.SE Nyhetsbrev om Internets styrning

november 2013

Blogg:

Nyhetsbrev:

Internetutvecklingen styrs idag endast i begränsad utsträckning av samma aktörer som för fem eller tio år sedan. Anspråken på hur nätet ska styras kommer från flera håll samtidigt. Det är en komplex uppgift bara att överblicka alla försök till styrning av nätets utveckling.

På .SE vill vi med detta brev bidra till omvärldsbevakningen av denna process. Brevet kommer månadsvis. Sammanställningen gäller utvecklingen i Sverige, EU och globalt, och fokuserar i första hand på händelser som rör Internets styrning och hoten mot det öppna Internet. Brevets innehåll är en kortfattad inventering och pekare mot aktuella frågor. Tematiska fördjupningar, kommentarer och åsikter ligger i bilaga. Ibland ligger åsikter också i halvårssummeringar.

Innehåll

Kommentarer, synpunkter eller frågor:

Staffan Jonson, .SE (Stiftelsen för Internetinfrastruktur), Box 7399, 103 91 STOCKHOLM,
tel 073-317 39 67, Staffan.jonson@iis.se , www.iis.se

Globalt

Frågor om Internets styrning tog upp en stor del av syret på novembers ICANN-möte i Buenos Aires. Som beskrivits i flera andra sammanhang råder något av hela havet stormar bland de internationella internet-organisationerna, där de flesta på olika sätt positionerar sig till det kommande ad-hoc-mötet i Brasilien våren 2014, och den princip-diskussion för internetstyrning som väntas äga rum där.
Civila organisationer och intresseorganisationer försöker på såväl möten som e-postlistor formera sig för sina inspel till sådana principer. Till exempel Internet Society har under parollen *Keep Internet Strong* öppnat en offentlig utfrågning om idéer till utveckling.[1]
Principerna samlade under sajten *necessary and proportionate* har hittills samlat över 300 signatärer av varierande kaliber och storlek.[2]

Energin i denna storm kommer givetvis från det gångna halvårets avslöjanden om den systematiska avlyssningen och kapprustningen på internet. Brasilien var tidigare en s.k. *swing state* i den bipolära dragkampen mellan ITU å ena sidan och ICANN-sfären å andra sidan. Under hösten kom landet emellertid att ta ledarskapet i initiativ till institutionell internetutveckling, dvs. regler för hur nätet ska styras framöver.

ICANN tog under hösten och på sin kant initiativ och ledarskap till Montevideo-deklarationen, manifesterad på 1net.org, och den panel av centrala personer i ekosystemet runt internet som infrastruktur (de s.k. I*-organisationerna). Det fanns bitvis nära koordinering mellan ICANN och Brasiliens insatser.
På ITU hölls också möte i den rådsarbetsgrupp som ska utveckla internet-relaterade policyfrågor i WSIS-fortsättningen från 2005.

Så inför 2014 finns minst två viktiga händelser som troligtvis kommer att ha stor effekt för nästyrningen. Det rör sig dels om Brasilienmötet 23-24 april i Sao Paulo och den s.k. fullmaktskonferensen (Plenipotentiary-mötet, den s.k. plenipoten) i Busan, Korea hösten 2014. Till det kommer eventuellt också FN-planerna på att hålla ett högnivå-möte i Ryssland i Sotio.[3]

Vi fick också bekräftat att Sverige sedan lång tid tillbaka ägnar sig åt offensiv spaning mot Ryssland. I riksdagen påpekade oppositionen att det är tveksamt om detta är förenligt med det mandat Riksdagen givit regeringen och FRA.

Nytt var också SÄPO:s utökade ambition av datalagringsdirektivets tillämpning. Där framgick bl.a. att s.k. rättsvårdande myndigheter omedelbart, momentant och automatiserat ska kunna ta del av internetoperatörernas insamling av persondata i samband med telefoni och internet-trafik.

[1] http://www.internetsociety.org/internet/keep-internet-strong
[2] https://en.necessaryandproportionate.org/text
[3] http://www.icann.org/en/news/press/releases/release-18nov13-en

Civilt motstånd mot avlyssning

I början av december publicerade mer än 500 författare från 81 länder ett upprop[4] mot stats-sanktionerad avlyssning och internetövervakning. I uppropet uppmanas FN att skapa en internationell lag för digitala rättigheter.
I skrivande stund tycks uppropet i Sverige också publicerats i Dagens nyheters pappersupplaga, men har också letat sig in till redaktionellt material.

Där formuleras fyra tydliga argument varför det är ett problem med alltför omfattande övervakning:[5]

- *Surveillance violates the private sphere and compromises freedom of thought and opinion.*
- *Mass surveillance treats every citizen as a potential suspect. It overturns one of our historical triumphs, the presumption of innocence.*
- *Surveillance makes the individual transparent, while the state and the corporation operate in secret. As we have seen, this power is being systemically abused.*
- *Surveillance is theft. This data is not public property: it belongs to us. When it is used to predict our behaviour, we are robbed of something else: the principle of free will crucial to democratic liberty.*

FN-institutionerna

Generalförsamlingen – resolution för rätten till integritet online

I slutet av november beslutade generalförsamlingen så om den resolution om potentiella hot mot mänskliga rättigheter online, som beskrivits tidigare. Under parollen *The right to privacy in the digital age* begärde signatärerna bl.a. att FN:s *High Commissioner for Human Rights* ska författa en rapport om skyddet av integritet också online. Vidare beslutades bl.a. att frågan ska tas upp på nytt nästa år igen i Generalförsamlingen.

