dataskydd.net
ORG.NR 802495-4797 – HTTPS://DATASKYDD.NET – INFO@DATASKYDD.NET

Dataskydd.net Sverige
Alsnögatan 18
116 41 Stockholm

Försvarsdepartementet
103 33 Stockholm

Falun 2017-07-24

Inlaga till utredningen om personuppgiftsbehandling inom Försvarsmakten och Försvarets radioanstalt – Fö 2017:03 || Kommittédirektiv 2017:42

Dataskydd.net är en svensk ideell, partipolitiskt obunden förening som verkar för bättre tekniskt och juridiskt dataskydd för privatpersoner i Sverige.

Innehåll

Förslag (sammanfattningar)

Förslag 1: Markera mot förhastade utredningar

Utredaren bör påtala för regeringen att det inte är konstruktivt att förhastat tillsätta utredningar om dataskydd vars juridiska bas och konventionella stöd inte är klart på grund av pågående rättsprövningar.

Utredaren bör också påtala för regeringen att det skadar möjligheterna för insyn i den svenska offentliga makten att utredningar tillsätts som inte har någon förutsättning att göra sakliga genomlysningar av ett område mot bakgrund av oklarheten kring den juridiska basen och det konventionella stödet.

Se vidare s. 4–6.

Förslag 2: Definiera nationell säkerhet och försvarsintressen tydligt

Begreppen *nationell säkerhet* och *försvarsintressen* bör definieras tillräckligt snävt för att att verksamheterna ansvariga för utövandet av denna säkerhet och dessa intressen inte ska tvingas kompensera för regeringens ovilja att ta tag i näringspolitiska problem på det öppna och förutsägbara sätt som regeringen borde hantera näringspolitiska problem.

Se vidare s. 7–9.

Förslag 3: Separera tydligt nationell säkerhet från allmän säkerhet

Myndigheter som jobbar med nationell säkerhet och myndigheter som arbetar med allmän säkerhet bör hållas tekniskt och organisatoriskt separerade.

Se vidare s. 7–10.

Förslag 4: Begränsa informationsdelningen mellan nationell säkerhet och allmän säkerhet

Försvarsmakten och Försvarets radioanstalt bör *inte* tillåtas dela uppgifter med brottsbekämpande verksamheter, även i sådana fall då de brottsbekämpande myndigheterna nominellt ägnar sig åt underrättelseverksamhet.

Underrättelseverksamhet med syfte att skydda den *nationella säkerheten* eller *försvarsintressen* bör hållas separat från annan underrättelseverksamhet. Det bör framgå att tekniska system ska utformas mot bakgrund av att samverkan inte är tillåten. Direktåtkomst ska inte vara möjlig och elektroniskt eller icke-elektroniskt utlämnande av uppgifter myndigheterna emellan ska inte vara lagligt.

Se vidare s. 7–10.

Förslag 5: Försvarsunderrättelsedomstolen bör kallas för *försvarsunderrättelsenämnden*

Den nuvarande mekanismen för att godkänna underrättelseuppdrag bör inte kallas domstol eftersom det inte är någon domsol.

Utredaren bör bedöma lämpligheten i det nuvarande förfarandet för tvistelösning i försvarsunderrättelsefrågor utifrån de brett accepterade principerna och

frågeställningarna belysta av Venedigkommissionen.[a]

Se vidare s. 9–10 och s. 14–16.

Förslag 6: Allmän genomlysning av ansvarsfördelningen i enlighet med checklistan från Venedigkommissionen

Utredaren bör utifrån de brett accepterade principerna och frågeställningarna belysta av Venedigkommissionen[b] göra en genomlysning av strukturen kring de svenska underrättelsemyndigheterna och avgränsa sammanblandningen mellan de myndigheter som arbetar inom och utom försvarsverksamheter och den nationella säkerheten från de andra myndigheterna.

Se vidare s. 9–10.

Förslag 7: Ge tydliga besked kring de mänskliga rättigheternas status i Sverige

Flera framstående europeiska länder, bland annat Frankrike, Storbritannien och Turkiet, har annonserat att de ser de mänskliga rättigheterna som opraktiska i sitt arbete med den nationella säkerheten. Svenska regeringen bör vara likaledes tydliga om de inte längre anser mänskliga rättigheter vara ett funktionellt sätt att balansera makten mellan medborgare och stat. Det gäller i frågor som rör nationell säkerhet och underrättelsetjänst som för alla andra frågor.

Utredaren bör titta närmare på vilka av dess förslag som egentligen bör kräva att regeringen åberopar undantagstillstånd och belysa vilka konsekvenser ett sådant undantagstillstånd skulle ha för de mänskliga rättigheternas ställning i världen.

Se vidare s. 11–13.

Förslag 8: Avveckla Försvarets radioanstalts avlyssning av gränsöverskridande internettrafik

Utredaren bör föreslå att regeringen, i avsaknad av vilja från regeringen att införa undantagstillstånd, avvecklar Försvarets radioanstalts nuvarande insyn i internettrafik som färdas över landsgränserna. Försvarets radioanstalts befogenheter med avseende på teleoperatörer bör ställas tillbaka till vad som gällde innan 2008. Underrättelsearbetet bör, på det sätt som EU-domstolen klargjort för datalagring (*Tele2*-målet)[c] och Europadomstolen klarlagt för underrättelseverksamhet (*Szabo och Vissy mot Ungern*),[d] vara av en sådan karaktär att det är riktat och specifikt.

Se vidare s. 11–13.

Förslag 9: Säkerställ tillräcklig teknisk kompetens hos ansvariga tillsynsorgan

De ansvariga tillsynsorganen måste, förutom juridisk kompetens, också ha teknisk kompetens. Detta måste realiseras på något annat sätt än genom aspirativa skrivelser, till exempel genom en budgetökningar till ansvariga myndigheter eller direkta förslag genom förändrade regleringsbrev. Tillsynen är en viktig del av förtroendebyggandet gentemot medborgare, att staten är villig att följa sina egna lagar och regler.

Se vidare s. 14–16.

Förslag 10: Bättre rutiner för transparens kring IT-säkerhet

Om myndigheterna med ansvar för nationell säkerhet eller försvarsintressen får kännedom om en tidigare okänd sårbarhet eller metod för att utnyttja en sårbarhet (en så kallad *o-day*)[e] ska de omedelbart vidta åtgärder för att sårbarheten eller metoden att använda sårbarheten blir känd och kan åtgärdas.

Om en sårbarhet eller metod för att utnyttja en sårbarhet *köps in* för att integreras i myndigheternas befintliga IT-stöd eller i ett inköpt IT-stöd, ska sårbarheten eller metoden för att utnyttja sårbarheten senast tre månader efter inköpsdatum publiceras så att största antal svenska och europeiska företag, myndigheter och privatpersoner så snabbt som möjligt kan få hjälp och incitament att åtgärda sårbarheterna i sina egna maskiner.

Se vidare s. 17–18.

Förslag 11: Konsulttjänster och personuppgiftsskydd

Underrättelsemyndigheterna och försvarsmakten bör inte ägna sig åt konsultverksamhet på andra myndigheter. Deras inblandning motverkar direkt den för en säkerhetsekonomiskt väl fungerande incitamentsmodell så viktiga insynen från medborgare och konsumenter. Risken är att underrättelsetjänstens inblandning tas som ursäkt av konsult-upphandlarna för att slippa ta ansvar för säkerhetsbrister och problem, eftersom de genom sådan inblandning kan garantera en hög nivå av hemlighetsmakeri kring kring sina tillkortakommanden.

Förslag 12: Personaladministration

I syfte att säkerställa förutsägbarhet för personal anställd inom Försvarsmakten och på Försvarets radioanstalt gällande personalens mänskliga rättigheter, och utövandet av dessa rättigheter, bör de vanliga personuppgif sreglerna (det vill säga, reglerna från EU:s dataskyddsförordning) tillämpas vid personaladministration.

[a] Se fotnot 24.
[b] Se fotnot 24.
[c] Se fotnot 14.
[d] Se fotnot 2.
[e] För definitioner se s. 17.

Inledning

De förhastade utredningarnas land

Översynen av personuppgiftsbehandlingen inom Försvarets radioanstalts verksamhetsområde verkar vara förhastad. Centrum för rättvisas prövning av FRA-lagens förenlighet med Europeiska konventionen för mänskliga rättigheter drar sig till exempel snart mot sitt slut,[I] och ett inväntande av resultatet från den

[I] Centrum för rättvisa mot staten (FRA). http://centrumforrattvisa.se/personlig-integritet/centrum-for-rattvisa-tar-fra-lagen-till-europadomstolen/

prövningen hade kunnat bespara både departementet och utredningsväsendet (och därmed även skattebetalare) tid och pengar.

Tidigare utlåtanden från Europadomstolen om metadatabehandling vid övervakning i fall som rör nationell säkerhet indikerar att domstolen inte anser att sådan behandling ligger helt utanför tillämpningsområdet för de mänskliga rättigheterna. I *Szabo och Vissy mot Ungern* uttalade domstolen bland annat att saker som är ”operativt lämpliga” inte behöver vara ”strikt nödvändiga”.[2] I samma mål förklarade domstolen även att man avsåg återkomma med preciseringar om krav på behandlingar av metadata i senare mål.[3] Särskilt *Szabo och Vissy* borde alltså ha föranlett en försiktighet hos regeringen med de resurser en utredning innebär. Om ett beslut som går regeringen emot framtvingar flera på varandra följande utredningsförfaranden försenas implementationen av ett domslut från Europadomstolen som skyddar privatpersoners rättigheter, vilket inte är önskvärt om regeringen vill markera att den är en seriös aktör för de mänskliga rättigheterna.

