



INTERNATIONELLA HANDELSHÖGSKOLAN
HÖGSKOLAN I JÖNKÖPING

Signalspaning

Helgar ändamålet medlen?

Kandidatuppsats i Statsvetenskap

Författare: Gunilla Edwertz

Handledare: Benny Hjern

Jönköping Januari 2009

Kandidatuppsats inom Statsvetenskap

Titel:	Signalspaning – helgar ändamålet medlen?
Författare:	Gunilla Edwertz
Handledare:	Benny Hjern och Mikael Sandberg
Datum:	2009-01-19
Ämnesord	Signalspaning, terrorism, cyberterrorism, statsvetenskap, politik

Sammanfattning

Debatten om den kontroversiella signalspaningslagen är högst aktuell och det diskuteras öppet och intensivt om huruvida den är ett skydd mot hot utifrån eller om den hotar medborgarna i det svenska samhället. När uppsatsen avslutas har lagen trätt i kraft den 1 januari 2009, men kommer inte att träda i full kraft förrän i oktober 2009.

Terrorism är ett fenomen som har fått en ny betydelse för människor i det globala samhället. Det har alltid funnits i samtid som det demokratiskt politiska samhället, men betydelsen av detta fenomen, detta begrepp har varierat. Den har skiftat under åren från att vara en terrorism där grupper som IRA och ETA figurerade för att frigöra territorium från de stora länderna till att handla om att påverka politiska beslut genom att skrämma civila. Cyberterrorism är ett nyare fenomen inom begreppet och har en annan verkan då den riktar sig mot det nya informationstekniska samhället som har blivit allt mer sårbart ju längre utvecklingen går.

Syftet med uppsatsen har varit att undersöka vilket sorts inflytande som cyberterrorism har haft i utformandet av lagen, om lagen är ett hot mot Sverige eller ett skydd för Sverige samt huruvida signalspaning rättfärdigas av ändamålet, det vill säga att ge Sverige ett fungerande säkerhetsskydd.

Slutsatsen av denna uppsats är att cyberterrorism har ett visst samband med hur lagen har utformats, men det är inte en avgörande eller ensam faktor. Huruvida lagen är ett hot mot Sverige eller ett skydd för och om ändamålet helgar medlen har det kommit fram till att den till viss del kan vara ett hot, men att ändamålet att politikerna vill kunna ge Sverige ett fungerande säkerhetsskydd väger upp till en viss del vad lagen vill stå för. Det är fortfarande en hel del motsättningar mot lagen och det kommer det alltid att vara.

Bachelor thesis in Political Science

Title	Signals intelligence – do the aim justify the means?
Author:	Gunilla Edwertz
Tutors:	Benny Hjern och Mikael Sandberg
Date:	2009-01-19
Search words	Signals intelligence, terrorism, cyber terrorism, political science, politics

Abstract

This thesis has its origins in the controversial debate about the signals intelligence law that has been a highly intensive debate since the law was passed on June 18 2008. The debate mainly is about whether or not the law is a protection against threat towards the Swedish nation-state or if the law is at threat against the citizen of the Swedish society. The law will have been put in to force on January 1 2009, but won't be in full force until October 2009.

Terrorism is not a phenomena that is new, but it has gotten a new meaning to people in the global society. Though it has always existed with the democratic political society, it's meaning has been a target for change. The meaning has shifted from being about groups like IRA and ETA that fight for their own territories to be about influencing political decisions through scarring civilians. One of the more newer phenomena within terrorism is cyber terrorism and it has another effect because it directs itself towards the information technology of the modern society. The IT society has become more vulnerable because of the development and that is what cyber terrorism is attacking the vulnerability.

The purpose of this thesis is to examine what kind of influence that cyber terrorism has had in the design of the law, if the law is a threat against Sweden or a protection for Sweden, that is what arguments surrounds this case, and do the aim, that is protecting the society, justify the means, that is signals intelligence in giving Sweden a functional security.

The conclusion in this thesis is that cyber terrorism has had an indirect connection to how the law has been designed, but the threat of cyber terrorism has not been a deal breaking or alone factor. Whether the law is a threat or not depends on who you talk to, but it might be a threat to a certain extent if the lawmakers don't hear the critics and change the law to the extent that it involves a fully protection for the privacy of the citizens. In the end it is partly true that the aim does justify the means.

Innehåll

Akronymer och förkortningar	1
1 Introduktion	2
1.1 Problemformulering	2
1.2 Syfte och frågeställningar.....	2
1.3 Avgränsningar	3
1.4 Metod	3
1.4.1 Begreppsanalys.....	3
1.4.2 Kvalitativ textanalys.....	3
1.4.3 Metodkritik.....	4
1.5 Material.....	4
1.5.1 Källkritik.....	4
1.6 Disposition	5
2 De fyra stora terrorattackerna	6
2.1 USA den 11 september 2001	6
2.2 Bali den 12 oktober 2002	7
2.3 Madrid den 11 mars 2004	8
2.4 London den 7 juli 2005	9
3 Terrorismen förr och nu	11
3.1 Svårigheten att definiera terrorism.....	12
3.2 Definitionerna av begreppet terrorism.....	15
3.3 Cyberterrorism.....	17
4 Försvarets radioanstalt och signalspaning	20
4.1 Försvarets radioanstalt	20
4.2 Signalspaning	21
4.2.1 Personlig integritet.....	23
4.3 Lagen och dess kritiker.....	24
4.3.1 Europadomstolen	25
4.4 IT-relaterade hot.....	26
5 Resonemang kring studien och slutsats	28
5.1 Uppsatsens syfte.....	28
5.2 Eventuella kopplingar mellan cyberterrorism och FRA-lagen.....	28
5.3 Det så kallade skyddet för Sverige.....	29
5.4 Slutsats	29
Referenser	31

Litteratur.....	31
Artiklar	32
Internet	34
Svenskt offentligt tryck.....	35
Annat offentligt tryck	36

Akronymer och förkortningar

CFR = Centrum för Rättvisa

ETF = Electric Test Facility

EU = Europeiska Unionen

FRA = Försvarets radioanstalt

FRA-lagen = lag (2008:717) om signalspaning i försvarsunderrättelsetjänsten

FUV = Försvarsunderrättelseverksamhet

ICT = Interception of Communications Tribunal

KOS = kommunikationsspaning

RIPA = Regulation of Investigatory Powers Act

TES = teknisk signalspaning

1 Introduktion

Inom loppet av sex månader har en av de mest kontroversiella lagarna som regeringen lämnat in en proposition för och som riksdagen röstat igenom skapat debattstormar som pågår i skrivande stund. Lag (2008:717) om signalspaning i försvarsunderrättelsetjänsten (FRA-lagen) har trätt i kraft och därmed satt en markering i svensk politik och rättssamhälle för framtida beslutsfattare och debattörer om huruvida det svenska rättssamhället och det svenska politiska samhället skall skyddas. För ett skydd mot hot har aldrig varit ifrågasatt i debatten, vad som har ifrågasatts är snarare medlet som används att skydda samhället.

Det är inte första gången en lag om signalspaning skapats, Sverige är inte ensamma om att ha skapat en lag där signalspaning är en grund. Länder som Nederländerna och Schweiz har även de valt att legalisera signalspaning på liknande sätt (Prop. 2006/07:63, 2006, s.24-25). Det kan verka som att en uppsats endast skulle kunna handla om de bakomliggande besluten kritiken mot lagen och det skydd den skall ge, men istället kände jag att det fanns ett behov av att undersöka om cyberterrorism, ett relativt nytt fenomen inom det politiska begreppet terrorism, hade en del i det hela.

Den tidigare forskning som finns inom det teoretiska område jag har valt är rätt stor, terrorism är inget nytt, men för att nämna några böcker och namn som dessutom figurerar i uppsatsen så kan jag nämna dessa:

De nya krigen av Herfried Münkler (2004).

Fighting Terror in Cyberspace av Mark Last och Abraham Kandel (2005).

1.1 Problemformulering

Problemet som jag ställde mig till ursprungligen handlade om ifall lagen var en form av cyberterrorism, då det diskuterades om all den inskränkning och kränkning som skulle begås på det personliga integritetsskyddet, men under tiden som jag läste mig in på ämnet och de olika delarna, ställer jag mitt problem till om lagens utformande är en följd av cyberterrorism. Denna fråga tillsammans med två andra har fått utgöra grundstenarna i denna uppsats.

1.2 Syfte och frågeställningar

Det huvudsakliga syftet med denna uppsats är att undersöka huruvida de problem, klagomål och kritik som FRA-lagen har fått sedan den gick igenom den 18 juni 2008, utifrån den teori jag har valt, är tillräckligt allvarliga för att det bör bli ännu en förändring innan lagen blir fullt brukbar i oktober 2009. Detta är en dagsaktuell debatt, därmed inte heller den allra enklaste att undersöka, men undersökningen av lagen och signalspaning kommer att bedrivas med hjälp av ett litteraturanalytiskt ramverk som ligger till grund för denna uppsats. Med hjälp av teorin är syftet att undersöka huruvida definitionen av cyberterrorism har påverkat lagens utformande och om FRA-lagen verkligen bör ses som ett hot eller ett skydd för Sverige, vilket det råder skilda åsikter om i den politiska debatten.

Har syftet med FRA-lagens utformande rättfärdigat den eventuella inskränkning som görs på medborgarnas integritet för att skydda Sverige från cyberterrorism?

Har cyberterrorism varit en påverkan i hur lagen har utformats?

Finns det några argument eller orsaker som pekar på att lagen skulle kunna vara ett hot för eller ett skydd för Sverige?

1.3 Avgränsningar

Jag valde att använda mig av terrorism, ett svårdefinierbart politiskt fenomen som jag egentligen skulle kunna göra ett helt arbete om. Inom terrorism finns det flera underkategorier och av dessa valde jag att begränsa mig till cyberterrorism för att jag ser det som en teori som har blivit utforskad, men inte till den graden att det känns uttjatat och söndertrasat. Det finns fortfarande en hel del att ta av därifrån. Jag vill också nämna att jag har valt att undvika utsvävningar om gerillakrigföring och andra liknande organiserade krigföringar och separatistgrupper trots att det ofta är gerillakrigföring och terrorism som hamnar inom samma område. Det känns inte som att det är väsentligt för arbetet och inte är heller en mer ingående kunskap om vad lagarna i Schweiz och Nederländerna säger då dessa inte har varit uppe i Europadomstolen, men det har Storbritanniens och Tysklands. Jag valde därför att ta med dessa två för att de liknar den svenska lagstiftningen och detta har betydelse i kritiken mot lagen.

1.4 Metod

Uppsatsen är uppdelad i tre delar. Dessa delar innefattar metoder som binds samman och kopplas ihop i ett slutförande resonemang och analys av uppsatsen. En kvalitativ textanalys har genomförts samt en begreppsanalys av begreppen terrorism och cyberterrorism som skall tillföra en klarare bild i den slutförande diskussionen kring de frågeställningar jag använder mig av. Denna uppsats är en teorikonsumerande uppsats där fallet, FRA-lagen och signalspaning, sätts i centrum, vilket betyder att resultaten inte måste vara giltiga för andra fall som inte tas upp i denna uppsats (Esaiasson, Gilljam, Oscarsson, Wängnerud, 2004, s.34).

1.4.1 Begreppsanalys

Med begreppsanalys menas det att jag som forskare vill förtydliga vad begreppet innebär. I denna uppsats innebär det flera politiska begrepp, men främst terrorism och cyberterrorism. Ett enkelt sätt att se på begreppsanalys är att begreppet har fem steg som under största möjlighet försöker bli följda i uppsatsen, trots att det inte är helt uppenbart; 1. Det som har skrivits om begreppet, i detta fall terrorism och cyberterrorism, söks och samlas in för bearbetning; 2. De olika definitioner av begreppet som finns sorteras och i detta skall kärnan i det begrepp som utreds samt skillnader sållas fram; 3. I tredje steget ska dessa definitioner prövas om de är logiskt konsistenta; 4. Här ska definitionerna eller definitionen prövas om den är användbar i en empirisk forskning; 5. I det femte steget skall det tas ställning för den "bästa" begreppsdefinitionen om det finns en möjlighet till detta (Esaiasson et al., 2004, s. 34).

1.4.2 Kvalitativ textanalys

Utöver att denna uppsats är en begreppsanalys i och med att den har en viss utredningsstudie av det politiska fenomenet terrorism och att den innehåller en fallstudie som det söks ett samband emellan så är denna uppsats en kvalitativ textanalys, en metod som är mycket

vanlig inom samhällsvetenskapen, just för att den i allmän mening används av alla forskare i tidigare forskningsinstanser (Esaiasson et al, 2003, s.233).

Varför är uppsatsen en kvalitativ textanalys? Svaret på frågan grundar sig i det faktum att uppsatsen är en genomgående idékritisk analys, det vill säga att jag vill få fram ett ställningstagande om huruvida det är rationellt att använda sig av en metod om total signalspaning och FRA-lagen för att motverka hot som terrorism och cyberterrorism, men att det då kan påverka samhället och dess civila befolkning negativt. Att använda textanalys framför den kvantitativa innehållsanalysen är att helheten i texten antas vara något som inte är en summa av delarna. Det vill säga att vissa delar av texten är viktigare än andra. Innehållet som forskare vill åt i en textanalys är ofta dolt under ytan och därmed något som tas fram vid en närläsning av texten (Esaiasson et al, 2003, s.233).

1.4.3 Metodkritik

Min uppsats bygger endast på ett fall och en teori, detta gör att det inte går att dra några allmänna generaliseringar i slutsatserna eftersom att jag här vill se om cyberterrorism ger en tillfredsställande förklaring till varför FRA-lagen ser ut som den gör, det är därför slutsatserna endast gäller området som uppsatsen tar upp (Esaiasson et al., 2004, s.98). Detta beror en del på att debatten fortfarande pågår och det finns inget slut som kan ge någon konkret slutsats. Detta gör att uppsatsen begränsas, men det är ett medvetet val jag har gjort och grundar sig i främst att det inte skulle vara möjligt att skriva klart uppsatsen om jag valt att lägga upp den på annat vis och haft in fler politiska begrepp som kan ha påverkat signalspaningsverksamhetens syfte och ändamål och FRA-lagens uppkomst.

1.5 Material

Uppsatsen bygger på två olika källor. Det ena är primärkällor såsom fakta från statliga myndigheter och offentliga, officiella publikationer. Primära källor har blivit funna via bibliotek, statliga myndigheters hemsidor och via Google. Det andra är sekundärkällor, vilket i denna uppsats är litteratur, internetkällor artiklar, både debattartiklar och nyhetsartiklar om cyberterrorism, signalspaning, terroristattacker i New York, Madrid, London och på Bali. Dessa sekundära källor har sökts i databasen Google och på tidningars hemsidor. Sökord som användes på svenska har varit *signalspaning, FRA, kritik mot FRA, cyberterrorism, terrorism, definition av terrorism och definition av cyberterrorism*. På engelska har sökorden varit *Signals intelligence, terrorism, cyberterrorism, London bombings, September 11, Madrid trainbombings och Bali bombings*.

