

First draft! Please do not quote without the permission of the author. Spelling and grammar have not yet been corrected.

Motstånd och makt i den digitala tidsåldern

"kontrollsamhällena opererar i den tredje maskinåldern, med informationsteknologier och datorer, vars passiva fara är störningar och vars aktiva fara är piratverksamhet och virus."

- Den 28 september 2007 är världssopinionen beroende av att rapporter, bilder och videoklipp lämnar Burmas territorier och landar hos internationella nyhetsbyråer. Mitt under pågående protester stängs de internationella kablarna mot Internet av, med förklaringen att en undervattensledning har havererat.
- Den 22 juli 2005 skjuts Jean Charles de Menezes till döds i Londons tunnelbana. Han matchade profilen av en terroristmisstänkt, och i och med att polisen hade förhöjd beredskap efter ett tidigare attentatsförsök, var beslutet om en dödsskjutning en 'förebyggande åtgärd'.
- Den 31 mars 2006 stängdes världens största fildelningssida ned, *The Pirate Bay*, genom att polisen beslagtogs de fysiska serverar som drev den så kallade *trackern*. 72 timmar senare var sidan återigen funktionsduglig genom att man hade flyttat till nya serverar utomlands.

Dessa tre fall har alla en gemensam nämnare i att informationsspridande verksamhet och övervakning löper i parallella spår. I samtliga fall finns en fysisk komponent inblandad; flödet av information och människor kontrolleras genom att begränsning eller nedstängning, och när det sker i de ovan nämnda fallen, vilka måste betecknas som extrema, så blottlägger man en skärningspunkt som visar på ett absolut tillfälle för statssanktionerad makt. Den blir synlig i och med att den visar upp sig i sin mest brutala form. Antingen så visar då de demokratiska *kontrollsamhällena* var gränserna för rörelsefrihet och informationsspridning går, eller så visar de auktoritära *disciplinära* samhällena var striden börjar, en strid som ofta blir mycket blodigare i slutändan. Denna essä kommer att behandla vilka de grundläggande förutsättningarna för motstånd i olika sociotekniska sammanhang är, och hur man kan förstå dessa dels som empiriska fall och dels som måttstockar på hur stor toleransen för yttrandefrihet är i ett samhälle är.

Grunden för studier av digitalt motstånd ligger i ett utvidgat informationsbegrepp. Det som flödar genom Internets alla kablar och servrar är ett or och nollor, digital information, som ibland formar kognitivt meningsskapande texter som människor läser, ibland utgörs det av instruktioner för hur maskiner ska bete sig, och ibland visar sig dessa flöden bestå av bilder, videoklipp eller virtuella världar. Denna information kan vara farlig för en regim, men den kan lika väl vara helt ointressant. Den kan vara upphovsrättsskyddad och ägd av ett företag, eller så kan den vara allmängods som alla kan dela fritt. Den kan få din dator att exekvera program, men den kan lika väl bestå av ett virus som får stora delar av Internet att kollapsa. Så vad vi talar om är inte bara information som budskap, utan istället bör vi betrakta information som en logik till vilken digitala motståndsstudier alltid måste förhålla sig; som en bas som sätter villkoren för informationsspridningens vara. En viktig sak att påpeka är dessutom att det inte finns något som på ett enkelt sätt kan reduceras till att *bara* vara digitalt motstånd. Tvärtom är denna domän *en del av en helhet* som ibland är viktig och avgörande, och ibland är mindre relevant. När det gäller motstånd i en auktoritär regim kan digitala kanaler utgöra ett medel för att nå vissa mål och sprida viktig information, och även om det inte är tekniken som står i fokus kan det ändå vara av högsta relevans vem som har kontrollen över den. Gäller det däremot lokalt motstånd på en arbetsplats så är betydelsen av informationsteknologier mindre eftersom informationen kanske istället sprids från mun till mun. Vad denna essä kommer att fokusera på är de digitala villkoren i vilka

motståndspraktiker befinner sig, och hur dessa både kan bidra till social förändring samtidigt som de kan användas som repressiva instrument. Men för att kunna bearbeta denna roll måste vi först tänka maktens former, och placera in information och informationsteknologierna i ett sådant sammanhang.

