SNUS Remissvar avseende departementspromemoria: Förstärkt integritetsskydd vid signalspaning.

Föreningen SNUS (Swedish Network Users' Society) har beretts möjlighet att lämna synpunkter på rubricerade promemoria. Detta remissvar behandlar enbart det förslag på förändringar som promemorian innebär och tar inte ställning till den tidigare beslutade lagstiftningen som sådan. Dessutom berör detta svar enbart de frågor som ligger inom SNUS kompetensområde, d.v.s. främst de tekniska aspekterna av förslaget.

SNUS anser att den föreslagna lagtexten inte uppfyller den politiska överenskommelsens intentioner. Tydligast är detta i det centrala avsnittet kring förbud mot inhämtning av inhemsk trafik (5.2).

Förslaget innebär med hänsyn till hur kommunikation över Internet i praktiken fortsatt ett fribrev för ansvariga myndigheter att avlyssna samtliga medborgare i Sverige eftersom det i många fall inte går att avgöra om trafiken gått via utlandet eller inte.

Bevisbördan för att visa att trafiken går mellan två individer varav minst den ena befinner sig utomlands, måste ligga hos den signalspanande myndigheten. För att lagtexten ska uppfylla den politiska överenskommelsens intentioner anser föreningen SNUS att bevisbördan måste inverteras.

Utifrån en teknisk synvinkel finner vi två delar av promemorian problematiska och diskuterar dessa i detalj nedan.

Avsnitt 5.1 Avskiljande av de signaler som behövs för verksamheten.

I flera av promemorians skrivningar framgår att det trots allt finns en förståelse för att det inte nödvändigtvis är samma aktör som äger en kanalisation, äger och/eller förfogar över en kabel, hyr en våglängd i denna kabel alternativt tillhandahåller en operatörstjänst.

Trots denna förståelse används begreppet *operatör* så som det definieras i LEK (2003:389), vilket är problematisk för det syfte man vill uppnå. Givet så som definitionen av operatör i 6 kap, § 19a av LEK är skriven kommer endast de operatörer som **samtidigt** äger tråd som passerar landsgräns att tvingas överföra information till samverkanspunkter. Därmed ser vi inte att målet med lagstiftningen uppnår sitt syfte. I de fall där en operatör inte förfogar över den kabel som används för överföring av signaler över landsgräns (vilket är vanligt) är regleringen idag mycket otydlig.

Baserat på denna typ av problem anser vi denna reglering vara förvirrande och förefaller bristfällig. Ett annat exempel på problematik är att ordvalet *samverkanspunkter* skulle kunna indikera att promemorians författare kan ha tolkat det samtrafikutbyte som sker mellan vissa

operatörer på gemensamma knutpunkter (t.ex. i regi av företaget Netnod) som det dominerande sättet att utbyta trafik och att det därför finns ett fåtal punkter där avskiljandet av signaler enkelt kan ske.

I realiteten utbyts endast en del av Internets trafik via dessa knutpunkter och kommunikation passerar landsgränser i en stor mängd nät, såväl publika som företagsinterna. Både över nät där operatören äger kabeln, där operatören förfogar över kabeln, och de fall där operatören enbart hyr transmission via kabeln. I den rådande lagstiftningen där en operatör får utse en eller flera punkter för avtappning av trafik, kombinerat med kravet på snabbt införande av nya avskiljningsregler kan det handla om hundratals platser dit kontrollmyndigheten måste ha beredskap att upprätta avskiljning (och vidare transmission till signalspaningsmyndigheten). Om förslaget ändras så att ansvaret för detta arbete (och därmed kostnaderna) överförs till operatörerna kan detta förväntas bli så kostnadsdrivande att det bör utredas separat.

Lagstiftningen berör inte enbart Internettrafik, utan generell signalspaning i kabel. Det innebär att även andra former av kabelbunden trafik som passerar gränsen (t.ex. privat hyrd signalöverföring) som skall kunna avlyssnas. Denna kommunikation passerar inte dessa knutpunkter. Trafik som hanteras av en operatör som hyr en extern transmissionstjänst från ett annat företag (som inte definieras som en operatör under LEK) behöver således inte passera samverkanspunkter. Här förefaller lagstiftningen bli i bästa fall otydlig, i värsta fall godtycklig.