1.5.1 Källkritik

Litteraturkällorna i uppsatsen anser jag har hög tillförlitlighet. Författarna av den litteratur som har använts är insatta i ämnesområdet och det finns mycket mer litteratur inom ämnesområdet som inte har tagits med i uppsatsen av den anledning att jag inte sett dem som relevanta för mitt syfte med uppsatsen. Artiklar som har tagits med i uppsatsen har använts är nyhetsartiklar och debattartiklar, skillnaden mellan dessa är att debattartiklar ofta innehar en eller flera personers åsikter om ämnet. En nyhetsartikel ska vara objektiv och styrks av den litteratur som används i uppsatsen. Ett exempel på att detta förekommer är hur de olika bombattacker beskrivs. Dessa har främst litteraturkällor, men även nyhetsartiklar och bland annat en rapport gjord av den Nationella Kommissionen i USA styrker det som nyhetsartiklarna rapporterar om hur händelseförloppet gick till när flygplanen kraschade in i

World Trade Center och Pentagon. Viss sänkt tillförlitlighet får artiklarna då de är hämtade från ett fåtal länder, främst Storbritannien och BBC, men detta anser jag inte vara ett problem när uppgifterna i artiklarna, återigen, styrks av det som sägs i annan litteratur.

Debattartiklarna som förekommer i fjärde kapitlet om kritiken mot FRA-lagen och signalspaningen är svårare att ge tillförlitlighet till eftersom att debattartiklar inte är nyhetsartiklar på samma sätt. Dessa artiklar är skrivna av människor med åsikter, men viss högre tillförlitlighet har de fått eftersom att den kritik de ger och vad de ger kritik på styrks av det fakta som propositioner, motion och andra offentligt tryckta primärkällor talar om i resten av kapitlet.

Då de flesta artiklar, pdf-filer och liknande källor har hämtats från Internet kan problemet uppstå att länkarna inte fungerar, vid tidig upptäckt av detta har jag undersökt vart de refereras i texten och sedan letat upp om informationen finns på annat håll, om detta görs har jag skrivit om texten och refererat om på nytt. Länkarna för Internetkällor fungerade de datum de hämtades.

1.6 Disposition

Upplägget av uppsatsen ser ut som sådan att i kapitel 1, där vi är nu, introduceras uppsatsen med problem, syfte, avgränsningar och metod/material. Här läggs hela tanken med uppsatsen fram. I kapitel 2 kommer det finnas information om de terroråd som har gjort ett stort intryck på hur terrorism ser ut idag, bland annat terrorattentaten den 11 september 2001 i New York, på Bali den 12 oktober 2002, i Madrid den 11 mars 2004 och i London den 7 juli 2005. I kapitel 3 diskuteras terrorism förr och nu, svårigheten att definiera terrorism och några definitioner a terrorism visas upp. Efter detta lägger jag fram cyberterrorism som ett av de nyare fenomenen inom terrorism. Kapitel 4 innehåller vad signalspaning är, myndigheten som skall ha ansvar för detta, lagen och dess kritik, samt vad Europadomstolen beslutade i två andra fall och vad som innebär med personlig integritet allmänt och i Sverige. Kapitel 5 görs en slutförande diskussion och sist lämnas en referenslista över litteratur, artiklar, internetkällor och offentligt tryck i Sverige och från övriga länder i världen.

2 De fyra stora terrorattackerna

Den empiriska bakgrunden av terrorism täcker de fyra större terrorattacker som skett sedan år 2000. Nedan beskrivs vad som hände, i kronologisk ordning, i USA den 11 september 2001, på Bali den 12 oktober 2002, den 11 mars 2004 i Madrid och i London den 7 juli 2005. Det har självklart funnits fler händelser än dessa under åren, men dessa terrorattacker har haft stor betydelse för Sverige då det i minst två av attackerna svenska liv har skördats och attackerna visar att synen på terrorism har kommit att förändrats.

2.1 USA den 11 september 2001

Den 11 september 2001 var en dag som ingen hade förväntat sig att något ovanligt skulle hända. Det var en strålande höstdag och miljontals människor beredde sig att gå till eller var redan på väg till arbetet. World Trade Centers sju byggnader, med sina karaktäristiska tvillingtorn, var en arbetsplats som en del av de miljontals människorna åkte till. Den dagen lyfte fyra plan; American Airlines Flight 11, United Airlines flight 175, American Airlines flight 77 och United Airlines flight 93 från tre flygplatser (Nationella kommissionen, 2004, s. 1, 4,6,8-9). Alla fyra planen kapades av fyra till fem terrorister, men bara tre plan nådde sina mål. Åtminstone sex av de totalt nitton terrorister som steg ombord planen hade gått på flygplansskola i USA och besökt landet sedan år 2000 (Migaux, 2007, s.329).

Flight 11 var det första kapade planet som nådde sitt mål och kraschade in i norra tornet av World Trade Centers tvillingtorn i New York City, de 92 personer ombord inklusive terroristerna och flygpersonalen dödades tillsammans med ett okänt antal människor i tornet (BBC News, 2008c). Flight 175 var plan nummer två att krascha in i det södra tornet där samma utgång som det första planet hade (Nationella kommissionen, 2004, s.4, 6, 8-9); utöver ett okänt antal personer i byggnaden dödades de 65 personer som fanns ombord planet, inklusive flygplanspersonal och terroristerna (BBC News, 2008d). Planet med flight 77 kraschade i Pentagon. Däremot var det annorlunda med flight 93, ingen vet exakt var planet skulle krascha men misstankarna var att det skulle krascha in i en viktig amerikansk symbol som Capitol Hill eller Vita Huset. Planet nådde aldrig fram utan kraschade på ett öde fält i Shanksville, Pennsylvania (Nationella kommissionen, 2004, s. 1, 4, 6, 8-9, 12-13).

I samma stund som det första planet kraschade i det norra tornet utgick ett larm från *FDNY:s Emergency Medical Services* till New Yorks brandförsvaret (Socialstyrelsen, 2004, s. 18). Planet hade kraschat mellan 95 och 103 våningen. Arbetande individer var redan på plats vid sina kontor och på 106e våningen fanns 80 kockar och kökspersonal som arbetade i restaurangen. Människor som befann sig på sina kontor mellan våningarna där planet kraschade dödades direkt (BBC News, 2008f). Kaos utbröt och jetbränslet från de kraschade planen gav upphov till tjock rök som drog sig uppåt i byggnaderna¹. Larmcentralen var nedringd av ögonvittnen och flera av dem kunde rapportera om vad som hade attackerats och några kunde även identifiera planet som ett trafikplan. Planet med Flight 175 kraschade något lägre än flight 11 i det södra tornet, och många i det södra tornet hade sett kraschen som skett mot det norra, vilket resulterade i att flera redan var på väg att försöka lämna byggnaden (BBC News, 2008g). Det södra tornet var det första som kollapsade, ca 1 timme efter att planet hade kraschat in i det, men samtidigt hade det fler möjligheter för människorna i tornet att ta sig ut. Trappuppgångar som ledde från 91 våningen var helt eller del-

¹ Detta beskrivs om endast det norra tornet, men då båda tornen träffades är det en slutsats att tjock rök som steg uppåt skedde i båda byggnaderna.

vis fria enda ned. Då Flight 175 hade kraschat lägre än Flight 11, jämförelsevis hade flight 175 kraschat mellan 77-80 våningen, lättade möjligheten för de som flydde att ta sig ut ovanför kraschen. Det norra tornet var jämförelsevis mer skadat och när det kollapsade dödades de människor som fortfarande fanns på våningarna över planets träffpunkt (Nationella kommissionen, 2004, s. 278-280).

Flight 77s krasch med Pentagon har beskrivits av civila som att det var en missil genom luften över Washington och under tiden som personal inne i Pentagon hade tittat på bilderna från New York, träffade planet bygget. Flygplansattackerna i New York hade redan skapat ett oroskaos, när Pentagon blev utsatt för en liknande attack steg paniken till en nivå ingen hade trott var möjlig (Borger, Campbell, Porter & Millar, 2001). Kraschen mot Pentagon har kommit i skymundan, men hade vilken annan dag som helst, blivit ihågkommen som en enskild händelse. Detta beror på att World Trade Center katastrofen orsakade förstörelse 300 meter ovanför marken som hotade tiotusentals människors liv. Åtgärderna mot kraschen i Pentagon var i princip felfri och en succé på grund av tre skäl; den starka och förtroendefulla relation som deltagande i insatserna hade till varandra, ett befälssystem fanns på plats och det fanns ett regionalt förhållningssätt i insatserna. De flesta av de inblandade brand- och polismyndigheterna hade tidigare erfarenhet av regionalt förhållningssätt i insatserna. Totalt dödades 189 personer och 106 människor skadades (Nationella kommissionen, 2004, s. 303-304). Av dessa var det 64 personer i planet som dödades, varav dessa var två piloter och fyra ur flygplanspersonalen (BBC News, 2008e).

De passagerare som befann sig på det fjärde flygplanet hade fått höra talas om de andra attackerna och bestämde sig därmed för att övermanna de flygplanskapare som fanns ombord (Hoffman, 2006, s.18). Planet som kraschade på ett öde fält i Pennsylvania blev kapat, men passagerarna ombord planet överföll kaparna och tvingade dem att krascha på fältet (Nationella kommissionen, 2004, s. 13). Det skulle ta lite över tre år innan någon tog ansvar för terrorattacken och i oktober 2004 gjorde Osama bin Laden, ledare för terroristorganisationen al-Qaida, ett framträdande där han för första gången tog ansvar för terrorattackerna den 11 september 2001 (CBC News, 2004).

Kapningen av det slag som skedde den 11 september hade aldrig tidigare beskådats i USA och inte på minst 30 år i omvärlden (Nationella kommissionen, 2004, s.10).

2.2 Bali den 12 oktober 2002

Den 12 oktober, 2002 exploderade två bomber strax efter varandra på den populära turistön Bali. Bomberna exploderade utanför de populära turistställena Sari Club och Paddy's bar (Australian Federal Police, 2008). Den första bomben bars in på Paddy's bar under en väst på en självmordsbombare och den andra bomben fanns gömd i en Mitsubishi minibuss vilken hade blockerat trafiken på gatan utanför Sari club. De två utställena låg femton meter ifrån varandra. Sari Club, en populär turistklubb på Kuta Beach har ett förbud att inhemska invånare på Bali inte får festa på klubben, de blir stökiga av alkohol var motiveringen (Socialstyrelsen, 2006a, s. 20), men på klubbarna fanns bland annat svenskar, australiensare, briter, tyskar, kanadensare och indonesier som dog inne på klubben. Den största andelen av dödsoffer var australiensare (the Guardian, 2002). Totalt dödades 202 människor och över 300 skadades (Socialstyrelsen, 2006a, s. 9).

Oklarheter i den efterföljande utredningen uppstod och händelserna på Bali var det ingen som visst exakta detaljer om (Socialstyrelsen, 2006a, s.21). De båda bomberna detonades samtidigt, ca 11:05 på kvällen lokal tid (Brace, 2002). Explosionen på Paddy's bar skall ha

varit en som skett i det närmaste obemärkt då den exploderade inomhus och endast orsakade skada i byggnaden, men bomben utanför Sari Club orsakade mycket mer. Åtta bilar demolerades fullständigt och en kraftig brand utbröt strax efter explosionen. Skador på 50 byggnader och all elförsörjning i grannskapet slogs ut på grund av att fyra transformstationer exploderade. Skadeplatsen blev omedelbart mörklagd. Utöver de två bomber som exploderade vid de populära utställena, tjugo minuter efter att den andra bomben exploderat utanför Sari Club exploderade en tredje bomb i närheten av de amerikanska och australiska konsulaten, men ingen skadades (Socialstyrelsen, 2006a, s.21).

Bombdådet på Bali är en av de värsta attackerna i Indonesien sedan 60-talet och skedde under en tid då säkerhetsaspekten har växt i området. Den radikala muslimska extremistgruppen Jemaah Islamiya var den mest troliga ansvariga för attentaten. De är kända för att vilja skapa en muslimsk stat i Sydostasien (Brace, 2002). Gruppen skall under 2001 ha planerat ett antal bombattentat mot västerländska ambassader i Singapore, men inget blev bekräftat. Samtidigt kom det rapporter att al-Qaida försöker få fäste i Indonesien, på grund av att det är ett land med en muslimsk majoritet i befolkningen (Tran, 2002). Gruppen Jemaah Islamiya är en av de större och mer kända terroristgrupperna i Indonesien och påstås ha ett samarbete med al-Qaida. I utredningen visade det sig att valet av de populära turistmålen som attentatsmål gjordes medvetet och på grund av att västerlänningar vistades där. Orsaksbefolkningen, balineser, är inte välkomna till dessa utställanden och den enda oavsiktliga skada som var tänkt att åstadkommas skulle endast drabba hinduer (Socialstyrelsen, 2006a, s.26-27, 101).

Efterföljande uppdagningar har visat sig att det skall ha funnits rapporter som delgetts från amerikanska FBI till allierade. Där skall det ha uppgetts att en medlem av terroristgruppen Jemaah Islamiya hade planerat att attackera västerlänningar på barer och nattklubbar, både i Thailand och Indonesien. Rapporten skall ha distribuerats bara några månader innan händelsen (Wilkinson, 2003). I rapporten var två populära turistmål identifierade som terrormål och dessa låg inte långt ifrån Sari Club eller Paddy's bar. Rekommendationerna var en generell turistvarning, men ingenting skedde (Asian Pacific News Service, 2003). Att ingen sådan varning skedde berodde på att den inte skulle ha gjort någon skillnad i resmönstret bland turister (Stewart, 2004).

2.3 Madrid den 11 mars 2004

I Madrid, den 11 mars 2004, en dag där 20 tåg var i rörelse och människor var på väg till sina arbeten, lastades fjorton sprängladdningar på fyra tåg på stationen Alcalá de Henares, öster om Madrid. Sprängladdningarna detonerade vid fyra olika stationer; centralstationen utanför Atocha, Santa Eugeniastationen, El Pozostationen och Téllez (Socialstyrelsen, 2006b, s. 26). Sprängladdningarna låg i väskor som, förutom dynamit, var fyllda med spik för att göra mer skada än det som orsakades av explosionerna (Hamilos, 2007). Den värst drabbade stationen var El Pozo där flest människor dödades, 67 stycken. Anledningen är att det tåg som inkom hade två våningar och det visade sig sedan att dörrarna var stängda och trycket blev därmed större och få överlevde. Under rensningsarbetet av El Pozo fann tekniker två sprängladdningar som inte hade detonerat. Tåget som var på väg in till centralstationen utanför Atocha hade blivit försenat några minuter och därmed dödades eller skadades endast de i tåget och inga utanför. Efter nästan tre timmar hade alla skadeplatser evakuerats (Socialstyrelsen, 2006b, s. 30-31).

Terrorattacken i Madrid är den allvarligaste i Europa, sedan Lockerbie 1988² (Homeland Security, 2008), med 191 döda och över 1800 personer skadade (BBC, 2008b). Bara tio av de fjortonsprängladdningarna detonerades, de fyra intakta omhändertogs av polis och oskadliggjordes av deras bomtekniker. Största skälet till att dessa bomber aldrig detonerades var att timern var inställd tolv timmar för sent, därmed eliminerat möjligheterna att göra ännu större skada (Socialstyrelsen, 2006b, s. 26). Från början misstänktes den baskiska separatistgruppen, men utredningar släppte misstankarna och riktade dem senare istället mot *Moroccan Islamic Combatant Group* (MICG) (Homeland Security, 2008), trots detta vidhölls det i Spanien att det var ETA som utfört dådet. Inte förrän polisutredningarna visade bevis på att det inte fanns några länkar mellan dåden och ETA kunde spanska officiella representanter medge annat (Hamilos, 2007). MICG hade sedan tidigare misstänkta anknytningar till al-Qaida och hade år 2002 blivit uppsatt på Förenta Nationernas terrorlista för samröreelse med al-Qaida och egna dåd (Homeland Security, 2008). Dåden skall ha blivit inspirerade av en internetsida och de unga män som utförde dåden dedikerade till gruppen och al-Qaida (Hamilos, 2007).