Resolutionen skrevs under av en intressant samling länder:
Argentina, Österrike, Bolivia, Brasilien, Chile, Cuba, Nordkorea, Ecuador, Frankrike, Tyskland, Guatemala, Indonesien, Irland, Liechtenstein, Luxemburg, Mexico, Nicaragua, Peru, Slovenien, Spanien, Schweiz, Östtimor, och Uruguay.[6]

---

[4] http://www.change.org/petitions/a-stand-for-democracy-in-the-digital-age-3

[5] http://www.change.org/petitions/a-stand-for-democracy-in-the-digital-age-3
http://www.theguardian.com/world/2013/dec/10/surveillance-theft-worlds-leading-authors
http://www.dn.se/kultur-noje/nyheter/jag-hoppas-pa-det-civila-samhallets-motstandsvilja/

[6] http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1
http://www.diplomatmagazine.nl/2013/11/03/brazils-speech-internet-68th-unga/
http://www.reuters.com/article/2013/09/24/us-un-assembly-brazil-idUSBRE98N0OJ20130924

WSIS + 10 i Ryssland 2015?

Även i det s.k. andra utskottet utmanades internetstyrningen. Tioårsuppföljningen av WSIS[7] ser ut att formuleras som ett nytt världstoppmöte som ska hållas 2015 i Sotji, Ryssland. Enligt uppgifter ska det mötet helt domineras av regeringars aktiva deltagande, och utan civilt samhälle eller andra intressenter.[8]

Internationella teleunionen – inför fullmaktskonferensen 2014

I november hölls möte i en rådsarbetsgrupp i ITU rörande internet-relaterade policy-frågor.
Arbetsgruppen bildades vid Plenipoten 2010. Arbetet syftar till fullmaktskonferensen i Busans, Korea hösten 2014.[9]

Internets styrning i Brasilien

Ett globalt ad-hoc-möte i Brasilien

Den brasilianska samarbetsorganisationen för internetfrågor CGI har i ett pressmeddelande aviserat att ad-hoc-mötet för internets styrning till 23 och 24 april 2014 i Sao Paulo.

Mötet ska ha en bred ansats (multistakeholder participation), med representanter för regeringar, civilt samhälle, akademi, internationella organisationer, tekniska – och affärsmässiga intressen. Prof. Virgílio Fernandes Almeida är utsedd som koordinator i Brasilien.

Mötet ska organiseras i fyra kommittéer:

- High-Level Multistakeholder Committee: Responsible for conducting the political articulation and fostering the involvement of the international community.

- Executive Multistakeholder Committee: Responsible for organizing the event, including the agenda discussion and execution, and for the treatment of the proposals from participants and different stakeholders

- Logistics and Organizational Committee: Responsible for overseeing every logistic aspect of the meeting

- Governmental Advisory Committee: Will stay open to all governments which want to contribute to the meeting.

---

http://www.pcworld.com/article/2067420/un-panel-passes-draft-resolution-on-privacy-threats-in-the-digital-age.html

[7] World Summit on the Information Society

[8] http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N13/552/87/PDF/N1355287.pdf?OpenElement

[9] http://www.itu.int/council/groups/CWG-internet/
http://www.itu.int/md/S09-CL-C-0105

Processen inför mötet att sätta samman en agenda ser ut att falla ner i tre parallella processer:
Område 1: Förslag till konferensens arbetssätt och processer
Område 2: Inspel till universella (globala) principer för internetstyrning
Område 3: Ett institutionellt ramverk för mångfalds- (multi-stakeholder) styrning av internet.

Område 3 faller i sin tur ner i frågorna
a) internationaliseringen av ICANN
b) andra frågor
Denna struktur för arbetet är emellertid högst preliminär.[10]

1net.org - En panel från det globala tekniska internetsamfundet inför Brasilien

Det har i det internationella internetsamfundet vuxit fram en fristående panel på ett 20-tal personer. Gruppen är tänkt att vara representativ för olika geografiska regioner och intresseorganisationer.[11]
Panelen ska senast i mars 2014 bidra med en uppsättning principer för globalt internetsamarbete, och en rapport med förslag till samarbetsformer. Tidtabellen är med andra ord särskilt designad för det kommande Brasilien-mötet. Även om ICANN har en stor betydelse för panelens tillblivelse, har man samtidigt ambitionen att knyt den till en annan global organisation för att på så sätt säkra dess självständighet från ICANN.
I gruppen kommer bl.a. Vint Cerf (Google), Fadi Chehadé (ICANN), Olaf Kolkman (f.d. IAB ordförande), Lynn StAmour (Avgående VD för ISOC) ingå.

Den Europeiska intreseorganisationen för toppdomänadministratörer (Centr) har publicerat en utförlig beskrivning av panelens tillblivelse.[12]

ICANN

ICANN-mötet i Buenos Aires

I november beslutade ICANNs styrelse i ytterligare ett beslut att utöka ICANN:s engagemang då det gäller styrningen av internet. ICANNs VD fick redan i september 2013 ett utökat mandat att arbeta med andra organisationer för att etablera en koalition för internetstyrning tillsammans med andra organisationer.[13]

---

[10] http://cgi.br

[11] I* organizations that led to the Montevideo Statement on the Future of Internet Cooperation. (See http://www.1net.org/news/entry/montevideo-statement-on-the-future-of-internet-cooperation/en).