Dataskydd.net vill också påminna om att innebörden av Europadomstolens praxis är bindande för domstolar i Sverige även i sådana tillfällen där domsluten inte riktar sig specifikt mot Sverige eller svensk lagstiftning.[4]

Möjligen kan regeringen invända att EU:s dataskyddsreform påkallar skyndsamhet i utvärderingen av det nu gällande regelverkets förenlighet med det kommande europeiska. EU-kommissionen och de andra medlemsstaterna hade dock säkerligen kunnat förstå ifall svenska regeringen ville invänta större klarhet från Europadomstolen innan man vidtar några större förändringar i regelverket kring FRA:s verksamhet. EU-kommissionen har till exempel haft stor tålmodighet med regeringen vad gäller bristerna i de svenska spellagarna.

---

[2] Europeiska domstolen för mänskliga rättigheter, Szabo och Vissy v. Hungary (Application no. 37138/14), 12 januari 2012. Para. 75:

> *However, given the particular character of the interference in question and the potential of cutting-edge surveillance technologies to invade citizens' privacy, the Court considers that the requirement "necessary in a democratic society" must be interpreted in this context as requiring "strict necessity" in two aspects. A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation. In the Court's view, any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal. The Court notes that both the Court of Justice of the European Union and the United Nations Special Rapporteur require secret surveillance measures to answer to strict necessity (see paragraphs 23 and 24 above) – an approach it considers convenient to endorse.*

[3] Para. 70, *ibid*.

> *The Court would add that the possibility occurring on the side of Governments to acquire a detailed profile (see the CDT's submissions on this in paragraph 49 above) of the most intimate aspects of citizens' lives may result in particularly invasive interferences with private life. Reference is made in this context to the views expressed by the Court of Justice of the European Union and the European Parliament (see paragraphs 23 and 25 above). This threat to privacy must be subjected to very close scrutiny both on the domestic level and under the Convention. The guarantees required by the extant Convention case-law on interceptions need to be enhanced so as to address the issue of such surveillance practices. However, it is not warranted to embark on this matter in the present case, since the Hungarian system of safeguards appears to fall short even of the previously existing principles.*

[4] *Se t. ex.* NJA 2013 s. 746.

Överdrivna textmassor är inte transparens

De många utredningarna om dataskydd och personuppgiftsskydd som regeringen parallellt har tillsatt under det senaste året, för att så snabbt som möjligt utreda effekterna av EU:s nya dataskyddslagar även på områden som uppenbarligen faller utanför EU-lagarnas tillämpningsområde (till vilket det nationella säkerhetsintresset som Försvarsmakten och Försvarets radioanstalt tillhör), framstår mer som ett försök att spamma offentligheten med ofantliga kvantiteter onödig utredningstext än som ett genuint försök att upprätthålla eller säkerställa förenlighet mellan svensk lagstiftning och europeisk.

Att spamma är ett lika dåligt sätt att motarbeta transparens, insyn och begriplighet i maktutövande som det vore att i överdriven utsträckning sekretessklassa information om personuppgiftsbehandling. Det gör det helt enkelt omöjligt att ta reda på vad som gäller, i synnerhet för medborgare och journalister vars heltidssysselsättning det inte är att läsa och skriva ofantligt långa dokument om dataskydd.

Utredningens uppdrag

Försvarsdepartementet har inte givit utredningen i uppdrag att i så hög utsträckning som möjligt säkerställa sig om att förutsättningarna för varken integritetsskyddet eller FRA:s verksamhet inte förändras,[5] trots de övergripande förändringarna i dataskyddet som kommer inträda genom EU:s dataskyddsreform. Det gör det svårt för både utredningen själv, men också intressenter utanför myndighetsväsendet, att förutsäga i vilken utsträckning större förändringar kan, borde eller måste resultera av utredningsuppdraget.

Vi har skrivit den här inlagan med förståelsen att lagstiftning på området för nationell säkerhet ska följa systematiken i den allmänna dataskyddslagstiftningen. Så har det varit hittills i Sverige, och det har också fördelar i det att lagstiftningen blir mer överskådlig och begriplig för landets medborgare och för myndigheternas anställda och IT-ansvariga.[6]

Vi har också skrivit den med avseende på några särskilda problemområden som vi ser i lagstiftningen om personuppgiftsbehandlingen hos Försvarets radioanstalt och inom Försvarsmakten idag. Till dessa hör insyn och tillsyn, de nuvarande befogenheterna att på ett allomfattande sätt kartlägga svenska och utländska medborgares information via maskinell insamling av metadata och kommunikationsdata, samt inverkan av vissa spaningsmetoder i bruk på myndigheterna på vanliga svenska medborgares och konsumenters informationssäkerhet och tekniska säkerhet.

Utan vidare övervägningar anser vi att personaladministrativa ärenden ska hanteras inom ramen för de vanliga personuppgiftsreglerna. Det skapar bättre förutsägbarhet för anställda inom verksamheterna och berövar dem inga mänskliga rättigheter som de skulle ha haft om de arbetat någonstans.

[5] Dir. 2017:42.

[6] Även om det inte är helt uppenbart utifrån de nuvarande utredningsmassorna och de till synes spretiga, illa definierade informationssäkerhetsstrategierna att man faktiskt anser att överskådlighet och begriplighet är fördelar.

Sammanfattning.

Utredaren bör påtala för regeringen att det inte är konstruktivt att förhastat tillsätta utredningar om dataskydd och personuppgiftsbehandling vars juridiska bas och konventionella stöd inte är klart på grund av pågående rättsprövningar.

Utredaren bör också påtala för regeringen att det skadar möjligheterna för insyn i den svenska offentliga makten att utredningar tillsätts som inte har någon förutsättning att göra sakliga genomlysningar av ett område mot bakgrund av oklarheten kring den juridiska basen och det konventionella stödet.

Definitionen av nationell säkerhet och försvarsintressen

EU:s dataskyddslagstiftning medger att staten gör undantag från personuppgiftsskyddet med hänvisning till nationell säkerhet och försvarsintressen, förutsatt att dessa går att motivera i ett demokratiskt samhälle och är strikt nödvändiga.[7]

Det påkallar frågan vad *nationell säkerhet* är. Nationell säkerhet är uppenbarligen skilt från *allmän säkerhet*, vilket observerats av utredningen om en ny brottsdatalag.[8] I EU:s dataskyddsförordning får man också intrycket av att det är skilt från *försvarsintressen*. Men vad är nationell säkerhet och försvarsintressen?

Brottsdatalagsutredningen beskriver inte vad nationell säkerhet är,[9] utan lämnar det underförstått. Enligt Artikel 29-gruppen har nationell säkerhet i en oroande utsträckning använts som övergripande ursäkt för åtgärder som stater inte vill eller kan motivera i mer specifika termer.[10] På grund av begreppets flexibla karaktär kan det tas som intäkt för varje form av handling som går medborgarens rättigheter eller intressen emot. Även andra internationella organ har problematiserat begreppet nationell säkerhet:

De två senaste högsta representanterna för mänskliga rättigheter i Förenta nationerna har till exempel påtalat att de generösa tolkningarna som görs av begreppet riskerar att undergräva den förutsägbarhet vi hoppas att medborgare ska uppleva vad gäller deras staters maktutövning.[11] Även Europadomstolen har bekymrats över den nationella säkerhetens svårgreppbara och till synes ständigt

Amöbisk. Definitionen av nationell säkerhet sväller ständigt och äter upp kringliggande fenomen, utifrån vad den statliga organismen i stunden finner nödvändigt för sin trevnad.

Bild: Illustration av Christian Gottfried Ehrenberg, känd tysk zoolog, död 1876.

[7] Förordning 679/2016, Art. 23.1.a och 23.1.b.

[8] SOU 2017:29, kap. 7.1.3, 7.2.1 eller eller 10.4.2 till exempel.

[9] *Ibid*. kap. 7.2.1.

[10] Artikel 29-gruppen, WP 215, 819/14/EN, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes skriver:

> *There is currently no common understanding of what is meant by national security. No clear definition has been adopted by the European legislator, nor is the case law of the European courts conclusive. However, the exemption must not be extended to the processing of personal data for purposes for which they cannot legally be used.*
>
> *Another part of the question that needs to be answered is to what extent an exemption focused on national security continues to reflect reality, now it appears the work of the intelligence services is more than ever before intertwined with the work of law enforcement authorities and pursues several different purposes. Data is shared on a continuous and global basis, leaving aside the question which nation's security is to benefit from the analysis of these data. The Working Party therefore calls upon the Council, the Commission and the Parliament to come to an agreement in order to define the principle of national security and be conclusive as to what should be regarded as the exclusive domain of the Member States.*

[11] Se nedan fotnot 30 och fotnot 31.

expanderande ramverk.[12]

Det är en otillfredsställande ordning att ett undantag från de mänskliga rättigheterna kan vara så brett och diffust. I Dataskydd.net:s mening bör utredningen därför följa Artikel 29-gruppens rekommendationer[13] och specificera vad begreppet *nationell säkerhet* specifikt ska innebära i svensk rätt. Utredningen bör också noggrannt begrunda vilken sorts undantag för det definierade säkerhetsintresse utredningen landar i som, med beaktande av proportionalitetsprincipen, kan vara *strikt nödvändiga* och *faktiskt svarar mot mål av allmänt samhällsintresse*, mot bakgrund av Europadomstolens och EU-domstolens befintliga praxis.[14]

Det är vår mening att begreppet bör snävas in på sådant sätt att det inte innefattar det som idag lite luddigt kallas *inre hot*. Inre hot bör istället hanteras som problem av karaktären *allmän ordning*[15] och därför hanteras av den öppna polisen.

