkluderande både passiv och aktiv infrastruktur.

IX – Internet Exchange Point, dvs. teknisk knutpunkt där internetoperatörer utbyter trafik direkt med varandra med IP-protokollet (IPv4 eller IPv6).

Knutpunkt – Med knutpunkt eller mötesplats menas här en plats där fysiska nät möts så att de som använder dessa nät kan utbyta trafik.

Kryptering – Omvandlare av ett meddelande i klartext till ett meddelande som är obegripligt för obehöriga. Kryptering på internet sker med assymetrisk kryptering dvs. med användandet av två nycklar, en publik och en privat.

Nod – I detta sammanhang menas med nod, eller Särimner-nod, den enhet som levererar innehåll till slutanvändare.

Nätverkstopologi - Speglar relationer mellan nätverksenheter som är sammanbundna i ett nätverk. De kan vara fysiska eller logiska.

Nödsite - En i förväg lagrad kopia på en webbtjänst som man kan välja att visa i ett läge då ursprungskällan är otillgänglig för en Särimnernod.

Passiv infrastruktur – Infrastruktur i passiva nätdelar som rymmer andra nätdelar utan att själva bli aktiva, exempelvis kanalisation, ledningar, master mm.

Peer-to-peer – Nätverk där alla anslutna datorer kommunicerar med varandra som jämlika (peers).

Peering – Förmedling av trafik mellan operatörer utan betalning

Proof-of-concept (POC) – Koncepttest, dvs demonstration av att en idé är genomförbar.

Proxy/Proxyserver – En mellanserver som förmedlar meddelanden och förfrågningar riktade till andra datorer med syfte att dels minska belastningen på nätet dels för att höja säkerheten.

Redundans – Dubbel eller flerdubbel uppsättning av viktiga komponenter för att utrustningen ska fungera även om något går sönder. När det gäller infrastruktur gäller att kommunikation kan vandra flera vägar i nätet för att detta ska upplevas som redundant.

Router – Nätverksenhet som hittar en rutt för meddelanden från sändare till mottagare på internet eller i ett lokalt nätverk.

Robust – Förmågan att motstå störningar och avbrott samt förmågan att minimera konsekvenserna om det ändå inträffar.

Samhällsviktig information – Information som aktörer som bedriver samhällsviktig verksamhet behöver kommunicera till allmänheten.

Samhällsviktig verksamhet – De verksamheter i funktioner som är av betydelse för befolkningen liv och hälsa, samhällsfunktionalitet och våra grundläggande värden.

Scraping – Att utvinna information direkt från webbsidor med hjälp av specifika program.

SLA - Service Level Agreement; överenskommelser om tjänstenivåer.

SSL – Secure Socket Layer, dvs. säkerhetsprogram för webbkommunikation.

Svartfiber – Optisk fiber utan nätverksutrustning

VMA – Viktigt Meddelande till Allmänheten, det varningssystem som används vid olyckor eller allvarliga händelser.

5.2. Bilaga 2 Intervjupersoner

Namn	Organisation	Titel/Funktion
Ove Landberg	Post- och telestyrelsen	Enhetschef Nätsäkerhetsavdelningen
Fredrik Olofsson	Post- och telestyrelsen	Jurist Nätsäkerhetsavdelningen
Börje Josefsson	Vetenskapsrådet/SUNET	Operativt ansvarig och biträdande avdelningschef
Leif Johansson	Vetenskapsrådet/SUNET	Säkerhet, identitet, standardisering, strategi
Fredrik Korsbäck	Vetenskapsrådet/SUNET/SOF	Nätverksarkitekt SUNET, Ordförande SOF
Patrik Fältström	Netnod	Teknik- och Säkerhetsskyddschef
Mattias Ahnberg	Netnod	Head of Architecture and Development
Mattias Karlsson	Netnod	Head of Engineering
Anne-Marie Eklund Löwinder	Internetstiftelsen	Säkerhetschef
Eva Sartorius	Internetstiftelsen	Utredare
Jeanette Gustafsdotter	Tidningsutgivarna	VD
Jimmy Persson	Stadsnätsföreningen	Chef Utveckling och Säkerhet
Anders Sjödin	IT-Norrbotten	Nätansvarig
Tomas Sundström	LUNET	VD
Pia Stenervall	Stockholms stad	Kommunikationsstrateg och biträdande enhetschef
Ola Williams	Stockholms stad	Webbstrateg
Vesna Lucassi	Stockholms Läns Landsting	Informationssäkerhetschef
Henrik Brodin	Stockholms Läns Landsting	Handläggare
Stefan Lian	SVT	Sändningschef
David Karlsson	SVT	
Fredrik Widlund	SVT	
Kristian Palm	MSB	Ansvarig för krisinformation.se
Tim Georgiou	MSB	IT-säkerhetsansvarig
Ulrik Rosén	MSB	System- och nätverkstekniker
Fredrik Jensen	MSB	Systemutvecklare
Jonas Lindau	MSB	Systemutvecklare