The New York Review of Books

**De svenska kungarna av cyberkrig**

*Hugh Eakin*

Den 24 april 2013, bara några veckor innan Edward Snowden gick ut offentligt med sina läckor om massövervakning av National Security Agency (NSA), välkomnade General Keith B. Alexander, dåvarande chef för NSA, en grupp svenska underrättelsetjänstemän till ett hemligt tredagarsmöte på NSA-högkvarteret i Fort Meade, Maryland. I delegationen ingick Ingvar Åkesson, mångårig chef för Sveriges Försvarets radioanstalt (känd som FRA), en ljusskygg svensk statlig underrättelsetjänst, och fem medlemmar av Åkessons högre stab. Ett av syftena med mötet var att diskutera Sveriges ökande betydelse för NSA.

I en lag från 2008 hade FRA fått utökade befogenheter av den svenska regeringen att dammsuga upp all kommunikation som reser över fiberoptiska nät till och från Sverige - inklusive e-post, textmeddelanden och telefonsamtal. Detta var av stort intresse för NSA, inte minst eftersom en stor andel av den ryska kommunikationen gick via Sverige. År 2011 började svenskarna dela sina övervakningsdata med NSA, som inkluderade - som NSA-tjänstemän beskrev det vid tidpunkten för mötet - en "unik samling [av kommunikationsdata] om högprioriterade ryska mål som ledarskap, inrikespolitik och energi."

NSA-tjänstemän noterade den svenska spionbyråns ovanliga tekniska förmågor och rykte för sekretess och såg det också som en idealisk samarbetspartner på sitt hacknings- och cyberkrigsprojekt, kallat Quantum. Ett av Quantum-programmen var en ambitiös operation som heter WINTERLIGHT, som syftade till att i hemlighet hacka sig in i utländska datorer och datornätverk med högt värde för att få inte bara kommunikationsdata utan också all information som lagras på hårddiskarna eller servrarna i fråga. Möjliga mål kan vara administratörer av utländska datanätverk, ministerier, olje-, försvars- och andra stora företag, samt misstänkta terroristgrupper eller andra utsedda individer. Liknande Quantum-operationer har riktat sig mot OPECs högkvarter i Wien, liksom Belgacom, ett belgiskt telekombolag vars kunder inkluderar Europeiska kommissionen och Europaparlamentet.

Enligt NSA-dokument använde sig WINTERLIGHT av en komplex attackstrategi för att i hemlighet implantera ett skadligt program på måldatorn eller nätverket som var aktuellt. NSA:s skadliga program skulle sedan avleda alla signaler mellan dessa datorer och Internet via "oseriösa" (rougue) höghastighetsövervakningsservrar, kallade "FoxAcid" -servrar, vilket möjliggjorde för NSA att i hemlighet få tillgång till nästan alla användarens personuppgifter - och till och med att manipulera data som överfördes från en användare till en annan. Konsekvenserna för både spioneri och offensiva cyberoperationer var omfattande. *Wired* har beskrivit hur attacken mot den belgiska telekomsektorn kunde [kartlägga] de digitala spåren av utvalda arbetare, identifiera IP-adresserna [internetprotokoll] för arbets- och persondatorer samt Skype, Gmail och sociala nätverkskonton som Facebook och LinkedIn. Sedan skapade de förfalskade sidor, som var värd på FoxAcid-servrar, för att till exempel efterlikna en anställds legitima LinkedIn-profilsida.

*[text under foto: President Barack Obama med dåvarande Sveriges utrikesminister Carl Bildt på Stockholm Arlanda Flygplats, september 2013. Vid en gemensam presskonferens samma dag med dåvarande statsminister Fredrik Reinfeldt diskuterade Obama NSA:s övervakning.]*

Intressant nog var WINTERLIGHT en gemensam insatts mellan NSA, den svenska FRA och brittiska GCHQ, men det verkar som om hackerattacker mot datorer och datanätverk har initierats av svenskarna. FRA satte upp implantaten på riktade datorer - känd i NSA-språk som "tippning"– för att omdirigera deras signaler till övervakningsservrarna, vilket möjliggjorde för GCHQ och NSA att få tillgång till deras data i vad som kallas "skott". Vid tidpunkten för mötet i april 2013 rapporterade NSA att "förra månaden fick vi ett meddelande från vår svenska partner att GCHQ fick FRA QUANTUM-tips som ledde till 100 skott."