Det är också vår mening att begreppet bör snävas in på sådant sätt att det inte omfattar *ekonomiska frågeställningar eller företags förehavanden*. Konsumenters intressen av en stark informationssäkerhet och ett starkt dataskydd tjänas inte bäst av att statliga myndigheter som arbetar under stark sekretess drar med sig, eller väver in, ekonomiska aktörer i det arbetet. Snarare uppstår en risk för att de statliga myndigheterna favoriserar vissa företag över andra och därmed gör det svårare för konsumenter att välja bort företag som är uppenbart dåliga för dem.

Begreppen *hybridkrig* och *fake news* har letat sig in det försvarspolitiska vokabuläret[16] och likaledes i de utrikespolitiska biståndsreglerna.[17]

Samtidigt förefaller många påstådda instanser av *fake news* vara framdrivna av den webbaserade annonsmarknadens främsta monetiseringsverktyg: antalet klick eller besök något särskilt innehåll på webben kan erhålla.[18] Detta skapar inte bara problem med upprörande men påhittad information om valbara politiska kandidater, utan är i allmänhet ett stort problem för hela annonsindustrin som ingen har något riktigt svar på. Bloomberg har kartlagt fenomenet med hajpad trafik och klick redan 2015, och det är på intet sätt begränsat till östeuropeiska bloggare.[19] Frågan är om de försvarsorienterade verksamheterna har någon egentlig förutsättning att komma till rätta med ett marknadsproblem för webbannonser, eller om det är en näringspolitisk genomlysning av problemen med *clickbait* som snarare behövs.

Det ligger givetvis bortom utredningens uppdrag att förändra hur de politiska makthavarna i Sverige anser sig behöva ta tag i problem på marknaden för webbaserade annonstjänster, men utredaren har möjligheten att närmare se över hur de undantag från privatpersoners grundläggande rättigheter ska formuleras

”Det geniala med hybridkriget, enligt teoretikerna, är att det är så mycket billigare än pansarvagnar. Att sprida skräck, desinformation och missuppfattningar kräver lite logistik eftersom det mesta kan ske via internet.

Därmed blev hybridkriget det perfekta kriget för skrivsbordsgeneralerna. Äntligen utkämpades [kriget] inte på något avlägset slagfält. Skyttegraven gick rakt över skärmen. Striderna böljade fram och tillbaka med varje liten twitterkommentar. Ärans väg låg plötsligt öppen för varje militärt överintresserad person beväpnad med en smartphone.”

– Martin Aagård i Aftonbladet, 25 juli 2016.

[12] Se *Szabo och Vissy* i fotnot 2, men också avgörande i *Zakharov mot Ryssland* (Application no. 47143/06), 4 december 2015..

[13] Se ovan fotnot 10.

[14] *Jfr. ovan* fotnot 2 och avgörande i ECLI:EU:C:2016:970, *Tele2 v Sweden*, C-203/15.

[15] SOU 2017:29, kap. 7.1.3.

[16] Dagens nyheter (30 mars 2017) Debatt, Stefan Löfven: Så ska vi skydda valrörelsen från andra staters påverkan.

[17] Den Sverige-finansierade kosovanska nyhetssidan *Kosovo2.0* har till exempel som uttalad nyhetsredaktionell linje att ta ställning *för* homosexuellas och kvinnors rättigheter, istället för att vara neutrala i sin rapportering enligt en presentation av deras verksamhet utförd på *Digital-Born Media Carnival* i Kotor, Montenegro, sommaren 2017.

[18] *Se* Wikipedias artikel `https://en.wikipedia.org/wiki/Pay-per-click` eller vilken annan artikel som helst ur *Internet Advertising*-serien.

[19] Bloomberg. Ben Elgin, Michael Riley, David Kocieniewski, och Joshua Brustein (24 september 2015) The Fake Traffic Schemes That Are Rotting The Internet.

som tillåter personuppgiftsbehandling inom Försvarsmakten och Försvarets radioanstalt i syfte att kompensera för kraftlös näringspolitik. Dataskydd.net föreslår att utredaren är restriktiv med sådana undantag och att utredaren påminner regeringen om att försvarspolitiken inte kan kompensera för en dålig näringspolitik.

Sammanfattning.

Begreppen *nationell säkerhet* och *försvarsintressen* bör definieras tillräckligt snävt för att att verksamheterna ansvariga för utövandet av denna säkerhet och dessa intressen inte ska tvingas kompensera för regeringens ovilja att ta tag i näringspolitiska problem på det öppna och förutsägbara sätt som regeringen borde hantera näringspolitiska problem.

Informationdelning mellan myndigheter

Försvarets radioanstalt och Försvarsmakten har de senaste åren fått dramatiskt utökade mandat att samla in personuppgifter om privatpersoner från Sverige och andra europeiska länder. Det gäller inte bara övervakningen av samtlig kabeltrafik som rör sig över landets gränser, utan även tillämpning av offensiva cyberförsvarsåtgärder. Eftersom offensiva cyberförsvarsåtgärder har samma tekniska konsekvenser som ett dataintrång,[20] kommer vi hädanefter att hänvisa till denna insamlingsmetod som ett *sanktionerat dataintrång* (se även terminologilistan på s. 17).

Som vi påtalat även i vårt remissyttrande över Ds 2016:31 om utökat informationsutbyte inom ramen för Nationellt centrum för terrorhotbedömningar[21] och i våra inlagor till utredningarna om hemlig dataavläsning[22] och modernisering av husrannsakan och beslag,[23] finns det en risk att den dramatiskt utökade informationsdelningen mellan olika underrättelsemyndigheter och brottsbekämpande myndigheter innebär att tvångsmedel kan användas mot svenska eller utländska privatpersoner, inom ramen för brottsutredningar, utan att tvångsmedlen erkänns som sådana.

I Venedigkommissionens checklista för rättssäkerhet och rättsstater rör många av frågeställningarna just uppdelningen av uppdrag mellan olika myndigheter.[24] Men i Sverige finns, till skillnad från i Storbritannien och USA, inga starka väggar mellan myndigheterna. Vi har fri bevisprövning i våra domstolar, vilket innebär att en domstol inte nödvändigtvis kommer att undersöka metoden genom vilken en viss bevisning förvärvats.

Eftersom en brottsutredning kan framställa bevisning som tillkommit olovligt — till exempel genom skvaller mellan myndigheter som är ålagda begräns-

Venedigkommissionen. En ny checklista över kriterier mot vilka man kan bedöma rättsstater sätter, vid första anblick, Sverige i en dålig sits. Sverige saknar en konstitution, har inget omedelbart sätt att kräva överprövning av lagar och avgränsningarna mellan olika myndighetsfunktioner, särskilt på underrättelseområdet, fungerar dåligt. Därtill är det inte uppenbart att förutsebarhetskrav tolkas på samma sätt i den svenska myndighetsapparaten som i de internationella organ som tillser mänskliga rättigheter världen över och i Europa, och medan en stor medvetenhet byggts upp i den internationella människorättsdoktrinen kring potentiella integritetskränkningar som följer av profilering, beteendekartläggning och andra former av metadatabehandling är Sverige fortfarande kvar i samma tankebanor som på 1970-talet (Integritetskommittén undantagen).

Bild: Yilmaz Oevuenc (CC-BY-SA) 2009, Flickr.

[20] Kärt barn har många namn. Övriga begrepp som använts inom statliga utredningar är husrannsakan på distans, digital husrannsakan och hemlig dataavläsning.

[21] Dataskydd.net, Remissyttrande över Ds 2016:31.

[22] Dataskydd.net och Föreningen för digitala fri- och rättigheter (DFRI) skickar en skrivelse till den pågående utredningen om hemlig dataavläsning.

[23] Dataskydd.net och Föreningen för digitala fri- och rättigheter (DFRI) skickar en skrivelse till den pågående utredningen om modernisering av beslag och husrannsakan.

[24] *Rule of Law Checklist* (CDL-AD(2016)007), Study No. 711 / 2013, Adopted by the Venice Commission at its 106th Plenary Session (Venice, 11-12 March 2016), Endorsed by the Ministers' Deputies at the 1263th Meeting (6-7 September 2016), Endorsed by the Congress of Local and Regional Authorities of the Council of Europe at its 31st Session (19-21 October 2016).

ningar och underställda tillsyn och myndigheter som är ålagda få begränsningar på sina verksamheter och som bara svårligen kan underställas tillsyn — utan att ifrågasättas av domstolen. Inte heller kan någon utanför rättsväsendet på något enkelt eller lagligt sätt påvisa att överträdelser har skett, finns en risk för missbruk.[25]

Missbruksrisken uppstår på grund av det som kallas *incitamentslära* eller *rational choice*. Om det är rationellt, effektivt och enkelt för en aktör att bete sig på ett visst sätt som uppfattas som gynnsamt för den aktören, kommer aktören sannolikt att bete sig på det sättet.

I de fall vi beskriver ovan och som implicit uppmuntras genom informationsdelningsstrukturen vid till exempel Nationellt centrum för terrorhotbedömningar har både den öppna polisen, Säkerhetspolisen och säkerhetstjänsterna starka incitament att dela information, även olovligen. De lider väldigt låg upptäcksrisk om de gör detta. Ju mer information som lovligen kan delas mellan myndigheter i denna sfär, desto enklare är det att göra det olovligen dessutom.

Incitamentsläran innebär inte att dessa myndigheter är ondskefulla bara för att de gör det som är lättast. Det är inte heller givet att någon av myndigheterna alltid kommer att agera på det sätt som är mest rationellt i bemärkelsen att det kräver minst arbete. Däremot vore det bara dumt av myndigheterna att aldrig agera rationellt i denna bemärkelse, och därför kan man anta att de kommer att ägna sig åt olovliga handlingar. De svenska informationsdelningsstrukturerna lånar sig helt enkelt väl till missbruk, och då är det rimligt att anta att missbruk kommer ske.

