Lunds universitet
Statsvetenskapliga institutionen

STVK01
HT10
Handledare: Martin Hall

Politisk aktivism utan gränser

En studie av begreppet digitalt korrekt hacktivism

Jacob Dexe

Abstract

In a world where we can find and do almost anything online, social sciences are obliged to look to online activities as a way of describing how we live our lives. One of the most fascinating things is the emergence of online political activism. The author develops existing theories on hacktivism, digitally correct hacktivism and tries to broaden and problematize these concepts. The reasoning revolves around the online hacktivism focused around the green revolution in Iran during the summer of 2009. The topic is extremely current with reports of hacktivism in media almost weekly, yet few people know what hacktivism is. Reasoning in the thesis is founded on a selection of literature and interviews with key activists.

Previous research is based on inductive reasoning but lacks a quantity of examples needed for qualified generalization. That is why this thesis is a valuable addition to the field, touching on both the past and current examples. In the end, the author predicts that the digitally correct hacktivism will be a more frequent phenomenon in the future, and calls for more extensive research in the field, but at the same time establishes that the existing theories lack internal criticism against existing definitions.

Nyckelord: Hacktivism, digitally correct hacktivism, political activism, Iran, hacking, civil disobedience, mass online hacktivism
Antal ord: 9513

Innehållsförteckning

1 Inledning

1.1 Inledande problemformulering

Internet kan belysas på många olika sätt. Man kan förhålla sig till det med fascination, skepticism, beundran, motvillighet eller likgiltighet. Oavsett vilken inställning man har till fenomenet så är ett åtminstone säkert, på ett eller annat sätt måste man förhålla sig till det. I december 2010 räknar man med att det finns ungefär 2 miljarder personer i världen som är anslutna till nätet (Internet World Stats). Det är ungefär 30 procent av världens befolkning. Det är ett oerhört viktigt medium att studera inom många områden, så även inom statsvetenskapen. Till skillnad från tidigare medier som fått stor spridning så sammanför internet flera olika egenskaper som gör det möjligt att till exempel arbeta med politisk aktivism, och även att kommunicera och leva, på ett nytt sätt. Där telefonen kräver att man vet något om den på andra sidan, och TV, radio och tidningar inte är ett utbyte av information så skapar internet möjlighet för främlingar att sammanstråla trots geografiska avstånd för att uppnå gemensamma mål.

När nätet omfattar en så stor del av världens befolkning kommer även konflikter och till och med krig att i allt större utsträckning förekomma på nätet, och skapar även helt nya möjligheter för individer att påverka dessa konflikter. Det kan handla om personliga eller politiska konflikter, de kan påverka smala eller stora intressen och de kan engagera miljoner eller skapas av ett fåtal. I denna uppsats vill jag titta på en form av aktivism som har vuxit fram på nätet och som kopplas till den aktivism vi kan se vid sittstrejker, blockader och civil olydnad. Denna aktivism kallas ”hacktivism” och innebär att man använder digitala verktyg för att föra fram politiska budskap och nå politiska mål. Det är ett område som till viss del har fallit i glömska inom vetenskapen, samtidigt som konflikten mellan olika sorters hacktivism och även hur hacktivismen kan rättfärdigas belyses på ett nytt sätt.

Denna konflikt mellan olika delar av hacktivismen tog sig under sommaren 2009 konkret uttryck i den digitala aktivism som riktades mot Iran och demonstrationerna som utbröt efter presidentvalet där den 12e juni. När missnöjda väljare ansåg sig lurade av regimen då presidenten Mahmoud Ahmadinejhad åter igen segrade med oerhört stora siffror så började en revolution utveckla sig på gatorna, en revolution som till stor del samordnades via nätet. Men det intressanta i denna uppsats är inte hur aktivisterna i Iran använde nätet för att sprida information mellan sig, utan hur hacktivister utanför Iran agerade när regimen började stänga ner åtkomst till internet för medborgarna. ”Digitalt korrekta” hacktivister gjorde det möjligt för aktivister i Iran att kommunicera ut information säkert och se till att information från omvärlden kunde nå Iran, trots att regimen