[12] https://www.centr.org/system/files/agenda/attachment/centr-ig_update-20131107.pdf

[13] http://www.icann.org/en/groups/board/documents/resolutions-17nov13-en.htm

En branschplattform för dialog om mänskliga rättigheter i elektronisk kommunikation

Flera stora ISP:er har i mars 2013 satt upp plattformen *Telecommunications industry dialogue*. Det är en grupp ISP:er som gemensamt vill uppmärksamma yttrandefrihet och rätten till integritet online i telekombranschen. Samarbetet grundades till följd av de vägledande principer som i FN:s råd för mänskliga rättigheter i mars 2011.[14]

Universella principer för internetavlyssning

Paraplysajten Necessary and Proportionate samlar ett stort antal organisationers engagemang att författa universella principer då det gäller internetövervakning och avlyssning. Sajten samlar de över 300 organisationer som skrivit under på de 13 principer som utvecklades redan under 2012.
De sju principer Sverige genom Carl Bildt stödde i sitt tal i Korea i oktober 2013 har en tydlig likhet med några av de 13 principerna.[15]

Ökad övervakning i Ryssland

EDRI rapporterar att Ryssland planerar att skruva upp kraven på internetleverantörer då det gäller datainsamling (data retention). Den ryska säkerhetstjänsten ska utöka sin övervakning av internet-trafiken genom att internetleverantörerna från juli 2014 ska åläggas lagra all trafik under 12 timmars tid, och göra den tillgänglig till säkerhetstjänsten *Federal Security Service* (FSB).[16]

Indisk filtrering

Indiska högsta domstolen har kontaktat landets *Department of Telecommunication* för att få råd om hur man ska kunna blockera sajter som innehåller pornografi, särskilt barnpornografi.
I sin begäran påpekar domstolen att de flesta brott begångna mot kvinnor, flickor eller barn förstärks av pornografi. Domstolen vet också att sådana bilder succesivt blir värre.[17]

---

[14] http://www.business-humanrights.org/media/documents/ruggie/ruggie-guiding-principles-21-mar-2011.pdf
http://www.telecomindustrydialogue.org/
[15] https://en.necessaryandproportionate.org/take-action/privacyinternational

[16] http://www.edri.org/edrigram/number11.21/russian-government-internet-spy
https://publicaffairs.linx.net/news/?p=10141
[17] http://www.thehindu.com/news/national/sc-seeks-dots-reply-on-ways-to-block-pornography/article5363759.ece

Europa

Europarådet

Europarådet höll i början av december en särskild konferens kallad *Octopus Conference Cooperation against Cybercrime*.
Konferensens huvudfokus sägs varit *cybercrime*, samt *safeguard and data protection: criminal justice versus national security*. Den diskuterade införandet av den s.k. budapestkonventionen mot cyberbrottslighet, och en eventuell revision av densamma.[18]

Ny europeisk strategi för internetstyrning?

EU-kommissionen aviserade redan i oktober en offentlig remissvända om internetstyrning.
Några svar publiceras här:[19]

Enligt andra uppgifter förbereder EU-kommissionen en ny politik för internetstyrning. Den sägs förstärka staters inflytande, på bekostnad av dagens modell där civilt samhälle antas ha en mer framträdande roll.
Än så länge finns bara läckta versioner av dokumentet, men dokumentet kan antas vara färdigställt i god tid före Brasilienmötet i april 2013.
Bloggen som rapporterar händelsen visar bl.a. hur multistakeholder-modellens legitimitet ifrågasätts av Kommissionen, vilket är en radikal och tydlig kursändring. I förlängningen av en sådan policy ligger bl.a. en fullt ut nationalstatskontrollerat internet. Förslaget är därmed också på direkt kollissionskurs med den svenska linjen på området, som varit oförändrad i minst 10 år.[20]

EU: Det tredje telekompaketet

EU-kommissionens senaste och hastigt bearbetade förslag till ny reglering för bl.a. internetåtkomst har även i november rönt stort intresse.[21]

18
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_octopus2013/Octopus2013_en.asp
https://ameliaandersdotter.eu/2013/12/02/letter-complaint-regarding-octopus-cyber-crime-conference
Cyberbrottskonventionen/Budapestkonventionen:
http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

19 Centr: http://centr.org/CENTR-Comment-EC_consultation
ICANN: https://ec.europa.eu/digital-agenda/en/content/europe-internet-global-context

20 http://www.internetgovernance.org/2013/12/06/europe-at-a-tipping-point-leaked-ec-document-stirs-internet-governance-controversy/

21 N2013/4192/ITP
Förslag till Europaparlamentets och rådets förordning om åtgärder för att fullborda den europeiska inre marknaden för elektronisk kommunikation och upprätta en uppkopplad kontinent och om ändring av direktiven 2002/20/EG, 2002/21/EG och 2002/22/EG samt förordningarna (EG) nr 1211/2009 och (EU) nr 531/2012.

I Sverige visade Riksdagen nyligen begränsad entusiasm över förslaget[22], och Computer Sweden redovisade redan i förväg vad IT-ministern skulle komma att säga på ministerrådet i december.[23]
Digital Civil Rights in Europe (EDRI) har gjort en genomarbetad analys av förslaget, och dess behandling i Parlamentet.[24]

EU: Återupptagen förhandling om transatlantiskt handel (TTIP)

Euractive rapporterar att EU och USA i november återupptagit förhandlingarna om *Transatlantic Trade and Investment Partnership* (TTIP). Förhandlingarna stängdes tidigare pga. den amerikanska statens inrikespolitiska spel om budgeten, och därpå följande stängning av förvaltningen under hösten.