Två sociala diagram - Disciplinär vs. kontrollerande makt

I vad Michel Foucault¹ och Gilles Deleuze² och kallade för disciplinära samhällen är den teknologiska strukturen en central del av själva förhållandet av makt och motstånd. Oavsett om det gällde fängelsets inspärning, militärtjänstgöringens baracker, eller skolans inlärningstekniker, så skapades i de disciplinära samhällena ett socialt diagram av en maktapparat vars funktioner var så allomfattande att den kunde föras över på subjekten själva, så att den till slut fungerade per automatik³. Den disciplinära makten innehåller alltså konkreta inspärningstekniker, såsom murar och stängsel, men även regler, normer och förordningar, för att vid andra sidan av ett kontinuum även innefatta de regimer som subjektet ålägger sig själv. Det sociala diagram som fungerar som modell för den disciplinära makten kallade Foucault *panopticon*, ett begrepp som ursprungligen myntades av Jeremy Bentham, och som innebär att fängelset genom total insyn överför en självregim på fången som gör denne lydlig och villig att underkasta sig makten. Men från denna konkreta användning abstraherade sedan Foucault denna observation till att gälla som ett mönster för maktens former under artonhundratalet, ett mönster som var nedsänkt i produktionsförhållanden (fabriker), teknologier (energibaserade, mekaniska) och utbildningsformer (lydnadsbaserad skola).

Deleuze argumenterar i *Postskriptum om kontrollsamhällena* att detta diagram har utsatts för konkurrens av ett annat; *kontrollsamhället*, dels på grund av att det inspärrande sociala diagrammet håller på att kollapsa. Istället för disciplinering genom just inspärning, oavsett om denna sker materiellt eller immateriellt, består den centrala maktutövningen i kontrollsamhällena av att denna är allt mer frånvarande, samtidigt som den när som helst kan dyka upp. Den är *dispersiv*, alltså utspridd, och varhelst vi rör oss är kontrollmekanismer ständigt närvarande, kanske helt utan att vi aktivt är medvetna om dem. De digitala teknikerna, exempelvis, innebär att information ständigt kan kopieras,

lagras och genomsökas, och därmed kan stora populationer kontrolleras utan att man aktivt behöver övervaka, eller ens ingjuta en känsla av detta hos subjekten. Istället kan man med reaktiva medel göra stickprov, sökningar och punktinsatser. För att ge några exempel kan vi se hur förmannens inspektionsbås på fabriken tidigare var central i produktionen genom en övervakande *blick* (omnipotens). I en kontrollerande logik, där övervakningskameror visserligen kan ingå som ett övervakande moment, är det istället utvärderingen och optimeringen av produktionen som anger och *varnar* för det avvikande genom att *studera* det normala beteendet. När något avviker eller inte fungerar åtgärdas problemet (reaktiv makt). Därmed kan företaget se till så att de anställda inte konsumerar pornografi eller spenderar allt för mycket arbetstid i sociala nätverk genom en serie av kontroller. Internetanslutningen kan filtreras eller loggföras, passerkortet anger tiden spenderad på arbetsplatsen, och i rapporteringssystemet kan lönen moduleras efter prestation. Men detta system övervakar inte bara passivt, utan kan omedelbart övergå till att reagera med att blockera och hindra. Spärrar kan slås av och på, och för digitala motståndsstudier blir detta centralt eftersom kontrollen över tekniska system handlar om hur flöden stängs av eller släpps på. Internet går att blockera, på samma sätt som en dörr kan spärras genom att ett passerkort dras in. Det viktiga är varken kortet eller dörren, utan den dator som behandlar din status som behörig eller icke. Övervakningen, som nödvändigtvis inte behöver vara panoptisk, har förvandlats till en kontroll av flöden, flöden som inte alltid visar sig vara så enkla att styra över.