De fyra ansvariga som lastade på sprängladdningarna blev tipsade om att polisen var efter dem och sprängde sig själva för att undgå arrestering. Minst fyra till försvann, det har rapporterats att en av dem utförde en självmordsbombning i Irak. Fortfarande lever människor med minnena av händelserna och det är svårt att ibland orka gå vidare. Rättegångarna har varit en rensande erfarenhet för de överlevande och anhöriga. En möjlighet att få gå vidare. Andra har känt att det varit traumatiserande och gjort saker och ting värre. Politiken har spelat en stor roll i det hela, vilket har gjort att många överlevande offer känt sig utsatta och ansett att politikerna endast haft terroristattacken som en pjäs i sitt maktspele, men frågor om vem som finansierade själva attacken finns fortfarande kvar och överlevande menar på att det inte är slutet trots rättegångar (Hamilos, 2007).

2.4 London den 7 juli 2005

Den 7 juli 2005 dödades 52 människor och över 700 skadades när London drabbades av en omfattande terroristattack. Fyra bomber exploderade i centrala Londons transporttrafik inom loppet av en timme (Murphy, 2006, s.2). Tre av dessa i tunnelbanesystemet och den fjärde på en dubbeldäckare (BBC News, 2008a). I samband med explosionerna i tunnelbanan lades tunnelbanesystemet ner och på driftcentralen kom indikationer om elavbrott (House of Commons, 2006, s.7). När explosionen på dubbeldäckaren inträffade togs beslutet att även busstrafiken skulle stoppas (Deverell et al, 2006, 41). Myndigheterna förklarade oroligheterna med att en stor olycklig händelse hade inträffat innan dåvarande premiärministern Tony Blair gick ut på eftermiddagen och förklarade att London hade blivit utsatt för terroristattacker (House of Commons, 2006, s.7).

Vittnen berättade om en man med olivfärgad hy som, strax innan bomben på bussen exploderade, hade nervöst fumlat med sin ryggsäck, senare på skadaplatsen fann polisen ett huvud utan kropp som kunde kopplas till identitetshandlingar funna inte långt ifrån. Rykten cirkulerade bland invånarna om att polisens prickskytte skulle ha skjutit en självmordsbombare, men inget bekräftades om detta.). Polisen fick under kvällen av den 7 juli ett

² Lockerbie är en liten ort mellan Carlisle och Dumfries nära de skotska gränserna. Där kraschade en jumbo jet 1988, 270 människor dog och anklagade och åtalade för detta blev två män som sades vara libyska säkerhetsagenter. De åtalades för att ha planterat en bomb som det återfanns rester av i den efterföljande utredningen. Den ena friades, medan den andra anklagade fick livstid. Hans förfrågan om frigivning år 2002 blev nekad (BBC News, 2008h).

snabbt genombrott då terroristen Hasib Hussains mor ringde och rapporterade att hennes son saknades. Polisen åkte till hemmet där de tog med sig fotografier och namn på hans vänner, namn som visade sig stämma med de namn som fanns på kreditkort och körkort som hade blivit funna vid flera av olycksplatserna (Deverell et al, 2006, 42-43).

Busstrafiken började rulla igen samma eftermiddag, men trafikansvariga valde att stoppa tunnelbanan helt, men återupptogs igen på morgonen den 8 juli. Det fanns ingen bekräftelse på att det skulle ha varit självmordsattacker som utförts. Under de nästkommande dagarna fann polisen indikationer på vilka de möjliga misstänkta varit och kunde begränsa sina sökkriterier ytterligare då de gick igenom allt material de fått in från övervakningskameror. Den 12 juli kunde polisen identifiera fyra män på tv-inspelningar som under den ödesdigra morgonen hade stått vid King's Cross tunnelbanestation, en av dem var Hasib Hussain. Bekräftelsen som världen väntat på kom samma dag, självmordsbombningar hade ägt rum för första gången i Storbritannien (Deverell et al, 2006, s. 43-44).

En förklaring till att bombattentatet i London skedde skulle ha kunnat vara kopplingen mellan Storbritannien och kriget i Irak, men dåvarande premiärministern Tony Blair avfärdade denna förklaring omedelbart efter tragedin skedde. Trots att det fanns hemliga dokument som läckt ut till media som påstod annat (Rai, 2006, s.1).

3 Terrorismen förr och nu

Detta kapitel handlar om hur terrorism har sett ut och hur det förändrats, ett samband med kapitel två som utgör de fyra stora attackerna där terrorismens förändring verkligen har bevisats.

Under 1900-talet skedde en rad händelser som skapade ett nytt mål; den civila befolkningen. Terroristhandlingar har skett tidigare än så (International Encyclopedia of terrorism, 1997, s.9), faktum är att terror har alltid varit förknippat med både förtryckarregimers, motståndsrörelser och upprorsförsökens historia (Münkler, 2004, 161), men det var under 1900-talet det blev en starkare medvetenhet om att civila kunde bli bra mål för terroristhandlingar. Denna förändring uppdagades främst under Andra världskriget och delvis var det Nazitysklands raspolitik som var grundaren. De var de första som försökte utrota hela raser eller folkgrupper. Japans grymhet speglade Nazitysklands handlingar, men på en mycket lägre nivå av extrema handlingar. Det gemensamma för dessa två är att icke-stridande, kvinnor, och barn blev dödade på helt gagnlösa grunder för det militära (International Encyclopedia of terrorism, 1997, s.9).

Det finns stora skillnader mellan terrorism för 30-40 år sedan och terrorismvågorna som kommer idag. Bland annat hur terroristgrupperna tedde sig politiskt. För 30-40 år sedan tenderade terroristgrupper att vara mer åt höger. Högerterroristerna höll sig till Turkiet, Italien och Guatemala, där deras aktioner hade större verkan på den inhemska arenan. En annan skillnad är att det under den tiden var att terroristorganisationer fick hjälp utifrån att etablera sig. Många grupper kunde expandera och börja arbeta utanför sina hemländers gränser vilket skapade förvirring bland dem som ville stoppa rörligheten av terrorism. Det var svårt att identifiera förövarna då tyskar arbetade i Sverige och Uganda, medan palestinierna rörde sig i Frankrike eller Paraguay, och japaner i Holland, Israel och Kuwait för att ge exempel (Laqueur, 2001, s.176).

De senaste 20 åren har terrorism förändrats till att bli något som associeras med religiös fundamentalism i den islamska världen istället för tidigare när terrorismens syfte och innebörd fokuserades mer på som en accepterad taktik använd av upprorsmakare. Upprorsmakare som använt sig av terroristiska taktiker har infunnit sig utöver större delen av de utvecklande länderna, men även den industrialiserade världen har blivit berörda. Till exempel har Irländska Republikanska Armén (IRA) på Nordirland blivit en av världens mest framgångsrika terroristgrupper (International Encyclopedia of terrorism, 1997, s.9-10). Till detta skall tilläggas att terrorism har mer och mer blivit terrorkrig som förs över hela världen och det finns ingen självrestriktion när offren väljs ut. Därmed har civilbefolkningen och den civila infrastrukturen blivit avgörande i terrorkrigen (Münkler, 2004, s.167).

Begreppet terrorism har under lång tid varit ett ihärdigt sätt att försöka få sin vilja fram. Det går inte att undvika att det existerar idag. Terrorism är mer vanligt att finna i stater av totalitära, auktoritära och autokratiska samhällen. Samhällen som sådana kan ge en ekonomisk, religiös, etnisk och regional bas där terrorism och extremism kan utvecklas (Crotty, 2005, s.8, 10). Rika privatpersoner finansierar aktionerna, men också stater och emigrerande grupper har visat sig ge sitt stöd till dessa organisationer (Münkler, 2004, s.9). Organisationerna kan därmed falla tillbaka på de stödjande nätverken i länder där hemmabaserna är placerade (Europeiska kommissionen, 2004, s.1).

Terrorism har länge använts som en strategi för att uppnå de syften som dess anförare har, men terrorism har även varit en del av ett känslolöst svar där det inte har funnits någon strategi, men handlingarna har utförts av grupper anknutna till en större organisation (Me-

rari, 2007, s.37). Terrorism sker inte i stundens hetta. Våldet som terrorism står för är enligt de som utför ett nytt legitimt sätt att få fram sin vilja, rationaliseringen av terrorismvåldet följs av att de förser en ideologi till sina anhängare och ett förtroendesystem som upphöjer dem som arbetar sig uppåt i organisationen genom terrorismhandlingar (Crotty, 2005, s.7). Detta för en in på området av rationalitet av terrorister och terrorism. Terrorism är ingen effektiv strategi, vilket har visat sig då de politiska mål som velats uppnå inte har infriats. Därför ses det ofta som irrationellt och terrorismens kamp ses som hopplös och irrationaliteten blir starkare i de fall där det syns att kampen som terroristerna kämpar är utsiktslös (Merari, 2007, s.37).

Frågan som många akademiker ställer är hur effektiv har terrorism varit? Ett kriterium för många terrororganisationer har varit att få regeringen att vika sig och få en politisk kontroll, i den aspekten har det endast varit ett fåtal grupper som har lyckats, bland annat Mau Mau i Kenya och *National Organization of Cypriot Fighters* på Cypern, anledningen att just dessa har lyckats har handlat om att syftet, frågan som de har brunnit för har betytt mer för de inblandade i organisationerna än för regeringarna. Majoriteten av de många grupperna som försökt sig på att övervinna en regim har misslyckats fatalt. Det vanligaste resultatet av terrorism är att det förs in i ljuset för befolkningens ögon, men att vara medveten om att det existerar har inte nog med effekt på folket som terroristorganisationer önskar. (Merari, 2007, s. 40-41).

Under 1980-talet finns en tydlig uppgång i hur många attentat klassade som terrorism skedde. Terroristattacker har blivit mer dödliga och dödsantalet efter attacken 11 september 2001 var den högsta noterade då. Varför det är så här beror på tre föreslagna faktorer; fler och fler terroristorganisationer motiveras av religiösa ideologier, det har blivit vanligare att amatörer utför dåden ensamma och de organiserade terroristorganisationerna har fått en ökad kunskap om vapen och blivit mer sofistikerade att använda dem (Lutz, 2004, s.19-21).

Utan dess historiska bakgrund skulle det inte finnas en möjlighet att analysera begreppet och finna en definition som ger innebörd till ordet (International Encyclopedia of terrorism, 1997, s.29). En fördel som terrorismen har är att de har möjlighet att utnyttja den angripna maktens politiska, rättsliga och moraliska självbindningar, med detta menas att de har ett övertag eftersom att den angripande makten inte kan svara med samma medel. Detta är ett stort skäl till att det främst är demokratiskt konstituerade, post-industriella samhällen som blir utsatta för terrorism (Münkler, 2004, s.169).

3.1 Svårigheten att definiera terrorism

De nämnda attackerna i kapitel två är bevis för att det behövs en klar och noggrann definition av terrorism och att det idag har blivit mycket viktigare, terrorism har blivit en del av det moderna samhället på ett helt annat sätt än tidigare. Före den 11 september 2001, har tanken på att definiera begreppet terrorism inte funnits i lika stor utsträckning och frågan om det funnits någon nytta i att ha en legitim definition av terrorism har varit en väsentlig del i diskussionen. Det har menats på att begreppet är för otydligt och tvetydigt för syftet, samt att begreppet inte uppehåller ett legitimt syfte (Golder & Williams, 2004, s.270-271).

Terrorismens ursprungliga innebörd var nära relaterat med demokrati och moral. Under Franska revolutionen hade begreppet en positiv mening och användes till att etablera ordning under en tid då anarki var framträdande och som följdes av tumult och kaos. Det var den revolutionerande staten som använde begreppet som ett instrument för att regera i den nyetablerade staten. Både terrorism under franska revolutionen och i dagens moderna sam-

hålla delar karaktäristiska drag som bland annat är att de förefaller vara avsiktliga, organiserade och systematiska handlingar som utförs. Det andra karaktäristiska draget faller inom kategorin politiska syften (Hoffman, 2006, s.3-4).

Idag har begreppet terrorism fått en helt annan plats i samhället, men de flesta har ändå bara en vag aning om vad terrorism är, det är ingen som konkret kan uttala sig om vad begreppet egentligen betyder. Det ligger till det normala att begreppet ofta blir hopblandat med gerillakrigföring och vanlig organiserad kriminalitet (Whittaker, 2003, s.5). Det har därför blivit en viktig diskussion i politiska debatter och internationella, samt nationella legitima organ att försöka komma fram till en definition som är tydlig och klar i sitt syfte (Golder & Williams, 2004, s.271). Frasen ”en mans terrorist är en annan mans frihetskämp” har blivit allt vanligare att höra både i debatt och samhället, den är med få ord innehållsrik och trycker på de problem och svårigheter som idag finns i debatten om en generell definition (Wardlaw, 1989, s.3).

Terroristhandlingar kriminaliseras och poliskåren har fått större befogenheter att utöva sitt yrke i syfte att arresteras och utreda misstänkta handlingar. Individer som misstänks för terrorism eller är associerad med en terroristorganisation kan nekas visum, få tillgångar frysta, och stater som stöttar organisationer får sanktioner insatta mot sig (Golder & Williams, 2004, s.271). Inte minst har media påverkat på hur kriminella handlingar såsom etnisk rensning, massakrer på civila av militär, förgiftade produkter på mataffärers hyllor har framställts och klassificerat det som terrorism. Det har inte funnits någon gräns för vad som skall klassas terrorism, synen som media har framställt har varit oberoende från var handlingens order har kommit från, det har inte gjorts någon skillnad på regeringar, anti-regeringar, organiserad brottslighet eller militanta grupper i protest (Whittaker, 2003, s.5). Väsentligheten kring termen terrorism har blivit starkare och mer påtaglig än för cirka tio, tjugo år sedan. Att felaktigt kalla någon för terrorist kan ge stora konsekvenser inom det juridiska, sociala, politiska och ekonomiska samhället (Golder & Williams, 2004, s.271). Det existerande problemet av att definiera begreppet terrorism grundar sig ofta i att en del politiskt våld rättfärdigas medan andra inte gör det (Wardlaw, 1989, s.4).

Användandet av ordet terrorism har under tid förändrats i samband med hur det politiska klimatet har utvecklats och förändrats. Att därmed finna en konkret och konsistent definition av begreppet har blivit svårare (Whittaker, 2003, s.7). Det går att särskilja två metoder för att fastställa en definition av begreppet terrorism. Dessa två är en detaljerad metod och en mer allomfattande metod. Metoderna skiljer sig på så vis att en detaljerad definition går in mer specifikt på vilka handlingar som kan klassas som terrorism utan att gå in på vad terrorism egentligen är, till exempel flygplanskapningar. Problemet med en detaljerad definition är att den politiska aspekten inte tas i anspråk. Aspekten undviks för att det inte ska bli någon möjlighet för politiker att bli partiska. Ett annat problem som utgör ett hinder för att en detaljerad definition skall kunna ge en rättvis bild av vad terrorism innebär, är att en definition baserad på en metod där kriminella handlingar utpekats som terrorism, men där terrorism inte beskrivs i dess innebörd, inte helt kan skilja mellan en terroristhandling och en vanlig, organiserad, kriminell handling. Den allomfattande definitionen väljer att lyfta fram kriterium som gäller vad det finns för motiv, uppsåt och vad terrorism innebär (Golder & Williams, 2004, s.286-287). En definition där motiv, uppsåt och liknande aspekter utgör grunden i definitionen har en nackdel att det sällan finns tillgänglighet av konkreta bevis för uppsåten, motiven för det kollektiva våldet (Tilly, 2004, s.7).