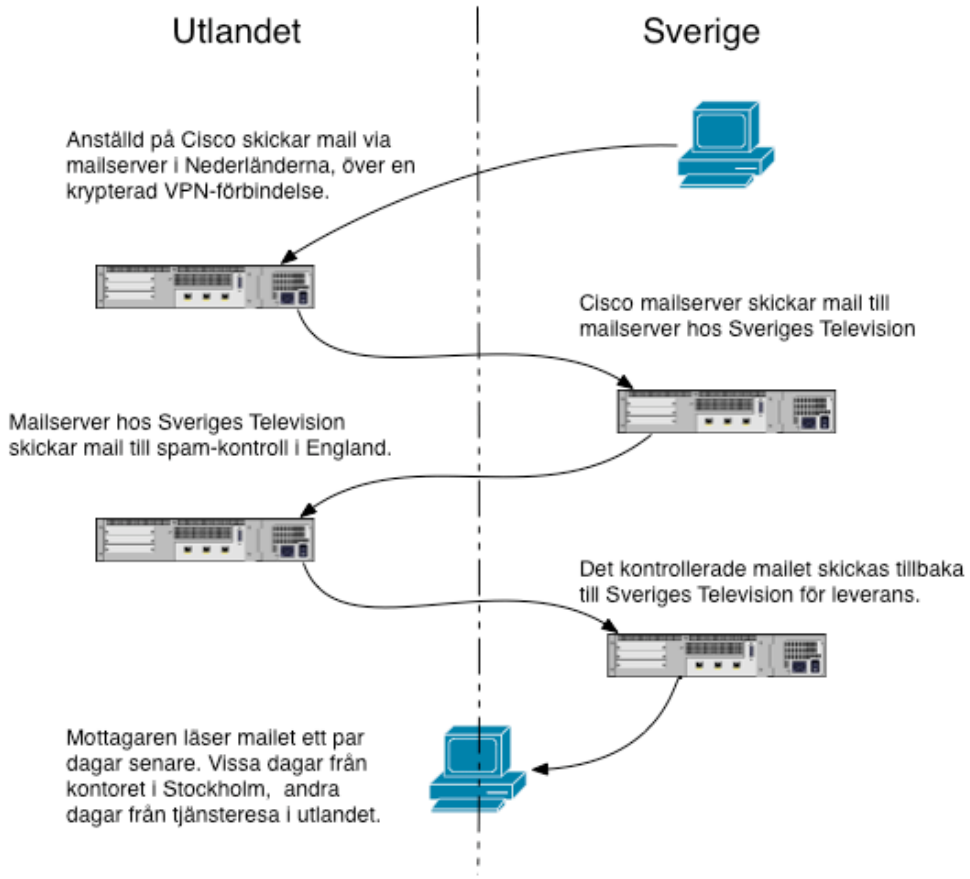
Avsnitt 5.2 Förbud mot inhämtning av inhemsk trafik

Lagstiftningen säger att signalspaning endast får avse utländska förhållanden och den politiska överenskommelsen betonar att ingen kommunikation får avlyssnas där sändare och mottagare båda befinner sig i Sverige.

I den lagtext som presenteras har detta formulerats som att trafik som avskiljs där mottagare och avsändare i något steg av behandlingen kan identifieras ha befunnit sig i Sverige ska förstöras så snart denna identifiering gjorts.

Detta innebär en omvänd bevisbörda i förhållande till den överenskommelse som gjorts. Denna omvända bevisbörda blir problematisk eftersom det för en icke oansenlig mängd kommunikation inte är möjligt att avgöra i vilket land både avsändare och mottagare har befunnit sig.

Denna typ av problematik gäller för en många av de protokoll som används för kommunikation över Internet idag. I detta remissvar illustrerar vi detta med två vanliga exempel på kommunikation över Internet, e-post och chatt (Instant Messaging).

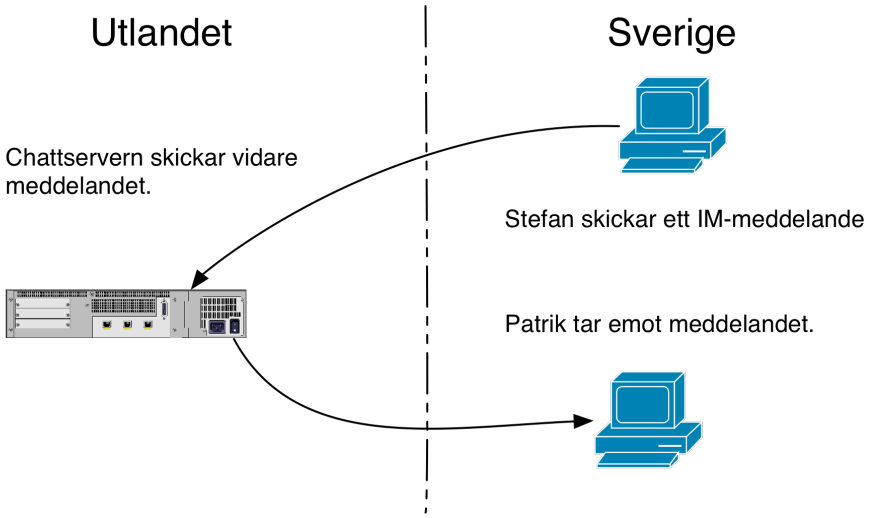


Figur 1: Två personer bosatta i Sverige skickar mail mellan varandra, varvid detta mail passerar Sveriges gräns minst 4 gånger.