Om vi ser till mediehistorien så har nittonhundratalet inneburit många förändringar, och dessa har i viss mån satt agendan för motståndets roll i tekniska system. De figurativa medieteknikerna för första halvan av seklet var press, radio och television vars abstrakta logik innebär att informationsflödet är enkelriktat och att tekniken är kostsam. Filmmediets förhandscensur och pressens konstitutionella tryckfrihet, som visserligen garanterade det fria ordet, fungerade självreglerande genom att en institutionaliserad pressetik förhindrade vem som helst att skriva vad som helst. Internetteknikerna däremot, även om de lyder under samma konstitutionella ramverk som press- och etermedier, opererar i en *decentraliserad och dubbelriktad* logik. Informationen behöver inte gå genom centrala tekniska arrangemang, utan varje användare blir oundvikligen en potentiell spridare av information. Detta är givetvis problematiskt i auktoritära länder där förhandscensur används och där den

aktiva faran ligger redan i att information sprids och läses. I länder där detta är mindre intressant existerar istället Internet som en öppen yta, även om det finns undantag för bland annat barnpornografiskt material som ofta blockeras aktivt. Men det som är den huvudsakliga principen för kontrollsamhällena är den reaktiva manövern, som i huvudsak inte är panoptisk - Internetteknikerna medför nämligen nya möjligheter inte bara för informationsspridning utan också för övervakning. Internetoperatörer sparar loggfiler, hemsidaägare för statistik över besökare, sociala nätverk profilerar användaren och lagrar dess modulerade identiteter, och militär signalspaning söker efter nyckelord i informationsflödet. Decentraliseringen medför svårigheter att aktivt hindra att informationen sprids, men den medför å andra sidan nya typer av register, loggar och sökverktyg.

Det är här motståndet kommer in i bilden. I en decentraliserad nätverksstruktur kan anonymitet uppnås exempelvis genom att man använder sig av proxy-servrar, routers och kryptering. Detta gör så att vi kan driva anonyma bloggar, posta till Youtube utan att kunna bli spårade, och skicka e-post till redaktioner i andra länder. Samtidigt som den nya tekniken möjliggör nya former av övervakning, så skapas det nya flyktvägar och kryphål i den decentraliserade strukturen, och dessa är inte så lätta att täppa till. Men det är en försvinnande liten del av Internetanvändarna som ordnar sin kommunikation efter dessa praktiker. Mer och mer digitaliseras därmed blir även potentialen för övervakning allt större. Gilles Deleuze och Felix Guattari kallade detta för *universell modulation*. Med modulation så menas att man skapar digitala kategorier av analogt material, en teknik som bland annat används i modem. Det som tidigare var kontinuum delas upp i sekventiella informationsbitar. Allt fler saker moduleras; våra kreditkortsräkningar ger oss digital tillgång till vårt konsumtionsbeteende, Facebookprofiler ger oss statistiska variabler för våra vänskapsrelationer, hur länge vi bläddrar på en hemsida ger en indikation på våra intressen och vilken typ av filer vi laddar hem visar vår musiksmak. Detta gör att allt fler register kan samköras. De nya teknikerna är dessutom mer eller mindre osynliga och ofta billiga i drift, vilket ofta gör att de implementeras med en ekonomisk rationalitet⁴. Mobiltelefoni är ett exempel som bara under loppet av en tioårsperiod medförde att användare snabbt kunde positioneras geografiskt genom att lokalisera vilken antenn som vid ett visst tillfälle sände till en viss telefon, samtidigt som samtalen och

textmeddelandena potentiellt kunde avlyssnas.

Det som tidigare var en fråga för beteendevetenskaperna att *förstå* har förändrats till en uppgift för statistik och probabilitet att *kalkylera*. Våra rörelser i stadsrummet är tidssekvenser mellan mobiltelefonmaster och våra arbetstider är inte längre förmannens ansvar - våra passerkort har redan registrerat vårt schema på ett effektivare sätt. Denna modulering av vår tillvaro är oftast något vi aldrig märker. Det är bara där som en bakgrund, och för det mesta har vi accepterat varje steg av processen genom att klicka på ”godkänn” när vi exempelvis surfar på nätet. Motståndets gränslinje går alltså vid modulationen, och kryptering och vidarekoppling är två medel för att stoppa eller fly undan denna. Om panoptikon inducerade ett medvetande om att ständigt vara övervakad, så är modulationen istället närvarande men osynlig. Internetövervakning sker så långt borta att ingen ser de servrar som analyserar trafiken. Denna existerar å andra sidan på grund av juridiska variabler, exempelvis i *patriot act*, eller som end-of-licence-agreements (EULA) som man undertecknar när man skapar ett e-postkonto. Men den kanske mest centrala aspekten av kontrollsamhället är att *det suveräna subjektet* själv tar initiativ och inordnar sig i de system som utför kontrollen⁵. Vi låter oss modularas utan motstånd genom att köpa mobiltelefoner, surfa på Internet och röra oss i stadsrummet.

