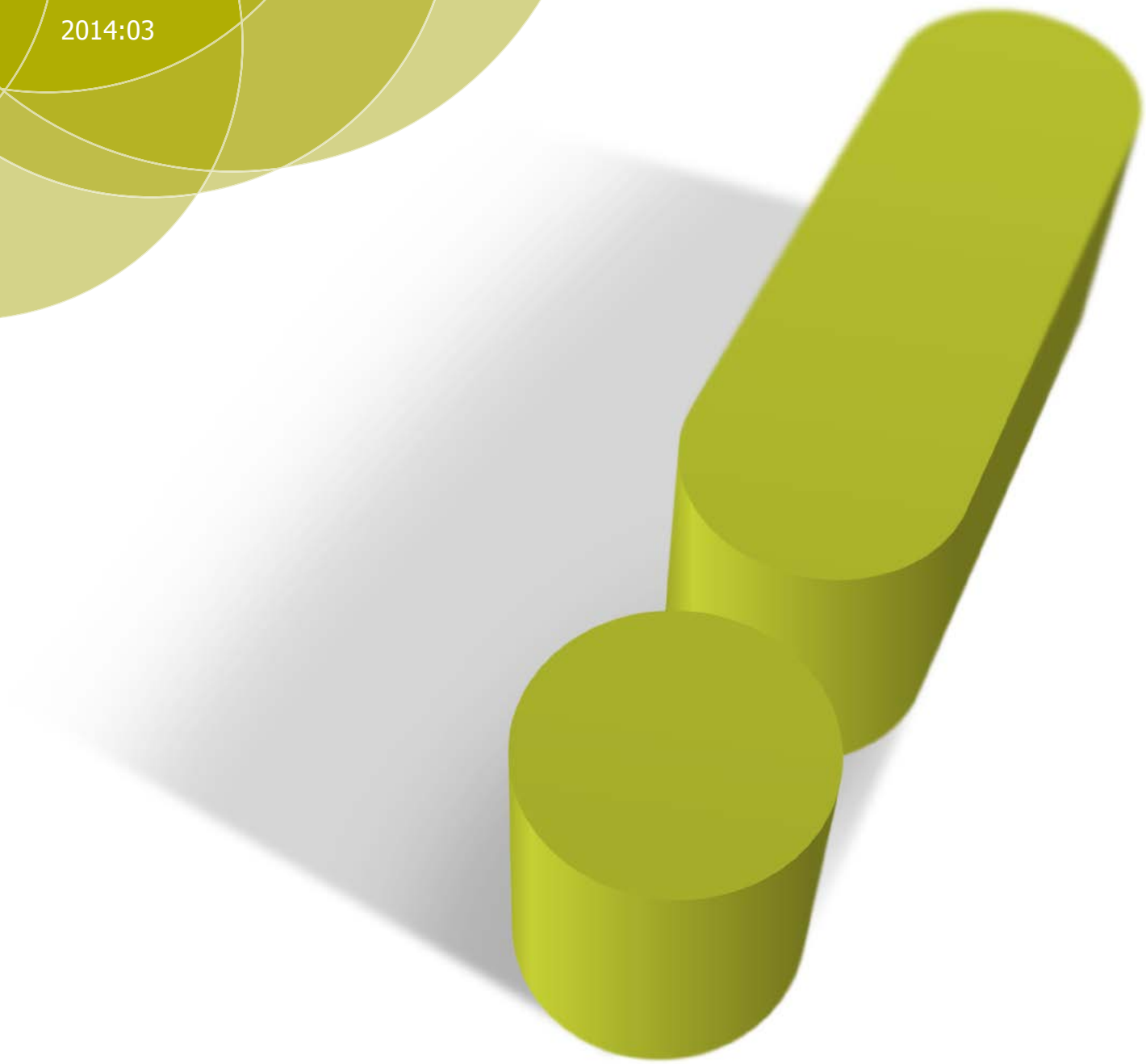
Svar Direkt
2014:03



Hänt i världen **våren 2014**

Informations- och kommunikationsteknik (IKT)

Tillväxtanalys samlar och analyserar kortfattat och två gånger per år händelser, trender och utvecklingsmönster i omvärlden som är strategiskt viktiga för Sveriges tillväxt. Underlaget är framtaget av Tillväxtanalys kontor i Brasilien, Indien, Japan, Kina, Stockholm och USA. I rapporteringen ingår också en beskrivning av utvecklingen i Sydkorea och i utvalda europeiska länder.

tillväxtanalys

Dnr: 2014/107

Myndigheten för tillväxtpolitiska utvärderingar och analyser
Studentplan 3, 831 40 Östersund
Telefon: 010 447 44 00
Fax: 010 447 44 01
E-post: info@tillvaxtanalys.se
www.tillvaxtanalys.se

För ytterligare information kontakta: Andreas Larsson
Telefon: +46 10 447 44 80
E-post: andreas.larsson@tillvaxtanalys.se

Förord

På uppdrag av Näringsdepartementet sammanställer Tillväxtanalys två gånger per år händelser, trender och utvecklingsmönster som är strategiskt viktiga för Sveriges tillväxt. Underlaget är framtaget av Tillväxtanalys utlandskontor och rapporteringen sker inom följande områden:

- Energi och hållbar utveckling
- Infrastruktur och transporter
- Innovation och näringslivsutveckling
- Informations- och kommunikationsteknik (IKT)
- Livsvetenskaper och hälso- och sjukvård
- Forsknings-, innovations- och utbildningspolitik

Denna rapport behandlar temat informations- och kommunikationsteknik (IKT). Det finns ytterligare fem rapporter, en för vart och ett av ovanstående teman. Dessa kan hämtas på www.tillvaxtanalys.se. Rapporterna har den gemensamma huvudtiteln Hänt i världen våren 2014.

Tveka inte att kontakta oss om du har frågor eller vill ha ytterligare information om någon specifik del eller fråga.

Tematiskt ansvariga:

Energi och hållbar utveckling:	Martin Flack
Infrastruktur och transporter:	Martin Flack
Innovation och näringslivsutveckling:	Andreas Larsson
Informations- och kommunikationsteknik (IKT):	Andreas Larsson
Livsvetenskaper och hälso- och sjukvård:	Martin Wikström
Forsknings-, innovations- och utbildningspolitik:	Martin Wikström

Stockholm, mars 2014

Enrico Deiaco
Avdelningschef, Innovation och globala mötesplatser
Tillväxtanalys

Innehåll

Diskussion och analys

Digitala fotavtryck- IT-användning, delaktighet och tillit

> *”Målet för IT-politiken är att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter. För att uppnå detta krävs ökad digital delaktighet så att fler vill och vågar använda digitala tjänster.”*[1]

En grundförutsättning för att öka den digitala delaktigheten är just att fler vill och vågar använda digitala tjänster. Diverse studier har visat att tillgång till dator och uppkoppling, ålder och datorvana traditionellt har varit viktiga faktorer som förklarat begränsad IT-användning, även känd som den digitala klyftan. En ny faktor som inte härrör från den traditionella digitala klyftan men som potentiellt kan påverka IT-användning negativt är bristande tillit.

Edward Snowdens avslöjande om USAs internationella övervakningsprojekt via NSA[2]och det svenska företaget Lexbase[3] som sålde uppgifter om personer som dömts för brott är två exempel som kan skada tilliten till IT. Spaningarna i denna rapport indikerar att attityder till IT-användning, övervakning/säkerhetspolicy, internationella samarbeten, förändrad lagstiftning, trans-border data flow, market of trust och internet goverance i stort är några områden som kommer att stå på framtida dagordningar hos regeringar världen under år framöver.

Några konkreta internationella utblickar i denna rapport är[4]:

- Indien: Den nationella säkerheten (terrorhot) väger tyngre än rätten till personlig integritet- befolkningen står bakom behovet av övervakning.
- Japan: Snabb utveckling mot digitala kontanter leder även till diskussion om hantering av personlig information.
- Sydkorea: Rekordstort dataläckage leder till lagändringar.
- USA: Efter ett antal uppmärksammade dataintrångsskandaler lanserar administrationen flera cybersäkerhetsinitiativ för att stärka områden som får utökad relevans i en alltmer digitaliserad ekonomi.
- Kina: 18:e centralkommitténs tredje plenum yttrar en vilja att utöka möjligheter att övervaka och styra innehåll på internet.
- Frankrike: Landet betraktar cybersäkerhet som centralt för den nationella säkerheten, i paritet med väpnade konflikter eller terrorism.
- Storbritannien: Snabb utveckling inom öppna data får en backlash inom vårdområdet.