Vivianne Reding har tidigare tydligt aviserat att frågor om skydd av personlig data ska hållas från agendan tills vidare. Artikeln återger också rapporter från Financial Times som spekulerar i huruvida Tyskland kommer att kräva uttryckliga dataskyddsregler i TTIP. Även BBC vittnade om den griniga stämningen med anledning av den systematiska internetavlyssningen.[25]

Artikeln rapporterar att förhandlingar skett 11-15 november, att tredje rundan för förhandlingarna börjar 16 december, och att det i januari kommer att hållas en summerande erfarenhetsuppsamling mellan EU-kommissionär Karel de Gucht och USA:s handelsrepresentant Michael B. Foman.[26]

Mer om TTIP

- Hemlighetsmakeriet runt TTIP håller på att bli ett nytt ACTA: http://www.opendemocracy.net/holly-jarman/beware-secret-trade-deals-can-seriously-damage-your-health
- Sammanställning: http://infojustice.org/archives/31243
- ISOC:s statement: http://www.internetsociety.org/blog/2013/11/trans-pacific-partnership-agreement-risks-harming-internet
- Läcksida om TTIP:
  Coporate Europé Observatory har publicerat vad man menar är en läckt PR-strategi från EU-Kommissionen då det gäller hur man avser kommunicera handelsvatalet TTIP. http://ttipfakta.wordpress.com och http://ttippen.se

EU: NIS-direktivet

[22] http://www.riksdagen.se/sv/Dokument-Lagar/Utskottens-dokument/Betankanden/Arenden/201314/TU5/
http://www.riksdagen.se/sv/Dokument-Lagar/Utskottens-dokument/Betankanden/201314Subsidiarietsprovning-a_H101TU5/
[23] http://computersweden.idg.se/2.2683/1.536913/sverige-haller-operatorerna-om-ryggen
[24] http://www.edri.org/NN-EP
[25] http://www.bbc.co.uk/news/business-23221503
[26] http://www.euractiv.com/trade/eu-us-return-major-trade-negotia-news-531601

Det pågår fortsatta förhandlingar om NIS-direktivet[27] i Bryssel. Parlamentet och de nationell representationerna bearbetar.
Det finns förväntningar på att Parlamentet och Rådet skulle kunna vara färdiga under de första månaderna 2014, och att direktivet därmed kan beslutas inom nuvarande mandatperiod, dvs. innan valen i maj 2014. Om den tidtabellen håller kan NIS-direktivet bli nationell lag 2016.
Domännamnsoperatörernas samarbetsorgan Centr.org har publicerat en ståndpunkt runt NIS-direktivet.[28] Omröstning i Parlamentets IMCO-utskott väntas ske 22 eller 23 januari.

[27] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf
[28] http://www.centr.org/CENTR_opinion_on_EU_NIS_directive

Sverige

Integritetsdebatt i Riksdagen

Vänsterpartiet initierade i juni det som i början kom att bli en riksdagsdebatt om integritet på nätet. I debatten framkom att fr.a. vänsterpartiet ursprungligen begärde ett helt annat fokus på debatten, nämligen en debatt om de uppgifter som (då) avslöjats om en systematisk internetavlyssning. Debatten föregicks av att Försvarsutskottet dagen före vallades på FRA. [29]

Säpo vill se ett utökat och automatiserat datalagringsdirektiv i Sverige

svensk media med tidningen Ny Teknik i spetsen rapporterade i november att svenska myndigheter vill beredas direktåtkomst till uppgifter om användarnas telefoni och internettrafik från operatörerna (s.k. metadata). Enligt bl.a. SvD begär SÄPO att exempelvis Skattemyndigheten och Tullen ska kunna gå direkt in i operatörernas trafikdatabaser genom ett helt automatiserat system.
Ny tekniks beskrivning att den automatiserade dataöverföringen sker genom utveckling av det tekniska gränssnittet kallat ITS27. Där framgår också att polisen kan ta fram mer uppgifter om användare än enbart sådan metadata. Till exempel ska gränssnittet också kunna medföra att polisen kan samla in mobiltelefoners persnliga upplåsningskoder (s.k. PUK-koder).[30]

Det är tillämpningen av det redan beslutade datalagringsdirektivet som med detta förslag får nya avnämare. SÄPO vill att alla rättsvårdande myndigheter ska kunna få en direkt och automatiserad åtkomst till de databaser hos operatörerna som samlar metadata om internet-trafik och telefoni. Därmed ska alla de myndigheterna automatiserat och momentant kunna ta ner uppgifter om tele- och internetkunder.
Fler av de stora operatörerna har enligt egen utsago sagt blankt nej till denna praxis (t.ex. Teliasonera och Tele2). Det är oklart om staten på legal grund kan tvinga fram en sådan praxis, åtminstone utifrån det nuvarande datalagringsdirektivet. Eventuellt ligger det i det kommande s.k. tredje telekompaketet utökat legalt stöd för sådana tvångsåtgärder.

Det har också stormat runt det företag som för offentlig sektor ska tillhandahålla datalagringen. Företaget arbetar idag enligt egen utsago med ”Stadsnät, operatörsverksamhet, data & Telecom, affärsutveckling och programutveckling.”. Företaget är medlem i svenska stadsnätsföreningen (SSNf).

---

[29] http://www.riksdagen.se/sv/Dokument-Lagar/Kammaren/Protokoll/Riksdagens-snabbprotokoll-2013_H10924/
http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=5698393
http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=5697658

[30] http://www.nyteknik.se/nyheter/it_telekom/allmant/article3788288.ece
http://www.svd.se/nyheter/inrikes/sapo-vill-komma-at-data-direkt_8740078.svd
http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=5707919

Svenska stadsnätsföreningen aviserade först att man avsåg använda standarden ITS27 i sina nät, men gjorde dagen efter en helomvändning, i betydelse att man avbryter den automatiska utlämningen av data i sista steget av datalagringstjänsten.[31] Se vidare tolkning i bilaga.