I grund och botten är terrorism ett vida använt begrepp av politisk karaktär (Whittaker, 2003, s.5). Det finns akademiker som säger att terrorism anses vara unik i sin politiska natur och en förlängning och fortsättning av politik med andra metoder (Lutz, 2007, s.10). Det

innebär bland annat att terrorismen som våldsbegrepp eller hot om våld har politiska syften och begrepp karaktäriseras även av makt; att vilja ha makt, ett övertag och att använda detta övertag för att få till politiska förändringar. Samtidigt karaktäriseras terrorism som en systematiskt, planerad och kalkylerad handling (Whittaker, 2003, s.5). Terrorismen kan ses som en strategi där militärt svaga eller de allra minsta grupperingarna kan sätta in våld mot stor- och supermakter. Det krävs inte mycket medel för att kunna bygga upp en egen logistik, anskaffa vapen och utbilda och försörja medlemmarna i inom en terrororganisation (Münkler, 2004, s.170).

Karaktären av terrorism skiljer sig från annat politiskt och ideologiskt motiverat våld, det vill säga att det våld som utförs och klassas som terrorism är sådant politiskt våld där våldet har skett utanför ett samhälles regler. På grund av att terroristhandlingar har ett politiskt syfte och att de som utför terrordåd ofta vill tvinga på en inverkan på en regims politik, så blir inte brott som rån, mord och kidnappning en del av terrorism. Brott som sådana har sällan ett politiskt syfte, utan ett mer personligt syfte (Ruby, 2002, s.10, 13). Terrorister vill underminera och förstöra ett politiskt system, och deras mål är ofta oskyldiga civila inom en stat vars regering är legitim och accepterad av medborgarna. Genom sina attentat vill terrorister ta ner en demokratisk regering eller ersätta en inte så demokratisk regering med en som är värre och inte alls demokratisk utan snarare diktatorisk (Lutz, 2004, s.8).

Forskare menar på att en definition måste innehålla och framföra en förklaring av terrorism där motivation, social miljö, och andra politiska syften finns med. Svårigheten ligger i att det finns olika grupper som använder olika definitioner och fokus läggs olika på de beteendena och deras konsekvenser som skapas än faktorer som stärks av motiv och politik. Detta tydliggörs bland annat i hur exempelvis *the Palestine Liberation Organisation* (PLO) uppfattas av omvärlden. Det finns stater som anser att PLO är en terroristisk organisation utan politisk legitimitet och använder sig av metoder som är omoraliska, men det finns stater som ser PLO åt det motsatta hållet. Det vill säga att gruppen är en legitimt representativ grupp som använder sig av försvarligt våld för att nå rättvisa och möjliga mål. Definitionen av terrorism skall förklara vad begreppet innebär och inte rättfärdiga det (Wardlaw, 2003, s.4-5). Genomgående visar det att moral, beteende och legitimitet är tre begrepp som speglar terrorism utöver att utförandet bör ha ett politiskt syfte, motiv och uppsåt. Handlingen är terroristisk om det inte finns någon moral i utförandet. Exemplet med PLO kan utvecklas och visa på att liknande grupper som utför politiskt motiverat våldshandling är övertygade om att handlingen är nödvändig och moraliskt berättigad, därmed inte terroristisk, även ifall att stater fördömer handlingen som sådan. Organisationer som utför politiskt motiverat våld mot icke-stridande för jihad³ gör att denna konflikt mellan stater som fördömer och grupper som utför våldet är ett problem. Handlingar utförda i en jihads kamp anses av de som utför handlingen och stater som stöttar dem vara moraliskt berättigade och därmed inte terrorism (Ruby, 2002, s.12).

Under senare tid har det visat sig att ju mer dramatiska aktionerna blir desto mer uppmärksamhet får organisationerna. Filmer uppmärksammar hur terrorister skulle kunna utföra sina attacker, däribland användandet av skickliga hackers som tar sig in i högsofistikerade system och där igenom startar ett tredje världskrig. Att därmed bli en ny sorts terrorist där vapnet inte är fysiska vapen som gevär, pistoler, massförstörelsevapen, eller kemiska och biologiska vapen, utan istället fingrar och intelligens, förstörelseförmågan skulle bli minst

³ Innebär en strävan eller ansträngning i allmänhet. I islamistiskt språkbruk används ordet till att förklara en "andlig kamp" eller att bli fullkomlig, men är också ordet för ett krig som enligt islamisk lag är legitimt. Kalas ofta för heligt krig (Nationalencyklopedin, 2008d).

och om inte större än med tidigare använda vapen. Vad hindrar i så fall terrorister från att göra detta? En större anledning är att terrorister inte är eller har varit intresserade av ett totalt sammanbrott i det moderna samhället. Syftet är inte att eliminera motståndaren utan att få det förtryck eller ockupation eller annat politiskt mål, som motståndaren har, att upphöra (Kumm, 2002, s.236, 240-241).

Synsättet, förändringen av hur terrorismen ses kom i samma stund som det första planet kraschade in i det norra tornet av World Trade Center 11 september 2001. Att en terroristattack hade skett oprovocerat i ett land som USA var för de flesta svårt att greppa. Världen skulle aldrig mer bli sig lik, detta klagjordes gång på gång under det nästkommande dygnet. Terroristerna hade klivit över sina gränser, det handlade inte längre om terrorism mot sin egen stat, det har under de senaste sju åren handlat om terrorism utan gränser. Angreppet mot USA handlade inte bara om att ge sig på en supermakt som var en fiende, det handlade om att skrämma upp den västerländska demokratin att upplysa det moderna samhället om deras existens (Kumm, 2002, s.243, 260). I och med attackerna flyttades fokus från att enbart vara politiskt motiverade till att bli även religiöst motiverade attacker (Norell, 2002, s.7).

Enligt Laqueur är det omöjligt att definiera terrorism, men det hindrar inte att det finns möjlighet att kunna särskilja terrorism från andra typer av våld och därifrån identifiera de karaktäristiska drag som idag utgör terrorism och som kan användas till att lagstadga brotten på rätt sätt (Hoffman, 2006, s.34). Terrorism i det internationella samfundet kan ses som ett exklusionsbegrepp, det vill säga att aktörernas krav som ställs inte är förhandlingsbara så länge våld är inblandat. Terrorgrupperna gör hellre anspråk på att vara gerillagrupper som utför en kamp liknande partisaner för att befria sociala eller etniska grupper. Definitionsfrågan blir därför svår och omstridd då de som kallar en händelse terrorism vill se till att grupperna inte får politisk legitimitet i något avseende (Münkler, 2004, s.155).

3.2 Definitionerna av begreppet terrorism

Som redan nämnts ovan har det visat sig att terrorism är svårt att definiera, det finns flera definitioner och det har visat sig att alla ser olika på vad terrorism är. För en del är en handling gjord av separatistgrupper en handling av terrorism, men för andra är det en handling i frihetskämpande. Det behövs en definition för att det ska skapas lagar. Utan en definition blir det svårt att lagstadga hur terrorism skall straffas. USA har till exempel skapat tre definitioner av tre termer som alla tillhör området terrorism. De behandlar först av allt termen "terrorism" där ordet betyder politiskt motiverat våld vilket riktas mot icke-stridbara mål, det vill säga civila och militär personal som vid attacken är obeväpnade eller inte i tjänst. Termen "internationell terrorism" definieras som politiskt motiverat våld mot medborgare och landområden i flera stater. Sist definieras termen "terroristgrupp", en grupp eller underordnad grupp som praktiserar internationell terrorism. Det viktiga i dessa definitioner utöver att handlingarna riktas mot civila och icke-stridbara mål är att förövarna inte är en del av regeringen (Henderson, 2001, s.4).

Problemet med definitionerna av dessa tre termer är att de är ofullständiga. De beskriver inte relationen mellan terrorism och andra former av våld eller en våldshandling gjord av regeringen. Faktum är att regeringar sällan beskriver sina handlingar som terrorism. Teoretiker kallar det för statsterrorism och är bland annat en förklaring till dödspatruller i latinamerikanska länder som får order av dessa totalitära staters regeringar att utföra vissa uppdrag för att eliminera oppositionen (Henderson, 2001, s.5). Definitionen har funnits sedan 1983 och det är utrikesdepartementet som har utvecklat den. Att definitionen har varit

ståndaktig så länge är väldigt bra om det är ens önskan att göra longitudinella studier, men detta betyder inte att den passar till alla studier, istället kan det visa sig att en oföränderlig definition som den amerikanska inte fångar in studieobjektet på ett tillfredsställande sätt om det som skall studeras har ändrat karaktär. Den amerikanska definitionen av terrorism har problemet att den inte räknar in att ibland krävs det inte något våld, endast hot om våld, för att terrorister skall få sin vilja fram (Jervas et al., 2003, s.14-15).

Europeiska Unionen (EU) utvecklade efter den 11 september 2001 en definition av terrorism, relativt snabbt. Definitionen återfinns i rådets rambeslut 2002/475/RIF av den 13 juni 2002 där bekämpande av terrorism tas upp. I artikel 1 i rambeslutet fastställs det att varje medlemsstat skall vidta åtgärder nödvändiga för att bekämpa terroristbrott som allvarligt kan skada ett land eller internationell organisation. Terroristbrotten är brott enligt nationell lagstiftning som sker i syfte att hos en befolkning injaga fruktan, att tvinga offentliga organ eller organisationer att utföra eller avstå att göra en handling, eller på något sätt orsaka destabilisering i ett lands eller i en internationell organisations politiska, konstitutionella, ekonomiska eller sociala strukturer (EU, 2008). Ett antal punkter om brott som återfinns i den nationella lagstiftning listas och kan anses som terroristbrott om de begåtts i ovan nämnda syften. Bland annat människorov eller tagen som gisslan, allvarliga angrepp på en persons fysiska integritet, eller angrepp mot en persons liv som kan leda till döden (2002/475/RIF, 2002).

EU:s definition är annorlunda jämfört med den amerikanska definitionen, både i uppbyggnad och i produkt. EU:s definition kan ses mer som en politisk förhandlingsprodukt och den är inte lika öppen som den amerikanska. Den tanke som ligger bakom definitionen är att det skall gå att fylla på med ytterligare handlingar som uppfyller en eller flera kriterier. Problemet med den EU:s definition är att den inte är helt lätt att förstå. Kriterierna i definitionen är inte helt precisa och frågan är om det räcker att i första kriteriet skrämra upp eller injaga allvarlig fruktan i en befolkning. Utan ett politiskt syfte till den injagande fruktan kan det likväl vara en grupp mentalt skadade personer som ligger bakom brottet och inte terrorister. Däremot om tanken bakom kriteriet ligger i att den uppskrämda befolkningen skall vara en anledning för att få offentliga organ eller en internationell organisation att böja sig för terroristernas vilja är det rimligare att tala om terrorism, därför att myndigheterna i de flesta länder är politiskt direktstyrda. Det sista kriteriets problem gäller huruvida de menar att det grundläggande problemet eller störning skulle vara att störningen är tillräckligt omfattande för att det ska ge politiska konsekvenser i den ekonomiska och sociala strukturen. Det har varit en tidspress för unionen att få ihop definitionen, vilket lätt ses på de oklarheter som finns om de olika kriterierna (Jervas et al., 2003, s.16-17). Sverige har implementerat rambeslutet i lagstiftningen som lag (2003:148) om straff för terroristbrott.

Den svenska definitionen av terrorism återfinns i Svenska Akademiens ordlista över svenska språket, där terrorism beskrivs som en verksamhet där terror gynnas. Terror definieras som skräckvälde, våldsmetoder som injagar skräck för politiska syften och även termen terrorisera definieras, vilket är att injaga fruktan hos någon eller flera, samt att kuva eller behärska skräckåtgärder (Svenska Akademien, 2006). Vad som kan ses här och i den amerikanska definitionen är att de båda säger att terrorism och dess besläktade begrepp har politiska syften. Det görs ingen skillnad på om motiven är religiösa, ekonomiska eller sociala, så länge syftet är politiskt (Harmon, 2007, s.7). Tydligt är att EU:s definition är av senare datum än den amerikanska vilket framgår av att definitionen tar upp och nämner förstörelse av datasystem som en handling att anses som terroristisk (Jervas et al., 2003, s.18).

I nationalencyklopedin definieras terrorism, precis som i den Svenska Akademiens ordlista och amerikanska definitionen, som en våldshandling med ett politiskt betingat syfte och

utan att ta hänsyn till om oskyldiga drabbas påverka samhället eller ett lands politik. Vidare definieras statsterrorism, nationell terrorism och internationell terrorism (Nationalencyklopedin, 2008a), men vad som fortsättningsvis skall fokuseras på är en annan sorts terrorism, nämligen cyberterrorism.

3.3 Cyberterrorism

Cyberterrorism kan enklast beskrivas som brottslighet där informationssystem utnyttjas. Inom begreppet finns det ingen enighet om vad som ingår när det kommer till IT-relaterade hot. Upphovsmakaren till begreppet brukar tillskrivas den amerikanske säkerhetsanalytikern och forskaren Barry Collin som någon gång under 1980-talet lär ha använt sig av begreppet för att beskriva terrorismens inträde i cyberspace⁴ (Jervas et al., 2003, s.63-64). Internet expanderade stort under 1980-talet och ännu mer på 1990-talet. Det blev möjligt för företag, utbildnings- och forskningsinstitut, organisationer och myndigheter att lägga till sina egna profiler och hemsidor på det stora nätverket. Idag ger internet allt från kommunikationstjänster till informationssökningstjänster för nästa en miljard människor världen över. Användarna har ett behov av internet för att kunna kommunicera via olika tjänster och få fram information som behövs. Med den stora expansionen av internet är det inte endast positiva erfarenheter som får användare att söka sig till internet, extrema grupper med olika politiska syften samlas på nätet och använder sig av terroristliknande strategier fann sig på internet för att sprida sin propaganda och kommunicera med sina supportrar och göra allmänheten medveten om deras budskap och därmed även söka sympati för det (Weimann, 2006, s.19-20).

På kort tid har samhället och stora delar av världen fått se hur informationsteknik (IT) utvecklats snabbt och förändrat större delen av världen. IT har blivit något av en nödvändighet för samhället idag. Samhället är därmed beroende av tillgängligheten och det är nödvändigt att systemen som IT utvecklar finns att tillgå för att samhället skall kunna fungera. Störningar inom IT-systemen kan därför ge allvarliga konsekvenser. Störningar i IT-samhället och missbruk av det blir allt mer påtagligt när samhället blir allt mer beroende av IT-system. En ökad uppmärksamhet för informationssystem och sårbarheten i samhället drar till sig aktörer som vill utnyttja det (Jervas et al., 2003, s.61). Internets karaktär att vara lättillgängligt, vara internationellt, ge individer en anonym identitet om så önskas. Att det är globalt med en kaotisk struktur har gjort att terroristorganisationer givits en arena där de fått en friare grund att arbeta på och utföra sina handlingar (Weimann, 2006, s.16). Det ökade beroendet av teknologi som dagens samhälle har gör att cyberterrorism blir en attraktiv form av terrorism som lockar med den potentiellt stora skada som kan åstadkommas, den mentalitet som efteråt lämnas kvar hos de drabbade och hur media visar upp resultaten. I teorin har hotet från cyberterrorism blivit alarmerande. Samhällets beroende av informationsteknologi har lett till att terrorister har fått en chans att utnyttja mål de annars inte skulle haft tillgång till, exempelvis försvarssystem och flygplanskontrollsystem. Det faktum att terrorister därmed har möjlighet att ta sig in i system som dessa och slå ut dem gör att den potentiella faran av cyberterrorism fyller en funktion av rädsla som ibland kan vara överexponerad och ibland orättvis, men likväl finns (Weimann, 2006, s.148).