stängde av och övervakade nästan all nättrafik. Det jag vill göra är att beskriva fenomenet ”digitalt korrekt hacktivism” och dess roll dels i Iran samt även i förhållande till den hacktivism vi kanske är mer van vid. Jag vill utveckla de existerande teorierna och sätta dem i en mer aktuell kontext än de tidigare figurerat i. Och sist men inte minst vill jag belysa den relevans hacktivismen har för statsvetenskapen och politisk aktivism i stort.

1.2 Forskningsfrågor

Vad är digitalt korrekt hacktivism?
Vad särskiljer den digitalt korrekta hacktivismen från övrig hacktivism?
Är tidigare definition av digitalt korrekt hacktivism fortfarande giltig?

1.3 Syfte

Hacktivism i stort är ett outforskat område inom statsvetenskapen som jag tror kommer ha fortsatt påverkan på vårt samhälle, även om det i mångt och mycket är svårt för gemene man att förhålla sig till de konkreta handlingarna och effekterna av dem. Man bör också se till att begreppet utvecklas ständigt och att det behövs kontinuerlig forskning för att försöka förstå och förklara dessa företeelser som påverkar vår omvärld. Hacktivisterna befinner sig i en egen arena med lite insyn för den som inte besitter den tekniska kompetensen att ta sig in. I många fall finns det ingen reglering eller lagstiftning i området de rör sig på, vilket gör det svårt att utvärdera deras handlingar utifrån etablerade ramar för aktivism. Dessa aktivistgrupper agerar bortom det vi kan se med blotta ögat och det som medierna rapporterar. Vi hör talas om tårtkastning mot politiker, om protester vid klimattoppmöten eller husockupationer. Men att enskilda individer kan bryta staters informationsmonopol och öppna upp gränser utan någon sorts våldsam påverkan hör vi väldigt sällan om i media.

Samtidigt är det ett område som påverkar statsvetenskapen. Det finns klara demokratiska problem med en teknisk elit som kan manipulera information eller politiska kampanjer utan någon som helst extern inblick. Samtidigt ger det en informationskanal som kan vara svår att förhålla sig till, den är intensiv och exklusiv samtidigt som det ofta handlar om människor utan journalistisk utbildning som ska försöka filtrera informationen som sprids ut från konflikthärdar. Det finns världspolitiska problem där nätaktivister kan underminera staters suveränitet genom några rader kod. Och det finns etiska

problem angående vad som är önskvärt och bra när människor har så stor möjlighet att påverka.

1.4 Material

Litteraturen jag har att luta mig på är dels litteratur om hacktivism så som den såg ut runt millennieskiftet, dels litteratur om aktivism och slutligen verk som överbryggar dessa områden. Med tanke på bristerna i litteraturen, generellt sett behandlas inte ”digitalt korrekt hacktivism” och informationen om hacktivism är bristfällig eller väldigt vinklad, och då målet är att beskriva begreppet med hjälp av händelser som tidigare inte finns nedtecknade är det lämpligt att jag även använder mig av intervjuer där jag talar med hacktivister. Intervjuerna avhandlade vad personerna anser att ”digitalt korrekt hacktivism” är, vad som hände kring Iran och hur aktivistgrupperna som sysslar med hacktivismen ser ut och har för tankar.

1.5 Avgränsning

Det finns många avgränsningar som måste göras när man har ett område med så stor intern diversion och samtidigt ett begränsat utrymme. Från början var det menat att arbetet skulle vara en kategorisering av hacktivismen på samma sätt som man skulle kunna kategorisera 'vanlig' aktivism. Det skulle kräva ett tämligen stort material med väldigt många olika företeelser att kategorisera i allt för subjektiva grupperingar som inte gör det politiska fenomenet rättvisa. Därför måste jag avgränsa mig så att jag lägger större vikt vid de direkta hacktivistiska handlingar som är mer komplicerade och kräver större engagemang än att till exempel gå med i en grupp på Facebook.