Hur kan vi då använda oss av uppdelningen mellan disciplinära och kontrollerande samhällen för att förstå motståndets förutsättningar? För att utveckla denna tanke kommer jag att ta upp två aktuella fall där båda dessa sociala diagram kan skönjas. Syftet är inte att renodla eller dra upp skarpa gränser, utan snarare att se vilka typer av tekniker, strategier och villkor som existerar i olika sammanhang. Först diskuteras fallet Burma, som i kraft av ett auktoritärt styre artikulerar tekniker och apparater på ett speciellt sätt. Därefter tar jag upp fallet Storbritannien som av konstitutionella och historiska omständigheter artikulerar förutsättningarna för motstånd på ett annorlunda sätt.

Fallet Burma - 2007

Internetanvändandet har under de senaste åren ökat markant i Burma. Under 2005 beräknades antalet användare överstiga 63 000⁶, en siffra som troligtvis är mycket högre om man räknar in internetcaféer och delade anslutningar (exempelvis trådlösa nätverk).

Men Internet i Burma är strängt övervakat och kontrolleras i flerfaldiga lager⁷ av disciplinära och kontrollerande sociotekniker, vilka i sin tur producerar olika former av motstånd. Enligt en studie genomförd av Open Net Initiative är varje Internetcafé skyldigt att ta en skärmbild var femte minut på de datorer som de hyr ut. Dessa skärmbilder skall sedan brännas på en CD-skiva som sedan skickas till Myanmar Information Communications Technology Development Corporation (MICTDC) för arkivering⁸. En sådan teknik följer främst det disciplinära sociala diagrammet, eftersom dess främsta effekter inte kommer ur den information som skärmbilderna ger. Snarare är Internetanvändarens ständiga medvetenhet om det faktum att hon är övervakad det som producerar en censurerande självregim. Denna typ av övervakning har vissa likheter med avancerad realtidsövervakning, som till exempel det förslag som Försvarets Radioanstalt (FRA) vill införa i Sverige, som innebär att all Internettrafik som lämnar landet söks igenom. Men den burmesiska övervakningen är mycket mera direkt och närvarande, om än mindre effektiv än de mera avancerade systemen som är på väg att installeras i andra länder. Men detta är bara ett av flera lager. I Burma är många internationella sidor även blockerade direkt. Dagstidningar och politiska organisationer som är regimkritiska är blockerade tillsammans med många E-posttjänster och webhotell⁹. Även de populära tjänsterna för videodelning, exempelvis Youtube, samt IP-telefoni (exempelvis Skype), är blockerade. Varje dator måste dessutom registreras vid Burmas post- och televerk annars hotar ett femtonårigt fängelsestraff¹⁰. Den direkta blockeringen stoppar information från att lämna eller komma in i landet på en direkt nivå, utan straffmässig påföljd. Den arbetar istället med den styrka en totalitär regim kan uppbringa genom att ha full kontroll över ett tekniskt system. För burmeser är det omöjligt att ta del av vissa delar av Internet, som i många fall istället har liknats vid ett Intranät. Men trots dessa överlagrande tekniker finns det motstånd. Genom att använda tunnlar och proxyservrar kan burmesiska Internetanvändare kringgå både blockeringen av utvalda hemsidor samtidigt som de undgår att bli upptäckta. Motståndet sker alltså på båda nivåer, genom att riva den kontrollerande barriären och att vägra inordna sig i den disciplinerande lydndsstrategin (som är socioteknisk par excellence). En tunnel via en proxyserver fungerar så att man ansluter till en dator utanför den så kallade brandväggen som en regim har satt upp för att hindra tillgången till vissa sidor. Datorn utanför brandväggen har full tillgång till Internet och på