Sedan de extraordinära avslöjandena om att den ryska regeringen försökte påverka det amerikanska presidentvalet 2016 med information hackad från datorerna i den demokratiska nationella kommittén och högt uppsatta demokratiska tjänstemän har cybersäkerhet blivit en brådskande nationell prioritet. Som amerikanska tjänstemän påpekar är DNC-hackningen bara den senaste i en accelererande serie av Ryssland-kopplade cyberattacker riktade mot politiska och andra institutioner i väst, inklusive den estniska regeringen och media 2007, den tyska förbundsregeringen (Bundestag) 2015, Ukrainas elnät 2015 och svenska medier i mars 2016. Mycket mindre noterat har dock varit i vilken utsträckning USA själv har samordnat med Sverige och andra allierade för att utveckla hacknings- och övervakningsverktyg som är mycket mer avancerade än de e-post "phishing"-strategier som används i de senaste ryska attackerna. Ett viktigt mål för denna teknik är Ryssland själv.

NSA-tjänstemän beskriver sina svenska motsvarigheter som "extremt kompetenta, tekniskt innovativa och pålitliga" och berömde dem för att vara "skickliga i att samla in en mängd olika kommunikationer." Noterbart är att svenska FRA hade fått tillgång till NSA:s mest kraftfulla analysverktyg, kallat XKeyscore, som enligt NSA:s dokument gör det möjligt att hämta "nästan allt en användare gör på Internet" från massövervakningsdata.

NSA noterade vidare i sin rapport från april 2013 att FRA "fortsätter att få tillgång till mer data från ytterligare telekommunikationsföretag" och att ny svensk lagstiftning också hade gett FRA utökade befogenheter att bekämpa terrorism. Enligt den amerikanska byrån hade FRA:s breda spelrum gjort Sverige till en mer pålitlig övervakningsallierad än Storbritannien. Ett dokument om NSA: s WINTERLIGHT-program rapporterar att "fortsatt GCHQ-engagemang kan vara i fara på grund av brittiska juridiska- / policybegränsningar, och i själva verket har NSA: s mål hela tiden varit ... ett bilateralt avtal med den svenska partnern."

I början av juni 2013, mindre än sex veckor efter att den svenska delegationen besökte Fort Meade, publicerades de första rapporterna om NSA:s spioneri baserat på Edward Snowden-läckorna i *The Guardian* och *The Washington Post*. Under de följande veckorna och månaderna utlöste Snowdens avslöjanden om NSA:s globala övervakningsinsatser, och i synnerhet dess program för massinsamling av data, kallat PRISM, en utdragen debatt i USA och fick slutligen kongressen att genomföra nya restriktioner för NSA 2015. Liknande granskning gjordes av Storbritanniens GCHQ och dess eget program som heter TEMPORA, som syftade till att direkt ansluta sig till de transatlantiska fiberoptiska kablar för att fånga upp vad *The Guardian* beskrev som "stora mängder globala e-postmeddelanden, Facebook-inlägg, internethistorik och samtal", som den delade med NSA. Men kontroversen slutade mestadels där.

I redogörelsen som framkom i den brittiska och amerikanska pressen framställdes NSA- och GCHQ-programmen i allmänhet som farliga avvikelser - fall av omfattande underrättelseöverskridande av de två mäktigaste regeringarna i västalliansen. I den mån kontinentaleuropeiska regeringar nämndes var det som offer för brittiskt och amerikanskt spioneri: målen för den ena eller den andra hade inkluderat Frankrikes presidentpalats och, mest notoriskt, den tyska förbundskanslern Angela Merkels mobiltelefon. Men tänk om vissa europeiska regeringar själva bedrev massinsamling av data om privata medborgare, med exakt samma metoder - och kanske med ännu mindre tillsyn?