Samtidigt som det finns många exempel på incidenter så är det alltjämt uppenbart att molntjänster/distribuerad datalagring, öppna data, stora data och samkörning av databaser

[1] http://www.regeringen.se/sb/d/2373
[2] National Security Agency, NSA
[3] Lexbase var/är en svensk webbplats och databas som möjliggjorde att allmänheten kunde söka efter personer och företag som har varit föremål för juridisk prövning i svenska tingsrätter med flera domstolar mot betalning. Företaget använde sig av som använde sig av svenska tryckfrihetsförordningen, rätten till allmänna handlingar, offentlighetsprincipen och utgivningsbevis på ett tvivelaktigt sätt.
[4] (för längre beskrivningar, se separata landkapitel)

har stor potential att förenkla, förbättra och effektivisera samhällsservice till medborgare och företag. Många länder mobiliserar därför resurser för att skydda medborgare och företag med målet att få full utväxling på de tekniska framstegen ovan.

I exemplen från USA och Kina förefaller tilliten till IT dock tillta trots otalet incidenter. I Indien har man pekat ut IT-säkerhet som ett tillväxtområde/exportområde. På internationell statsnivå kan konstateras att cybersäkerhet står på många agendor när regeringschefer träffas. Internationella samarbeten kring cybersäkerhet mellan stater formeras men även friktion uppstår på regeringsnivå då exempelvis USA anklagar Kina för att flera dataintrång skulle vara uppbackade av den kinesiska staten.

1 Indien: Informationssäkerhet och informationstrygghet – medborgarförtroende, molntjänster och övervakning

I takt med utvecklingen av molntjänster och ökad tillämpning av Big Data-analyser höjs röster som betonar vikten av att utveckla lagstiftningen för att skydda den personliga integriteten.[5] Värnandet av den personliga integriteten är dock ett ämne som är förhållandevis frånvarande i den offentliga debatten. När säkerheten på internet diskuteras sker det ofta genom att frågan om att skydda vitala samhällsfunktioner från cyberangrepp uppmärksammas, liksom att cyberangrepp inte drabbar all den kommersiella verksamhet som äger rum på internet.

Ny lag förbereds för att värna den personliga integriteten

I Indien finns i dagsläget vad som kallas Security Practices Rules, en kontroversiell regel, som ger indiska myndigheter rätt att begära ut personlig information från företag, exempelvis mobiloperatörer eller internetförmedlare. Regeringen är dock i färd med att utarbeta ny lagstiftning avsedd av skydda den personliga integriteten men arbetet går mycket långsamt och det är inte troligt att det utkast som finns kommer att godkännas av Indiens lagstiftade församling innan valet till det nya parlamentet äger rum, vilket sker under april och maj. Få detaljer om det nya lagförslaget avseende den så kallade Privacy Bill är kända men vad som dock står klart är att tanken är att den nya lagen ska ges tolkningsföreträde över de andra 58 lagarna som är aktiva idag och som i någon bemärkelse berör integritetsfrågor. Vidare ska värnandet om den nationella säkerheten väga tyngre än rätten till personlig integritet.[6]

Frågan om personlig integritet handlar dels om vilken övervakning staten ska få ägna sig åt, dels vilken information företag har rätt att samla in och hur denna information sedan används. När det gäller utarbetandet av Privacy Bill kan även nämnas att en expertgrupp, tillsatt av Indiens Planeringskommission, i oktober 2012 presenterade sitt slutbetänkande med förslag på hur ovanstående frågor ska kunna hanteras.[7] Expertgruppens utredning skulle samtidigt fungera som underlag för det fortsatta arbetet med lagförslaget, ett arbete som leds av Department of Personnel and Training (DOPT) vid Ministry of Personnel, Public Grievances and Pensions. I dess slutrapport föreslog expertgruppen att en så kallad integritetskommissionär (Privacy Commissioner) inrättas på federal och regional nivå samt ett system för gemensam reglering, med vilket avses ett system där organisationer (industrisammanslutningar exempelvis) ges möjlighet att själva utarbeta standarder för att värna den personliga integriteten, vilka måste godkännas av ovan nämnda integritetskommissionär. Expertgruppen rekommenderade även begränsningar vad gäller företags rätt att samla in personlig information och hur denna information sedan används. Ett system där individer ges möjlighet att godkänna vilken information som samlas in

[5] Behovet av lagstiftning för att värna den personliga integriteten uppmärksammades exempelvis i samband med NASSCOM:s konferens "Big Data and Analytics Summit 2013", i Hyderabad, 27 juni 2013

[6] http://articles.economictimes.indiatimes.com/2013-12-02/news/44657689_1_privacy-bill-law-ministry-draft-bill

[7] Press Information Bureau, Government of India, 16 oktober 2012, "Group of Experts on Privacy Submit Report", tillgänglig på: http://pib.nic.in/newsite/erelease.aspx?relid=88503 För hela rapporten, sehttp://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

föreslås också. I och med att utkastet till Privacy Bill inte har offentliggjorts än är det oklart i vilken omfattning dessa förslag har vunnit något gehör.

Omfattande internetövervakningssystem införs

Under tiden som arbetet med ny integritetslagstiftning pågår har regeringen beslutat inrätta olika typer av system för internetövervakning och informationsinhämtning i stor skala. Som exempel kan nämnas National Intelligence Grid (NATGRID)[8] som lanserades i maj 2013 av Ministry of Home Affairs i samarbete med National Institute of Smart Government, liksom inrättandet av vad som i Indien kallas Centralised Monitoring System (CMS) som bland annat syftar till att bevaka landets mobil- och internettrafik.[9] Ett tredje exempel på övervakningssystem går under benämningen Netra och inriktas på att övervaka internettrafik som går via Skype, e-post och sociala medier som Facebook och Twitter exempelvis. Netra har utvecklats av Centre for Artificial Intelligence and Robotics (CAIR), en enhet inom Indiens Defence Research and Development Organization (DRDO).[10] Regeringen motiverar dessa övervakningssystem bland annat med behovet att motverka att sociala medier används för att piska upp våldsinriktade stämningar som sätter olika etniska och religiösa grupper emot varandra. Den här företeelsen vill man motverka och ökad internetövervakning skulle kunna vara en möjlighet att åstadkomma det.[11]

I den indiska debatten upptar inte integritetsfrågor särskilt stor uppmärksamhet även om enskilda händelser bidrar till att öka uppmärksamheten något. Som exempel kan nämnas arresteringen av två unga kvinnor 2012 efter att de på Facebook hade ifrågasatt begravningsarrangemanget för en hindunationalistisk ledare och det faktum att Mumbai i det närmaste stannade upp helt under den tid begravningen pågick. Efter protester släpptes de två och brottsmisstankarna (att ha uttryckt sig på ett sätt som kunde väcka anstöt och skapa hat och illvilja mellan klasser) avskrevs.