Sammanfattning.

Försvarsmakten och Försvarets radioanstalt bör *inte* tillåtas dela uppgifter med brottsbekämpande verksamheter, även i sådana fall då de brottsbekämpande myndigheterna nominellt ägnar sig åt underrättelseverksamhet i syfte att främja den egna brottsbekämpande funktionen.

Underrättelseverksamhet med syfte att skydda den *nationella säkerheten* eller *försvarsintressen* bör alltså, enligt vårt förslag, hållas separat från annan underrättelseverksamhet. Det bör framgå att tekniska system ska utformas mot bakgrund av att detta inte är tillåtet, det vill säga, direktåtkomst ska inte vara möjlig och elektroniskt eller icke-elektroniskt utlämnande av uppgifter myndigheterna emellan ska inte vara lagligt.

Myndigheter som jobbar med nationell säkerhet från myndigheter som arbetar med allmän säkerhet bör hållas tekniskt och organisatoriskt separerade. Detta förslag har inverkningar på vissa av de samarbeten som upprättats mellan myndigheter från försvarssfären och myndigheter från den civila utredningssfären under de senaste åren.

Utredaren bör utifrån de brett accepterade principerna och frågeställningarna belysta av Venedigkommissionen[a] göra en genomlysning av strukturen kring de svenska underrättelsemyndigheterna och avgränsa sammanblandningen mellan de myndigheter som arbetar inom och utom försvarsverksamheter och den nationella säkerheten från de andra

[25] Dataskydd.net har tagit upp detta även i vårt remissyttrande över SOU 2016:7 om stärkt straffskydd för integriteten.

myndigheterna. Vid behov bör utredaren också föreslå insnävningar av uppdrag för de myndigheter som inte faktiskt primärt är verksamma inom försvar och nationell säkerhet.

[a] Se fotnot 24.

Från lagbrott till sedvänja

Det finns en tendens hos svenska underrättelsemyndigheter, precis som hos många andra myndigheter vars verksamhet är huvudsakligen dold från allmänhetens insyn, att tänja på regler som kommer i vägen för den aktivitet underrättelsemyndigheten ser sig vara i behov av. När regelbrotten pågått under en längre tid, blir de till sedvänja vilket försvårar ansvarsutkrävande av enskilda tjänstemän. Detta har att göra med att tjänstemän inte kan göra sig skyldiga till tjänstefel om de inte visste att handlingen de vidtog var lagstridig.[26] Sådan insikt kan så klart inte infinna sig om man gör ”så som man alltid gjort”.

Att lagbrott kan bli till sedvänja, och därigenom uppnå juridisk status av lagligt förfarande i Sverige, skapar ett förutsebarhetsproblem i den svenska lagstiftningen.[27] En medborgare som läser lagen kan inte förutse hur sedvänjor hos myndigheter utvecklar sig i lagens absoluta yttergränser.

Behandling av personuppgifter i underrättelsesyfte

En viktig del av EU:s dataskyddsreform är att alla européer ska tilldelas samma skydd för deras grundläggande rätt till dataskydd oavsett vilken medborgarskap de har. Men detta är också en bärande tanke med Europakonventionen för mänskliga rättigheter som Sverige skrev under redan 1952. Svenska regeringen har alltså förpliktigat sig att behandla inte bara svenska medborgare på ett lagligt och korrekt sätt och med respekt för dessas rättigheter, utan även utländska medborgare.

Samtidigt har det skett en anpassning av den svenska retoriken där man pratar om *den svenska delen av internet* som en plats där de mänskliga rättigheterna ska gälla extra mycket, bland annat i regeringens pågående, starka ansträngningar för digitalisering.[28]

Det finns, enligt oss, två möjliga sätt att tolka det här.

[26] *Se t. ex.* riksåklagarens beslut i överprövningsärendet ÅM 2017/2285:

> *För att väcka åtal för tjänstefel ska det kunna förutses att det går att bevisa att åtgärden är objektivt felaktig, att det finns subjektiv täckning samt att gärningen inte är att bedöma som ringa.*

[27] *Jfr. ibid.* där riksåklagaren också menar att det i dag juridiskt tvivelaktiga förfarandet att beordra en *husrannsakan på distans i en dator via ett elektroniskt nätverk* möjligen inte är ett dataintrång, så som intrång i andras datorsystem utan deras kännedom och samtycke normalt skulle vara, på grund av att Åklagarmyndigheten skrivit en FAQ om husrannsakan på distans. Riksåklagaren skriver:

> *Jag vill också peka på att det numera även finns en vägledning för åklagare i form av en webbaserad guide (FAQ) vid brott med it-anknytning. Åklagarmyndighetens rekommendation enligt FAQ:n är att åklagare avråds från att fatta beslut om husrannsakan på distans utom i mycket sällsynta undantagsfall.*

Normalt borde Europakonventionens artikel 8, som kräver just förutsebarhet vid användning av övervakning eller tvångsmedel, förhindra att man i ”mycket sällsynta undantagsfall” använder ett tvångsmedel som inte är etablerat lagligt.

[28] Regeringen, För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi (N2017/03643/D).

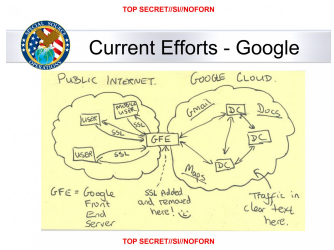
Antingen så har regeringen givit upp på sina ambitioner att efterleva Europeiska konventionen för mänskliga rättigheter, och vill inte längre respektera alla privatpersoners rättigheter. Därför understryker man extra noga att den svenska delen av internet är förbehållen olika skyddsåtgärder som andra, mindre värda nationaliteter inte ska förvänta sig.

Men en annan tolkning som är lite mindre upprörande är att regeringen menar att man ska respektera de mänskliga rättigheterna, i enlighet med modern europeisk tradition, extra mycket på sådana nätverk som finns på svenskt territorium och sådan trafik som färdas genom nätverk som finns på svenskt territorium.

En konsekvens av denna senare tolkning om respekt för allas mänskliga rättigheter på ett sådant eventuellt svenskt cyberterritorium är att Försvarets radioanstalts möjlighet att övervaka internettrafik dramatiskt måste begränsas. Trafik in och ut ur landet bör inte längre gå genom utvalda knutpunkter som kan övervakas av Försvarets radioanstalt på myndighetens initiativ och efter myndighetens eller någon uppdragsgivares upplevda behov. Istället skulle övervakningen behöva riktas och begränsas till sådan övervakning som är relevant och nödvändig för uppfyllandet av en specifik målsättning som ryms inom ramen för det nationella säkerhetsarbetet eller arbetet med försvarsintressen (för detaljerade juridiska hänvisningar se s. 5).

Om utredaren väljer att föreslå att man ska frångå den storskaliga, maskinella övervakningen av internettrafik, metadata och kommunikationsdata som korsar landets gränser, är det också huvudsakligen i linje med Europarådets parlamentariska utskotts betänkande om hur övervakning ska bedrivas för att vara förenlig med de mänskliga rättigheterna.[29]

Fakum är att många internationella organ uttalat sig emot massövervakning de senaste åren, till exempel vidare Förenta nationernas tidigare utsände för yttrandefrihetsfrågor,[30] den innevarande utsände för yttrandefrihetsfrågor,[31] FN:s tidigare högste representant för mänskliga rättigheter,[32] FN:s människo-



Oförenligt med mänskliga rättigheter. Massövervakning, eller att man maskinellt hämtar in all kommunikation som rör sig över landets gränser för att genom tekniska förbehandlingar säkerställa sig om huruvida något behöver granskas manuellt, är inte förenligt med staters förpliktelser gentemot sina medborgare enligt internationell rätt. Bara med avsevärd fantasi och vilja går det europeiska rättighetsramverket att tolka som om att detta vore tillåtet och acceptabelt. En möjlighet är att försöka få till någon sorts undantagstillstånd som Sverige kan uppleva och åberopa, men det borde, enligt Dataskydd.net, se illa ut att anstränga sig så mycket att gå emot så många indikationer på att massövervakning faktiskt inte är acceptabelt. Vi förordar att Sverige föregår med gott exempel på det internationella planet och följer människorättsförpliktelser i sitt nationella säkerhetsarbete.

Bild: National Security Agency, USA. Beskriver hur NSA:s cyberkommando lyckades ta sig runt Googles kryptering för att ändå tömma servrarna på information om privatpersoner, deras metadata och kommunikation.

[29] Council of Europe, Parliamentary Assembly, Resolution 2045 (2015) "Mass surveillance" Text adopted by the Assembly on 21 April 2015 (12th Sitting), med tillhörande Recommendation 2067 (2015).

> *The consequences of mass surveillance tools such as those developed by the United States and allied services falling into the hands of authoritarian regimes would be catastrophic. In times of crisis, it is not impossible for executive power to fall into the hands of extremist politicians, even in established democracies. /.../*
>
> *In several countries, a massive "surveillance-industrial complex" has evolved, fostered by the culture of secrecy surrounding surveillance operations, their highly technical nature and the fact that both the seriousness of alleged threats and the need for specific counter-measures and their costs and benefits are difficult to assess for political and budgetary decision makers without relying on input from the interested groups themselves. There is a risk that these powerful structures could escape democratic control and accountability and threaten the free and open nature of our societies. /.../*
>
> *The Assembly /.../ notes that, according to independent reviews carried out in the United States, mass surveillance does not appear to have contributed to the prevention of terrorist attacks, contrary to earlier assertions made by senior intelligence officials. Instead, resources that might prevent attacks are diverted to mass surveillance, leaving potentially dangerous persons free to act.*

[30] *Report of the Special Rapporteur to the Human Rights Council on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression*, 2013, A.HRC.23.40 EN

[31] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A.HRC.35.22 EN (2017).