Att jag inte höll mig till hacktivism i stort beror på att mycket av den litteratur som finns på området visserligen är cirka 10 år gammal, men den bär fortfarande relevans för den hacktivism som beskrivs som ”mass action hacktivism” i senare litteratur. Den digitalt korrekta hacktivismen är en avart med ett annat fokus än tidigare och mer konventionell hacktivism och samtidigt är det en sorts aktivism som genererar stor sympati världen över eftersom man ofta arbetar med mål som de flesta av världens länder anser vara goda.

Samtidigt kan jag inte bara beskriva en händelse då det inte kan hållas lika generellt som mitt mål med uppsatsen trots allt är. Hade jag bara fokuserat på att beskriva förloppet i Iran utan att ta in annan information hade det blivit en ganska platt uppsats som inte hade haft speciellt stor varken inom- eller utomvetenskaplig relevans. I stället måste det ske en avgränsning även gällande Iran. Det är en

fortlöpande revolution som pågår där och därmed kan man inte säga precis vad fenomenet är. Det man kan göra däremot är att exemplifiera den digitalt korrekta hacktivismen med hjälp av vad som hände i Iran sommaren 2009. När jag hädanefter säger ”händelserna i Iran” menar jag de inslag av hacktivism och nätaktivism som var involverade i, eller arbetade med följderna av, revolutionen i Iran sommaren och hösten 2009.

1.6 Disposition

Jag har börjat med att ge en kort inledning till uppsatsen och har förklarat syftet, begränsningar och framför allt lagt fram en frågeställning att besvara genom uppsatsen. I kommande kapitel kommer resonemang kring de metodologiska val som gjorts, dels angående den övergripande undersökningen, dels kring intervjuerna som genomförts. Därefter kommer jag att ta upp tankar kring reliabilitet och validitet.

Efter den metodologiska och uppsatstekniska biten kommer en redogörelse för hacktivismens begreppsliga bakgrund och fenomenet som en säkerhetsfråga för att senare kunna göra en ordentlig distinktion av den digitalt korrekta hacktivismen. Därefter påbörjas uppsatsens huvudsakliga illustration med händelseförloppet samt aktivismen relaterad till revolutionen i Iran. Nedslag kommer göras i två olika aktivistgruppers verksamhet och filosofi för att påvisa en förändring från tidigare hacktivism. Den avslutande delen i brödtexten är en begreppslig redogörelse av digitalt korrekt hacktivism och vad fenomenet består av. Sist i uppsatsen kommer en slutgiltig redogörelse för vad jag kommit fram till, samt några tankar om framtida forskning på området.

2 Metod

Här kommer jag att resonera lite kring de metodologiska val jag har gjort i denna uppsats. Mina största problem har legat i bristen på material rörande huvudfrågan, ”digitalt korrekt hacktivism”, men jag kommer här att försöka motivera min undersökning, redovisa den intervjuteknik som använts, se till materialets tillförlitlighet och sist men inte minst skriva ut förklaringar av några av de termer jag kommer använda mig av frekvent igenom uppsatsen.

2.1 Teoriutvecklande och begreppsbeskrivande studie

Eftersom jag utforskar en del av ett begrepp som hittills inte har analyserats i speciellt stor utsträckning i den statsvetenskapliga litteraturen så kommer ambitionen för uppsatsen att vara i viss mån beskrivande, och i viss mån teoriutvecklande. Beskrivande i den mån att jag måste beskriva fenomenet ”digitalt korrekt hacktivism” för att kunna ge läsaren en uppfattning om vad begreppet involverar och kunna sätta det i kontrast till det större hacktivistbegreppet. Den kommer vara teoriutvecklande i den mån att det inte finns några färdiga teorier om fenomenet och att man därmed har möjlighet att formulera en teori utifrån den information man kan få fram i intervjuer och från litteraturen. Dock gäller det att inte dra på för stora växlar när man talar om vad ”digitalt korrekt hacktivism” är och vad det kan få för konsekvenser, men likväl borde och ska man försöka göra generella slutsatser för att tillföra något till det statsvetenskapliga fältet.