Den massiva övervakning som Edward Snowden blottlagt har inte heller fått särskilt stor uppmärksamhet. Detta sammantaget kan tolkas som att integritetsfrågor inte intar samma centrala plats i människors medvetande i Indien som i andra delar av världen, exempelvis i Nordamerika och Europa. En möjlig förklaring är att Indiens säkerhetspolitiska verklighet, med den överhängande risken för terrordåd, gör att människor faktiskt föredrar en omfattande övervakning om det bidrar till att upprätthålla säkerheten. En annan förklaring skulle kunna vara att relativt få människor känner sig berörda, internetanvändningen uppgick i slutet av förra året till endast 16 procent av befolkningen, det vill säga 200 miljoner människor. Den siffran väntas öka till 243 miljoner under 2014.[12]

När det gäller inställningen i fråga om personlig integritet och IT-säkerhet i allmänhet är det även viktigt att kort nämna det indiska personnummersystemet Aadhar (även kallat Unique Identification, UID). I slutet av det här året beräknas 700 miljoner indier ha ett Aadhaarnummer och tanken är att det ska vara möjligt att utnyttja flera förvaltningstjänster via internet med hjälp av detta unika nummer. Det ska dels vara möjligt att öppna bankkonton och utföra bankärenden med hjälp av Aadhar, dels vara möjligt utnyttja e-

[8] http://mha.nic.in/pdfs/NATGRID-050613.pdf
[9] http://pib.nic.in/newsite/erelease.aspx?relid=54679
[10] http://www.livemint.com/Politics/To4wvOZX7RmLM4VqtBshCM/India-to-deploy-Internet-spy-system-Netra.html
[11] http://timesofindia.indiatimes.com/tech/social-media/Government-planning-to-monitor-Facebook-Twitter-Shinde/articleshow/29005580.cms
[12] http://timesofindia.indiatimes.com/tech/tech-news/internet/With-243-million-users-by-2014-India-to-beat-US-in-internet-reach-Study/articleshow/25719512.cms

förvaltningstjänster. I takt med att fler och fler övergår till att använda internet samtidigt som fler och fler tjänster möjliggörs via Aadhaar är det troligt att kraven på skydd av den personliga integriteten också kommer att öka, liksom krav att säkerhetsåtgärder vidtas för att exempelvis undvika identitetsstölder på internet. En annan viktig utveckling som säkerligen kommer att bidra till att öka medvetenheten om frågor rörande den personliga integriteten är den ökande användningen av elektroniska patientjournaler inom den indiska sjukvårdssektorn.

Big Data-analyser viktiga under indisk valrörelse

Vid sidan av dessa tre mer eller mindre hemliga program för internetövervakning rapporteras i indisk media att både det regeringsbärande Kongresspartiet och det största oppositionspartiet, Bharatiya Janata Party (BJP), satsar stora resurser på att analysera väljarnas beteenden med hjälp av Big Data-analyser. Syftet är att kartlägga vilka politiska frågor som väljarna inom specifika valkretsar tycker är särskilt angelägna för att sedan paketera ett politiskt budskap som tilltalar dessa väljargrupper. Denna typ av informationsinhämtning är inte helt oproblematisk och givetvis finns risken att information som erhålls genom Big Data-analyser kan komma att missbrukas i andra sammanhang.

National Cyber Security Policy 2013 införs

2013 lanserades Indiens nya National Cyber Security Policy. Policydokumentet innehåller ett antal målsättningar, dock inga detaljerade handlingsplaner som anger hur dessa mål ska uppnås. Exempelvis anges att Indien bör sträva efter att utbilda 500 000 säkerhetsexperter inom IT-frågor under de kommande fem åren och att inhemskt producerad utrustning bör upphandlas för användningsområden som är av betydelse för den nationella säkerheten (det preciseras dock inte vilka områden som avses). Vidare betonas vikten av internationella samarbeten liksom fortsatt forskning och utveckling inriktad på cybersäkerhet.[13]

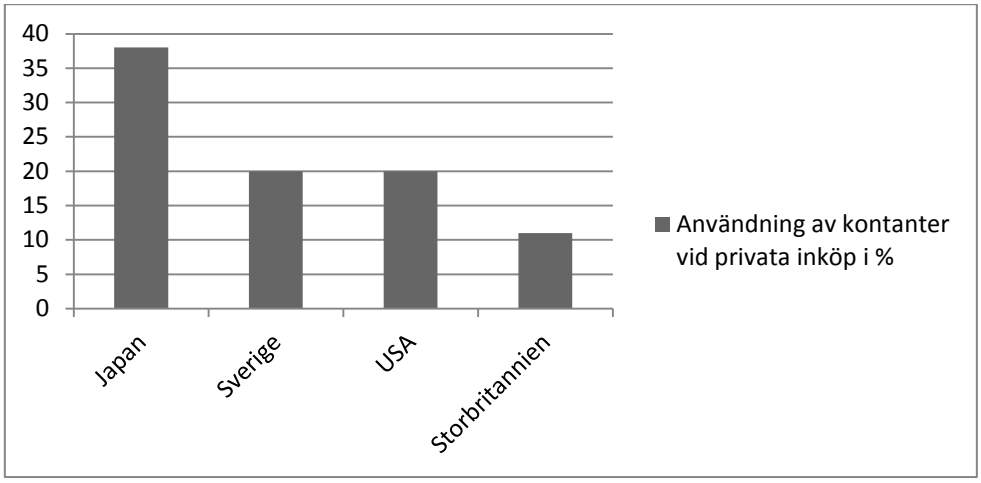
När det gäller internationella samarbeten kan nämnas att Storbritannien och Indien förra året beslutade att inrätta en gemensam arbetsgrupp för att bekämpa IT-brottslighet. Samarbetet mellan brittiska och indiska myndigheter ska stärkas för att skydda båda parter från cyberattacker. Cybersäkerhet var också ett ämne som berördes när Sydkoreas och Japans regeringschefer, var för sig, besökte New Delhi tidigare i år.[14]

[13] http://deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf
[14] Se http://www.mea.gov.in/bilateral-documents.htm?dtl/22752/India+Republic+of+Korea+Joint+Statement+for+Expansion+of+the+Strategic+Partnership respektive http://www.mea.gov.in/bilateral-documents.htm?dtl/22772/Joint+Statement+on+the+occasion+of+Official+Visit+of+the+Prime+Minister+of+Japan+to+India+January+2527+2014

2 Japan: Snabb utveckling mot digitala kontanter leder till diskussion om hantering av personlig information

Trots att Japan på många sätt kan anses vara ett modernt land nära teknikens framkant är betalning med kontanter ett vanligt inslag i vardagen. Användningen av betal- och kreditkort är lägre än i många andra utvecklade länder. Därför står den kraftiga ökningen av betalningar med digitala kontanter, ”e-pengar” ut i färsk statistik. De digitala kontanterna är laddade på ett återuppladdningsbart kort, ett kontantkort, som utnyttjar NFC-teknik (där NFC står för Near Field Communication) och används för att betala tåg-, buss- och tunnelbaneresor samt varor i vissa dryckes- eller godisautomater och livsmedelsbutiker. Mellan januari och november 2013 skedde 3040 miljoner transaktioner, vilket är en ökning med 21 procent från föregående år. Det totala värdet av dessa betalningar/transaktioner översteg 200 miljarder SEK (3000 miljarder JPY). Enbart i Tokyoregionen finns mer än 43 miljoner kort registrerade. Ur ett tillitsperspektiv kan framgången härledas till att NFC-tekniken och dessa digitala kontanter möjliggör ett snabbare och kontaktlöst alternativ till vanliga kontanter, kredit- och betalkort.

Paradoxalt nog kan den höga graden av tillit mellan medborgare i Japan även ge en förklaring till den fortfarande höga andelen kostsam kontanthantering. Enligt Mastercard betalas fortfarande 38 procent av privata handelstransaktioner med kontanter och det kan presenteras ett flertal skäl till denna höga nivå av kontantanvändning. Om vi jämför Japan med andra länder finner vi exempelvis att i Sverige och USA används cirka hälften så mycket kontanter som i Japan, det vill säga i 20 procent av fallen.



Figur 1 Användning av kontanter vid privata inköp

Ett av de starkare argumenten till den stora förekomsten av kontantbetalningar i Japan är att landet är mycket säkert, bortsett från risken för eventuella naturkatastrofer. Att det är säkert att vistas utanför hemmet, utan risk för rån, gör att många vågar ha på sig kontantmängder som skulle vara svårmotiverade i andra länder. Tilliten till sina medmänniskor kan därmed anses vara hög och användningen av kontanter riskfri.

Ett annat troligt skäl till att kredit- och betalkort inte är vanligt förekommande är den betydande mängden mindre butiker och restauranger som existerar i landet. Dessa har inte möjlighet att förhandla sig till låga hanteringsavgifter för kort, vilket gör att många näringsidkare troligtvis väljer bort alternativet helt. På ett närliggande spår kan det även tänkas att kontanters svårighet att spåras lockar vissa typer av företagare till att endast ta emot kontanta betalningar.