[32] FN:s högste representant för mänskliga rättigheter, 27 sessionen. Rapport A/HRC/27/37 av den 30 juni 2014.

rättsråd,[33] FN:s generalförsamling,[34] och Europarådets människorättskommissionär.[35]

På vissa sätt finns det ett så löjligt starkt internationellt konsensus kring att nationalstater, som Sverige, beter sig dåligt och oförenligt med god sed kring mänskliga rättigheter att det blir konstigt att försöka upprätta någon sorts fullständig förteckning över alla dessa dokument. Venedigkommissionens checklista för rättsstater och deras institutionella sammansättning är ytterligare ett tecken på att det internationella regelverk Sverige underordnat sig för att säkerställa en god balans mellan medborgares makt över stater och staters makt över medborgare nu är satt i gång för att åstadkomma en rimlig balans mellan dessa motstående intressen även efter internet och webben. Inte heller verkar det som att det konventionella regelverket för mänskliga rättigheter nödvändigtvis landar i att verksamheter som de som bedrivs inom Försvarsmakten och på Försvarets radioanstalt faktiskt balanserat intressena väl, eller ens alls.

I syfte att stärka de internationella institutioner och organ som givits uppdraget att säkerställa respekten för och efterlevandet av en global miniminivå för mänskliga rättigheter, bör svenska regeringen frånta Försvarets radioanstalt, och i förekommande fall även de försvarsrelaterade underrättelsemyndigheterna, möjligheten att ägna sig åt massövervakning genom att på maskinell väg avlyssna all datatrafik som rör sig över svenska gränser.

Dels tappar Sverige moralisk trovärdighet mot andra länder genom att ihärda med aktiviteter som återkommande fördömts av internationella människorättsorgan. Dels bidrar Sverige genom att hålla fast vid massövervakning till att respekten för de demokratiska principerna och normerna urholkas även på det inhemska planet.

Sammanfattning.

Flera framstående europeiska länder, bland annat Frankrike, Storbritannien och Turkiet, har annonserat att de ser de mänskliga rättigheterna som opraktiska i sitt arbete med den nationella säkerheten. Svenska regeringen bör vara likaledes tydliga om de inte längre anser mänskliga rättigheter vara ett funktionellt sätt att balansera makten mellan medborgare och stat. Det gäller i frågor som rör nationell säkerhet och

Examples of overt and covert digital surveillance in jurisdictions around the world have proliferated, with governmental mass surveillance emerging as a dangerous habit rather than an exceptional measure. Governments reportedly have threatened to ban the services of telecommunication and wireless equipment companies unless given direct access to communication traffic, tapped fibre-optic cables for surveillance purposes, and required companies systematically to disclose bulk information on customers and employees. Furthermore, some have reportedly

[33] Förenta nationernas människorättsråd, 34 sessionen, Resolution A/HRC/34/L.7/Rev.1 *The right to privacy in a digital age.*

Noting also that, while metadata may provide benefits, certain types of metadata, when aggregated, can reveal personal information that can be no less sensitive than the actual content of communications and can give an insight into an individual's behaviour, social relationships, private preferences and identity,

[34] General Assembly resolution A/C.3/69/L.26/Rev.1, The right to privacy in the digital age, (25 november 2014).

[35] CommDH/IssuePaper(2014)1. 8 december 2014. *The rule of law on the Internet and in the wider digital world. Issue Paper published by the Council of Europe Commissioner for Human Rights.*

underrättelsetjänst som för alla andra frågor.
Avvecklande av övervakningen av all internettrafik.
Utredaren bör föreslå att regeringen, i avsaknad av vilja från regeringen att införa undantagstillstånd, avvecklar Försvarets radioanstalts nuvarande insyn i internettrafik som färdas över landsgränserna. Det vill säga i praktiken rullar tillbaka Försvarets radioanstalts befogenheter med avseende på teleoperatörer till den situation som gällde innan 2008. Underrättelsearbetet bör istället, på samma sätt som EU-domstolen klargjort för datalagring, vara av en sådan karaktär att det är riktat och specifikt.

Insyn och tillsyn av verksamheten

Insyn och tillsyn av verksamheten som bedrivs hos särskilt Försvarets radioanstalt sker på olika sätt: genom Försvarsunderrättelsedomstolen, genom SIUN och genom Datainspektionen.

Vi är eniga med den kritik som lyfts av Ottarsen och Wejedal i deras två artiklar om Försvarsunderrättelsedomstolens tillkomst och existens i Svensk juristtidning under 2016.[36] Försvarsunderrättelsedomstolen påminner mer om en nämnd än om en domstol. Det urholkar domstolsbegreppet och skadar rättsmedvetandet hos medborgarna, eftersom det inte blir tydligt vad en domstol är och gör. Utredningen har inte mandat att komma till rätta med denna fadäs, men bör påtala för regeringen att den svenska nationalstatens intressen inte tjänas av att regeringen försöker föra sin egen befolkning bakom ryggen i rättssäkerhetsfrågor.

Vi tror även att tillsynen av och strukturen för den svenska underrättelseverksamheten, både inom Försvarsmakten och inom Försvarets radioanstalt, skulle vara betjänt av en genomlysning utifrån Venedigkommissionens checklista för rättssäkerhet.[37]

[36] Tormod Otter Johansen och Sebastian Wejedal, ”Mot ett funktionellt domstolsbegrepp – Ett bidrag med anledning av den så kallade Försvarsunderrättelsedomstolen”, SvJT 2016 s. 10 res 191. Utdrag från s. 131–134:

> *Annorlunda uttryckt: Eftersom medborgarna inte kan få insyn i själva verksamheten är det av central betydelse att den ”organisatoriska lösningen” som sådan inger förtroende. Häri ligger bland annat att tillståndsprövningen ska vara oberoende, och eftersom domstolar per definition är oberoende bör prövningen utföras av domstol. Att tillståndsprövningen var ”helt främmande” för domstolarnas verksamhet var således inte längre ett skäl som talade emot domstolsprövning — i alla fall inte med tillräcklig styrka. Prövningens särdrag ta- lade visserligen emot en prövning hos de befintliga domstolarna, men detta problem kunde ju lösas smidigt och enkelt genom att det skapades en ny domstol, som således kunde verka utanför det ”processrättsliga systemet”. /.../*
>
> *Som synes anförde dock regeringen inga argument för att prövningen borde ankomma på en domstol istället för exempelvis en domstolsliknande nämnd. Om den kompetens som en domare normalt innehar är helt irrelevant vid den aktuella tillståndsprövningen, varför eftersträvades domstolsprövning överhuvudtaget? Den enda förklaring som står att finna är att regeringspartierna hade kommit överens om att tillståndsprövningen skulle ske i ”domstol”, vilket löstes genom att den nya myndigheten kallades för domstol. I samband med att lagförslaget remitterades till Lagrådet för granskning konstaterade också Lagrådet — i anslutning till remisskritiken — att förslaget gav upphov till frågan om den föreslagna domstolen verkligen förtjänade “att betecknas som domstol eller om den hellre bör benämnas nämnd”.*

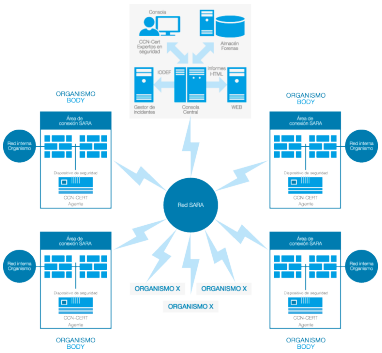
[37] Se fotnot 24.

De bortkollrade tillsynsmyndigheterna

En utmaning vid tillsynen av väldigt tekniskt orienterade verksamheter så som Försvarsmaktens underrättelseverksamhet och Försvaret radioanstalt är att tillsynsobjekten besitter mycket högre teknisk kompetens än tillsynsmyndigheterna. Eftersom frågor om avlyssning, teknisk apparatur, tekniska standarder, övervakning, informationsteknologi och juridik ofta kräver stor kännedom om både tekniska och juridiska system för att meningsfullt kunna utvärderas,[38] och utvärderingen misslyckas om man *inte* har full koll på alla dessa delar blir tillsynen bristfällig.