Medan mycket fortfarande är oklart om det svenska programmet, väcker FRA: s status som en av NSA: s mest uppskattade utländska partners stora frågor om huruvida de amerikanska och brittiska ansträngningarna var så ovanliga. Även om det knappast har nämnts i internationell press, har Sveriges avancerade internet-avlyssningssystem noterats av självaste Snowden. I ett videoinspelat vittnesmål till Europaparlamentet i mars 2014 sa Snowden: "När det gäller frågan om massövervakning är skillnaden mellan ... NSA och [svenska] FRA inte en fråga om teknik, utan snarare om finansiering och arbetskraft." (FRA har för närvarande en budget på cirka 100 miljoner dollar och cirka 700 anställda; NSA tros ha en budget på cirka 10 miljarder dollar och mer än 30 000 anställda.)

Svenska tjänstemän har inte gjort några offentliga uttalanden om WINTERLIGHT-hackningsprogrammet, men i juli 2013, när Tyskland och Frankrike pressade EU att hålla samtal med amerikanska tjänstemän för att lära sig mer om NSA-spionering i Europa, gick Sverige med Storbritannien i veto mot flytten och hävdade att EU inte hade någon befogenhet att diskutera frågor om nationell säkerhet och underrättelse.

*[Text under foto: Ingvar Åkesson, chef för Sveriges Försvarets Radioanstalt (FRA) från 2003 till 2013. I april 2013 deltog han i ett hemligt tre dagars möte med dåvarande NSA-direktören Keith Alexander i Fort Meade, Maryland, för att diskutera Sveriges ökande betydelse för NSA.]*

På senare tid har den nuvarande svenska regeringen, under ledning av Socialdemokraterna, erkänt att Sverige bedriver "offensiv" cyberkrigföringsförmåga - vilket skulle inkludera hackning - samt teknik för att försvara sig mot cyberattacker. "Snowden-dokumenten bekräftade att det finns ett mycket intensivt samarbete mellan Sverige och USA", berättade Mark Klamberg, en svensk rättsspecialist som har skrivit om FRA-lagen. "Överst har du NSA, och under det har du GCHQ, och under det har du... Sverige."

I själva verket har Sverige gått i spetsen för en snabb expansion av statlig övervakning i norra Europa. Sedan Snowdens vittnesmål har Europa upplevt flera terroristattacker, rekrytering av tusentals medborgare som utländska stridande i Syrien och en bredare motreaktion mot invandrare och asylsökande. Under de senaste månaderna har länder som Frankrike och Tyskland till Nederländerna, Österrike, Danmark, Finland och Norge övervägt eller antagit lagstiftning som syftar till att möjliggöra ökad övervakning av deras befolkningar.

Den 17 november antog det brittiska parlamentet Investigatory Powers Act, vilket legaliserar en mängd olika hacknings- och spionageaktiviteter av den brittiska regeringen; *The Guardian* har beskrivit det som att det ger "de mest omfattande övervakningsbefogenheterna i västvärlden." Och med den tillträdande administrationen av Donald Trump som talar om en storskalig expansion av nationella säkerhetsprogram i USA, inklusive en möjlig återgång till massinsamling av telefondata av NSA – vilket påstås ha övergivits i NSA-reformen från 2015 - kan de avancerade västerländska demokratierna vara på väg in i en ny era av hemlig regeringsövervakning.

I många avseenden framstår Sverige som ett osannolikt land att leda detta angrepp. Den svenska staten anses allmänt vara en modellsocialdemokrati och är känd för sitt förespråkande av mänskliga rättigheter, dess breda skydd av sociala friheter, dess regering genom konsensus och dess expansiva välfärdsstat. I motsats till USA och Storbritannien har nationell säkerhet aldrig varit en överordnad angelägenhet: Sverige har följt en politik av officiell neutralitet i mer än tvåhundra år, det tillhör inte Nato, och det har bara haft en marginell del i "kriget mot terrorismen". Under en stor del av det senaste decenniet har den svenska regeringen också varit en ledande förespråkare för internetfrihet i utvecklingsländerna, vilket den hävdar är ett centralt inslag i demokratin.