så sätt får även datorn innanför brandväggen samma tillgång genom tunneln. Dessutom undviker man att bli upptäckt eftersom trafiken är krypterad. Reportrar utan gränser har satt samman en handbok för hur journalister kan ta del av dessa tekniker¹¹, och många av dessa har visat sig fungera väl i exempelvis Kina, där liknande censur existerar. På grund av att den strikta kontrollen misslyckas med att helt och hållet stoppa den information som oundvikligen lämnar landet blev bloggande och e-postande en viktig ingrediens i de protester som tog sin början i augusti 2007. Burmesiska bloggare försåg de internationella medierna med bilder och videofilmer direkt från demonstrationerna, alltså med material som inte hade varit tillgängligt genom en ordinär medielogik. Motståndet mot den sociotekniska kontrollapparaten blev så småningom för stort, och det enda alternativet för att stoppa flödet av information blev att stänga ned hela infrastrukturen. Den 28 september stängdes Internettrafiken av, med den officiella förklaringen att en undervattenskabel hade brutit, och Internetcaféer stängdes.

Open Net Initiative, ett forskningsprojekt mellan nordamerikanska universitet, har publicerat en rapport över hur Internet stängdes ned. Burma visar sig då vara det andra landet i världen efter Nepal som genomföra en så pass drastisk åtgärd. Rapporten hävdar att eftersom flera Internetcaféer har installerat proxyservrar och andra lösningar hade den Burmesiska regimen inget annat val, ett val som möjliggjordes av att samtliga tele- och Internetoperatörer är statligt ägda eller reglerade¹².

Fallet Storbritannien

The Surveillance Studies Network skriver i en rapport om det brittiska övervakningssamhället att det finns oöverskådligt många lager av övervaknings- och kontrollteknologier. Dessa har under de senaste åren genomgått en rad förändringar som inte bara är tekniska i en strikt bemärkelse. Storbritanniens 4,2 miljoner övervakningskameror¹³ tar inte bara bilder. En framväxande teknisk trend är dessutom att man tillför digital metadata, exempelvis automatisk ansiktsgenkänning, uträkningar av beteenden, och databaser som innehåller registreringsnummer på bilar. På så sätt är inte övervakningskameran *bara* optisk, utan även ett register som man kan söka i och som kan synkronisera ett helt nät av övervakningstekniker. Den traditionellt optiska tekniken har

kompletterats med datorns sorterings- och sökförmåga. Surveillance har blivit *dataveillance*¹⁴. Men denna tekniska expansion är inte bara en tillämpning av avancerade system, utan det är även invävt i ett socialt diagram där varken individen eller massan är primärt intressanta. Istället kalkylerar systemet individueller i en bank av data. När Jean Charles de Menezes blev skjuten av misstag i Londons tunnelbana reagerade systemet inte på honom som individ, utan på hur hans beteende sammanföll med en misstanke om hur en terrorist beter sig, och vilket utseende och social status en sådan kan tänkas ha. Polisen letade efter terrorister med ett visst utseende, och när Menezes passerade en av Londons tusentals kameror passade han in i en sådan bild - jakten kunde påbörjas. Menezes betalade och passerade spärrarna som ledde ned till tunnelbanan, och väl nere på plattformen började han springa för att hinna med tunnelbanetåget. Det är oklart exakt vad som hände inne i tunnelbanevagnen, men Menezes blev skjuten med flera skott i huvudet, vilket är standardprocedur för terroristmisstänkta eftersom de kan bära bomber runt bröstet. Denna illustration ger givetvis ingen utförlig beskrivning av den brittiska situationen som helhet, men den ger en bild av kontrollsamhällets sociala diagram som inte har massan som objekt, utan som letar efter en viss uppsättning egenskaper för att därefter ingripa. Terroristhotet är inte en massa som måste kontrolleras, utan snarare en avvikelser som kan mätas med kategorier, som när de sammanfaller skickar en signal. Moduleringen sammanställer information, som när den uppvisar ett visst mönster avger en varningssignal; regelbundna besök i moskéer, invandrad muslim, internationella banktransaktioner, snabba rörelser på en offentlig plats, etc. Kontrollsamhällets främsta mål är *pre-emptive* istället för *preventative*¹⁵. Istället för att förhindra och minimera skadan så är det optimala att ta bort skadan innan den ens har inträffat. Menezes är ett utmärkt exempel på detta, där informationsbehandlingen syftar till att behandla probabiliteter som kan ligga till grund för handling.