Dataskydd.net kan exemplifiera med en nylig tillsynshändelse på Datainspektionen:

> Datainspektionen genomförde 2010 en granskning av Försvarets radioanstalts personuppgiftsbehandling som ledde inspektionen att dra slutsatsen att Försvarets radioanstalt ”har lagt ned mycket tid och resurser på att skapa rutiner och utbilda personalen på ett sådant sätt att risken för otillbörliga intrång i den personliga integriteten minimeras” och att deras intryck därför var ”på det hela taget positivt”.[39] År 2015 kom Försvarets radioanstalt på att de vill bygga en så kallad SOC (*security operation center*).[40] Under hösten 2016 gjorde Datainspektionen en ny tillsyn där de kom ihåg att de 2010 hade föreslagit att Försvarets radioanstalt borde överväga mer loggning och ville därför att Försvarets radioanstalt skulle bygga klart sin SOC.[41] I maj 2017 annonserade Försvarets radioanstalt att SOC:en skulle färdigställas på det avsedda sättet.[42]
>
> En SOC är emellertid ingen lösning på något särskilt tekniskt eller organisatoriskt *dataskyddsproblem* som rimligen kan ligga under Datainspektionens tillsynsområde.[43] I alla fall är det inte givet att det är en sådan lösning, och absolut inte utifrån vad Försvarets radioanstalt redovisat i allmänna handlingar för Datainspektionen, eller som Datainspektionen kan redogöra för vid direkt fråga. Vad SOC:en normalt kan göra är att kontrollera att alla datorer (i bred bemärkelse) som ska vara uppkopplade mot ett nätverk också är uppkopplade mot ett nätverk vid det tillfället. Eftersom kommunikationen mellan datorer i ett nätverk allt oftare är krypterad är det svårt att logga mer än att dator A har pratat med dator B vid något givet tillfälle (eller för den delen att de definitivt inte pratat med varandra under en given tidsperiod). Det går inte, typiskt sett, att kontrollera *vilken specifik information* som skickats mellan dator A och dator B, om någon information har skickats.
>
> SOC:ar kan göra allt möjligt och behöver därför ett väldigt väl definierat syfte för att ens ha möjlighet att fungera bra i dataskyddssammanhang.[44] Normalt rekommenderas att man noggrannt åtskiljer loggning som sker i syfte att följa upp *policies* (den sorts uppföljning som möjligen kan ha dataskyddande kvaliteter) och loggning som sker i syfte att följa upp *ett IT-nätverks tekniska funktion*. Det är till exempel skillnad på omständigheten att en skrivare används för mycket klockan 18:00, eller att en dator inte är uppkopplad som borde vara det, och



Spanska sensorsystemet SAT-SARA. I Spanien publicerar CCN-CERT en schematisk bild över vilka sorters interaktioner och kommunikationer som kan fångas upp av CCN-CERT:s tidiga varningssystem, som likt en SIEM eller SOC kan användas för att kontrollera att datorer som ska prata med varandra faktiskt också gör det. Statistiken från SAT-SARA är sekretessklassad, liksom statistiken från den publika motsvarigheten SAT-INET. Även INES-rapporterna, som kontinuerligt utvärderar offentliga ansträngningar på IT-säkerhetsområdet, är otillgängliga för allmänheten. Det gör det svårt att veta om systemen har någon positiv effekt för säkerheten i realiteten, och någon positiv effekt för spanska medborgares integritet är systemet inte ens avsett att ha.

Bildkälla: `https://www.ccn-cert.cni.es/`

[38] Detta har observerats för konsumentsammanhang i flera högkvalitativa studier utförda av professor Lorrie Cranor vid Carnegie Mellon University, USA, (specialist på användbar säkerhet eller *usable security*) och flera av hennes masterstudenter och doktorander.

[39] Datainspektionens redovisning av regeringsuppdraget Fö2009/355/SUND, 6 december 2010.

[40] Försvarets radioanstalt, promemoria inlämnad till Datainspektionen 28 april 2017, Redogörelse avseende regelbunden logguppföljning i försvarsunderrättelseverksamheten.

[41] Datainspektionen, Dnr 2331-2015, Tillsyn över behandlingen av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet.

[42] Se fotnot 40.

[43] Datainspektionen hänvisar i beslutet i fotnot 41 till 3 kap. 2 § första stycket lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet.

[44] Herman Slatman, Unboxing Security Analytics: Towards Effective Data Driven Security Operations, Master Thesis Computer Science, Universiteit Twente.

att en medarbetare använder uppgifter om privatpersoner på ett olagligt sätt. Det framgår varken från Datainspektionen eller från Försvarets radioanstalt vilket uppdrag SOC:en har eller att någon uppdelning av SOC:en policy-funktioner och tekniska funktioner har gjorts. Utifrån Försvarets radioanstalts inlämnade beskrivning till Datainspektionen framstår det som att det är en SOC för IT-nätverkets tekniska funktion som avsetts.

Har Datainspektionen förstått de tekniska funktionerna som Försvarets radioanstalt velat införa och i vilka situationer sådana tekniska funktioner typiskt sett är användbara för att säkerställa bättre efterlevnad av reglerna som ligger inom Datainspektionens ansvarsområde? Det är inte uppenbart.

En underligare omständighet är så klart att Datainspektionen försöker framställa det som att de riktat kritik mot Försvarets radioanstalt redan 2010 när det inte är uppenbart utifrån utredningen från 2010 att de faktiskt gjort det.[45] De har *föreslagit* att Försvarets radioanstalt gör ett *övervägande*. SOC:ar fanns redan 2010, så om det var en SOC som saknades borde detta ha kunnat observeras uttryckligen 2010. Inte heller är det uppenbart varför Försvarets radioanstalt i sådana fall skulle ha dröjt i hela fem år med att låta sina *överväganden* resultera i att det var en SOC-brist som Datainspektionen uppmärksammat 2010.[46]

Det har observerats i andra sammanhang, bland annat av utredningen om tillsyn av den personliga integriteten,[47] att Datainspektionen behöver mer resurser för att kunna dra till sig kompetent IT-säkerhetspersonal. En ytterligare utmaning lär vara att Datainspektionen också kommer tvingas rekrytera säkerhetsklassad personal, vilket tills vidare bara är möjligt att tilldela svenska medborgare.[48] Kompetensförsörjningen för tillsynsarbetet är alltså en komplicerad historia som särskilt vid aktiviteter som innebär en hög risk för hela befolkningens kollektiva och personliga integriteter och samtidigt är av en väldigt teknisk art skapar dåliga förutsättningar för privatpersoner att säkerställa sig om att deras rättigheter respekteras och att de själva kan utöva sina rättigheter.

Sammanfattning.

Utredaren bör utifrån de brett accepterade principerna och frågeställningarna belysta av Venedigkommissionen[a] göra en genomlysning av strukturen kring de svenska underrättelsemyndigheterna och avgränsa sammanblandningen mellan de myndigheter som arbetar inom och utom försvarsverksamheter och den nationella säkerheten från de andra myndigheterna. Vid behov bör utredaren också föreslå insnävningar av uppdrag för de myndigheter som inte faktiskt primärt är verksamma inom försvar och nationell säkerhet.

[a] Se fotnot 24.

The number and variety of tasks that a SOC may perform, some of which we have mentioned above, is indeed daunting. A SOC should not focus on performing all of these all at once, but gradually increase the number of capabilities and services offered and only when enough resources are available. It is better to get good at only a number of the tasks than to be mediocre or bad at all or some of them [103, 106]. Another factor that plays a role in what specific services and capabilities are offered by a SOC is the organization of the SOC, which we describe next.

[45] Se ovan fotnot 39.
[46] SOC-projektet påbörjades först 2015 enligt dokumentet i fotnot 40.
[47] SOU 2016:65.
[48] SOU 2015:25, kap. 18.7.

Åtgärder mot sämre informationssäkerhet för enskilda och konsumenter

I inlagorna till utredningarna om modernisering av beslag och husrannsakan (Ju 2016:08)[49] och hemlig dataavläsning (Ju 2016:12)[50] har Dataskydd.net tillsammans med Föreningen för digitala fri- och rättigheter utvecklat hur användningen av *sanktionerade dataintrång* (det som i den försvarsorienterade verksamheten kallas för *offensiv IT-säkerhet*) skadar konsumenters och privatpersoners intressen av pålitliga, tekniska verktyg att genomföra sina dagliga kommersiella och sociala sysslor, samt uppfylla sina förpliktelser gentemot offentliga organ.

Vi gör följande terminologiska uppdelningar:

Teknisk säkerhet.

Teknisk säkerhet innefattar tekniska funktioner: funktioner som kan konstrueras, uppfinnas och omsättas på en marknad. En brist på teknisk säkerhet gör till exempel att man kan utföra kort-skimning (kopiera magnetremsan på ett kreditkort), stjäla inloggningsuppgifter, infektera en privatpersons dator med virus, trojaner, och dylikt.

Juridisk säkerhet.

Juridisk säkerhet innefattar konsumentinformation, riskfördelning, produktansvar, och frågeställningar om bevisbörda, till exempel vid tvister om vad ett avtal har sagt eller huruvida en produkt fungerat så som en konsument eller privatperson förväntat sig.

Sanktionerade dataintrång.

Sanktionerade dataintrång Att hacka, begå dataintrång, genomföra hemlig dataavläsning, husrannsakan i en dator, husrannsakan på distans och offensiv IT-säkerhet används omväxlande för att beskriva samma tekniska funktioner, nämligen att man utan lov från innehavaren av en viss elektronisk utrustning bereder sig tillgång till funktioner (så som att ändra, läsa, spela in, kopiera, radera eller manipulera data, filer, eller programvaror) på utrustningen. Vi kommer att använda begreppet ”sanktionerade dataintrång” som samlingsterm för samtliga dessa begrepp.

Sårbarhet.

En sårbarhet i ett IT-system, även kallat bugg eller säkerhetshål, är ett säkerhetsfel som gör det möjligt att utnyttja IT-systemet på ett sätt det inte är tänkt (till exempel att någon kommer åt funktioner i systemet olovligen).

Åtgärda en sårbarhet.

Att åtgärda en sårbarhet betyder att man ser till att sårbarheten inte längre kan användas för att bereda tillgång till funktioner olovligen. Det innebär oftast att man skriver om programkoden som används för att styra IT-systemet, men kan också innebära till exempel att man gör en ny och bättre standard för den bakomliggande utrustningen.

0-day.

0-day är ett tekniskt begrepp som beskriver en metod att utnyttja tidigare okända sårbarheter i IT-system, som på grund av att de inte tidigare är kända därför inte heller har åtgärdats. Ordet *0-day* används också för att beskriva en tidigare okänd metod att utnyttja en tidigare känd sårbarhet, som på grund av att sårbarheten inte uppfattats som säkerhetskritisk kanske inte har åtgärdats.