Begränsning av offentlighetsprincipen i Sverige

DN rapporterar om ett lagförslag som syftar till att begränsa den svenska offentlighetsprincipen då det gäller EU-dokument. I januari 2014 beslutar riksdagen om en ny lag som möjliggör för myndigheter att hemligstämpla dokument med anknytning till EU. Regeringen kallar samma sak (prop.2012/13:192) *Sekretess i det internationella samarbetet*.

Lagen sägs syfta till att underlätta för den svenska förvaltningen att ta del av dokument som är hemligstämplade i annat EU-land, utan att de därmed behöver prövas för offentliggörande, alt hemligstämplande. Lagändringen är exempelvis relevant för vilka dokument i de transatlantiska TTIP-förhandlingarna som ska behövas bli offentliggjorda.[32]

Som jämförelse har en arbetsgrupp kallad *Foundation for a Free Information Infrastructure* i flera månader uppvaktat Europaparlamentet för att få tillgång till dokument om ACTA.[33]

Kraftig tillväxt av FRA

DN rapporterar i november i en journalistisk gärning att FRA expanderat kraftigt den senaste fem åren. Enligt DN har myndigheten tillförts ökade anslag med 230 miljoner kronor. På fem år har verksamheten ökat med 39%. 2013 avsätter staten 822 miljoner kronor till verksamheten. Anslagsökningarna sammanfaller i tid med FRA-lagen.[34]

Koordinering av IKT-tjänster i staten (s.k. e-förvaltning)

E-delegationen har efter fyra års arbete i oktober 2013 publicerat SOU 2013:75 kallad *Organisering av framtidens e-förvaltning*.[35]

---

[31] http://www.maintrac.se
http://www.ssnf.org/puffar-pa-forsta-sidan/Fragor-och-svar-om-Maintracs-datalagringstjanst/
http://www.ssnf.org/Nyheter/Nyhetslistning/Stadsnaten-stoppar-inforandet-av-automatisk-dataoverforing/
http://news.cision.com/se/bahnhof/r/varnade-for-overvakning--hotas-av-stamning,c9503871

[32] http://www.regeringen.se/sb/d/108/a/223755
http://www.dn.se/nyheter/sverige/eu-dokument-kan-bli-hemliga-med-ny-lag/
http://www.euractiv.com/trade/eu-us-return-major-trade-negotia-news-531601

[33] http://acta.ffii.org/?p=1956

[34] http://www.dn.se/nyheter/sverige/hundratals-miljoner-till-forsvarets-signalspaning/

[35] http://www.regeringen.se/sb/d/17075/a/227678

E-delegationen konstaterar att för att åstadkomma förenkling för så många som möjligt behövs en *"... ökad förvaltningsövergripande digital samverkan mellan statlig och kommunal sektor."*

E-delegationen föreslår:

- "... att samordningen av de gemensamma e-förvaltningsfrågorna förs in i en medlemsorganisation liknande en kollegiemodell, till exempel på det sätt Arbetsgivarverket idag är uppbyggt. För att stärka samverkan med den statliga och kommunala sektorn bör den nya organisationen upprätta ett särskilt samarbetsorgan med kommunal sektor.
- E-delegationen föreslår att en utredare utses för att a) utforma regler och andra beslut som krävs, b) föreslå former för samordningen inom hela offentlig sektor, c) lämna förslag på de uppgifter som ska tillföras funktionen.
- Vidare föreslås, för att undvika avbrott, att E-delegationens mandat fortsätter till dess en ny organisation kan överta den verksamhet som beslutas."

Avlyssningens effekter

Computer Sweden rapporterar att svenska företag blivit mer tveksamma till molntjänster.[36]Artikeln menar att det finns ett samband mellan avslöjandena om systematisk avlyssning och oviljan till molntjänster.

SvD Rapporterar att Danska Telenor överväger att upphöra med att förmedla sin internet-trafik genom Sverige. Enligt uppgifterna har idén väckts sedan danska Berlingske publicerat en artikelserie om den svenska FRA-lagen.[37]

Internetdagarna

Så har det fjortonde året av Internetdagarna gått av stapeln.
Alla sändningar från sessionerna samlas på nätet[38]

Kronofogden hackad

DN rapporterar hur Kronofogdemyndighetens databas över skuldsatta människor hackades för knappt två år sedan. Det var i samband med intrång i Logicas servrar som flera myndgiheters känsliga uppgifter kapades. Bland annat ska 10 000 skyddade personnummer, och listor över polisanställda kommits över. Enligt uppgifter ska myndigheten försökt tysta ner stölden.[39]

---

http://www.regeringen.se/content/1/c6/22/76/78/7dc5b8a2.pdf

[36] http://computersweden.idg.se/2.2683/1.533435/efter-nsa--svenska-foretag-nobbar-molnet

[37] http://www.svd.se/nyheter/inrikes/danska-telenor-vill-slippa-fra_8767926.svd

[38] http://internetdagarna.se/nyheter/alla-sandningar-fran-internetdagarna-2013/

[39] http://www.dn.se/ekonomi/en-halv-miljon-kansliga-uppgifter-stals-fran-kronofogden/

Kalendarium

Integritetskonferens, 22-24 januari, 2014
Domännamnsmarknadens intresseorganisation Centr håller sitt årliga *General Assembly* i Stockholm 12-13 mars 2014
ICANN 49 i Singapore 22-27 mars, 2014
ITU World Telecommunication Development Conference (WTDC), Sharm el-Sheikh, 30 mars – 11 april, 2014
WSIS-mötet efter WTDC, 14 april 2014
Brasilien ad hoc-möte – 23-24 april Sao Paoulo, Brasilien
Stockholm Internet Forum (SIF 14), 27-28 maj 2014
ICANN 50 i London 22-26 juni 2014
ICANN 51 i Los Angeles 12-16 oktober 2014
High level WSIS +10 Review, 2014 Kairo
IGF 2014 2-5 september i Istanbul
ITU Plenipotentiary (PP) 2014: 17 oktober – 5 november Busan, Korea

Bilaga 1 – Del 5 Global avlyssning och internet-kapprustning.