Nu övergår dock Japan på relativt kort tid till en mer digital pengahantering, i storstad såväl som på landsbygd. Det sker utmed ett spår som är ganska unikt i en värld som domineras av de stora kreditkortsföretagen. Japanska konsumenter ser många fördelar med e-pengar jämfört med traditionella betalkort, och nya incitamentssystem testas löpande av kortutgivarna. Den uppenbara fördelen är att betalningarna som tidigare nämnts sker snabbt och kontaktlöst. Användarna begränsar dessutom sin utsatthet för stölder till enbart det belopp som faktiskt finns på kortet, vilket kan jämföras med ett i japanska ögon mer riskabelt kreditkort med belåningsmöjligheter. I Sverige kan det dras paralleller till de bankkontor som inte hanterar kontanter: utsätts de för rån är den finansiella skadan minimal i jämförelse med de eventuella konsekvenserna om ett kontanthanterande kontor utsätts.

Ett annat incitament till att använda e-betalning är de bonusprogram med återbäring direkt på kortet som vissa livsmedelsbutiker erbjuder. Genom att kortet direkt laddas med återbäringen behöver kunden inte hålla reda på eventuella bonuscheckar vilket underlättar bonusprogrammets användning ur kundens perspektiv. Ett annat exempel på fördelarna med kontantkorten är kopplade till den i april i år planerade momshöjningen från 5 till 8 procent. Flera av de företag som är ansvariga för lokaltrafiken i Tokyoregionen har exempelvis bestämt att kontantpriset ska öka med 10 JPY (cirka 60 öre), medan trafikanter som betalar med hjälp av e-pengar endast ser en ökning på 1 JPY (cirka 0,6 öre) för samma sträcka.

Användandet av kort laddade med e-pengar generar mycket data då inte bara pris, tid och inköpsställe loggas. Även ålder, kön och ID-nummer loggas då detta är registerat på kortet. Brist på tydliga lagar och regler hejdar dock nya affärsmöjligheter relaterade till denna typ av data, exempelvis försäljning av den. Idag gällande lag förbjuder exempelvis att persondata delges till en tredje part utan individens medgivande. Däremot är det oklart vad lagen säger om delgivande av anonymiserad data, där den personliga informationen tagits bort. Denna brist på tydliga regler har gjort många företag motvilliga till att utnyttja den data de har tillgång till. Den japanska regeringen avser att förenkla och förtydliga lagar och därmed göra det lättare för företag att kapitalisera på sina data, men lagförändringar lär komma tidigast 2015. Ett av de nya lagförslagen innebär att anonymiserad data ska kunna erbjudas till tredje part utan individens medgivande men att det då sedan tidigare finns ett generellt medgivande. Personer som inte vill att information om deras inköp delas till tredje part ska inte heller riskera att detta sker.

Trots otydliga lagar har försäljning av data redan skett. I juli 2013 sålde Japans största tågoperatör East Japan Railway Company (även känt som JR East) anonymiserad information om sina passageras resehistorik till bland annat Hitachi, ett stort elektronikföretag som är verksamt inom onlinetjänster och databehandling. Detta var första gången som information om digitala transaktioner sålts till tredje part, vilket startade en debatt på både bloggar och Twitter kring individens rätt till anonymitet och vikten att omöjliggöra igenkänning vid försäljningar likt den som nämns ovan. Hitachi hävdade att data enbart rörde passagerarstatistik och att allt därför gått rätt till. Eftersom lagen ännu är

otydlig, är det oklart vilken sida som har rätt; de som sålt och köpt informationen eller de som känner att privatpersoners integritet kan ha rubbats. Oavsett vilket gick köpet igenom. Det har i efterhand kritiserats av både politiker och privatpersoner eftersom användare av kortet inte haft möjlighet att ge sitt medgivande till försäljningen av dennes information.

3 Sydkorea: Rekordstort dataläckage leder till lagändringar

Sydkorea har nyligen skakats av det största läckaget av personlig information någonsin. Den 8 januari greps en IT-entreprenör anklagad för att ha stulit personlig information från cirka 20 miljoner sydkoreanska kreditkortsanvändare – nästan hela den arbetsföra befolkningen i landet. Läckaget omfattade inte bara finansiella data utan även en del av de ytterligare personuppgifter som bankerna lagrar om sina kortinnehavare. IT-entreprenören arbetade för Korea Credit Bureau, ett företag anlitat av banker för att beräkna kreditrisker, då han under ett års tid hämtade ut den känsliga informationen med hjälp av ett enkelt USB-minne. I princip alla landets banker drabbades eftersom de delar mycket informationen om sina kunder, och det blev smärtsamt klart hur tillgängligt och känsligt det finansiella systemet är för attacker. Att även uppgifter om bankkunder utan kreditkort ingick i den läckta informationen ökade känslor av både otrygghet och förvåning.

Det är svårt att avgöra den negativa effekten på tilliten till de finansiella institutionerna och myndigheterna samt val av IT-lösningar detta dataintrång har haft eftersom tilliten under normala fall inte mäts regelbundet och systematiskt i stor skala. De inblandade bankerna har dock drabbats då kunder börjat säga upp sina kreditkort. Under de första tre dagarna efter skandalen hade cirka 2,6 miljoner personer avslutat sina kreditkonton.

Myndigheternas svar på dataintrånget har varit kraftigt för att snabbt återställa tilliten till elektroniska betalningar i det sydkoreanska samhället. Sydkorea har flest (fem) antal kreditkort per person i världen. Regeringen har tillsatt en arbetsgrupp för att se över de nuvarande reglerna för skydd av personliga data samt för att föreslå skärpta sanktioner mot företag med bristande IT-säkerhet. Det har redan annonserats att Sydkoreas finansiella tillsynsmyndighet ska kunna skicka inspektörer till finansiella företag för att undersöka deras interna kontrollsystem för IT-säkerhet.

Skandalen visar dock på de inneboende begränsningarna även i de allra senaste säkerhetssystemen. En enskild betrodd person med så enkel teknik som ett USB-minne kunde relativt snabbt skapa stor skada. Trots att det sedan 2012 finns en lag som kräver kryptering av databaser hos de flesta finansiella företag har kryptering inte använts i det aktuella fallet. Det leder till frågor om hur myndigheter ska kunna bli bättre på att stödja eller tvinga företagen till bättre förvaltning. Inom kort förväntas lagändringar med kraftigt skärpta straffsatser, med 10-årigt fängelsestraff om man läcker personlig finansiell information, och böter motsvarande en procent av företagets årsomsättning för företag som använder sådan information. Under 2015 kommer dessutom Finansinspektionen att lansera ett Financial Security Center vilket ska verka för att skydda finansiella kunder och företag från intrång och stöld.

Frågan är öppen om i vilken utsträckning tillsynsmyndigheter ska kunna sätta upp krav på ny säkerhetsteknik på privata företag. Mer indirekta incitament kan finnas för hur staten reglerar ansvarsfrågan efter att ett brott uppstått. Om ett företag har varit proaktivt och kan visa att det med hjälp av egenvald ny teknik försökt skydda sina kunder, ska företaget kunna få lättade sanktioner och ett starkare försvar mot eventuella stämningar i efterdyningarna.

Vid diskussioner om datasäkerhet och tillit bör poängteras att alla läckage inte grundar sig i kriminellt uppsåt, utan kan handla om rent slarv. Avsiktliga eller oavsiktliga läckor

orsakade av anställda eller betrodda affärspartners och konsulter är fortfarande en av de största säkerhetsriskerna. Sydkorea har efter en genomgripande lagändringsprocess under 2011 beskrivits ha Asiens strängaste lagstiftning inom personuppgiftsskydd, vilken inte gör några undantag för läckage på grund av misskötsel. I ett uppmärksammat fall från 2013 dömdes en av landets största telekomoperatörer för ett dataläckage som varken orsakats av kriminella avsikter eller av företagets avsiktliga försummelse, utan av slarv och misskötsel av personuppgifter.