Metoder för att utnyttja sårbarheter.

Metoder för att utnyttja sårbarheter är det svenska begrepp vi kommer att

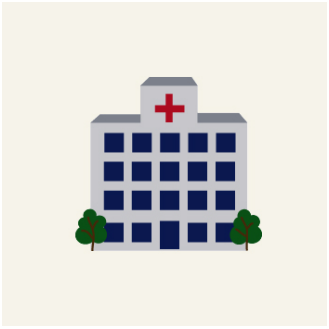
[49] Se ovan fotnot 23.
[50] Se ovan fotnot 22.

använda för att beskriva det som på engelska kallas *exploits*. Dessa metoder kan begagna sig av redan kända sårbarheter (vilket är normalfallet), eller tidigare okända sårbarheter (i vilket fall metoden är en *0-day*).

En offensiv IT-säkerhetsåtgärd gör inte bara skada vid själva avlyssnings- och övervakningstillfället, utan kan fortsätta göra skada tills dess att de tekniska åtgärder som vidtagits av underrättelsemyndigheterna görs ogjorda på de datorer som de tekniska åtgärderna utförts på. Utredaren kan jämföra med datorvirus, som inte försvinner från den drabbades dator förrän ett antivirusprogram letat fram och tagit bort den skadliga koden, eller man har ominstallerat sitt operativsystem.

Den kan också vara svårt (om inte omöjligt), rent tekniskt, att säkerställa sig om att den metod man använt för att nå ett IT-system på distans bara faktiskt når det IT-system som det är avsett för. Otillbörlig spridning av metoder för att utnyttja sårbarheter skedde till exempel i Tyskland 2011,[51] och för de oavsiktligen drabbade finns ingen hjälp att få så länge det inte är känt hur man kan laga det introducerade säkerhetsproblemet. Senast under våren 2017 drabbades flertalet större administrativa system för offentliga verksamheter inom kommuner och i sjukvården, i både Sverige[52] och utomlands,[53] av utpressningstrojanen WannaCry. Trojanen utvecklades i sin tur på bas av underrättelseutvecklade metoder för att utnyttja sårbarheter i ett IT-system.[54]

Sanktionerade dataintrång, oavsett vad man kallar dem, har alltså redan bevisligen orsakat risker och skador för civila verksamheter i hela världen, till en hög kostnad, och det finns inga sätt att garantera att just de sanktionerade dataintrång som svenska försvarsmyndigheter och underrättelsemyndigheter eller säkerhetstjänster ägnar sig åt i den offensiva IT-säkerhetens namn inte kommer att orsaka motsvarande skador. Förfarandet bör alltså av säkerhetsskäl och hänsyn till de icke-militära verksamheterna begränsas.



Egalt vems fel attackmjukvaran är. För att sjukhus är det ovidkommande vem som utvecklat en attackmjukvara eller sårbarheterna och metoderna att utnyttja sårbarheterna som attackmjukvaran använder sig av. Om flertalet datorer låser sig till följd av en utpressningstrojan så är det ju så, även om sårbarheten som trojanen använder för att snirkla sig in i datorn utvecklades av en (svensk) underrättelsetjänst.

Det finns idag ett relativt stort antal företag som professionellt ägnar sig åt att ta fram metoder för brottsbekämpande myndigheter och underrättelsetjänster att utföra sanktionerade dataintrång. Dessa företag drivs inte sällan av och med personer som kommer från offentlig sektor, till exempel från underrättelsetjänster eller från de brottsbekämpande myndigheterna.[55,56,57,58] Företagen rekryterar tidigare offentliganställda, och utvecklar eller köper in metoder att utnyttja sårbarheter på uppdrag av offentlig sektor.

För myndigheterna finns det fördelar med att outsource:a verksamheten. Privat sektor omfattas inte av några krav på transparens och offentlighet. Det

[51] Graham Cluley (10 oktober 2011) ”German ‘Government’ R2D2 Trojan FAQ”, Naked Security (Sophos).

[52] NyTeknik. Kalle Wiklund (17 maj 2017) Timrå kommun: Miss hos it-leverantör öppnade för Wannacry.

[53] The Guardian. Alex Hern och Samuel Gibbs (12 maj 2017) What is WannaCry ransomware and why is it attacking global computers?

[54] Wired. Matt Burgess (28 juni 2017) Everything you need to know about EternalBlue – the NSA exploit linked to Petya.

[55] Andy Greenberg (21 March 2012). ”Meet The Hackers Who Sell Spies The Tools To Crack Your PC (And Get Paid Six-Figure Fees)” Forbes.

[56] Adrianne Jeffries (13 September 2013). ”Meet Hacking Team, the company that helps the police hack you” The Verge.

[57] Vernon Silver (8 november 2012) ”MJM as Personified Evil Says Spyware Saves Lives Not Kills Them” Bloomberg.

[58] Der Spiegel, 9 november 2014 ”BND will Informationen ueber Software-Sicherheitsluecken einkaufen”.

gör att varken företag eller myndigheter behöver redovisa om de har kunskap om metoder för att utnyttja sårbarheter. Marknaden för kunskap om metoder för att utnyttja sårbarheter är delvis kartlagd och delvis vit,[59] men den är ofta också inte vit och inte kartlagd.[60] De företag som hjälper brottsbekämpande myndigheter hitta sårbarheter i elektroniska produkter som används av slutkonsumenter har dock bevisligen haft att göra med sådana sårbarheter som också används vid aktiviteter som skadar enskildas och konsumenters intressen.[61] Behovet av regler för denna marknad har lyfts i europeiska sammanhang av bland andra europeiska dataskyddstillsynsmannen,[62] men i Sverige saknas en sådan diskussion.

Eftersom de mässor och konferenser som äger rum för försäljning och marknadsföring av dataintrångsprodukter omgärdas av sekretess (antingen via offentliga sekretessregler eller genom *non-disclosure agreements*)[63] har det visat sig vara svårt att få en bild av vad marknaden är, vem som utvecklar saker, till vilket pris och till vilka sårbarheterna säljs.

När det väl finns företag som ägnar sig åt att förmedla metoder för utnyttjande av sårbarheter i IT-system till underrättelsemyndigheter, blir dessa företag en egen intressegrupp som utövar politiskt inflytande på de underrättelsemyndigheterna och på politiker. Vid Torontos universitet i Kanada, har CitizenLab-gruppen kartlagt vad de menar utgör ett ”*cyber-war industrial complex*” som omsätter åtskilliga tiotals miljarder dollar per år.[64,65,66] Företagens egenintresse kan antas vara att framställa sig som ovärderliga och nödvändiga för effektiv underrättelseverksamhet, eftersom deras huvudsakliga intäktskälla är just samarbete med underrättelsemyndigheter.

Det här skapar ett behov av ytterligare regler kring hur underrättelsemyndigheter som ägnar sig åt nationell säkerhet eller försvarsintressen får befatta sig med sårbarheter, så att inte den nationella säkerheten och försvarsintressena börjar agera menligt mot den egna befolkningens intressen. Vi har alla ett intresse av att våra smartphones, våra webbläsare och våra arbetsstationer fungerar på det sätt vi tror och vill att de ska göra.

Sammanfattning.

Om myndigheterna med ansvar för nationell säkerhet eller försvarsintressen får kännedom om en tidigare okänd sårbarhet eller metod för att utnyttja en sårbarhet (en så kallad *0-day*, för definition se s. 17) ska de omedelbart vidta åtgärder för att sårbarheten eller metoden att använda

[59] Se ovan fotnot 55.

[60] SpiderLabs Research (31 maj 2016) Zero Day Auction for the Masses, Trustwave Spiderlabs Blog.

[61] Peter Pi (7 juli 2015) ”Unpatched Flash Player Flaw, More POCs Found in Hacking Team Leak”, Trendlabs Security Intelligence Blogs.

[62] EDPS, Opinion 8/2015: Dissemination and use of intrusive surveillance technologies.

[63] Ryan Gallagher (1 november 2011) ”Governments turn to hacking techniques for surveillance of citizens” The Guardian.

[64] Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton, “For Their Eyes Only: The Commercialization of Digital Spying,” Citizen Lab Research Brief No. 17, April 2013.

[65] Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton, “You Only Click Twice: FinFisher’s Global Proliferation,” Citizen Lab Research Brief No. 15, March 2013.

[66] Morgan Marquis-Boire (lead technical research) and Jakub Dalek (lead technical research), Sarah McKune (lead legal research), Matthew Carrieri, Masashi Crete-Nishihata, Ron Deibert, Saad Omar Khan, Helmi Noman, John Scott-Railton, and Greg Wiseman, “Planet Blue Coat: Mapping Global Censorship and Surveillance Tools,” Citizen Lab Research Brief No. 13, January 2013.

sårbarheten blir känd och kan åtgärdas.

Om en sårbarhet eller metod för att utnyttja en sårbarhet *köps in* för att integreras i myndigheternas befintliga IT-stöd eller i ett inköpt IT-stöd, ska sårbarheten eller metoden för att utnyttja sårbarheten senast tre månader efter inköpsdatum publiceras så att största antal svenska och europeiska företag, myndigheter och privatpersoner så snabbt som möjligt kan få hjälp och incitament att åtgärda sårbarheterna i sina egna maskiner.