Men vi behöver inte exemplifiera med våldsamma terroristjakter för att se hur det brittiska övervakningssamhället har brett ut sig. Framväxten av *gated communities* är ett annat bra exempel. Istället för att hålla människor inspärrade, som i de disciplinära institutionerna, har grindsamhället istället som uppgift att släppa in endast de som har rätt behörighet.

Motståndets former

Hur kan vi då förstå motståndsbegreppet, och det faktiska motståndet, mot bakgrund av det sociotekniska intermezzo som målas upp med exempel från Burma och Storbritannien? Svaret är blir beroende av vilket uttryck makten tar sig. I Burma har vi den auktoritära makten som måste undvikas eller bekämpas, och här ligger det primära i möjligheten att ta sig igenom de informationsteknologiska murarna som står på spel, samt möjligheten att göra sig anonym. Proxy- och routingtjänster är därmed figurativa motståndsformer, tillsammans med liberala Internetcaféer. Den aktiva faran är ständigt närvarande, och består av att bli gripen, kanske torterad och kastad i fängelse. Kontrollen av information är till för att stoppa den innan den sprids, och för att stoppa den innan den kommer in i landet. Därför är kontakten med omvärlden bruten och begränsad för att regimen inte vill att Burmeserna skall veta om omvärlden, och för att omvärlden ska veta om Burma. Denna generella logik, sätter existensbetingelserna för motstånd inte bara i Burma, utan likaväl i andra auktoritära länder såsom Kina, Kazakstan, Iran, Eritrea, Uzbekistan, Nordkorea, med flera¹⁶. Det finns i dessa staters maktutövning stora likheter med vad Foucault kallade för disciplinära samhällsformer. Makten syftar till *inspärning* och *koncentration/fördelning* i rummet. Informationen får inte lämna landet, den måste hållas inom brandväggarna, och på så sätt får endast begränsad information ta sig in och ut. Brandväggen och filtret är på så sätt den ena sidan av de auktoritära samhällenas tekniker. Men likaväl har vi, som i fallet med skärmavbilderna, där *individen* utskiljs i en *massa*, det panoptiska sociala diagrammet som syftar till att forma den lydiga individen. Motståndet arbetar emot båda dessa logiker. Många Internetcaféer är både liberala när det gäller att tillåta att folk surfar anonymt och att styra trafiken genom proxyservrar. Detta ledde, som vi såg, fram till en situation där regimen fick utöva sin absoluta spärrmakt, och därmed stänga ned alla förbindelser till omvärlden.

I Storbritannien, som delar många erfarenheter med andra liberala demokratier, blir det däremot mera komplicerat. Vad finns det egentligen som man kan göra motstånd mot? Den nya övervakningen har ju varken primärt samhällskroppens helhet som objekt (biopolitik)¹⁷, och inte heller opererar den kring inspärningens sociala diagram. Deleuze ställer upp just denna utmaning i sista stycket av *Postskriptum till kontrollsamhället*, men

ger inga svar på hur ”nya former av motstånd” skulle kunna se ut.

Men ett exempel är *sousveillance*, som har rötter tillbaka till bland annat situationismen. *Sousveillance* syftar till att medvetandegöra den dolda övervakningen i samhället genom att re-situera övervakningsteknikerna hos vanliga medborgare, och på så sätt motövervaka genom att skapa ett ”inverterat panoptikon”. Denna motståndsstrategi, även kallad reflektionism, får på så sätt ett avslöjande och synliggörande syfte¹⁸. Rent konkret har detta bland manifesterat sig i att motövervakarna filmar och fotograferar människor i det redan övervakade stadsrummet för att sedan projicera bilderna på gatan och därmed ställa den implicita frågan till människor, huruvida övervakningssamhället egentligen är ett sunt samhälle att leva i eller inte. Även om detta grepp har tveksamma grundantaganden om människors förmågor som samhällsmedborgare, innefattar det åtminstone en tanke om motstånd som konkret praktik.