⁴ Cyberspace brukar tillskrivas sciencefictionförfattaren William Gibson som använde termen i sin bok *Neuromancer* från 1984. Cyberspace betraktas som en metafor av den virtuella värld som kommunikationen över Internet har skapat (Jervas et al., 2003, s.64).

Det har blivit allt vanligare att terroristorganisationer använder sig av Internet för att kommunicera. Användning av informationstekniken bland terrorister blir allt mer oroande då det skapar problem för polisiära myndigheter och fler handlingsmöjligheter för terroristerna. Det har blivit lättare för terrorister att kunna utnyttja den sårbarhet och beroende som samhället har fått av informationstekniken och dess utveckling. Terrorister har därmed fått möjlighet att kunna slå till mot eller via IT-systemen, men de terroristanknutna sabotage som uppmärksammats har hittills varit av enklare art, både vad gäller angreppsmål och angreppsmetoder. Kopplingen mellan internet och terrorism handlar om kommunikation och möjligheten att sprida propaganda och instruktioner, samt att terrorister attackerar nätet istället för att använda sig av det, men detta är fortfarande nytt och idag används och utnyttjas internet mer än vad det attackeras (Weimann, 2006, s.21).

Sabotagen kan ske på flera sätt, antingen genom att förändra eller förstöra webbsidor, eller tillgänglighetsattacker, det vill säga attacker på nätdatorns kommunikationsvägar. Att förändra en webbsida kan i det närmaste och harmlösaste kallas för klotter, men att förstöra eller radera information på en myndighets hemsida kan betecknas som sabotage. Den andra typen är mer omfattande och kan få allvarigare konsekvenser (Jervas et al., 2003 s.62-63). Det brukar kallas för ”denial of service attack” (Henderson, 2001, s.27). Kommunikationen blockeras successivt genom att stora och otillåtna mängder datatrafik skickas till utvalda måldatorer (Jervas et al., 2003, s.62-63). Ett exempel på en sådan attack skedde år 2000 mot hemsidor såsom Amazon.com, Yahoo! och eBay där de blev bombarderade med information som hade ursprung från datavirusprogram. Det gjorde det svårt eller nästintill omöjligt för användare att handla online (Henderson, 2001, s.27). Det önskade resultatet att skapa en allmän oro behöver inte ens vara ett resultat av konkreta bevis eller ens genomförande av attackerna, det räcker med hoten (Weimann, 2006, s.27).

Cyberterrorism kan visa sig på flera sätt, men tre sätt som är väsentliga och som gör datorer användbara för cyberterroristiska attackers mål är att se på datorer som verktyg, som behållare av bevis och det tredje sättet är att se datorer som mål. Användandet av datorer som verktyg har blivit mer påtagligt och kan bland annat framgå genom att terrorister sprider sin propaganda och använder Internet för olika insamlingar, de sprider budskapet och ber folk att stödja dem med pengar. Genom att använda tekniker för att hacka in sig på servers använder terrorister sig av datorn och internet för att samla in data från den privata sektorn och känslig eller oklassad information från regeringar (Vatis, 2001, s.3). Det har visat sig att Internet på flera sätt har blivit ett idealiskt nätverk för terrorister och deras aktiviteter. En stor anledning för detta är att internet gjort det möjligt för en global kommunikation emellan grupperna och där de kan använda internet som en plattform för sin propaganda, det har också blivit en möjlighet att kunna komma åt information på internet om potentiella mål för terroristiska syften. Med dagens internet ges därför terrorister en frihet som inte existerar för dem utanför nätverket. Ett exempel på en terroristorganisation som har funnit ett fullt användande av internet är Hamas som under årtal har använt internet för att skicka skyddade filer och meddelanden till sina medlemmar (Wagner, 2005, s.7-8).

Det finns ingen generell definition av cyberterrorism, inte ens Barry Collin har försökt sig på en sådan, men Collin menar på att gränsytan mellan det virtuella och den fysiska världen är det som skapar förutsättningar för cyberterrorism. Collin listar däremot exempel på handlingar som kan betecknas som cyberterrorism, det kan bland annat handla om datorkontrollerade sprängladdningar, angripande på banker och internationella finansiella transaktioner samt aktiemarknader, kollisioner mellan två passagerarflygplan och det kan vara en terrorist som ändrar den kemiska sammansättningen på läkemedel som är livshotande (Jervas et al., 2003, s.64). Allmänt är cyberterrorism definierat som att användandet av data-

fik göra det möjligt att sabotera statliga infrastrukturer, såsom energi, transportkommunikationer och liknande (Weimann, 2006, s.16). Andra system som kan attackeras och ses som en cyberterroristisk handling är att slå ut nödvändiga funktioner såsom trafikkontroll och elektricitet (Henderson, 2001, s.27). Rent tekniskt är de genomförbara även om exemplen är orealistiska. Kritiken mot Collins exempel har bland annat handlat om för liten hänsyn till tekniska eller mänskliga kontrollfunktioner. FBI-agenten Mark M. Pollit har försökt sig på att definiera cyberterrorism och har använt sig av den amerikanska definitionen av terrorism som utgångspunkt, det vill säga att ”cyberterrorism är överlagda, politiskt motiverade attacker utförda av subnationella grupper eller hemliga agenter, riktade mot information, datorsystem, datorprogram och data som resulterar i våld mot icke-stridande parter” (Jervas et al., 2003, s.64-65).

Cyberterrorism skulle kunna ingå i begreppet informationskrigföring. Den angräpnade måste alltid kunna försvara sig medan cyberterroristen alltid kan försöka på nytt om han eller hon skulle misslyckas med en attack. Något som gynnar cyberterrorism är att datornätverk och uppkopplingen till Internet har ökat, samt att säkerhetsarbetet inte håller jämna steg med utvecklingen vilket ökar målet för terroristernas attacker. Lättillgängligheten har blivit större och en terrorist har ofta inga svårigheter att bli medlem i olika sammanslutningar och diskussionsforum. Dock säger bedömare att existerande terroristorganisationer inte har tekniken och kompetensen för att utföra terroristattacker, andra menar att detta inte stämmer och att utvecklingen haft hög framfart i de flesta delar av världen, därmed gjort det möjligt för terroristorganisationer att öka sin verksamhet (Jervas et al., 2003, s.72-73). Flera terroristorganisationer har egna hemsidor i syfte att sprida sina budskap (Henderson, 2001, s.28).

Som ett led i den nya tekniken och den nya vägen att kommunicera för terrorister har cyberterrorism kommit att bli toppprioritet för missbrukande av internet. Hur allvarligt hotet om cyberterrorism är finns det delade åsikter om. Det finns inga klara bevis för att det skall ha skett en större attack mot nätverkssystem via internet av någon av de större terroristorganisationerna (Wagner, 2005, s.24-25). Hotet från cyberterrorism kan i teorin vara tillräckligt stort för att allmänheten bör reagera. I teorin är all viktig infrastruktur en utsatt del för cyberterrorism och skulle kunna slås ut. Att behovet att använda sig av IT har ökat blir allt mer påtagligt och detta ger terrorister mål som annars skulle vara otillgängliga för dem, exempelvis försvarssystem och flygtrafikkontroller (Weimann, 2006, s. 148). Under de senaste åren har det kommit fram bevis på att terroristorganisationer har ordnat egna serverar som därmed gör att tillgängligheten av internet för sina medlemmar blir enklare. Det har blivit lättare för terrorister att gömma sig bakom organisationer som specialiserar sig på att köpa bandbredd och som registrerar sig med konton, dessa organisationer har blivit lättare att identifiera, men gör det svårare att komma åt den riktiga bakomliggande organisationen (Wagner, 2005, s. 11).

4 Försvarets radioanstalt och signalspaning

De fyra fall som jag skriver om i kapitel två kan se ut att vara helt osammanhängande med vad som skrivs här, men kopplingen mellan dem och det fall jag framför här är att terrorism har förändrats, det är tydligt i det anseende att det inte längre går att se på terrorism som varit aktuell före 11 september. Grupper såsom ETA och IRA finns visserligen kvar, men deras syften har delvis ändrats vilket kan påvisas i kapitel 3.

Under en mycket lång tid har det varit ett faktum att krig har stått mellan två stater, mellan två nationer, men denna modell verkar ha utvecklats till att bli historisk förankrad. Terrorism har blivit ett sorts terrorkrig i den mening att det nu kan finansieras av rika privatpersoner, vilket nämdes i förra kapitlet (Münkler, 2004, s.9).

Terrorism har utvecklats och blivit allt svårare att definiera och fallit ut i flera nya grenar som visar på att det inte längre är terrorism mot staten i politiska syften som diskuteras utan det finns terrorism, till exempel cyberterrorism, som väljer att riktas mot oskyldiga civila och staten för politiska syften. Detta visades redan under terroristdåden i kapitel 2, det var inte staten själv som skadades utan civila som endast valt att gå till jobbet i tre av fallen och i det fjärde fallet valt att endast ha roligt. Terrorism är inte krig i den mening att krig är något som sker mellan två stater, men som nämns i kapitel 3 är det ett svårdefinierat begrepp och vissa grupperingar med islamsk bakgrund väljer att se sina handlingar som jihad, heligt krig, vilket därmed rättfärdigar deras aktioner.

Kapitel 4 tar upp en samhällelig funktion som idag fortfarande är nytt för det svenska samhället, åtminstone i det avseendet att det inte har blivit lika uppmärksammat som det har blivit under året. Kapitel 3 och dess koppling till kapitel 4 handlar om att det idag har blivit en ny gren i terrorism som i dagens moderna samhälle blivit mer och mer verksam, cyberterrorism. Kapitel 4 tar upp en del av vad hoten mot Sverige ser ut, men idag handlar det inte längre om en invasionsrisk från en annan stat, istället handlar det om hot från terrorism, sönderfallande stater och IT-attacker. Ett väl fungerande försvar mot särskilt IT-attacker är därför ytterst viktigt (Regeringen, 2008a).

4.1 Försvarets radioanstalt

Försvarets radioanstalt (FRA) bildades år 1942. Det är en central förvaltningsmyndighet vars verksamhet regleras genom förordningen (1994:714) med instruktion för FRA (SOU 2003:30, 2003, s. 43-44). De är en civil myndighet som har till uppgift att bedriva signalspaningsverksamhet, vilket innebär inhämtning av underrättelser via radiosignaler (FRA, 2007). FRA är vad en uppdragstagande myndighet, därmed får myndigheten instruktion av exempelvis Försvarmakten, där bland annat målsättningen och syftet med signalspaningen anges. Utöver att vara uppdragstagare skall FRA samarbeta med andra organisationer inom informationssäkerhetsområdet, både inrikes och utrikes (SOU 2003:30, 2003, s. 43-44). Verksamheten skall även kunna:

1. stödja insatser vid nationella kriser med IT-inslag,
2. medverka till identifieringen av inblandade aktörer vid IT-relaterade hot mot samhällsviktiga system,
3. genomföra säkerhetsanalyser,
4. ge annat tekniskt stöd (SOU 2003.30, 2003, s.44).

En annan funktion som FRA skall fylla är att genom signalspaning vara till stöd för svensk utrikes-, säkerhets- och försvarspolitik för politikområdena Totalförsvaret och Skydd och be-

redskap. FRA har till uppgift att rapportera underrättelser för att dess uppdragsgivare; regering, Försvarmakten med flera, skall få sina behov tillgodosedda och möjliggöra skapande av underlag för planering, beslut och genomförande av verksamhet (SOU 2003:30, 2003, s. 43-44).

Utveckling av system, utbildande av personal och att minska risken för och konsekvenser av olyckor och svåra påfrestningar i fred är en viktig del av FRA:s verksamhet. De skall värna om civilbefolkningen och därmed trygga en livsnödvändig försörjning, samt trygga de viktigaste samhällsfunktionerna. Utöver detta skall FRA bistå Försvarmakten vid väpnat angrepp och krig i omvärlden (SOU 2003:30, 2003, s.45-46). Utöver att stå till förfogande för sina uppdragsgivare och kartlägga yttre militära hot har FRA i uppdrag att kartlägga och övervaka de nya hoten som uppkommit, det vill säga icke-militära hot där bland annat terrorism och annan grov internationell brottslighet hör till (FRA, 2008a).

FRA har ett ansvar att medverka i det svenska deltagandet i internationells säkerhetssamarbete. Bland verksamhetens uppgifter handlar det om att stödja svenska förband i internationell tjänst med signalspaningsutrustning och metodik för att förbanden skall kunna få förvarningar om hot mot dem. Förändringen av signalspaning är en annan del av verksamheten och syftar till att se hur den tekniska utvecklingen fortgår och hur signalskyddet kan förbättras. FRA kan därmed utföra IT-säkerhetsanalyser för att skydda information och informationsteknik mot dataintrång och informationskrigföring (SOU 2003:30, 2003, s.49-50).

4.2 Signalspaning

Hur skall signalspaning definieras? Det som menas med signalspaning när det talas om det i folkmun är informationssökning som inskränker enskilt eller i en kombination på all sorts kommunikationsinformation, elektronisk kommunikation och utländsk teknisk signalspaning (Department of the Navy, 1999, s. 1). Signalspaning är inte ett fenomen som uppstått på senare år. Det har funnits under större delen av 1900-talet och var speciellt viktigt under andra världskriget, men också kalla kriget. Det har visat sig att det har funnits stora gap i vetenskapen om hur stort signalspaning egentligen har varit i omvärlden efter andra världskriget och under kalla kriget. Det beror främst på att det har under lång tid varit hemligstämpelat om ämnet och vad det har gjort. Faktum är att forskare, akademiker och andra vetenskapsmän fortfarande hellre diskuterar ämnet *sotto voce* för att undvika att åka dit för att bryta mot någon lag som satt restriktioner på att diskutera signalspaning under denna period. Signalspanare har därför fått arbeta hårt och i största hemlighet för att bevisa att sådan vetenskap som signalspaning kan ge är värdefullt för berörda, såsom militär verksamhet (Aid & Wiebes, 2001, s.1-2).

Under kalla kriget hade Sverige, tillsammans med Finland och Norge, och till viss del Danmark, en stor viktig geografisk del i signalspaningen. De tre länderna hade första parckett till flera stora händelser och det faktum att de låg nära dåvarande Sovjetunionen gjorde att länderna var utmärkta baser för att samla in information ifrån det stora landet i öst. Detta var i sig en stor risk för de skandinaviska länderna, med tanke på den militära makt och grund som Sovjetunionen då stod på. I utbyte mot att hämta in information om Sovjet skulle de skandinaviska länderna, förutom Finland och till viss del Sverige, få stå under det amerikanska atombombsskyddet, samt få ta emot finansiella och materiella hjälpmedel. Under kalla kriget fick Sverige bland annat göra flera flygningar med DC-3 plan som var utrustade med teknologi från USA som skulle hjälpa dem att samla in information och signalspana över Sovjetunionen. Bland annat handlade insamlingen om information om den sov-

jetiska radarutrustningen, FRA gjorde dessutom kopior och genomläsningar av den diplomatiska korrespondensen som skickades mellan den sovjetiska ambassaden i Stockholm och Moskva, samt sändningar från KGB (Jacobsen, 2001, s. 209-210, 223).