Med uppkomsten av Internet befann sig FRA - en spionbyrå som ägnar sig åt radio, radar och annan "signalspaning" – i fara att bli föråldrad. I början av 2000-talet började man utveckla teknologi för att avlyssna de fiberoptiska undervattenskablar som nästan alla interkontinentala e-postmeddelanden, telefonsamtal och annan kommunikation nu går igenom, och 2007 och 2008 föreslog den svenska regeringen, då ledd av de borgerliga Moderatpartiet, lagen som ger FRA bred tillgång till kabeltrafik. Spionbyrån skulle även kunna lagra metadata som den extraherade - enligt uppgift på en enorm databas som heter Titan - i ett år. Vid den tiden hölls det offentliga protester på Riksdagens trappor och grupper som USA-baserade Electronic Frontier Foundation föreslog att sådana omfattande övervakningsbefogenheter skulle vara oöverträffade. Men i juni 2008, efter att regeringen gjort några eftergifter, inklusive inrättandet av en hemlig tillsynsdomstol, passerade lagen snävt och debatten slutade i stort sett.

Fem år senare, när en svensk tv-kanal avslöjade Snowden-dokumenten som visade Sveriges omfattande samarbete med NSA för att spionera på Internetanvändare - och till och med hacka sig in i deras datorer - var svaret dämpat. Till skillnad från i USA hölls inga parlamentariska utfrågningar. Enligt Klamberg, en

svensk rättslärd, förblir riksdagsledamöter i mörkret om många aspekter av FRA-programmet och det kan fortfarande finnas brist på medvetenhet om dess omfattning. "När lagstiftningen antogs", sa han, "var budskapet att den var väl reglerad och att endast små mängder data skulle lagras. Men när jag studerar lagen och läser rapporterna från den svenska Datainspektionen framträder bilden motsatt: övervakningen och lagringen av data är enorm, särskilt när det gäller metadata."

För NSA och GCHQ, hävdar andra analytiker, har FRA-lagen gett en täckning för övervakningsprogram med tvivelaktig laglighet. Den 21 december ställde sig EU-domstolen på utmanarnas sida mot svepande lagar i Sverige och Storbritannien som kräver att telekomföretag lagrar samtal och textmeddelanden och fann att "EU-lagstiftningen utesluter nationell lagstiftning som föreskriver generell och urskillningslös lagring av data." Observatörer har noterat likheter mellan den vagt formulerade FRA-lagen och en amerikansk lag som kallas FISA Amendments Act, som också antogs 2008 och som NSA har citerat som rättslig grund för sitt eget PRISM-program. Den svenska regeringen har också varit skicklig på att undvika granskning av sitt övervakningssamarbete med USA, kanske genom att hålla några av dessa arrangemang informella. (Enligt ett diplomatiskt telegram publicerat av Wikileaks, när en amerikansk delegation besökte Sverige i november 2008 för att försöka ingå ett underrättelsesamarbetsavtal, tvekade svenska justitiedepartementet att säga ja och hävdade att "befintliga informella kanaler, som täcker ett brett spektrum av brottsbekämpning och anti-terrorismsamarbete, skulle granskas mer intensivt av riksdagen och kanske äventyras.")

Sverige var inte heller det enda skandinaviska landet som anammat massövervakning under åren före Snowdens avslöjanden. Flera NSA-dokument nämner också den norska underrättelsetjänsten (NIS), och i december 2013 rapporterade den norska tidningen *Dagbladet*, i samarbete med den amerikanska journalisten Glenn Greenwald, att Norge försåg NSA med tiotals miljoner meddelanden varje månad. Med hjälp av NSA-dokument och källor i Norge avslöjade tidningen att NIS riktade sig mot Ryssland i synnerhet och "bedrev övervakning mot politiker" samt ryska militära och energimål. Den noterade också att NIS, med hjälp av NSA, förvärvade en hundramiljoner-dollars "Windsor Blue-derivatsuperdator", kallad STEELWINTER, för att analysera krypterad övervakningsdata, och att NIS arbetade med NSA: s kryptanalysavdelning för att göra det.