En av vägarna till att nå kunskap är induktiv metod, att utifrån en mängd observationer kunna uttala sig generellt om olika företeelser (Teorell, Svensson 2007:49). När det gäller ”digitalt korrekt hacktivism” är fallen så pass få att de induktiva metoderna faller till föga eftersom vi med få exempel inte har samma möjlighet att generalisera och säga något om verkligheten. Eftersom de senaste exemplen jag har i litteraturen kommer från 2004, och även där bygger på tidigare observationer är det värdefullt att fortsätta exemplifiera begreppet för att kunna generalisera och förklara verkligheten mer noggrant och exakt. Självklart är dock induktiva resonemang svåra (Teorell, Svensson 2007:49) då det alltid finns en möjlighet att nästa observation säger emot den världsbild man har skapat eller som finns nedtecknad sen tidigare. Därför är det oerhört viktigt att vara tentativ, det vill säga ödmjuk och försiktig, i sina slutsatser och generaliseringar om vad

begreppet är för något. De slutsatser jag kommer att komma fram till i denna uppsats har alltså en viss risk att kunna falsifieras i framtiden, men det är samtidigt charmen med forskning i ett så pass dynamiskt område som jag har valt i uppsatsen.

2.2 Intervjuteknik

Intervjuerna kommer att genomföras via mail, och vid ett tillfälle i en chatt, med personer som varit involverade i olika hacktivistnätverk eller som på egen hand har spelat centrala roller i hacktivismen som utspelades kring Iran sommaren 2009. De kommer att utformas som samtalsintervjuer som inleder med ett par större, övergripande frågor och därefter fokuserar på intressanta frågeställningar som dyker upp efter att respondenternas svar har analyserats. Att jag väljer att utforma en textbaserad intervju på detta viset är att en frågeundersökning, eller enkätundersökning, enbart får fram svar på de frågor jag ställer och därefter finns det ingen möjlighet att ställa följdfrågor och få in analyserande svar. I och med att forskningsområdet inte har utvecklats vetenskapligt tidigare så måste man i så stor utsträckning som möjligt försöka få fram all relevant information av intervjuobjekten, och med detta syfte så är samtalsintervjuer optimala att använda. Då går det att lokalisera trender i anledningar och motiv som inte hade kommit fram om man hade lagt fram 20 frågor med enkla svarsalternativ. (Esaiasson et al 2007:283)

Jag kommer inte att använda en intervjuguide i vanlig mening då en sådan är uppbyggd kring ett muntligt samtal och därmed har ett annat flyt än vad intervjuer i textformat har. Det är därför viktigt att formulera frågor som respondenterna både kan och vill svara på utan att för mycket resurser läggs på att förklara meningen med frågeställningen och vad som är önskvärd information att få från respondenten. Samtidigt går det inte att kunna använda små, korta frågor som ”Vad hände då?”, ”Hur gick det till?” (Esaiasson et al 2007:298) eftersom dessa kommer göra att mailväxlingen drar ut på tiden mer än vad som är hälsosamt under ett arbete som detta. Därför måste man komplettera de små, korta frågorna med till viss del riktade frågor för att informationen som kommer fram ur intervjuerna ska vara relevant för uppsatsen och de resonemang som förs däri. Det innebär alltså att det är en balansgång mellan att behöva få ut specifik och användbar information i intervjuerna, och samtidigt inte leda svaren i allt för stor utsträckning då tanken är att intervjuobjektens svar, inte frågorna som ställs, är det som ska föra uppsatsen och forskningen framåt.