Signalspaningen består främst av två olika sätt att inhämta information. Det ena är kommunikationsspaning (KOS), vilket innebär att verksamheten inhämtar information från radiosignaler, det vill säga telefoni, telegrafi och dataöverföringar. Det andra sättet att inhämta information är genom teknisk signalspaning (TES), denna signalspaning riktas främst mot signaler som inte behandlar kommunikation, exempelvis radar-, navigerings- och vapenrelaterade system (FRA, 2008c). Inhämtning av information via KOS och TES har gett vitala fördelar och analyser för diplomatiska och militära handlingar. Signalspaning har därmed blivit en strategisk och viktig roll för inhämtning av information som kan vara viktig i syfte att hjälpa militären ute i fält. Bland annat ger signalspaning möjlighet att kunna följa hur trupper förflyttar sig eller visa var radarsystem för luftkontroll finns. Vilket har gett stor betydelse för skyddet av nationens säkerhet (Pierson & Kovacs, 2003, s.1). Signalspaning är mycket användbart, men det kräver mycket kunskap om produkten eftersom att exempelvis en order om strid kan hänga på en korrekt analys av KOS och TES (Federation of American Scientists, 1998, s.142).

Signalspaning i Sverige är en militär verksamhet som har till syfte att kartlägga, avlyssna och skaffa information om motståndares potential inom operativa och tekniska resurser (Nationalencyklopedin, 2008b). Tekniken som finns i dagens samhälle utvecklas och den blir allt mer avancerad, den teknik som FRA är försedd med idag för signalspaningsverksamhet är anpassad för att inhämta signaler från eter och inte för den elektroniska kommunikation som sker via tråd och kablar i dagens samhälle (Prop. 2006/07:63, s.57). Signalspaning har länge varit viktig därför att det bland annat är en informationsinhämtning som är passiv, men en nackdel är att den sker oftast utan att den som utsätts för det känner till att det sker en övervakning (Aid & Wiebes, 2001, s.4).

I och med den nya utvecklingen i teknik som världen får erfara har FRA:s inhämtning av information via signalspaning begränsats och mängden av underrättelse har till följd minskat. Därför lämnade regeringen in en proposition för en anpassad försvarsunderrättelseverksamhet till riksdagen år 2006. Utöver att signalspaningen diskuterades valde regeringen att också föreslå att mandatet för försvarsunderrättelseverksamheten (FUV) skulle anpassas från ”yttre militära hot” till ”yttre hot”⁵ i lagen om försvarsunderrättelseverksamhet. Signalspaningen diskuterades så till vida att en lag föreslogs, lag om signalspaning i försvarsunderrättelseverksamhet, där FRA:s verksamhet utökas från att bara övervaka eter till att ge tillgång till både eter- och trådburen kommunikation (Prop. 2006/07:63, 2006, s.57).

Signalspaningen som skall kunna tillgodoses med lagen är signalspaning som i framtiden skall ge försvarsunderrättelseverksamheten möjlighet att skydda Sverige lika bra och bättre som den gör idag. Enligt regeringen skulle detta bli möjligt då FRA får tillgång att utföra signalspaning både i kabel och eter (Regeringen, 2008a).

⁵ Yttre hot innebar inledningsvis all internationell terrorism och annan kvalificerande gränsöverdragande brottslighet som utgör hot mot rikets säkerhet (Prop. 2006/07:63, s.134), men har under hösten dragits ner till att innebära sju punkter, bland annat yttre militära hot mot landet, säkerhetspolitiska konsekvenser vid internationell terrorism och allvarliga yttre hot mot samhällets tekniska infrastruktur (Bynert & Johannisson, 2008).

4.2.1 Personlig integritet

I samband med att lagen antogs den 18 juni 2008, blev det även sagt att det skulle göras tillämpningar till hur det personliga integritetsskyddet skulle uppehållas och kompletteringar har gjorts för att integritetsskyddet skall bli starkare. Dessa var bland annat att det skall preciseras för vilka signalspaning får bedrivas, ansökan om tillstånd för signalspaning skall lämnas in av FRA och endast de trafikstråk som domstolen bestämmer skall FRA få utöva signalspaning på. Det skall även bara vara regeringen, regeringskansliet och försvarsmakten som får ge FRA uppdrag om signalspaning, och vid en övervakning av en enskild person, skall denna person uträttas, detta blir en skyldighet (Statsrådsberedningen, 2008). Däremot är det inte lätt att förstå vad det är som skyddas om inte begreppet definieras. Följande är en förklaring till vad personlig integritet innebär samt var det regleras idag i den svenska lagen.

Personlig integritet är ett begrepp som faller inom det större begreppet integritet. Personlig integritet kan definieras som att en person har rätt att få sin inre omgivning och egenart respekterad av andra. Det har ett nära samband med människans värdighet (Nationalencyklopedin, 2008c). Personlig integritet kan även syfta till att en individ väljer att hålla sig till sitt moraliska tankesätt och ha ett visst ansvar där moralitet och att vara korrekt är en viktig del i ens personlighet. Oftast är det baserat på individens egna instinkter. Därmed är det heller ingenting som säger att personlig integritet är objektiv utan berörs av hur en individ lever och beter sig i sin omgivning (Stanford Encyclopedia of Philosophy, 2001).

I § 2 i regeringsformen⁶ står det att ”den offentliga makten skall utövas med respekt för människans lika värde och för den enskilda människans frihet och värdighet”, dock är detta inte en definition i sig av vad personlig integritet är, utan det förklarar snarare vilket ansvar som svenska staten har mot sina medborgare för att trygga deras säkerhet inom olika välfärder (Regeringsformen, 1974:152). Det andra kapitlet i regeringsformen är den del av lagen som har blivit det reglerande kapitlet av den personliga integriteten och har delats upp i fem underbegrepp; rumslig integritet, materiell integritet, fysisk personlig integritet, ideell personlig integritet, och kroppslig integritet. Andra lagar som på något sätt skyddar den personliga integriteten, människans värde, är brottsbalken och personuppgiftslagen (Prop. 2006/07:63, 2006, s.61).

Förutom att personlig integritet är fastställd i svensk lag är den till viss del fastställd i det internationella samfundet genom internationella konventioner. Sverige har, sedan inträdet i Europeiska Unionen (EU) den 1 januari 1995, haft Europakonventionen⁷ som en gällande reglering med tilläggsprotokoll genom lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Prop. 2006/07:63, 2006, s.64) Artikel 8 i Europakonventionen reglerar personlig integritet, punkt 1 talar om vad som gäller och punkt 2 förklarar vad som krävs för att en rättighetsinskränkning skall få göras, exempelvis att skydda nationens säkerhet (EU, 1950, s.6).

⁶ Regeringsformens formella titel är Kungörelse (1974:152) om beslutad ny regeringsform, men är allmänt känd som regeringsformen.

⁷ Europakonventionens fullständiga titel är Europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.

4.3 Lagen och dess kritiker

FRA-lagen antogs den 18 juni 2008. Detta innebär att från och med den 1 januari 2009 träder lagen i kraft (FRA-lagen, 2008:717), men inför årsskiftet har valde försvarsdepartementet och riksdagen att FRAs signalspaningsverksamhet inte får rätt att inhämta signaler i kabelburen form förrän den 1 oktober 2009, inte förrän då har operatörer en skyldighet att överföra signaler som går över Sveriges gränser till FRA (Regeringskansliet, 2008, s.13). Den 25 september 2008 kom alliansen överens om femton ändringar som bland annat skall öka det personliga integritetsskyddet och ge förbättrade kontrollmöjligheter av signalspaningen. De nya förbättringarna till lagen blev uppbackade av den borgerliga majoriteten i riksdagen (Regeringen, 2008b), men Socialdemokraterna och Miljöpartiet är fortfarande kritiska. FRA-lagen har, sedan den antogs, blivit starkt kritiserad för dess brist på att skydda den personliga integriteten. I propositionen stod det klart att endast signaler som flyttades över Sveriges gräns skulle bli övervakad och inhämtad (Prop. 2006/07:63, 2006, s.84-85), men kritiker menar på att det idag är så många tjänster på Internet som ligger på servrar utomlands att svenska medborgares förehavanden ändå blir föremål för inhämtning av signalerna (Nilsson et al, 2008).

FRA-lagen ger tillstånd till massavlyssning enligt kritikerna. Försvarsministern Sten Tolgfors har inte förstått att problemet och kärnan i den kritik, som har varit genomgående i debatten, är att det är en stor mängd inhemsk data- och teletrafik som kopieras direkt till en statlig myndighet. Problemet som kritikerna anser att varken regeringen eller försvarsministern förstår är att det är staten som kommer att få tillgång till den mängd kommunikation och information som kommer skickas till signalspaningsverksamheten, vilken statlig myndighet som utför det har ingen betydelse. Tillgången till information och den kommunikation som florerar måste begränsas (Nilsson et al., 2008b).

Kritiker mot FRA-lagen ser lagen som ohållbar, på grund av att det är ett mycket stort antal webbtjänster som ligger på utländska servrar och som används av svenska medborgare. Konsekvensen blir att svensk data- och teletrafik skickas till FRA för bearbetning. Det är irrelevant om FRA inte har kapacitet att lyssna på och höra allt, det handlar om att den integritetskränkning som skulle uppstå inte kan upphävas eller uppvägas (Nilsson et al, 2008b). Inhemsk trafik skall filtreras bort, men filtreringsutrustningen som behövs kostar. Telebolagen uppger att det kan komma att röra sig om över 100 miljoner kronor och anser att det är något som FRA bör stå för (Holmström, 2008). Granskningen av såväl lagen som signalspaningsverksamheten och FRA bör fortsätta, Datainspektionen som redan har utrett anonyma klagomål om FRAs sätt att behandla personuppgifter bör få utökade arbetsuppgifter där de signaldatabaser och analysdatabaser FRA förfogar över bör omfattas (Klamberg, 2008a). Konsekvensen av att signalspaning som eftersöks att lagstadga i FRA-lagen redan genomförs blir att företag flyttar sina servrar utomlands för att undgå spaningen. CFR är främst kritiska på fem punkter som uppkommer i FRA-lagen. Bland annat gäller det att signalspaning genom elektronisk kommunikation redan utförs utan stöd från lagen, att 'yttre hot' hänvisar till allt från internationell terrorism till 'ekologiska obalanser'(Centrum för rättvisa, 2008, s.3). CFR lämnade in ett klagomål till Europadomstolen i juli, men i september 2008 gick regeringen ut med sju punkter som skulle sätta ramarna för signalspaningen. Dessa sju punkter gör, enligt riksdagsledamoten Fredrik Federly, centerpartist, att det går från en förordning till lag och att det tydliggörs att det inte är svenskar som utsätts för spaningen (Bynert & Johannisson, 2008).

Lagen bör rivs upp och en parlamentarisk utredning bör tillsättas. Detta trots de förändringar som gjordes och antogs den 25 september. Det anser miljöpartiet och socialdemo-

kraterna i en motion till riksdagen. Riksdagen bör upphäva FRA-lagen samt tillägg om lagen i andra berörda lagar såsom lagen (2003:389) om elektronisk kommunikation och lagen (2000:130) om försvarsunderrättelseverksamhet. En parlamentarisk utredning skulle få syftet att en lösning som tillgodoser behovet av underrättelsetjänst och medborgarnas rätt till integritet och rättssäkerhet (2008/09:Fö269, 2008).

4.3.1 Europadomstolen

Den 14 juli 2008 lämnade den ideella insamlingsstiftelsen Centrum för Rättvisa (CFR) in ett klagomål till Europadomstolen. I klagomålet begärdes det att domstolen skulle pröva om FRA-lagen uppfyller de krav som ställs från Europakonventionen på att skydda den personliga integriteten. Dessutom vill CFR med sitt klagomål få FRA-lagen prövat om det klarar kravet att låta enskilda som blivit övervakade få rätten att pröva sina fall i domstol. CFR anser att det är möjligt att göra ett klagomål som detta redan innan lagen har trätt i kraft därför att det redan pågår spaning av elektronisk kommunikation och därmed bör det vara rättfärdigat att domstolen tar upp fallet redan innan lagen hunnit träda i kraft (Centrum för Rättvisa, 2008, s.1-2).

CFR ser kritiskt på att FRA-lagen inte är skriven i så pass tydlig form att det är lätt att förstå hur själva proceduren skall gå till. Det vill säga, det är svårt för den enskilde att förstå hur undersökningen, användandet, kommunikationen och lagringen av hämtad information ser ut. Inte heller finns det några tydliga direktiv till hur informationen får eller skall bli raderad. Den sista kritiken som CFR riktar mot FRA-lagen gäller huruvida den enskilde har rätt att få ut information om det finns misstanke om att den enskilde är övervakad. Därmed saknas det möjlighet att den enskilde får möjlighet att få sin sak rättsligt prövad (Centrum för Rättvisa, 2008, s.3).

FRA-lagen är inte den första signalspaningslag som kan bli föremål för att prövas i Europadomstolen i syfte att se om den klarar kraven för personlig integritetsskydd och rätten att få sin sak prövad i domstol. Tidigare fall av detta slag som behandlats i Europadomstolen är ett fall från 2006 där Tyskland friades från att inte ha uppnått de krav som ställts i Europakonventionen och ett färskt fall som avgjordes sommaren 2008 där Storbritannien fälldes för att inte ha uppnått kraven i Europakonventionen (Centrum för Rättvisa, 2008, s.3).

Weber och Saravia mot Tyskland kallas fallet i Europadomstolen från 2006 där de två ansökanden Gabriele Weber och Richard Saravia valde att ställa tyska staten inför domstolen på grund av det tyska dokumentet från 1968 om ”Restriktioner om sekretess belagda handlingar såsom e-post, brev och telekommunikation” (G10-dokumentet) som uppdaterades år 1994. Klagomålet som Weber och Saravia framförde gällde det utökade ansvaret och auktoriteten som den tyska försvarsunderrättelsetjänsten fått när det kom till att spela in telekommunikation och systematisk kontrollering av privat data som insamlats och sändning till andra myndigheter (Europadomstolen, 2006, s.1). I det tyska fallet friades lagen då den endast tillämpades på tio procent av all telekommunikation och hade dessutom ett tydligt och klart syfte och precisa regler för signalspaningen. I den tyska lagen finns det även notering om att en person som blir avlyssnad har rätt att bli upplyst om detta och få det rättsligt prövad (Centrum för Rättvisa, 2008, s.4).

Det brittiska fallet gällde en anmälan mot Storbritannien som skickats in av ett antal organisationer på grund av att det brittiska försvarsdepartementet hade under 1990-talet använt sig av en *Electric Test Facility* (ETF), något som hade byggts för att kunna snappa upp 10 000 olika telefon kanaler samtidigt. Med ETF påstod Liberty och andra organisationer att deras

samtal med varandra under den tiden skall ha blivit uppsnappat och övervakat av ETF utan vetskap. När rapporter om ETF kom fram på tv under 1999 valde organisationerna att gå vidare med sitt fall till *Interception of Communications Tribunal* (ICT). De ville att ICT skulle klargöra om det funnits någon legitimitet i efterlysningarna som gjorts i samband med organisationernas kommunikation med varandra. ICT svarade att detta inte var något som de kunde veta i förhand (Europadomstolen, 2008, s. 2, 5).

Den lag och politik som är relevant vid detta skede är ICT lagen från 1985 som år 2000 ersattes med en ny lag kallad *Regulation of Investigatory Powers Act* (RIPA). Under tiden för den teleövervakning som ägde rum, blev en rad undantag gjorda trots att den som gjorde en sådan övervakning var skyldig till brott (Europadomstolen, 2008, s. 2, 5). Den brittiska regeringens representanter medgav att mellan 1990-1997 fanns det en möjlighet för vem som helst att hämta ut information om kommunikation som sträckte sig över de brittiska öarnas gränser, så länge de hade stöd av ICT lagen från 1985 där en fullmakt utfärdats. Enligt lagen hade myndigheterna stort utrymme för att bestämma vilken kommunikation som skulle övervakas och inhämtas (Europadomstolen, 2008).