Kan staten ses som yttersta garant för att personliga data inte läcker ut och missbrukas? Frågan är inte oproblematisk. Ett belysande exempel är den sydkoreanska regeringens nya policy för att öka statsförvaltningens användning av cloud computing, där privata företag i allt högre utsträckning ansvarar för driften. Regeringen har tydligt signalerat att de vill främja tillväxten av högt förädlade tjänstebranscher med tillväxtpotential, och då särskilt cloud computing. Ministry of Science, ICT and Future Planning la därför under våren fram en strategi där offentliga organisationer rekommenderas att använda molntjänster som tillhandahålls av privata företag, med mål att minst 15 procent av offentliga organisationer ska använda sig av privata molntjänster år 2017. Tidigare har huvudargumentet för att använda enbart den statliga plattformen för molntjänster, G Cloud, varit just frågetecken om IT-säkerhet.

En ytterligare dimension av frågan om tillit är att inte enbart se till digital kommunikationsteknik, utan hur den grundläggande tilliten mellan medborgare och den offentliga sektorn ser ut. I Sydkorea är den lägre än i Sverige, vilket regeringen vill ändra på. Personliga kontakter mellan myndighetshandläggare och medborgare sker i högre utsträckning i Sydkorea och andra asiatiska länder, jämfört med Sverige, e-förvaltningens uppenbara kostnadsfördelar till trots. Personliga möten är i teorin ett effektivt sätt att bygga tillit. När nya program – till exempel nationellt skattefinansierat småföretagsstöd – lanseras, budgeteras genomgående för fysiska kontor utspridda över landet, med personal för att kunna genomföra personliga möten. En tolkning av en sådan kostsam strategi är att dessa kontor ur ett tillitsperspektiv är nödvändiga som komplement till e-tjänster.

Under våren har i Sydkorea förts en intensiv debatt om regelverket för telemedicin kan ändras för att bättre ta tillvara förutsättningarna i ett av världens mest uppkopplade länder. Relationen mellan läkare och patient har kulturellt varit helt baserad på personliga möten, vilket också återspeglas i lagstiftningen. Patientkontakter via videomöten har hittills inte varit tillåtna, vilket nu Ministry of Health vill se över. Det återstår att se om fördelarna för medborgare på landsbygden, som idag har sämre tillgång till vård, kommer överbrygga den kulturella preferensen att besöka ett sjukhus. Fokus i vården i Sydkorea håller på att ställa om från att behandla patienter till att hålla individer friska, så lagändringen kommer åtminstone att innebära förbättrade möjligheter för insamlandet av data via telemedicintjänster för förebyggande insatser.

En debatt länkad till frågor om tillit som är mer avsevärt mer dämpad, vilket kanske förvånar en svensk betraktare, rör den sydkoreanska statens internetcensur. Det är ett faktum att Sydkorea är världsledande inom bredbandspenetration, men medborgarna har inte tillgång till ett fritt och ofiltrerat innehåll på internet. Sydkorea rankas högt när World Wide Web Foundation (WWWF) årligen mäter internetanvändning inklusive till exempel e-förvaltningstjänster, men med ett undantag i form av “freedom and openness.” I WWWF:s senaste rapport varnas landet igen som liggande i riskzonen för ”överdriven övervakning av medborgare” baserat på flera dokumenterade fall där myndigheter systematiskt men till synes godtyckligt övervakar personlig kommunikation mellan

individer och att ha försökt dämpa politisk diskussion. Sydkoreas regering har en bred strategi för reglering av specifikt innehåll på internet, vilket har inneburit en censur av debatt särskilt runt inhemska valresultat och relationer med Nordkorea. Ett betydande antal webbplatser som regeringen anser vara subversiva eller socialt skadliga är helt blockerade, och möjligheter att föra fram åsikter anonymt är inskränkta. Trots en stark befintlig yttrandehetslagstiftning åberopar ansvariga myndigheter i fråga om filtrering av internet särskilda lagar för att skydda ungdomar, nationell säkerhet, och andra nationella områden där statens intressen är stora.

4 USA: Cybersäkerhet en prioriterad fråga

Administrationen lanserar flera cybersäkerhetsinitiativ efter ett antal uppmärksammade dataintrångsskandaler för att stärka områden som får utökad relevans i en alltmer digitaliserad ekonomi.

Enligt World Economic Forum genomgår 70 procent av världens stater fortfarande en digitaliseringsprocess[15]. I kontrast till den digitala utvecklingen står den moderna statens förmåga att etablera ett försvar mot cyberattacker och minimera risker i cyberrymden.

Legislativa åtgärder är i USA fortfarande begränsade, dock har de uppmärsammade incidenterna lyft frågor kring cybersäkerhet högt på den politiska agendan och administrationen har under året lanserat flera initiativ för att förebygga cyberattacker. I Obamas memorandum *Science and Technology Priorities for the FY 2014 Budget*[16] framhålls exempelvis forskning i enlighet med strategin *Trustworthy Cyberspace*[17] som ett område myndigheter förväntas prioritera i sina respektive budgetar under det kommande året.

I USA har flera dataintrångsincidenter förekommit som fått internet att framstå som ett mindre tillförlitligt medium för transaktioner, och kan begränsa allmänhetens tillit till IT-lösningar. I början av året annonserade till exempel två stora företag, varuhuskedjorna Target och Nieman Marcus, att de blivit utsatta för cyberattacker där kontokortsuppgifter stulits. Attacken uppskattats ha drabbat över 110 miljoner kunder. USA som i dag svarar för 27 procent av världens korttransaktioner står för hela 47 procent av världens kortbedrägerier. Kontokortsfiske har enligt konsultföretaget Celent ökat med 70 procent från 2004 till 2010[18]. USA är idag ett av de få länder som fortfarande tillåter kontokort med magnetremsa medan andra länder tenderar att över gå till EMV technologi (chip).

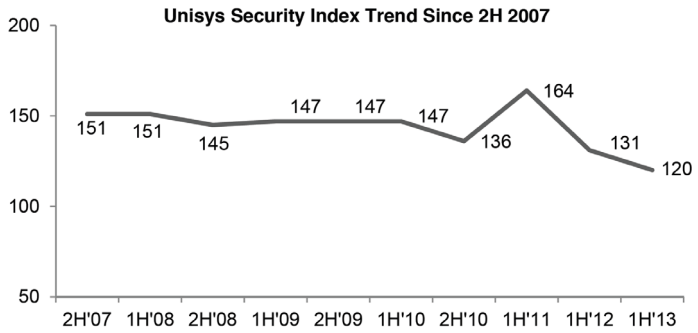
Advanced Persistent Threat (A.P.T) är ett begrepp som cirkulerar bland säkerhetsexperter och används för att beskriva mer riktade cyberattacker. A.P.T. associeras med de attacker som allokerats till kända kinesiska IP-adresser och ansetts ligga bakom flera dataintrång mot västerländska journalister och nyhetsbyråer[19]. Flera amerikanska nyhetsbyråer har i början av året meddelat att de blivit angripna, bestulna på inloggningsuppgifter och lösenord. Presidenten gjorde i mars förra året ett uttalande och påpekade att flera dataintrång är statsstödda. Detta har sedan dåvarande utrikesminister Clinton och dåvarande försvarsminister Panetta tagit upp vid möten med motparter i bland annat Kina. Potentiellt kan de nyligen uppmärksammade attackerna skada en redan skör diplomatiskt relation.

Med bakgrund i dessa uppmärksammade dataintrång finns det anledning att tro att allmänhetens förtroende för internet potentiellt skulle kunna minska.

Unisys Security Index[20] presenterar ett sammanvägt index kring individers oro för brister i frågor kopplade till nationell, finansiell personlig- och cybersäkerhet. Indexet visar för

[15] Georgetown Journal of International Affairs: International engagement on cyber part III: State building on a new frontier (2014)
[16] http://www.nitrd.gov/pubs/2014supplement/FY2014NITRDSupplement.pdf
[17] http://www.whitehouse.gov/sites/default/files/m-12-15.pdf
[18] http://www.nytimes.com/2014/01/24/business/neiman-marcus-breach-affected-1-1-million-cards.html?_r=1
[19] http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&_r=1&
[20] Unisys Security Index: http://www.unisyssecurityindex.com

närvarande en relativt måttlig grad av oro hos den amerikanska befolkningen. Historiskt sett har indexet präglats av en konstant nedåtgående trend sedan 2007, med undantag för år 2011. Kontokortsbedrägeri och identitetsstöld är de två primärt bidragande orosfaktorerna medan faktorer kopplade till nationell och personlig säkerhet är förhållandevis konstanta.