I november har vi lärt oss:

- Att NSA och GCHQ använt internet för att infiltrera datorerna på forskningsavdelningen hos de oljeproducerande ländernas samarbetsorganisation (OPEC)
- Att GCHQ utvecklat särskilda metoder att hacka individuella teknikers konton på tjänsten LinkedIn
- Att även privata pengaförmedlare som exempelvis Western unions transaktioner registrerats och samlats av CIA.[40]
- Fått bekräftat att svensk FRA under lång tid haft ett utvecklat samarbete med NSA när det gäller signalspaning.
- Att SÄPO utökat sin aptit för avlyssning i Sverige genom en egen tolkning och tillämpning av datalagringsdirektivet för s.k . rättsvårdande myndigheter. Förslaget innebär att sådana myndigheter omedelbart, momentant och automatiserat ska kunna ta del av internetoperatörernas insamling av persondata i samband med telefoni och internet-trafik.[41]

Utvecklingen

Där har kommit uppgifter om att NSA och GCHQ använt internet för att infiltrera datorerna på forskningsavdelningen hos de oljeproducerande ländernas samarbetsorganisation (OPEC). GCHQ ska bl.a. lyckats skaffa sig administratörsrättigheter i OPEC:s system, och har därmed haft full tillgång till hela nätverket. Enligt artikeln finns bl.a. en rapport från 2010 där amerikanska analytiker konstaterar att Saudiarabien lämnat felaktiga uppgifter om sin oljeproduktion. Enligt artikeln är det CIA, amerikanska inrikes- och energiministeriet som är de främsta avnämarna för sådana uppgifter. Artikeln nämner inte på vilket sätt denna uppgiftsinsamling har med terroristbekämpning att göra.[42]

Washington Post rapporterade att NSA samlar närmare 5 miljarder positioneringar för mobiltelefoner per dag. Tidningen och EFF visar hur den s.k. programvaran CO-TRAVELLER fungerar.[43]

---

[40] http://www.nytimes.com/2013/11/15/us/cia-collecting-data-on-international-money-transfers-officials-say.html

[41] http://www.nyteknik.se/nyheter/it_telekom/allmant/article3784822.ece

[42] http://www.spiegel.de/international/world/how-the-nsa-and-gchq-spied-on-opec-a-932777.html

[43] http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html
http://apps.washingtonpost.com/g/page/national/how-the-nsa-is-tracking-people-right-now/634/
http://www.theguardian.com/world/2013/dec/04/nsa-storing-cell-phone-records-daily-snowden
https://www.eff.org/deeplinks/2013/12/meet-co-traveler-nsas-cell-phone-location-tracking-program

Quantum insert

Der Spiegel utvecklade också sin rapportering om intrången eller intrångsförsöken i Belgacom, den s.k. *Operation Socialist*. Där framgår hur GCHQ identifierat enskilda tekniker (t.ex. anställda hos internetleverantören Belgacom) för riktade intrång. De kandidater som valdes ut fick sina datorer infekterade med malware genom falska speglingar av tjänster som LinkedIn eller Slashdot.org. Metoden har döpts till *Quantum Insert*.[44]

Det framkom att ytterligare 33 miljoner norska mobilsamtal övervakades, enbart under loppet av en månad.[45] Det senare avfärdades av vissa som ett missförstånd.

Dagens nyheter rapporterade i början av november att FRA har, och under lång tid haft, ett långtgående samarbete med NSA. Där blev bekräftat att Sverige tillsammans med brittiska GCHQ är en av de mer offensiva lyssnarna på bl.a. Rysk internettrafik. Jfr. bilaga om avlyssningens och kapprustningens terminologi.

Reaktionerna

Europa

I Europaparlamentet publicerade en rapport om nationella program för avlyssning, och hur de förhåller sig till Europeisk lag.[46] Rapporten är viktig bl.a. för att kunna identifiera när nationella regelverk står i konflikt med varandra. Detta är också viktigt för att kunna utveckla bilaterala överenskommelser mellan länder (s.k. *improved mutual legal assistance treaty*, MLAT). Se mer nedan.

11 november höll LIBE ytterligare en hearing i raden om massavlyssning av Europeiska medborgare.[47] På talarlistan den här gången stod bl.a. en amerikansk kongressledamot Sensenbrenner, och tillika ordförande i den underkommitté som hanterar brottslighet, terrorism, homeland security etc. i USA.