De klagande byggde sitt fall bland annat på artikel 8 i Europakonventionen, vilken säger att var och en har rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens. Organisationerna menade på att deras privatliv hade inskränkts på grund av den lag från 1985 som gällde under den tid då avlyssningen skedde (EU, 1950, s.6). Det första som domstolen visade på i fallet var att det fanns ett hot mot dem, som en lag där övervakning av kommunikation tilläts, var mål för lagen och dess syfte. Domstolen ansåg att de rättigheter som de klagande har enligt artikel 8 hade blivit inskränkta (Europadomstolen, 2008). Beslutet grundas på att den övervakning som gjorts inte var enligt artikel 8 § 2 där det klart och tydligt står att en informationsövervakning eller signalspaning måste ske med stöd av nationell lag och att det finns en hänsyn till nationell säkerhet (EU, 1950, s.6).

Risken finns att FRA-lagen kan fällas i Europadomstolen på liknande premisser som den brittiska lagstiftningen, men de ändringar som gjorts ses som förbättringar, men det återstår frågetecken som måste rätas ut enligt allmänheten (Nandorf, 2008).

4.4 IT-relaterade hot

I dagens samhälle har allt större krav ställts på att det ska vara lättillgängligt med information och de verksamheter som tillhandahåller möjligheten förlitar sig därmed på IT-system (Säkerhetspolisen, 2008, s. 44). Den generella hotbilden som finns mot Sverige i form av terrorhot har blivit allt mer komplex och det har blivit ett växande hot från terrorism efter attackerna i Madrid 2004 och i London 2005. Attentat har utförts och planerats i Sverige av grupper med ideologiska band knutna till större terrororganisationer (Säkerhetspolisen, 2008b). Faktum, som redan påvisats flera gånger i denna uppsats, är att utvecklingen inom informationsteknik går framåt och detta kan inte bortses från. I och med teknikens utveckling behövs det uppdatering av verksamhetens system för att de ska kunna följa med i utvecklingen. Den elektroniska kommunikationen har växt till en stor och dominerande del av människors kommunikation, antingen via internet eller via teletrafik. Möjligheten som FRA-lagen ger FRA, dvs. att spana på trafik som går via tråd eller kabel gör främst, som redan nämnts, att regelverket behöver förstärkas för att skydda den personliga integriteten, men en annan aspekt av det hela vore att möjligheten skulle bli större att upptäcka IT-relaterade hot. Med hjälp av de unika inhämtningsmetoder och de som har ett avancerat tekniskt kunnande finns det möjlighet för FUV att möta dessa yttre hot mot den svenska tekniska infrastrukturen (Prop. 2006/07:63, 2006, s.58-59).

Det behövs ett väl förebyggande arbete inom tekniska och administrativa säkerhetsarrangemang för att möjligheten att skydda den svenska tekniska infrastrukturen från IT-hot skall kunna ge resultat. Det har tidigare inte funnits stor möjlighet för underrättelseverksamheten att bidra till detta. Med FRA-lagen finns möjligheten, men även att kunna möta IT-hot tidigare än vad som idag gäller (Prop. 2006/07:63, 2006, s.59). Det handlar bland annat om tekniska och administrativa säkerhetsarrangemang. Hos flera myndigheter och företag fanns det år 2007 en hel del säkerhetsbrister och en grundläggande sådan var att det saknades säkerhetsanalyser. Säkerhetsanalyser hjälper till att se vilka uppgifter som skall hållas hemliga och skyddas med hänsyn till rikets säkerhet samt mot terrorism. (Säkerhetspolisen, 2008a, s. 44).

De dataintrångsförsök som skett mot samhällsviktiga myndigheter och organisationer under 2007 är mycket svåra att upptäcka och säkerhetssystem såsom brandväggar och antivirusprogram upptäcker dem inte alltid. Elektroniska attackers förövare är svåra att spåra och gör det svårare för verksamheten att skydda organisationer och myndigheter (Säkerhetspolisen, 2008a, s. 44). Hotbilden mot Sverige är idag låg, men det betyder inte att risken för terrorattentat har minskat, den har ökat. Det är risken för att attentat sker mot utländska intressen på svensk mark som har ökat på sista tiden och det har skjutits från militära intressen till att fokuseras på politik och teknik (Säkerhetspolisen, 2005, s.16).

5 Resonemang kring studien och slutsats

5.1 Uppsatsens syfte

Med uppsatsen har det funnits två frågor som varit syften till att denna uppsats har formats. Dessa två syften behandlade huruvida FRA-lagen har påverkats av fenomenet cyberterrorism och om FRA-lagen är ett hot mot eller ett skydd för det svenska samhället. Det har funnits stort motstånd mot FRA-lagen och i skrivande stund finns det fortfarande motsättningar mot lagen. Utöver dessa motsättningar som finns både inom riksdagsgrupperna, så är en reviderad upplaga av FRA-lagen i skrivande stund ute på remiss och som väntas ha blivit besvarad den 28 februari 2009. Detta gör att uppsatsen behandlar ett ämne som det inte finns något slut på och det finns inga klara resultat färdiga för hur FRA-lagen ter sig i samhället.

5.2 Eventuella kopplingar mellan cyberterrorism och FRA-lagen

Under studien och undersökningen av dessa två fenomen har hypotesen att FRA-lagen och cyberterrorism inte har ett direkt samband till varandra i utformande av lagen varit en del av syftet och det som skall besvaras. Inget säger klart och tydligt i lag eller i propositionen om lagen att den är till för att skydda Sverige mot cyberterrorism. Däremot säger lagstiftarna att lagen är utformad för att skydda Sveriges säkerhet mot yttre hot. Yttre hot, som nämns i kapitel 4, var till en början allt från terrorism till ekologiska obalanser, men blev sedan inskränkt och definierat till att bland annat innebära yttre militära hot och allvarliga yttre hot mot samhällets tekniska infrastruktur. Enligt Weimann så har terrorister fått nya möjligheter med internet och att kommunicera med varandra. Cyberterrorism handlar om att precis som med vanlig terrorism skapa oro och skräck hos civila och angripa systemen i ett politiskt syfte. Värderingarna för cyberterrorism har inte förändrats från det stora begreppet terrorism endast fått en riktning till var det riktar sig mot.

Anhängarna till FRA-lagen håller med Weimann om att i dagens samhälle och den nya teknologin som utvecklas konstant så har terrorister fått en helt ny möjlighet att kommunicera med varandra via internet. Sambandet mellan FRA-lagen och cyberterrorism kan därmed verkas vara direkt, men det är inte endast cyberterrorism som är en faktor till att lagen har skapats. Även om inte lagen har ett direkt samband och är utformat för att försvara riket från cyberterrorism är det tydligt att cyberterrorism har varit en del i diskussionen och debatten kring framtagandet av FRA-lagen. Regeringen har menat på att den stora teknikutveckling som sker i dagens samhälle bör utnyttjas till att ge FRAs signalspaningsverksamhet tillgång att inhämta signaler från den elektroniska kommunikation som sker. Därmed på uppdrag från myndigheter kunna hjälpa att hålla Sverige skyddat från eventuella kriser. Trots att det gjordes ändringar i september som bland annat definierade yttre hot och skärpte skyddet för personlig integritet finns det fortfarande motståndare som menar att lagen ännu är ofullständig och inte kommer att tillgodose det som den är till för.

Håller hypotesen? Nej, cyberterrorism kan mycket väl vara ett direkt skäl till att FRA-lagen skapades. Det är med all säkerhet inte den enda faktorn som spelade roll när lagen skrevs, men det kan inte nog understrykas att teknologin i dagens samhälle har utvecklats att bli allt mer avancerad och därmed har samhället också blivit mer beroende av tekniken, vilket till

följd gör samhället mer sårbart. Cyberterrorism är relativt ett nytt fenomen inom begreppet terrorism, men det blir allt mer påtagligt och går därför inte att undvika i längden.

5.3 Det så kallade skyddet för Sverige

Hypotesen är att FRA-lagen är ett skydd för Sverige, uppsatsen kan verka något partisk i sin framställning av FRA-lagen, men det har gjorts försök att balansera upp båda parter sida om vad FRA-lagen innebär. Med detta sagt är det utifrån den framställning som har gjorts uppenbart att det inte är helt lätt att säga om hypotesen stämmer eller inte. Motståndare har helt acceptabla argument för att FRA-lagen inte bör finnas, samtidigt stödjer Europadomstolens beslut av att fälla Storbritannien för deras signalspaningslag risken för att FRA-lagen skall gå samma väg då den i många avseenden liknar den brittiska lagen. Förespråkare för lagen, det vill säga regering och de statliga myndigheter som är inblandade, menar på att de har tagit till sig av vad kritiker har sagt och att de ändringar som gjorts i lagen skall göra att den kan klara en eventuell bedömning i Europadomstolen.

Signalspaning är ett känsligt ämne och ett svårt sådant att definiera, det är inte det att regering och statliga myndigheter vill ha tillgång till privatpersoners e-post om där inte finns misstanke om hot mot rikets säkerhet. FRA-debatten är aktuell än idag och därmed gör det svårt att kunna ställa sig på endera sidan. Lagen togs fram, den bearbetades, den kritiserades, den återremitterades och den har nu återigen fått ett klartecken att gå ut på remiss, ändå träder den inte i full kraft förrän oktober 2009. Ett starkt argument som motståndarna har för att inte vilja ha lagen alls är att risken finns att inhämtningen av information missbrukas. Förespråkarna för lagen har däremot en stark åsikt i att det finns hot mot Sverige som måste avstyras, signalspaningsverksamhetens utökande till att även gälla kabelburen trafik skulle vara ett stort steg i den riktningen.

Hur är det då med det personliga integritetsskyddet? Det skydd som skall se till att individer skyddas från att bli kränkta? Det har förstärkts, detta skedde i september, men är det tillräckligt? Regeringen tycker att det är det och att döma av att ändringarna gick igenom i riksdagen är det säkert att säga att det är nog för dem. Däremot är frågan om de ändringar som gjordes verkligen är nog för allmänheten, kritikerna verkar inte anse det och det verkar svårt att hitta någon sorts kompromiss för att minska friktionen mellan de olika parterna.

Den slutgiltiga frågan som bör ställas och som har försökt fått ett svar genom uppsatsen är om det är rationellt att använda sig av medlet, signalspaning för att helga ändamålet, att skydda riket Sverige mot terrorism, både cyberterrorism och terrorism generellt. Genom uppsatsen har det hela tiden påvisats att det finns möjliga hot av cyberterrorism, mindre har utförts terrororganisationer, men det har inte funnits något större som har varit framträdande, detta betyder inte att det inte kan uppstå. Sverige är inte det första landet som har skapat en sådan här lag, men den är förebyggande. Det regeringen och deras utredare har velat få fram i sitt förslag är inte att de vill förtrycka det svenska folket, men att de vill skydda mot eventuella hot mot Sverige. Detta görs på ett sätt som kan få negativ effekt hos allmänheten, och hos den lilla människan, effekter som regeringen inte helt har tänkt igenom, därav den stora anstormning att den personliga integriteten inte skyddas och att regeringen har fått sätta sig ner för att komma fram till hur skyddet kan stärkas.

5.4 Slutsats

Terrorism har ändrat fokus sedan 11 september 2001 i samma stund som World Trade Center föll. Det blev en chock för många att inse att de var sårbara, att terrorister hade

möjlighet att såra ett land så stort som USA och att lyckas med det, det vill säga att inte bara planera det, men att också utföra och nå det mål som de strävat efter. Något så stort som skedde i USA 2001 är inte troligt att det kommer att hända i Sverige, samtidigt är det inget som ska tas för givet eftersom att det var säkerligen ingen som förväntade sig attackerna i London, Madrid eller på Bali. FRA-lagens tillkomst har givit ett nytt skydd för en ny sorts terrorism, men frågan handlar om ifall den nya terrorism som uppstått i dagens samhälle i och med attacken den 11 september 2001 mot World Trade Center. Därmed har allt förändras och det överhängande hotet från terrorism och cyberterrorism har blivit allt mer påtagligt. Tekniken utvecklas och det är viktigt att samhället följer med i utvecklingen och inte låter dem som vill andra illa att ligga före.

Så helgar ändamålet medlen? Skyddas Sverige av lagen? Med andra ord kan FRA-lagen rättfärdigas då ändamålet den har är att skydda Sverige? Jag vill inte vara partisk, jag vill inte sätta mig på ena sidan eller andra, men med förbättringar och med fler tydliggöranden av vad FRA-lagen skall göra, vad signalspaning är och att svenska staten ger svenska folket en allmän inblick av förståelse så är det med all förmodan troligt att det finns rättfärdigande för den signalspaningsverksamhet som lagen tillåter för att ändamålet är så viktigt för alla.

Referenser

Litteratur

- Aid, M.M. & Wiebes, C. (2001), Introduction: The importance of Signals intelligence in the Cold War. I M.M. Aid & C. Wiebes (Eds.), *Secrets of Signals intelligence during the Cold War and beyond* (s.1-26), New York: Routledge.
- Crotty, W. (2005), Democratization and political terrorism. In W. Crotty (Ed.), *Democratic development and political terrorism: the global perspective* (s.3-16), Boston: Northeastern University Press.
- Deverell, E., Fors, F., Hjelm, J., Holm, S. (2006). *Terrorattackerna i London den 7 juli 2005 – Brittiska lokala och regionala myndigheters agerande och lärdomar för det svenska krishanteringsystemet*. Stockholm: Krisberedskapsmyndigheten.
- Esaissaon, P., Gilljam, M., Oscarsson, H. & Wängnerud, L. (2004), *Metodpraktikan - Konsten att studera samhälle, individ och marknad*, Stockholm: Norstedts Juridik AB
- Golder, B. & Williams, G. (2004). What is "Terrorism"? Problems of legal definition, *University of New South Wales Law Journal*, Volume 27(2), 270-295.
- Harmon, C. (2007), *Terrorism Today*. London: Routledge.
- Henderson, H. (2001). *Global terrorism: the complete reference guide*. New York: Checkmark Books.
- Hoffman, B. (2006). *Inside terrorism*. New York: Columbia University Press.
- International encyclopedia of terrorism. (1997). *International encyclopedia of terrorism*. Chicago: Fitzroy Dearborn Publishes.
- Jacobsen, A. (2001), Scandinavia, Sigint and the Cold War. I M.M. Aid & C. Wiebes (Eds.), *Secrets of Signals intelligence during the Cold War and beyond* (s.209-242), New York: Routledge.
- Jervas, G. (2003). *Terrorismens tid*. Stockholm: SNS Förlag.
- Kumm, B. (2002). *Terrorismens historia*. Lund: Historiska Media.
- Laqueur, W. (2001). *A history of Terrorism*. New Brunswick: Transaction Publishers.
- Lutz B.J. & Lutz J.M., (2004). *Global terrorism*. New York: Routledge.
- Merari, A. (2007). Terrorism as a strategy of insurgency. I G. Chaliand & A. Blin (Eds.), *The history of terrorism – from antiquity to Al Qaeda* (s.12-51), Los Angeles: University of California Press.
- Migaux, P. (2007). Al Qaeda. In G. Chaliand & A. Blin (Eds.), *The history of terrorism – from antiquity to Al Qaeda* (s.314-348), Los Angeles: University of California Press.
- Münkler, H. (2004). *De nya krigen*. Göteborg: Bokförlaget Daidalos AB.
- Norell, M. (2002). Terror i Guds namn. *Världspolitikens dagsfrågor nr.12*. Stockholm: Utrikespolitiska institutet.