Figur 2. Källa: http://images.politico.com/global/2013/06/03/unisys_sec_index_201305.html

Trots flera skandaler kring dataintrång som uppmärksammats mycket i media verkar dessa alltså inte ännu ha resulterat i någon mer allmän ökad oro, eller minskad tillit till IT transaktioner.

Legislativa åtgärder på cyberområdet har varit begränsade, bland annat beroende på förra årets budgetlåsning, men även oenigheter i kongressen kring en konkret lagstiftning som bland annat 2013 stoppade *The Cyber Intelligence Sharing and Protection Act*. Obama har dock på egen hand konkretiserat USA:s arbete kring cybersäkerhet genom att bland annat utfärda *executive order 13636* för att stärka infrastrukturens motståndskraft emot cyberattacker i brist på lagstiftning, där myndigheter inom ramen för sina ordinarie mandat, åläggs att göra mesta möjliga för att stärka skyddet mot cyberattacker[21].

Detta görs dels genom ökat informationsutbyte mellan offentliga och privata aktörer och dels genom ett ramverk för cybersäkerhet innehållande metoder, praxis, procedurer etcetera.

Informationsutbytet skall förbättras genom att federala myndigheter genom ordern åläggs att ta fram offentliga rapporter kring hot mot amerikanska infrastrukturföretag. Genom ordern expanderades också programmet *Enhanced Cybersecurity Services*[22] ett sammarbetsprogram mellan DHS kommersiella it-företag till att omfatta fler aktörer. Programmet syftar till att effektivisera incidentrapportering så att cyberattacker kan uppmärksammas nästintill i realtid.

Vidare gavs *National Institute of Standards and Technology* (NIST) i uppdrag att leda arbetet med att ta fram ett ramverk, tillsammans med aktörer från det privata näringslivet, för hur den kritiska infrastrukturen bäst ska kunna skyddas mot cyberattacker. Resultatet publicerades den tolfte februari. Cybersecurity Framework 1.0 är ett generiskt ramverk som skall betraktas som ett levande dokument baserat på god praxis och internationellt framtagna standarder. Ramverket skall hjälpa organisationer att själva utarbeta ett effektivt skydd emot cyberattacker. Bland annat genom att; dokumentera cyberaktivitet, överse

[21] Executive Order 13636—Improving Critical Infrastructure Cybersecurity. National Archives and Aministration Register Vol.78. No.33.
[22] http://www.dhs.gov/privacy-documents-national-protection-and-programs-directorate-nppd

rådande skydd, kontinuerligt göra riskbedömningar och utarbeta ett effektivt verktyg för att kommunicera suspekt cyberaktivitet till andra aktörer.

Ingen enskild händelse återspeglar kanske övervaknings- och cybersäkerhetsfrågor mer än Edward Snowdens avslöjanden kring NSA och GCHQ:s mycket omfattande övervakning- och datainsamling. President Obama gjorde den 17:e januari ett uttalande som klargjorde att det inte finns några ambitioner att begränsa den amerikanska underrättelsetjänstens befogenheter att samla in och analysera data. Samtidigt understryker administrationen ändå vikten av att de medborgerliga fri- och rättigheterna inte kränks av de åtgärder som vidtas[23]. Statliga insatser kommer däremot riktas för att säkerhetsställa att datainsamlingen sker enligt föreskrifterna som The United States Foreign Intelligence Surveillance Court (FISC) utfärdar, meddelade presidenten.

Den uppmärksammade NSA skandalen har resulterat i en grupptalan den tolfte februari då den republikanska senatorn Rand Paul tillsammans med FreedomWorks direktör Matt Kibbe lämnade in en stämningsansökan. Stämningsansökan ifrågasätter lagligheten i insamlandet av metadata från telefonregister och data som bedrivs enligt programmet *sektion 215.* Direktörerna för National Intelligence, FBI och NSA anklagas för att ha inkräktat på det fjärde tillägget i den amerikanska konstitutionen.

Med bakgrund i det nyligen avslöjade omfattande kontokortsfisket har de två fall som tilldelats störst medial uppmärksamhet resulterat i en diskussion kring vilka åtgärder som bör vidtas för att stärka det rådande konsumentskyddet. Drabbade parter vittnade i januari inför Senatens bankomitté om att det idag existerar relativt få medel och åtgärder för att bekämpa och förebygga cyberattacker och lyfter särskilt frågan kring effektiva antivirusprogram samt EMV-technologi. En fråga som troligtvis kommer adresseras av den lagstiftande församlingen under kommande år. Mastercard meddelade i mitten av januari att ambitionen är att övergå till EMV innan slutet av år 2015[24].

[23] http://www.scientificamerican.com/article/snowden-speaks-nsa-whistleblower-addresses-sxsw/
[24] Mastercard. Chris McWilton, President North American Markets. Public letter. January 8, 2014

5 Kina – en vilja att utöka möjligheter att övervaka och styra internet

Antalet internetanvändare i Kina har ökat explosionsartat under det senaste decenniet. Idag har fler än 600 miljoner kineser tillgång till internet – och antalet förväntas växa till 800 miljoner fram till år 2015. Tillväxten har varit möjlig genom stora satsningar på bredband och under senare år också på mobilt internet. Staten ser utveckling av IKT som nödvändig för fortsatt tillväxt och höjd innovationsförmåga. Utbyggnaden leder också till helt nya möjligheter för debatt och informationsspridning i ett samhälle där andra informationskanaler är helt eller delvis under statlig kontoroll. Regeringen arbetar aktivt för att även internet ska hamna under statens jurisdiktion. Staten motiverar sin kontroll över internet med att de vill bringa lag och ordning och skapa tillit till information och tjänster på nätet. Samtidigt är det omöjligt att blunda för att samma teknik används för att begränsa det fria ordet på internet.

Statens roll på internet

I den 12:e femårsplanen mellan 2011–2015 är IT-industrin utpekad som en av sju strategiskt viktiga industrier. IT-lösningar ses som ett viktigt verktyg för möta de många utmaningar Kina står inför och att skapa en väl utvecklad IKT-infrastuktur ses som avgörande för att höja landets teknicknivå och innovationsförmåga. Samtidigt är det fria ordet problematiskt för regeringen. Ledningen ser det som sin rättighet att styra och administrera internet innanför Kinas gränser.[25] Parallellt med utbyggnaden av internet har en omfattande kontrollapparat byggts upp. Statens huvudsakliga metod för att kontrollera innehållet på internet är den Gyllene skölden, populärt kallad ”the Great firewall”, vilken sköts av Ministeriet för offentlig säkerhet. Genom en rad tekniker, bland annat IP blockering, DNS filtrering och URL filtrering ger systemet långtgående möjligheter att kontrollera vad som publiceras på internet. En stor del av censuren sköts också av internetföretag och internetleverantörer vilka aktivt censurerar innehållet på sina egna servrar, detta för att tillmötesgå myndigheternas krav.

Censur och styrning grundar sig på nio principer vilka riktar in sig mot aktiviteter som staten ser som oönskade på internet. Aktiviteter ska stoppas om de:

1. Motverkar de grundläggande värderingarna i konstitutionen
2. Utmanar landets säkerhet, läcker statshemligheter, försöker att störta den politiska makten samt motverkar enigheten i landet.
3. Skadar den nationella äran och de nationella intressena
4. Underbygger hat mot folkgrupper, etnisk diskriminering samt motverkar den nationella enigheten i landet.
5. Motverkar den religiösa politiken i landet samt hjälper till att sprida onda sekter samt ”feodala” vidskepligheter
6. Sprider rykten, uppmuntrar till illegala folksamlingar, stör ordningen i samhället och motverkar stabiliteten i landet

[25] http://english.gov.cn/2010-06/08/content_1622956.htm

7. Sprider oanständigheter, pornografi, dobbel, våld, terrorism eller uppmanar till brott eller handel samt produktion av illegala produkter och smuggelgods.
8. Förtalar eller kränker andra samt kränker andra människors legala rättigheter. Felaktigt utger sig för att vara tjänsteman från statsorgan, offentlig organisationer eller annan juridisk person
9. Anses förbjudet enligt lag eller andra administrativa regler