Liksom Sverige betraktas Norge ofta som en framgångsrik socialdemokrati med en lång historia av förespråkande för mänskliga rättigheter. Norge i synnerhet är känt för sitt robusta skydd av yttrandefriheten och sin tradition av statlig öppenhet. Liksom Sverige har det länge rankats högt bland västerländska nationer i mått på medborgarnas förtroende för statliga institutioner. Och medan Norge är medlem i Nato, har det också hållit sig mestadels i periferin av kriget mot terrorismen. Ändå har norrmännen i stort sett varit oberörda av avslöjanden om deras regerings hemliga samarbete med NSA.

Efter *Dagbladets* reportage om Norges massövervakningsprogram blev det en kortvarig kontrovers i pressen. Men chefen för norsk underrättelsetjänst hävdade att de uppgifter Norge samlade in var från utländsk snarare än inhemsk kommunikation och kontroversen slutade snabbt. I Oslo berättade Karsten Friis, senior rådgivare vid Utrikespolitiska institutet i Norge, att många norrmän är stolta över att deras land har blivit så viktigt i amerikanska underrättelseinsatser. "Det fanns en känsla av att vi har den här kapaciteten och vi är inte rädda för att prata om det," sa Friis. I en artikel i *Dagbladet* bestred Greenwald den norske spionchefens påstående och hävdade att NSA-dokument visar att uppgifterna sannolikt inkluderar kommunikation från norrmännen själva.

Däremot är norrmännen oroade över övervakning av FRA, eftersom cirka 80 procent av norsk Internettrafik - även inhemska kommunikationer från en norrman till en annan - passerar genom Sverige. Delvis som ett resultat har det norska parlamentet börjat debattera en så kallad Digital Border Defenses-lag, som i praktiken skulle ge norsk underrättelsetjänst liknande tillgång till internationella fiberoptiska kablar som FRA har.

I oktober berättade Bjørn Erik Thon, chef för den norska dataskyddsmyndigheten, en myndighet som ansvarar för integritetsfrågor, att han hade allvarliga reservationer mot lagförslaget, eftersom det skulle vara mycket svårt att förhindra att norrmännens data också samlades in, trots planer på att "filtrera bort" dataflöden från Norges egna källor. Han sa att hans myndighet arbetade med en rapport som var kritisk till lagförslaget. Men Thon tillade att den föreslagna lagstiftningen har mött lite motstånd bland de största partierna eller i pressen och sannolikt kommer att gå igenom under de kommande månaderna. "Det är helt enkelt inte en stor oro här."

Hemlig regeringsavlyssning har en lång historia i Skandinavien. I kraft av sin position på Europas norra flank med Ryssland i öst var den skandinaviska halvön avgörande för västerländska underrättelsetjänstemän under det kalla kriget, och både Norge och Sverige utvecklade sofistikerade signalspaningsprogram. Enligt NSA-dokument har den amerikanska myndigheten haft nära band till norsk underrättelsetjänst så långt tillbaka som på 1950-talet. Med Norges position som Natos norra brohuvud mot öst fortsatte relationen fram till Gorbatjovperioden. En norsk tidning beskrev nyligen en avlyssningspost i Vardø, längst norr i landet vid gränsen till Ryssland, som ett "jättelikt öra mot öst".

Men NSA:s relation till Sverige kan vara den mest intressanta. Även om Sverige officiellt var neutralt byggde Sverige faktiskt mycket nära band till både Nato och USA: s säkerhetsetablissemang i slutet av 1940-talet och början av 1950-talet och var djupt involverat i kalla krigets spionoperationer. Bland underrättelsetjänsterna noterades svenskarna för sin tekniska skicklighet. Enligt den norske journalisten och underrättelsehistorikern Alf Jacobsen använde FRA på 1970- och 1980-talen den svenska ambassaden i Helsingfors för att avlyssna sovjetisk militär och diplomatisk kommunikation med hjälp av utrustning från NSA; och när de arbetade för CIA bröt svenskarna framgångsrikt de diplomatiska koderna för många länder, inklusive Brasilien, Zaire, Kina, Iran, Turkiet, Japan och Tjeckoslovakien.[1]