- Svenska Akademien (2006). *Svenska akademiens ordlista över svenska språket, 13. Uppl.*, Stockholm: Svenska akademien: Norstedts akademiska förlag.
- Tilly, C., (2004). Terror, terrorism, terrorists, *Sociological Theory, Volume 22(1)*, s.5-13.
- Vatis, M. (2001). Michael Vatis – Deputy Assistant Director and Chief, National Infrastructure Protection Center, Federal Bureau of Investigation. I Alexander Y & Swetnam M.S. (Eds.), *Cyber terrorism and information warfare: threats and responses* (s. 3-12). New York: Transnational Publishers , Inc.
- Wagner, A.R. (2005). Terrorism and the Internet: use and abuse. I Mark Last & Abraham Kandel (Eds.), *Fighting Terror in Cyberspace* (s.1-29). London: World Scientific Publishing Co. Pte. Ltd.
- Wardlaw, G. (1989). *Political Terrorism: Theory, tactics and counter-measures*. Cambridge: Cambridge University Press
- Weimann, G. (2006). *Terror on the internet – the new arena, the new challenges*. Washington: United States Institute of Peace Press
- Whittaker, David J (2003). *The Terrorism Reader*. London: Routledge.

Artiklar

- Asian Pacific News Service, (030626). “A conspiracy of silence around the Bali bombings”, *the Asian Pacific Post*, hämtad den 15 december 2008,
<http://www.asianpacificpost.com/portal2/402881910674ebab010674f4ad9312d5.do.html>
- Bynert, S. & Johannisson, E. (080926). “Militärt hot villkor för FRA-spaning”, *Svenska dagbladet*, hämtad den 30 december 2008,
http://www.svd.se/nyheter/inrikes/artikel_1788753.svd
- BBC News (2008a), “Indepth – London attacks: 7 July Bombings”, *BBC News*, hämtad den 7 november 2008,
http://news.bbc.co.uk/2/shared/spl/hi/uk/05/london_blasts/what_happened/html/default.stm
- BBC News (2008b),”Indepth – Madrid train attacks”, *BBC News*, hämtad den 11 november 2008,
http://news.bbc.co.uk/2/hi/in_depth/europe/2004/madrid_train_attacks/default.stm
- BBC News (2008c), “Indepth – America attacked: the four hijacks”, *BBC News*, hämtad den 15 december 2008,
http://news.bbc.co.uk/hi/english/static/in_depth/americas/2001/day_of_terror/the_four_hijacks/flight_11.stm
- BBC News (2008d), “Indepth – America attacked: the four hijacks”, *BBC News*, hämtad den 15 december 2008,
http://news.bbc.co.uk/hi/english/static/in_depth/americas/2001/day_of_terror/the_four_hijacks/flight_175.stm
- BBC News (2008e), “Indepth – America attacked: the four hijacks”, *BBC News*, hämtad den 15 december 2008,

http://news.bbc.co.uk/1/hi/english/static/in_depth/americas/2001/day_of_terror/the_four_hijacks/flight_77.stm

BBC News (2008f), "Indepth – America attacked: the four hijacks", *BBC News*, hämtad den 15 december 2008,

http://news.bbc.co.uk/1/hi/english/static/in_depth/americas/2001/day_of_terror/trade_center_disaster/1.stm

BBC News (2008g), "Indepth – America attacked: the four hijacks", *BBC News*, hämtad den 15 december 2008,

http://news.bbc.co.uk/1/hi/english/static/in_depth/americas/2001/day_of_terror/trade_center_disaster/2.stm

BBC News (2008h), "BBC On this day – 21 – 1988 : Jumbo jet crashes onto Lockerbie", *BBC News*, hämtad den 29 december 2008,

http://news.bbc.co.uk/onthisday/1/hi/dates/stories/december/21/newsid_2539000/2539447.stm

Borger, J., Campbell, D., Porter, C. & Millar, S. (010912), "Three hours of terror and chaos that brought a nation to a halt.", *Guardian.co.uk*, hämtad den 15 december 2008,

<http://www.guardian.co.uk/world/2001/sep/12/charlieporteronthemensfashion.september11>

Brace (021013), "Bombs kill at least 54 in holiday isle carnage", *Guardian.co.uk*, hämtad den 15 december 2008,

<http://www.guardian.co.uk/world/2002/oct/13/indonesia.theobserver>

CBC News (041029), "Bin Laden claims responsibility for 9/11", *CBC News*, hämtad den 2 januari 2009,

http://www.cbc.ca/world/story/2004/10/29/binladen_message041029.html

European Court of Human Rights (080701), "Press release issued by the Registrar - Chamber judgment: Liberty & other organisations v. United Kingdom", *European Court of Human Rights*, hämtad den 16 december 2008,

<http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=58243/00&sessionid=17570680&skin=hudoc-pr-en>

Försvarets Radioanstalt (071112) "FRA – för säkerhetsskull", *Dagens Nyheter*, hämtad den 7 november 2008, <http://www.fra.se/artikel-DN1.pdf>

Hamilos, G. (071031), "The worst Islamist attack in European History", *Guardian.co.uk*, hämtad den 15 december 2008, <http://www.guardian.co.uk/world/2007/oct/31/spain>

Holmström, M. (080830). "FRA-sällning kostar". *Svenska Dagbladet*, hämtad den 29 oktober 2008, http://www.svd.se/nyheter/inrikes/artikel_1638865.svd

Klamberg, M. (081020a). "Mark Klamberg: Fortsätt granska FRA". *Sveriges television*, hämtad den 29 oktober 2008, <http://www.svt.se/svt/jsp/Crosslink.jsp?d=35188&a=1280798>

McIntosh, N. (050707). "Bomb blasts plunge London into chaos". *Guardian.co.uk*, hämtad den 6 november 2008,

<http://www.guardian.co.uk/news/blog/2005/jul/07/explosionsplun>

Nandorf, T. (080927). "Nya beskeden om FRA tystar inte bloggare". *Dagens Nyheter*, hämtad den 29 december 2008, <http://www.dn.se/DNet/jsp/polopoly.jsp?a=833149>

- Nilsson, M., Petersson, A., Sandberg, M. (080708a). "Försvaret för FRA-lagen håller inte". *Svenska Dagbladet*, hämtad den 29 oktober 2008, <http://www.svd.se/opinion/brannpunkt/artikel:1443361.svd>
- Nilsson, M., Petersson, A., Sandberg, M. (081007b). "Nätverket Stoppa FRA-lagen: Tolgfors gör inget åt massavlyssningen". *Sveriges television*, hämtad den 29 oktober 2008, <http://svt.se/svt/jsp/Crosslink.jsp?d=35188&a=1268179>
- Statsrådsberedningen, (080925), "Alliansen enig om stärkt integritet, tydligare reglering, och förbättrad kontroll i kompletteringar till signalspaningslagen", *Regeringen*, hämtad den 17 december 2008, <http://www.regeringen.se/sb/d/10911/a/112332>
- Stewart, J. (040713), "FBI intelligence still under scrutiny", *Lateline*, hämtad den 15 december 2008, <http://www.abc.net.au/lateline/content/2004/s1153262.htm>
- The Guardian (021013). "Bali night club bomb kills 180", *guardian.co.uk*, hämtad den 11 november 2008, <http://www.guardian.co.uk/world/2002/oct/13/indonesia>
- Tran, M. (021013), "Finger of blame pointed at Jemaah Islamiya", *Guardian.co.uk*, hämtad den 15 december 2008, <http://www.guardian.co.uk/world/2002/oct/13/indonesia.marktran>
- Wilkinson, M. (030123). "FBI report pointed to Bali bombing", *theage.com.au*, hämtad den 15 december 2008, <http://www.theage.com.au/articles/2003/01/22/1042911437337.html>

Internet

- Australian Federal Police (2008), *Bali bombings 2002*, hämtad den 11 november 2008, http://afp.gov.au/international/operations/previous_operations/bali_bombings_2002
- Centrum för Rättvisa (2008), *Frågor & svar angående Centrum för rättvisas begäran att Europadomstolen granskar FRA-lagen*, hämtad den 8 december 2008, <http://www.centrumforrattvisa.se/images/File/FRA/fragorochsvarFRA.pdf>
- Department of Navy (1999), *Signals intelligence*, hämtad den 16 december 2008, http://www.combatindex.com/store/MCWP/Sample/INTELLIGENCE_OPERATIONS/MCWP_2-15_2.pdf
- Federation of American Scientists (1998), "Attachment 3 - Sources of Intelligence", *Air Force Pamphlet 14-210 Intelligence*, hämtad den 17 december 2008, <http://www.fas.org/irp/doddir/usaf/afpam14-210/part16.htm#page142>
- Homeland Security (2008), *Madrid train bombing*, hämtad den 11 november 2008, <http://www.globalsecurity.org/security/ops/madrid.htm>, *globalsecurity.org*
- Kovacs, J. & Pierson, J. (2003), *A new solution for signal intelligence*, hämtad den 16 december 2008, http://www.summitekinstruments.com/oasis/docs/PR/SpectrumMon-SIGINT_030106.pdf
- Nationalencyklopedin (2008a). *sökord: terrorism*, hämtad den 30 september 2008, <http://www.ne.se/artikel/1132090>

- Nationalencyklopedin (2008b). *sökord: signalspaning*, hämtad den 30 oktober 2008, <http://www.ne.se/artikel/1057092>
- Nationalencyklopedin (2008c). *sökord: personlig integritet*, hämtad den 28 oktober 2008, <http://www.ne.se/artikel/212289>
- Nationalencyklopedin (2008d). *sökord: jihad*, hämtad den 27 november 2008, <http://www.ne.se/artikel/216181>
- Stanford Encyclopedia of Philosophy (2008). *sökord: personal integrity*, hämtad den 9 december 2008, <http://plato.stanford.edu/entries/integrity/>
- Säkerhetspolisen (2008b). *Terrorhotet i Europa och Sverige*, hämtad den 17 december 2008, <http://www.sakerhetspolisen.se/terrorism/terrorhotetieuropaochsverige.4.7671d7bb110e3dcb1fd80002808.html>

Svenskt offentligt tryck

Lagar

Kungörelse (1974:152) om beslutad ny regeringsform

Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet

Propositioner, Motioner och Statens offentliga utredningar

Motion 2008/09:Fö269 Upphävande av FRA-lagen

Prop. 2006/07:63 En anpassad försvarsunderrättelseverksamhet

Försvarets Radioanstalt (2008a), *Frågor och svar om FRA*, hämtad den 7 november 2008, http://www.fra.se/omfra_faqshtml

Försvarets Radioanstalt (2008b), *Om FRA*, hämtad den 31 oktober 2008 <http://www.fra.se/omfra.shtml>

Försvarets Radioanstalt (2008c), *Signalunderrättelsetjänst*, hämtad den 31 oktober 2008, http://www.fra.se/omfra_signalspaning.shtml

Regeringen (2008a), *Frågor och svar om signalspaning: Varför behövs signalspaning?*, hämtad den 9 december 2008, <http://www.regeringen.se/sb/d/10810>

Regeringen (2008b), *Frågor och svar om signalspaning: Det talas om att integritetsskyddet har stärkts genom ett antal förändringar av det ursprungliga lagförslaget. På vilket sätt har detta skett?*, hämtad den 3 november 2008, <http://www.regeringen.se/sb/d/10810>

Regeringskansliet (2008), *Lagar och förordningar inför årsskiftet 2008/2009*, hämtad den 30 december 2008, <http://www.regeringen.se/content/1/c6/11/76/22/d4eebe7f.pdf>

Socialstyrelsen (2004), *Terrorattackerna mot World Trade Center 11 september 2001 – KAMEDO-rapport 84*, hämtad den 12 november 2008, <http://www.socialstyrelsen.se/NR/rdonlyres/9C9973A4-D63F-48F3-A06E-D1E33A6F4143/2843/200412335TerrorattackenmotWorldTradeCenter.pdf>

- Socialstyrelsen (2006a), *Terrorattacken på Bali 2002 – KAMEDO-rapport 89*, hämtad den 11 november 2008, <http://www.socialstyrelsen.se/NR/ronlyres/440AF135-CD99-45CB-8EE4-AC8464A44993/6453/200612322.pdf>
- Socialstyrelsen (2006b), *Terrorattacken i Madrid i Spanien 2004 – KAMEDO-rapport 90*, hämtad den 11 november 2008, <http://www.socialstyrelsen.se/NR/ronlyres/BA24C731-D94E-4E3A-9D73-B84749DF0E13/6525/200612340.pdf>
- Säkerhetspolisen (2005), *Säkerhetspolisen 2005*, hämtad den 16 december 2008, <http://www.sakerhetspolisen.se/download/18.7671d7bb110e3dcb1fd80009810/sakerhetspolisen2005.pdf>
- Säkerhetspolisen (2008a), *Säkerhetspolisen 2007*, hämtad den 3 november 2008 <http://www.sakerhetspolisen.se/download/18.59a6ce1f116807f34088000515/Sakerhetspolisen2007.pdf>
- Säkerhetspolitik (2008a). *Efter den 11 september*. Hämtad den 12 november 2008, <http://www.sakerhetspolitik.se/templates/Level2Page.aspx?id=400>
- Säkerhetspolitik (2008b). *Vad är terrorism?*, hämtad den 30 september 2008, <http://www.sakerhetspolitik.se/templates/Level2Page.aspx?id=397>

Annat offentligt tryck

Rambeslut i Europarådet

(2002/475/RIF) Rådets rambeslut av den 13 juni 2002 om bekämpande av terrorism

Europadomstolen (2006), *Third section decision as to the admissibility of: Application no. 54934/00 by Gabriele Weber and Cesar Richard Saravia against Germany*, hämtad den 7 november 2008, <http://www.centrumforrattvisa.se/images/File/FRA/CASE%20OF%20WEBER%20och%20SARAVIA%20vs%20TYSKLAND%20-%20FULL.pdf>

Europadomstolen (2008), *Fourth section – Case of Liberty and others v. the United Kingdom*, hämtad den 7 november 2008, <http://www.centrumforrattvisa.se/images/File/FRA/LibertyvUK.pdf>

Europeiska kommissionen (2004), *Terrorism: Europas svar*, hämtad den 3 december 2008, http://ec.europa.eu/justice_home/key_issues/terrorism/terrorism_0904_sv.pdf

Europeiska Unionen (1950), *Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna*, hämtad den 3 november 2008, <http://www.echr.coe.int/NR/ronlyres/1009F7DB-87E3-4056-8E17-8A8A41768BA7/0/SwedishSu%C3%A9dois.pdf>

Europeiska Unionen (2008), *Bekämpande av terrorism*, hämtad den 29 december 2008, <http://europa.eu/scadplus/leg/sv/lvb/133168.htm>

House of Commons (2006), *Report of the Official Account of the Bombings in London on July 7th 2005*, hämtad den 7 november 2008, http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/11_05_06_narrative.pdf

Intelligence and Security Committee (2006), *Report into the London terrorist attacks on July 7 2005*, hämtad den 7 november 2008, <http://www.official-documents.gov.uk/document/cm67/6785/6785.pdf>

Nationella kommissionen (2005). *11 september rapporten – nationella kommissionens slutrapport om terroristattacken i USA* (Wallin, K.E. översättare). Stockholm: Prisma (originalet publicerat 2004)