Amelia Andersdotter
Ordförande, Dataskydd.net

Källhänvisningar med länkar där möjligt

Akademi

1. Tormod Otter Johansen och Sebastian Wejedal, ”Mot ett funktionellt domstolsbegrepp – Ett bidrag med anledning av den så kallade Försvarsunderrättelsedomstolen”, SvJT 2016 s. 10.
2. Tormod Otter Johansen och Sebastian Wejedal, ”Mot ett funktionellt domstolsbegrepp – Ett bidrag med anledning av den så kallade Försvarsunderrättelsedomstolen”, SvJT 2016 s. 191.
3. Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton, “For Their Eyes Only: The Commercialization of Digital Spying,” Citizen Lab Research Brief No. 17, April 2013. https://citizenlab.org/storage/finfisher/final/fortheireyesonly.pdf
4. Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton, “You Only Click Twice: FinFisher’s Global Proliferation,” Citizen Lab Research Brief No. 15, March 2013. https://citizenlab.org/wp-content/uploads/2009/10/You-Only-Click-Twice-FinFisher%E2%80%99s-Global-Proliferation.pdf
5. Morgan Marquis-Boire (lead technical research) and Jakub Dalek (lead technical research), Sarah McKune (lead legal research), Matthew Carrieri, Masashi Crete-Nishihata, Ron Deibert, Saad Omar Khan, Helmi Noman, John Scott-Railton, and Greg Wiseman, “Planet Blue Coat: Mapping Global Censorship and Surveillance Tools,” Citizen Lab Research Brief No. 13, January 2013. https://citizenlab.org/wp-content/uploads/2015/03/Planet-Blue-Coat-Mapping-Global-Censorship-and-Surveillance-ToolsPlanet-Blue-Coat-Mapping-Global-Censorship-and-Surveillance-Tools.pdf
6. Slatman, Herman. Unboxing Security Analytics: Towards Effective Data Driven Security Operations, Master Thesis Computer Science, Universiteit Twente. http://essay.utwente.nl/69788/1/Slatman_MA_EEMCS.pdf

Offentliga tryck

1. Artikel 29-gruppen, WP 215, 819/14/EN, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf
2. EDPS, Opinion 8/2015: Dissemination and use of intrusive surveillance technologies. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-12-15_Intrusive_surveillance_EN.pdf
3. Europarådets människorättskommissionär, CommDH/IssuePaper(2014)1. 8 december 2014. *The rule of law on the Internet and in the wider digital world. Issue Paper published by the Council of Europe Commissioner for Human Rights.* https://wcd.coe.int/ViewDoc.jsp?id=2268589&Site=COE
4. Europarådets parlamentariska utskott, Resolution 2045 (2015) ”Mass surveillance” Text adopted by the Assembly on 21 April 2015 (12th Sitting), med tillhörande Recommendation 2067 (2015).
5. Europarådets Venedigkommission, *Rule of Law Checklist* (CDL-AD(2016)007), Study No. 711 / 2013, Adopted by the Venice Commission at its 106th Plenary Session (Venice, 11-12 March 2016), Endorsed by the Ministers’ Deputies at the 1263th Meeting (6-7 September 2016), Endorsed by the Congress of Local and Regional Authorities of the Council of Europe at its 31st Session (19-21 October 2016). http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)007-e
6. Förenta nationernas generalförsamling, Rapporter om mänskliga rättigheter till FN:s generalförsamling, 69 sessionen. Rapport A/69/397 av 23 september 2014. http://www.ohchr.org/EN/newyork/Pages/HRreportstothe69thsessionGA.aspx
7. Förenta nationernas generalförsamling, General Assembly resolution A/C.3/69/L.26/Rev.1, The right to privacy in the digital age, (25 november 2014). http://www.un.org/en/ga/third/69/propslist.shtml
8. Förenta nationernas människorättsråd, Högsta representantens rapport, 27 sessionen. Rapport A/HRC/27/37 av den 30 juni 2014. Tillgänglig på: http://ap.ohchr.org/documents/alldocs.aspx?doc_id=23880

9. Förenta nationernas människorättsråd, 34 sessionen, Resolution A/HRC/34/L.7/Rev.1 *The right to privacy in a digital age*. http://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=21442&LangID=E
10. Förenta nationernas människorättsråd, *Report of the Special Rapporteur to the Human Rights Council on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression*, A.HRC.23.40 EN (2013) http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf
11. Förenta nationernas människorättsråd, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A.HRC.35.22 EN (2017). http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/35/22
12. Försvarets radioanstalt, promemoria inlämnad till Datainspektionen 28 april 2017, Redogörelse avseende regelbunden logguppföljning i försvarsunderrättelseverksamheten. https://dataskydd.net/sites/default/files/fras_skrivelse_till_datainspektionen_28_april_2017_2.pdf
13. Regeringen, För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi (N2017/03643/D). http://www.regeringen.se/49adea/contentassets/5429e024be6847fc907b786ab954228f/digitaliseringsstrategin_slutlig_170518-2.pdf

Rättsfall

1. Europeiska domstolen för mänskliga rättigheter. Zakharov v. Ryssland (Application no. 47143/06), 4 december 2015. http://hudoc.echr.coe.int/eng?i=001-159324
2. Europeiska domstolen för mänskliga rättigheter. Szabo och Vissy v. Ungern (Application no. 37138/14), 12 januari 2016. http://hudoc.echr.coe.int/eng?i=001-160020
3. ECLI:EU:C:2016:970, *Tele2 v Sweden*, C-203/15. http://curia.europa.eu/juris/liste.jsf?num=C-203/15
4. NJA 2013 s. 746. https://lagen.nu/dom/nja/2013s746

Övriga källor

1. Bloomberg. Ben Elgin, Michael Riley, David Kocieniewski, och Joshua Brustein (24 september 2015) The Fake Traffic Schemes That Are Rotting The Internet. https://www.bloomberg.com/features/2015-click-fraud/
2. Centrum för rättvisa mot staten (FRA). http://centrumforrattvisa.se/personlig-integritet/centrum-for-rattvisa-tar-fra-lagen-till-europadomstolen/
3. Graham Cluley (10 oktober 2011) "German 'Government' R2D2 Trojan FAQ", Naked Security (Sophos). https://nakedsecurity.sophos.com/2011/10/10/german-government-r2d2-trojan-faq/
4. Dagens nyheter (30 mars 2017) Debatt, Stefan Löfven: Så ska vi skydda valrörelsen från andra staters påverkan. http://www.dn.se/debatt/sa-ska-vi-skydda-valrorelsen-fran-andra-staters-paverkan/
5. Dataskydd.net, Remissyttrande över Ds 2016:31, Behandling av personuppgifter inom Nationellt centrum för terrorhotbedömning. https://dataskydd.net/sites/default/files/ds201631_remissyttrande_dataskyddnet_20161216.pdf
6. Dataskydd.net, Remissyttrande över SOU 2016:7 om stärkt straffskydd för integriteten. https://dataskydd.net/sites/default/files/dataskyddnet_remissyttrande_sou201607_20160509.pdf
7. Dataskydd.net och Föreningen för digitala fri- och rättigheter (DFRI) skickar en skrivelse till den pågående utredningen om hemlig dataavläsning. https://dataskydd.net/sites/default/files/dir201636_dfri_dataskyddnet_slutgiltig_2.pdf
8. Dataskydd.net och Föreningen för digitala fri- och rättigheter (DFRI) skickar en skrivelse till den pågående utredningen om modernisering av beslag och husrannsakan. https://dataskydd.net/sites/default/files/dir201620_dfri_dataskydd_slutgiltig.pdf

9. Ryan Gallagher (1 november 2011) ”Governments turn to hacking techniques for surveillance of citizens” The Guardian. https://www.theguardian.com/technology/2011/nov/01/governments-hacking-techniques-surveillance
10. Andy Greenberg (21 March 2012). ”Meet The Hackers Who Sell Spies The Tools To Crack Your PC (And Get Paid Six-Figure Fees)” Forbes. http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/#b84a4e094483
11. The Guardian. Alex Hern och Samuel Gibbs (12 maj 2017) What is WannaCry ransomware and why is it attacking global computers? https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20
12. Adrianne Jeffries (13 September 2013). ”Meet Hacking Team, the company that helps the police hack you” The Verge. http://www.theverge.com/2013/9/13/4723610/meet-hacking-team-the-company-that-helps-police-hack-into-computers
13. NyTeknik. Kalle Wiklund (17 maj 2017) Timrå kommun: Miss hos it-leverantör öppnade för Wannacry. https://www.nyteknik.se/digitalisering/timra-kommun-miss-hos-it-leverantor-oppnade-for-wannacry-6849137
14. Peter Pi (7 juli 2015) ”Unpatched Flash Player Flaw, More POCs Found in Hacking Team Leak”, Trendlabs Security Intelligence Blogs. http://blog.trendmicro.com/trendlabs-security-intelligence/unpatched-flash-player-flaws-more-pocs-found-in-hacking-team-leak/
15. Vernon Silver (8 november 2012) ”MJM as Personified Evil Says Spyware Saves Lives Not Kills Them” Bloomberg. http://www.bloomberg.com/news/articles/2012-11-08/mjm-as-personified-evil-says-spyware-saves-lives-not-kills-them
16. SpiderLabs Research (31 maj 2016) Zero Day Auction for the Masses, Trustwave Spiderlabs Blog. https://www.trustwave.com/Resources/SpiderLabs-Blog/Zero-Day-Auction-for-the-Masses/
17. Der Spiegel, 9 november 2014 ”BND will Informationen ueber Software-Sicherheitsluecken einkaufen” http://www.spiegel.de/spiegel/vorab/bnd-will-informationen-ueber-software-sicherheitsluecken-einkaufen-a-1001771.html
18. Wired. Matt Burgess (28 juni 2017) Everything you need to know about EternalBlue – the NSA exploit linked to Petya. http://www.wired.co.uk/article/what-is-eternal-blue-exploit-vulnerability-patch