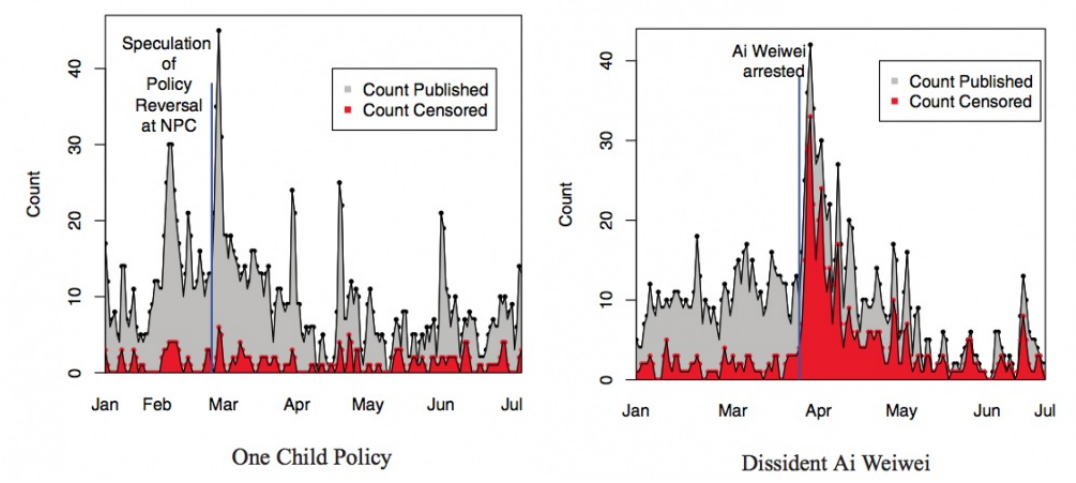
Regelverket öppnar upp för omfattande kontroll över internet. Endast en del av syftet är att kontrollera kritik mot staten och partiet. Styrningen ger också staten möjlighet att kontrollera aktiviteter som är reglerade i övriga samhället som till exempel spel om pengar. Att ”städa upp” på internet och inkludera internet under statens jurisdiktion är ett uttalat mål. Under 2013 genomfördes en kampanj mot ”ryktesspridning” på internet.[26] Kampanjen kritiserades för att vara en ny form av begränsningar av yttrandefriheten. Samtidigt menades från officiellt håll att syftet var att hålla personer ansvariga för vad de skriver på internet och att skapa tillit till information som sprids på internet. I den officiella retoriken heter det att man arbetar för att bevara den allmänna ordningen och stabiliteten i landet.

Hur kinas internetcensur faktiskt fungerar[27]

Att kinesiska regeringen ägnar sig åt att censurera internet är välkänt. Hur censuren faktiskt fungerar och vad den riktar in sig på har dock varit omdebatterat bland akademiker. I två studier som publicerades under 2013 lät Harvardprofessorn Gary King testa den kinesiska censuren för att bättre förstå logiken bakom den. I ett första test lät King samla in och analysera 11 miljoner inlägg på kinesiska sociala medier. Inlägg i 85 kategorier samlades in innan de hunnit censureras. Inläggen återbesöktes senare för att se om de blivit borttagna eller ej. Inläggen som samlades in spände över ett brett område från känsliga ämnen så som oroligheter i Inre Mongoliet till mer oskyldiga ämnen så som fotbolls-VM och trafikstockningar i Peking. I en andra studie publicerade King och hans kollegor över 1000 egna inlägg på kinesiska sociala medier för att bekräfta sina resultat från den första studien.

Kings slutsats är att det övergripande målet för den kinesiska internetcensuren inte är riktat mot kritiska åsikter. Istället ligger fokus på att stoppa folkliga aktioner, oavsett om de är kritiska mot ledningen eller ej. Bara att omnämna folkliga samlingar i någon form resulterar i omedelbar censurering. Precis som på andra platser i världen fluktuerar antalet poster stort över tid. Normalt censurerades omkring 10-15 procent av posterna i de utvalda ämnena inom 24-timmar efter postning. Men då intresset ökar kring ett ämne och detta bedöms kunna leda till folkliga åsiktsyttringar stiger andelen censurerade inlägg. I figur 3 ser vi hur detta händer efter Ai Weiweis arrestering då andelen censurerade inlägg steg till över 50 procent. Samtidig fanns ingen sådan ökning av andelen censurerade inlägg efter rykten om avskaffande av ettbarnspolitiken. King menar att detta beror på att den senare inte riskerade att trigga folkliga protester trots att en majoritet av inläggen var kritiska mot ettbarnspolitiken.

[26] Se Tillväxtanalys kvartalsrapport nummer 3, 2013.
[27] http://harvardmagazine.com/2013/09/reverse-engineering-chinese-censorship



Figur 3 Andel censurerade inlägg på sociala medier varierar kraftigt beroende på den bedömda risken för folkliga åsiktsyttringar. Källa: Harvard Magazine

Diskussion

Trots att kinesiska myndigheter idag redan har omfattande möjlighet att övervaka och styra internet visar beslut från artonde centralkommitténs tredje plenum en vilja att utöka dessa möjligheter. Skrivelsen är visserligen mycket vagt formulerad när det gäller vilka utökade befogenheter man söker, men ger ändå en viktig inblick i hur den kinesiska ledningen ser på internet och vad som oroar den. Centralkommittén menar att statens kontroll inte har hunnit med den snabba utvecklingen och internet alltjämt får större inflytande i samhället. Ett specifikt fokus i skrivelsen är att bygga upp ”ett robust system för att kontrollera plötsliga händelser på internet”, vad som åsyftas är förstås till viss del öppet för tolkning men det är inte långt borta att tänka på den typ av hastiga internettrender som King undersökt.

Kina har hittills visat att det faktiskt går att kontrollera informationen på internet i stor skala. Tekniken kan beskrivas som ett ”adaptiv auktoritärt styre” där myndigheterna fokuserar på att med kraft begränsa oönskade inslag på internet. Parallellt med detta tillåts den största delen av aktiviteterna på internet fortgå utan större statlig inblandning. Den kinesiska regeringen vill på detta sätt använda tekniken till sin fördel. Om detta är hållbart i längden återstår att se.

6 Frankrike: ny nationell IT-säkerhetsstrategi

Frankrike betraktar cybersäkerhet som centralt för den nationella säkerheten, i paritet med väpnade konflikter eller terrorism.

I Frankrike har diskussionen kring IT-säkerhet, ofta med nationella förtecken, varit ganska intensiv sedan Le Monde publicerade uppgifter från Edward Snowden som bland annat visade hur amerikanska NSA bedrivit industrispionage emot franska företag.[28]

Reaktionerna från franska politiker och företag på avslöjandena har varit upprörda, och regeringen har lovat att snabba upp åtgärderna för att stärka den franska nationella IT-säkerheten. Den 17 februari presenterade den franske premiärministern Jean-Marc Ayrault en nationell strategi för ”cybersäkerhet” för att möta vad regeringen anser vara ett växande IT-säkerhetshot i världen. I strategin definierar man det som en ”central strategisk utmaning” att säkra informationssystemen för det som klassas som sektorer av vital betydelse för Frankrike. Dessa specificeras i strategin som:

- **Statlig verksamhet**: statens civila och militära verksamhet, rättsväsendet, rymdverksamhet samt forskning.
- **Skydd för medborgarna**: verksamheter som rör hälsa, livsmedels- och vattenförsörjning.
- **Viktig ekonomisk och social infrastruktur**: energi, elektroniska kommunikationer, massmedia, transportinfrastruktur, finanssektorn och industrin.

Enligt strategin ska den franska IT-säkerhetsmyndigheten ANSSI förstärkas med 100 anställda under 2014 (från dagens 350 personer), och ytterligare 50 under 2015. Under perioden 2014–2019 anslås vidare cirka en miljard euro[29] för försvarsmakten till investeringar för att stärka Frankrikes cybersäkerhet och cyberförsvar. Regeringen betraktar risken för angrepp på franska informationssystem som en central säkerhetsfråga, i klass med risken för väpnad konflikt eller terrorism.