Under de senaste åren har geografisk närhet till Ryssland och utvecklingen av Internet gett nya skäl för Sverige att behålla sitt tekniska försprång: det finns väldigt få fiberoptiska undervattenskablar som förbinder Ryssland med omvärlden - bara sex, enligt kabelövervakningsorganisationen TeleGeography, av mer än tre hundra runt om i världen - och de viktigaste passerar under Östersjön. I juli 2008, när Sverige antog sin övervakningslag, noterade ett diplomatiskt telegram från den amerikanska ambassaden i Stockholm, senare publicerat av WikiLeaks, att eftersom "80 procent av Rysslands utländska kabelbaserade kommunikation går genom Sverige, legaliserar lagen Sveriges övervakning av majoriteten av Rysslands gränsöverskridande kommunikation."

Med den ryska militären som utgör ökande hot mot Nato-allierade sedan kriget i Ukraina har sådant spionerі blivit ännu viktigare. Precis som under kalla kriget rapporteras det ofta i svensk press om rysk ubåts- och militär aktivitet i regionen, och växande krav på en skärpt militärallians med Nato och USA. (I början av 2015 anslöt sig Sverige till Natos Cyber Defense Center, en forsknings- och träningsanläggning i Tallinn, Estland, och i juni 2016 undertecknade Sverige en ny "avsiktsförklaring" med Pentagon, som syftar till att stärka en försvarsallians.)

Det nyligen färdigställda finska undervattenskabelsystemet Sea Lion, som leder internettrafik från Finland direkt till Tyskland, kan dock göra det möjligt för många ryska kommunikationer att kringgå Sverige. I höstas började den finska regeringen diskutera en egen övervakningslagstiftning, som bland annat syftar till att få tillgång till de nya kabeluppgifterna. Vissa västerländska säkerhetsanalytiker ser nu Östersjön som en huvudarena i en ny kapprustning inom cyberkrigföring. I oktober 2015 rapporterade *The New York Times* att ryska ubåtar och spionfartyg aggressivt arbetar nära de viktiga undervattenskablarna som bär nästan all global internetkommunikation, vilket väcker oro bland vissa amerikanska militär- och underrättelsetjänstemän att ryssarna kan planera att attackera dessa linjer i tider av spänning eller konflikt.

Bland de många frågor som ställs av Skandinaviens omfamning av massövervakning är en som har dröjt kvar i marginalen under hela Snowden-debatten: Skiljer sig avancerade demokratier från sina auktoritära

motparter när det gäller att få bred tillgång till medborgarnas privatliv? I en fascinerande ny studie jämförde de svenska forskarna Johan Eriksson och Johan Lagerkvist de senaste cybersäkerhetsinsatserna i Sverige och Kina.[2] Vid första anblicken, som de noterar, kunde länderna inte vara mer olika: den kinesiska regeringen reglerar sina medborgares tillgång till Internet genom en enorm "brandvägg" och censursystem; Sverige har främjat Internetfrihet - tanken att obegränsad tillgång till Internet kan hjälpa till att mobilisera medborgare i utvecklingsländer och offentliggöra övergrepp mot mänskliga rättigheter - runt om i världen. Men när tillgången till Internet läggs åt sidan, konstaterar författarna, är det väldigt liten skillnad mellan de två:

Trots att Sverige är en liberal demokrati och Kina är en auktoritär enpartistat har båda staterna avancerade cyberövervakningssystem och erkände nyligen för första gången offensiv cyberkrigföringsförmåga.

Eriksson och Lagerkvist finner det "något förbryllande" att massinsamling av data och kommunikationsövervakning inte har blivit en stor fråga i valkampanjer i västerländska länder - trots "rättsliga och moraliska problem relaterade till medborgarnas integritet och privatliv, och den icke-transparenta karaktären av statlig övervakning." Sådana program har ofta satt västerländska ledare i en motsägelsefull situation. En av de mest högröstade förespråkarna för Internetfrihet är till exempel den tidigare svenska utrikesministern Carl Bildt. Men Bildt är också en ledande försvarare av Sveriges övervakningslag från 2008, som hans regering drev igenom. När Bildt 2013 frågades vid ett forum om Internetfrihet hur han kunde förena dessa två synsätt, förklarade han att Sverige utförde övervakning i ett gott syfte. "Det finns en skillnad mellan goda stater och något mindre goda stater", sa han.