En annan potentiell motståndsstrategi, som än så länge mest är en tentativ tanke och där det givna exemplet är tveksamt. Men det handlar om den storskaliga sociala organisationen. Eftersom kontrollsamhällena inte har samhällskroppen som objekt, utan endast de enstaka fienderna, så har den inget motvapen mot massrörelser eller okontrollerad social förändring. Fildelning är ett exempel på just detta. Runt en miljon svenskar byter filer med varandra vilket gör fenomenet till en omöjlighet att stoppa genom polisiärt ingripande, och den juridiska proceduren kan endast statuera ett symboliskt exempel. Inte ens en övervakningsapparat som kontrollerade varje filöverföring på Internet skulle mäka att motverka detta fenomen, och även om man med våld slår till mot fildelningssidorna uppstår de lika snabbt igen. Men räknas verkligen detta som motstånd? Man skulle kunna argumentera att fildelning endast är en vinstmaximerande praktik för att skaffa gratis musik och film. Eller om man vill vara lite mera generös skulle man kunna kalla det för en ”ny inställning” till kulturprodukter och konsumtion. Men, även om vi räknar bort detta, har vi att göra med ett icke-organiserat men samtidigt sammankopplat massfenomen mot vilket kontrollsamhället inte verkar ha några direkta verktyg.

Således... (fråga till seminariet - vad är egentligen slutsatsen av detta?)

Appendix - Sammanfattande tabula

<i>Sociala diagram</i>	<i>Panopticism</i>	<i>Kontroll</i>
<i>Figurativa tekniker</i>	Kamera, arkitektur, inspektion	Data mining, GPS, mobiltelefoner, loggfiler, ansiktigenkänning, register
<i>Sociala tekniker</i>	Visibilitet, självregim, lydnad, disciplinering, skenbart frikännande, signatur, nummer	Konkurrens, prestation, EULA, livslångt lärande, evig förhållning, modulation, lösenord, föreskrifter
<i>Övervakningsstrategier</i>	Surveillance	Dataveillance
<i>Motstånd</i>	Flykt ifrån instängning och visibilitet	Flykt ifrån modulering. Icke-organiserade massfenomen

1 Foucault, Michel (1977) Övervakning och straff.

2 Deleuze, Gilles (1990) Postskriptum om kontrollsamhällena, i "Skriftserien Kairos no. 4 - Nomadologin", Raster förlag.

3 Foucault, Michel (1977) Övervakning och straff.

4 Lianos, Michalis (2003) Social control after Foucault, in The Journal of Surveillance & Society, vol. 1, issue 3, p. 417

5 Ibid, p. 416

6 http://english.people.com.cn/200604/18/eng20060418_259227.html

7 http://www.rsf.org/IMG/pdf/index_2007_en.pdf

8 <http://www.opennetinitiative.net/studies/burma/#toc2g>

9 Ibid.

10 http://www.rsf.org/article.php3?id_article=18202

11 http://www.rsf.org/article.php3?id_article=15013

12 Wang, Stephanie (2007) Pulling the Plug – A Technical Review of the Internet Shutdown in Burma, Open Net Initiative Bulletin.

13 Wood, David M. (2006) A Report on the Surveillance Society - For the Information Commissioner by the Surveillance Studies Network.

14 Se även Delanda, Manuel (1991) War in the Age of Intelligent Machines, New York: Zone Books, s. 217ff

15 Ibid

16 http://www.rsf.org/article.php3?id_article=24025

17 Se även Foucault, Michel (1976/2002) Sexualitetens Historia. Band 1. Viljan att veta, Uddevalla: Gidlunds, s. 146ff

18 Mann, Nolan, Wellman (2003) Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments, in The Journal of Surveillance & Society, vol. 1, issue 3.