Sensenbrenner vittnade om det pågående lagstiftningsinitiativ som det f.n. skissas på, kallat USA FREEDOM Act. Enlig S ska det bidra till att begränsa NSA:s rätt att samla in data i bulk, oavsett om det avser amerikanska eller icke-amerikanska medborgare. I utskottet deltog också några av de stora internetbolagen (Facebook, Google och Microsoft).[48]

---

[44] http://www.spiegel.de/international/world/ghcq-targets-engineers-with-fake-linkedin-pages-a-932821.html

[45] http://www.digi.no/924804/overvaaket-33-millioner-norske-mobilsamtaler och http://www.dagbladet.no/2013/11/19/nyheter/snowden_i_norge/innenriks/edward_snowden/glenn_greenwald/30385896/

[46] http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET%282013%29493032_EN.pdf

[47] http://www.europarl.europa.eu/document/activities/cont/201311/20131107ATT74112/20131107ATT74112EN.pdf

[48] http://www.neurope.eu/article/personal-data-protection-us-perspective

Der Spiegel rapporterade under november om försöken till att etablera ett 'icke-spioneri-avtal' mellan Tyskland och USA. Tyska tjänstemän skickades till USA angående uppgifterna om avlyssning.[49]

En kvantifiering av företagens förluster

I The Atlantic kunde vi läsa om kvantifiering av förlusterna för företag, till följd av förlorat förtroende för internet. Förlorade försäljningsintäkter ska enligt Cloud Security Alliance uppgått till 35 miljarder US$ bara för amerikanska företag, under en treårsperiod.[50] Summan ska givetvis tas med en nypa salt, men är en av troligtvis många kommande kvantifieringar.

Företagen reagerar: en uppmaning om reform av nationalstaternas övervakning

Flera stora internetföretag kom i början av december med en uppmaning till nationalstaterna om reform av internetövervakning. Det är riktigt starka företag som gått samman för en gemensam uppmaning. Där finns America online, Facebook, Google,

Företagen uppmanar:

1) att nationalstaternas regeringar själva, genom rimlig reglering ska begränsa sin egen legala förmåga att tvinga sig till användardata, så att dess uttag av internetanvändares personliga uppgifter blir balanserat, och att det ger rimligt skydd av deras integritet, och deras tillit till internet.
2) Att nationalstaternas underrättelsetjänster bara ska få samla sin information under ett tydlig legalt regelverk, där de utförande aktörerna är underkastade revision av fristående och självständiga domstolar, och att ansvarighet ska kunna utkrävas mot övervakande domstolar.
3) Allmänheten behöver ges insyn i de övervakningsprogram som sätts upp. Exempelvis behöver företag tillåtas publicera antalet rekvisitioner av användardata etc. som nationella regeringar begär, samt ändamålet för de rekvisitionerna. Regeringarna bör på eget initiativ publikt dela dessa uppgifter.
4) Regeringar bör tillåta transit av internet-trafik och bör inte begränsa åtkomst av data som lagligt tillhandahålls från andra länder. Därmed bör regeringar inte tvinga fram lokal lagring av internetdata inom respektive land.
5) Det bör finnas ett principbaserat, öppet, robust och tydligt legalt ramverk för att hantera staters rekvisitioner av data också mellan länder (improved mutual legal assistance treaty, MLAT). I de fall där lagar i olika länder står i konflikt med varandra är det viktigt att regeringarna samarbetar för att lösa sådana problem.[51]

En tolkning av detta initiativ är att konflikter i legala aspekter av internetstyrning i första hand ska lösas praktiskt och mellanstatligt, snarare än utifrån generella globala principer.

---

[49] http://www.spiegel.de/international/germany/us-declines-no-spy-pact-with-germany-but-might-reveal-snowden-secrets-a-933006.html

[50] http://www.theatlantic.com/technology/archive/2013/11/a-fraying-of-the-public-private-surveillance-partnership/281289/

[51] I egen summarisk översättning. http://reformgovernmentsurveillance.com

Författare reagerar: en uppmaning om internationell lag för att skydda digitala rättigheter

I början av december publicerade mer än 500 författare från 81 länder ett upprop[52] mot stats-sanktionerad avlyssning och internetövervakning. I uppropet uppmanas FN att skapa en internationell lag för digitala rättigheter.
I skrivande stund tycks uppropet i Sverige också publicerats i Dagens nyheters pappersupplaga, men har också letat sig in till redaktionellt material.

Där formuleras fyra tydliga argument varför det är ett problem med alltför omfattande övervakning:[53]

- *Surveillance violates the private sphere and compromises freedom of thought and opinion.*
- *Mass surveillance treats every citizen as a potential suspect. It overturns one of our historical triumphs, the presumption of innocence.*
- *Surveillance makes the individual transparent, while the state and the corporation operate in secret. As we have seen, this power is being systemically abused.*
- *Surveillance is theft. This data is not public property: it belongs to us. When it is used to predict our behaviour, we are robbed of something else: the principle of free will crucial to democratic liberty.*

[52] http://www.change.org/petitions/a-stand-for-democracy-in-the-digital-age-3

[53] http://www.change.org/petitions/a-stand-for-democracy-in-the-digital-age-3
http://www.theguardian.com/world/2013/dec/10/surveillance-theft-worlds-leading-authors
http://www.dn.se/kultur-noje/nyheter/jag-hoppas-pa-det-civila-samhallets-motstandsvilja/

Bilaga 2: Säpo vill se ett utökat och automatiserat datalagringsdirektiv i Sverige

I FRA-lagens ursprungliga utförande begränsades rätten till spaning i trafiken av internettrafik som går över Sveriges gränser.
Som poängterats tidigare finns det emellertid ingen praktisk/teknisk möjlighet att göra denna distinktion annat än *efter* att all data samlats in, i samband med, och genom analys av det digitala innehållet (s.k. *deep packet inspection*). Det betyder att för att kunna avgöra om trafiken gått över svensk gräns eller inte behöver man titta i paketen, och analysera avsändare, mottagare, och eventuellt innehållet i paketen.

Trots detta samband har alltså även SÄPO efter lagändring 2012 beretts åtkomst till FRA:s insamlade data. Det är inte offentligt vilken data SÄPO får ta del av, men eftersom signalspaning behöver ske före s.k. gallring av trafikdata, är det troligt att SÄPO får tillgång till ALL den trafikdata FRA samlar in. Det är helt enkelt mest praktiskt att samla in alla data, och därefter filtrera den.