I själva verket kan de egenskaper som har gjort Sverige och Norge till framgångsrika förebilder för avancerad demokrati också ha gjort deras befolkningar mer mottagliga för statligt spioneri. I Norge har den regeringskommitté som lade fram den massövervakningslagstiftning som nu är före parlamentet hävdat att sådana åtgärder "kan motiveras som nödvändiga i ett demokratiskt samhälle." Och som svenska och norska forskare påpekar är skandinaviska medborgare benägna att anta att om regeringen säger att den behöver vissa befogenheter, så gör den förmodligen det.

I Oslo berättade Eirik Løkke, en forskare vid en liberal norsk tankesmedja som just har skrivit en bok om integritet i den digitala tidsåldern, att norrmännen är mycket mer bekymrade över Googles och Facebooks befogenheter att samla in information om privatpersoner än över deras underrättelsetjänsts spioneri för NSA. En sådan ståndpunkt, observerade han, kan vara motsatsen till USA, där konsumenter rutinmässigt frivilligt lämnar mycket av sina privata identiteter till internetföretag, samtidigt som de betraktar statlig övervakning med stor skepsis.[3]

Ändå är det långt ifrån klart om USA: s ansträngningar att tygla NSA kommer att fortsätta, efter de explosiva avslöjandena om rysk hackning och valet. Redan innan CIA: s slutsatser rapporterades i pressen, och trots Trumps egen vägran att erkänna den ryska attacken, fanns det indikationer på att den tillträdande administrationen skulle förespråka en dramatisk expansion av övervakningsbefogenheterna. I slutet av november noterade de att två Trump-utnämnda inom brottsbekämpning och underrättelsetjänst, Jeff Sessions som justitieminister och Mike Pompeo som chef för CIA, är "ledande förespråkare för inhemsk regeringsspionering", rapporterade *Bloomberg News* :

I en omvändning av de begränsningar som infördes efter Edward Snowdens avslöjanden 2013 om massinsamling av data av NSA, kan Trump och kongressen röra sig mot att återinföra insamlingen av masstelefonposter, förnya befogenheter att samla in innehållet i e-post och annan internetaktivitet, lätta på restriktionerna för hackning i datorer och låta FBI hålla förundersökningar öppna längre.

Samtidigt som vi fortsätter att urholka vår integritet är det tveksamt hur mycket dessa steg skulle förbättra den nationella säkerheten. Chris Soghoian, en integritets- och cybersäkerhetsexpert för ACLU, sa till mig, för alla miljarder dollar som NSA och dess allierade har investerat i "offensiv" cyberteknik, visade de ganska grova ryska attackerna mot DNC i vilken utsträckning vi har misslyckats med att genomföra grundläggande säkerhetsåtgärder mot cyberattacker hemma. Bland de många paradoxerna i det senaste amerikanska presidentvalet, måste en verkligen vara vågen av anti-etablissemang och populistisk ilska som har fört en regering till makten som står redo att inleda vad som kan vara den största expansionen av hemlig statlig övervakning sedan attackerna den 11 september. Om den gör det kan den komma att hamna i samklang med några av de mest öppna och avancerade demokratierna i Europa.

Källor:

---


1. The New York Times: The Surveillance Engine: How the NSA Built Its Own Secret Google (https://www.nytimes.com/2013/08/29/us/nsa-foils-much-internet-encryption.html)
2. The New York Times: Spy Agencies Probe Angry Birds and Other Apps for Personal Data (https://www.nytimes.com/2014/01/28/world/spy-agencies-scour-phone-apps-for-personal-data.html)
3. The Guardian: XKeyscore: NSA tool collects 'nearly everything a user does on the internet' (https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data)
4. The Guardian: How GCHQ stepped up its online spying game (https://www.theguardian.com/uk-news/2013/aug/02/gchq-nsa-prism)