Premiärministern har ANSSI till sitt förfogande för att utforma IT-säkerhetspolitiken och för att samordna statens insatser. I händelse av en allvarlig kris har premiärministern fyra nya befogenheter på området:

1. Fastställa nödvändiga säkerhetsregler för att skydda informationssystemen hos organisationer inom sektorer av vital betydelse (definierade enligt ovan).
2. Få rapportering om IT-incidenter som rör dessa sektorer.
3. Kontrollera säkerhetsnivån hos informationssystemen inom sektorerna.
4. Besluta om säkerhetsåtgärder som organisationerna i sektorerna måste implementera i händelse av en allvarlig IT-kris.

För att säkra statliga informationssystem innehåller strategin krav på att statliga IT-system ska vara krypterade. I upphandling av IT-säkerhetsprodukter och -tjänster måste statliga organisationer välja sådana som är certifierade av ANSSI. För franska e-posttjänster och meddelandehantering som går över franskt territorium krävs också kryptering.

[28] Se bland annat Tillväxtanalys kvartalsrapport nummer 3, 2013.
[29] Motsvarande knappt nio miljarder kronor.

Utöver de statliga åtgärderna pläderade premiärministern för behovet av en ledande IT-säkerhetsindustri. I oktober 2013 initierades en ”kommitté för säkerhet i industrikedjan”, vars syfte är att underlätta dialog mellan den offentliga och privata sektorn för att stärka medborgarnas säkerhet och näringslivets konkurrenskraft. IT-säkerhet utgör också en av de 34 prioriterade områden som pekas ut i den nya industripolitiska plan som lanserades av president Hollande i september 2013.[30] Regeringen har också särskilt pekat ut IT-säkerhet som ett forskningsområde som ska bli föremål för riktade utlysningar av forsknings- och investeringsmedel.

Frankrike har länge varit kritiskt gentemot USA:s dominans av styrningen av internet. När han presenterade den franska IT-säkerhetsstrategin poängterade premiärminister Ayrault igen att Frankrike vill se en stark och ambitiös politik inom Europa som syftar till att göra Europa ”autonomt på det digitala området”, så att man inte behöver förlita sig på utomstående aktörer för att lagra och hantera data som tillhör europeiska företag och medborgare.

[30] ”Plan de la Nouvelle France industrielle” presenterades översiktligt i Tillväxtanalys kvartalsrapport nummer 3, 2013.

7 Storbritannien: samlat system för digitala sjukjournaler fördröjs efter oro om datasäkerheten

Storbritanniens snabba utveckling inom öppna data får en backlash inom vårdområdet.

Under 2013 lanserades planer på att patientjournalerna inom det engelska sjukvårdssystemet NHS ska göras tillgängliga i ett samlat digitalt system. Bland fördelarna med det centraliserade systemet framhålls till exempel möjligheterna för behandlande läkare att få tillgång till patientens samlade sjukdomsbild, utan att denna själv har en sådan fullständig överblick. En minst lika viktig fördel ska vara att systemet möjliggör forskning och uppföljning av till exempel effekter och biverkningar av läkemedel samt effektuppföljningar av olika medicinska behandlingsformer.

Reaktionerna på systemet har emellertid inte varit odelat positiva. Framför allt har kritiken rört integritetsfrågor kopplade till det centraliserade systemet. För att bemöta kritiken skickade NHS ut en informationsbroschyr med titeln ”Better Information Means Better Care” till 26 miljoner hushåll i England under februari. Informationen presenteras också på en webbsida på NHS webplats.[31] Det finns en möjlighet för enskilda patienter att välja att inte få sina uppgifter registrerade i det centraliserade systemet. Undersökningar av mottagarna visar att en stor del av hushållen inte tagit till sig information om att man kan välja att inte få sina data registrerade eller hur man ska gå till väga för att göra det.[32]

Även privata vårdgivare kopplade till NHS ingår i systemet, vilket innebär att patientdata delas över organisationsgränser. För att kunna dra nytta av de samlade datamängderna ska även andra organisationer än vårdutförare kunna få tillgång till data, däribland universitetsforskare men även försäkringsbolag och läkemedelsföretag, efter ansökan till den nya myndigheten Health and Social Care Information Centre (HSCIC).

Om ansökan godkänns ska externa parter få tillgång till informationen i systemet. Informationen ska avidentifieras, men inte tillräckligt för att göra den helt anonym – ”pseudonymisering” är ett begrepp som används. Om ett företag har egna medicinska data som kan matchas mot de data man får ut från HSCIC är det teoretiskt möjligt att återidentifiera den data man får ut. Parlamentsledamoten David Davis är en av kritikerna av systemet, och använde sig själv som exempel: ”Jag har brutit näsan fem gånger. Om man vet det är jag förmodligen i en grupp med högst 100 personer i England. Om man sedan vet när jag blev vaccinerad mot difteri, normalt vid födseln, så är det bara jag kvar. Det är helt klart att människor kan identifieras genom dessa data.”[33] Davis kritiserar också att polisen ska få tillgång till hälsouppgifter om brottsmisstänkta i systemet utan särskilt domstolsbeslut, även om de valt att inte registreras.

Det centrala registret kommer att innehålla information från primärvård och sjukhus, och innefatta uppgifter om bland annat psykisk ohälsa, förskrivna läkemedel samt rök- och alkoholvanor. Kritiker menar att om man gör sådana uppgifter tillgängliga för exempelvis

[31] http://www.nhs.uk/NHSEngland/thenhs/records/healthrecords/Pages/care-data.aspx
[32] http://www.independent.co.uk/life-style/health-and-families/health-news/victory-for-privacy-as-nhs-database-is-delayed-9137136.html
[33] http://www.theguardian.com/society/2014/feb/06/police-backdoor-access-nhs-health-records

försäkringsbolag så kommer det att påverka hur öppenhjärtiga patienter kan vara mot sin husläkare.

Efter den starka kritiken meddelade NHS i februari att man fördröjer starten för det centraliserade systemet. Istället för den planerade starten i april kommer man nu att vänta till hösten med att samla informationen. Den extra tiden ska NHS använda för att bättre informera allmänheten om fördelarna med ett centraliserat system, vilka säkerhetsmekanismer som finns i systemet samt hur man kan välja att inte få sina data registrerade.

www.tillvaxtanalys.se

Tillväxtanalys, myndigheten för tillväxtpolitiska utvärderingar och analyser, är en gränsöverskridande organisation med 60 anställda. Huvudkontoret ligger i Östersund och vi har verksamhet i Stockholm, Brasilia, New Delhi, Peking, Tokyo och Washington D.C.

Tillväxtanalys ansvarar för tillväxtpolitiska utvärderingar, analyser och internationellt kontaktskapande och därigenom medverkar vi till:

- stärkt svensk konkurrenskraft och skapande av förutsättningar för fler jobb i fler och växande företag
- utvecklingskraft i alla delar av landet med stärkt lokal och regional konkurrenskraft, hållbar tillväxt och hållbar regional utveckling

Utgångspunkten är att forma en politik där tillväxt och hållbar utveckling går hand i hand. Huvuduppdraget preciseras i instruktionen och i regleringsbrevet. Där framgår bland annat att myndigheten ska:

- arbeta med omvärldsbevakning och policyspaning och sprida kunskap om trender och tillväxtpolitik
- genomföra analyser och utvärderingar som bidrar till att riva tillväxthinder
- göra systemutvärderingar som underlättar prioritering och effektivisering av tillväxtpolitikens inriktning och utformning
- svara för produktion, utveckling och spridning av officiell statistik, fakta från databaser och tillgänglighetsanalyser
- tillhandahålla globala mötesplatser och främja internationellt kontaktskapande inom tillväxtpolitiken

Svar Direkt:
Här redovisar Tillväxtanalys de uppdrag myndigheten får i dialog med våra uppdragsgivare och som ska redovisas med kort varsel.

Övriga serier:
Rapportserien – Tillväxtanalys huvudsakliga kanal för publikationer.
Statistikserien – löpande statistikproduktion.
PM – metodresonemang, delrapporter och underlagsrapporter är exempel på publikationer i serien.

Tillväxtanalys Studentplan 3, 831 40 Östersund
Telefon: 010 447 44 00 | info@tillvaxtanalys.se | www.tillvaxtanalys.se