Figur 1 beskriver hur ett meddelande skickas i ett scenario där två personer bosatta i Sverige korresponderar via e-post. Meddelandet passerar Sveriges gräns inte mindre än fyra gånger, varav en på ett företagsinternt nät som byggts med hjälp av krypterade förbindelser över Internet. Inte vid något av de tillfällen meddelandet passerar gränsen är det möjligt att avgöra var mottagare och avsändare befinner sig eftersom varje del av kedjan endast känner till var föregående och nästkommande mellanlagring kommer att ske.

Figur 2 beskriver hur ett meddelande skickas när två personer kommunicerar via en meddelandeserver utomlands (t.ex. använder MSNs chatt-funktionalitet).

Kommunikationen sker inte direkt mellan Person A och Person B utan sker med hjälp av en meddelandeserver. Först skickas ett meddelande från Person A till MSN-servern utanför Sveriges gränser. Sedan skickar MSN-servern ett meddelande till Person B. Den signalspaning som antingen fångar upp meddelandet från Person A, eller meddelandet till Person B känner enbart till MSN-servern, och inte huruvida personerna som kommunicerade befann sig i Sverige.



Figur 2: Två personer bosatta i sverige chattar via t.ex. MSN, AOL Instant Messenger eller Yahoo! Messenger. Båda kommunicerar med en dator i utlandet. Varken sändare eller mottagare har kännedom om i vilket land den andra parten befinner sig, endast var mellanhanden finns.

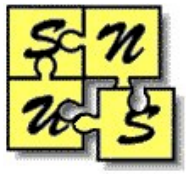
I den föreslagna lagtexten ska dessa meddelanden inte kasseras eftersom det inte går att identifiera som kommunikation mellan två personer i Sverige. I den politiska överenskommelsen är dessa meddelanden däremot något som omedelbart ska kasseras. För att uppfylla intentionen i den politiska överenskommelsen måste lagtexten ändras så att bevisbördan inverteras så att enbart trafik som kan visas härröra från personer utanför Sverige kan avlyssnas.

Detta innebär dock att en stor mängd trafik (i enlighet med överenskommelsen) inte längre kan användas för analys, vilket kan påverka de avvägningar som tidigare gjorts mellan nytta och nackdelar med den föreslagna lagstiftningen.

Sammanfattningsvis anser vi att det är tveksamt om de politiska målen kan uppnås utifrån den föreslagna lagtexten med de felaktiga antaganden som görs kring hur Internet fungerar. Detta innebär att finns anledning att på nytt diskutera lagstiftningens utformning och proportionalitet.

Stockholm 12 februari 2009

För SNUS, genom styrelsen.



Om SNUS
SNUS är en ideell förening för svenska nätverksanvändare. Vårt syfte är att höja nätverkskunskapen i Sverige och därmed vår nationella konkurrenskraft.

SNUS är föreningen för dig som är nätverkstekniker och arbetar med IP-nätverk. Föreningen har funnits i många år och är ett forum för tekniskt intresserade personer inom nätverksområdet. Vi ska verka för att medlemmarna får del av varandras kunskaper inom ramen för våra olika aktiviteter, främst genom arbetsgrupper, seminarier, testrapporter och medlemstidning. Genom dessa aktivitet är SNUS ett forum med verksamhet inriktad på att

- öka förståelsen för nätverksteknik och -användande i Sverige.
- driva på utvecklingen vad gäller samtrafik och samverkan.
- testa vad som fungerar i verkligheten sprida kunskap och erfarenheter.

Under SNUS historia sedan 1991 har fokus varit att sprida kunskap om leverantörsoberoende kommunikation (TCP/IP). SNUS har starkt bidragit till den tekniska utvecklingen av Internet vi har bl.a. initierat Swipnet (Det första kommersiella IP-nätet i Sverige) och medverkat till en överenskommelse om samtrafik för elektronisk post (mellan X.400- och Internet-världarna). SNUS har genomfört seminarier där intressanta ämnen inom TCP/IP-området tagits upp. SNUS är mest känt för att anordna Interoperabilitets-tester. Som bäst kan beskrivas som en avancerad provplats inför öppen ridå. Där de deltagande företagen genom hårt arbete och samarbete fått insikter och testat utlovade funktioner i praktiken. Testresultaten har presenterats dels direkt på plats, dels i detalj i testrapporter som publiceras här i vår Web. Vi har även arbetat med politiker, operatörer och övriga intressenter om vikten av fungerande interoperabilitet och samtrafik mellan de olika näten. SNUS har medverkat som sakkunniga i regeringens Internetutredning. Varit delaktiga i skapandet av den svenska delen av ISOC, Internet Society, som är det internationella värdorganet för IETF, Internet Engineering Task Force. SNUS har även varit värdorganisation för de svenska internetoperatörernas forum; SOF-gruppen.