Det nya i SÄPOs förslag kan alltså tolkas som att ännu fler myndigheter (de s.k. brottbekämpande myndigheterna) ska få tillgång också till svenska användardata. Den inhemska trafikdata som i teorin inte fick avlyssnas enligt den ursprungliga FRA-lagen (men som ändå samlas in), får nu också legalt stöd att direktanalyseras av brottsvårdande myndigheter. Därmed har man legitimerat signalspaning i all svensk trafik, såväl inhemsk som trafik som den som passerar svenska gränser. Nytt är som sagt också att denna åtkomst av data ska ske automatiserat, och tas direkt från operatören till myndigheten.

Bilaga 3 - Avlyssningens och internet-kapprustningens terminologi

Snart har vi i ett halvårs tid vecka för vecka hört nya avslöjanden om den pågående avlyssningen av nätet. Även vi som egentligen inte ville, kan nu knappast längre undvika att lära oss avlyssningens och internet-kapprustningens terminologi.

Om man exempelvis söker arbete på NSA, kan man s.a.s. direkt från hästens mun få beskrivet hur myndigheten ser på sin verksamhet. Här kan man lära om avlyssning, om offensiva attacker och om exploatering av säkerhetsbrister i andras IT-system.

Myndighetens verksamhet - Computer Network Operations (CNO) – bryts ner i tre huvudsakliga grenar:

- Attacker
- Försvar
- Exploatering

På sajten definieras de tre verksamheterna som:

Attacker	Computer Network Attack (CNA): Includes actions taken via computer networks to disrupt, deny, degrade, or destroy the information within computers and computer networks and/or the computers/networks themselves.	
Försvar	Computer Network Defense (CND): Includes actions taken via computer networks to protect, monitor, analyze, detect, and respond to network attacks, intrusions, disruptions, or other unauthorized actions that would compromise or cripple defense information systems and networks.	
Exploatering	Computer Network Exploitation (CNE): Includes enabling actions and intelligence collection via computer networks that exploit data gathered from target or enemy information systems or networks.	

Vi har redan under det gångna halvåret sett flera exempel på alla dessa fenomen, så egentligen är det mestadels terminologin som är ny. Men också bekräftelserna av det som tidigare misstänkts.

Tydligast är nog att avlyssningen bara är en liten del av det hela. Själva avlyssningen är en begränsad och passiva delmängd av något som har långt mer offensiva ändamål. *Attacker* (CNA) och *exploatering* (CNE) handlar såvitt det går att uttolka om kapaciteten att på distans förstöra infrastruktur i andra länder. I termerna ingår då rimligtvis också

traditionellt spioneri, dvs. stöld av data för att tillskansa sig främmande länders uppgifter om militära verksamheter, och i ökande grad även företagshemligheter.

När vi även väger in de andra offensiva delarna i avlyssningen ser vi med ens möjligheten att bedriva attacker över nätet (CNA), och exploatering (CNE) av exempelvis säkerhetsbrister i systemen. Det blir därför alltmer uppenbart att den kapacitetsuppbyggnad diverse myndigheter ägnar sig åt för nätet också handlar om en kapprustning, ytterst syftande till ett offensivt cyberkrig.

Med denna terminologi får vi alltså bekräftat både drivkrafter och aktörer.
De åtgärder vi ser i USA, Sverige, och andra länder handlar om målet om fullständig kontroll över nätets innehåll. Vi får ytterligare en bekräftelse på att målet är att kunna lyssna av ALL internettrafik. Tyvärr ser ingen av de drivande aktörerna något problem i detta.

De gröna hattarna (militära och halvmilitära organisationer) organiserar sig som bekant i verksamheter som attacker, försvar och exploatering. Deras drivkrafter baserade på yttre hot är alltigenom bekanta. Men till det kommer de blå hattarna (polis och rättsvårdande myndigheter), alla med varsitt behjärtansvärt ändamål för att behöva att ta del av, och samköra all vår data.
Ny teknik var häromveckan först med att avslöja SÄPOs ambitioner när det gäller datalagringsdirektivets tillämpning i Sverige. Tillsammans representerar de gröna och blå hattarna fullständig kontroll över alla våra uppgifter.

Här kommer ofta en vän av ordning in, med argumentet:
”*-Det där är ju ingen nyhet. Stater har alltid spionerat. -Jag är minsann inte en av de naiva som trodde att sådant inte skedde*”, osv. osv.

Visst är det så att signalspaning funnits också tidigare. Men det är också det mest irrelevanta argumentet av dem alla. För de som frenetiskt förfäktar att de skulle vara *naiva*, blundar därmed också för möjligheten att det går att göra något åt den uppkomna situationen.

För detta handlar inte om vad man gjort tidigare. Det handlar om vad som ska ske nu. Det handlar om användarnas integritet gentemot staters hela solfjäder av intressen. Det handlar om medborgarnas integritet över sitt elektroniska jag, kontra deras frihet. Det har tyvärr blivit så därför att det fredstida och civila samhället idag trängs i samma elektroniska infrastruktur som *det kalla krigets män*, och deras kapprustning för cyberkrig.

Därmed tillämpas ”krigets krav” också gentemot medborgarna, och trots att där inte råder krig. Därmed tillämpas polisens elektroniska spaning på alla, också de som inte ens är misstänkta för något. På grund av det får civila internetanvändare betala med sin personliga integritet, hela tiden, och varje dag. Det är vad det handlar om.