Frågorna kommer att inbegripa tre centrala teman för uppsatsen, men kommer inte att ordnas på något specifikt sätt då intervjuerna baseras på de svar som givits till stor del. De tre temana är viktiga för att förstå dels händelserna i Iran och dels begreppen hacktivism och digitalt korrekt hacktivism i respektive kontext. Det första området har att göra med hur aktivismen utvecklades dagarna och veckorna efter att revolterna i Iran tog fart, alltså ett försök till att hitta en kronologi att utforma min berättelse utifrån. Det andra området kommer att fokusera på de

tekniska aspekterna och hur grupperna som skötte teknikerna såg ut. Målet är att hitta varianser i hur en hackers verktyg används när det kommer till politisk aktivism och dels se vilken skillnad i teknikanvändande det finns mellan hacktivism i stort och digitalt korrekt hacktivism mer specifikt. Den sista delen i intervjun är mer filosofisk och spekulerande för att kunna lokalisera drivkrafter som finns bakom hacktivisternas engagemang och denna specifika aktivism som fenomen. Detta för att kunna generalisera kring vad det är som har skapat denna särart av hacktivism och se vilken relevans den har i statsvetenskap och inom den politiska aktivismen i stort.

2.3 Intervjuerna

De intervjuer som genomförts under arbetets gång har i samtliga fall ägt rum på nätet i någon form. Merparten har skett via mail och vid ett tillfälle har den i stället förts i en chatt. Det finns betänkligheter med att genomföra intervjuer på detta vis. För det första går det inte att vara säker på att de individer som intervjuas verkligen är dem de utger sig för att vara då de ofta gömmer sig bakom pseudonym. Detta är dock inget som nödvändigtvis påverkar uppsatsen då svaren som ges på frågor spelar större roll för resultaten än vilket titel individen må ha. Samtidigt ger svaren också en tydlig indikation på om huruvida personen verkligen har relevant kunskap för att kunna leda forskningsfrågorna vidare och styrka eller avfärda gällande teorier på området. Individerna som intervjuats har jag kommit i kontakt med genom att dels se till vilka nyckelpersoner som nämns i litteraturen, dels genom att söka mig till individer som har många kontakter i hacktivist- och nätaktivistkretsar via sociala nätverk som till exempel Twitter. Det gör ett tämligen subjektivt och kanske inte fullständigt representativt urval av människor, men med rätt kontakter går det att täcka in en stor del av den hacktivistiska sfären.

Bland de som intervjuats har vissa valt att vara anonyma eller gå under pseudonym. Det finns olika anledningar till dessa val. I vissa fall handlar det om att individen håller på med sådan verksamhet att om identiteten röjs kan det förekomma hot mot personen från motståndare, dels finns det möjlighet för polisiära åtgärder. I vissa fall kan det handla om att personen vill hålla sin nätidentitet skild från livet utanför nätet och att personen därmed anger falskt namn i vissa kretsar. Självklart måste jag respektera personernas val, och bör därmed i så stor utsträckning som möjligt undvika att ge ut sådan information som kan röja individerna.

2.4 Materialets tillförlitlighet och omfattning

Det finns ingen direkt anledning att misstro det litterära materialet för arbetet, det finns dock två stora begränsningar som måste tas hänsyn till när man här resonerar kring detta. Den första är att majoriteten av litteraturen som har att göra med hacktivism kommer från runt år 2000, de två senaste böckerna är från 2002 och 2004. Som jag tidigare nämnt bygger forskningen på en induktiv metod där man behöver många observationer för att kunna göra generaliseringar som är relevanta. Att det inte finns någon litteratur som täcker ett gap på i det närmaste åtta år av nätaktivism (boken från 2004 har sina senaste exempel från ca 2002) är en avsevärd brist. Visserligen är målet med arbetet att utveckla existerande teori just på grund av denna brist, men samtidigt skapar det problem då det är svårt att luta sig på en stabil teoretisk grund.

Ett annat problem är bristen på källor när det gäller ”digitalt korrekt hacktivism”. Eftersom begreppet i stort verkar vara outforskat måste beskrivningar och teori bygga på intervjuerna och den smala litteratur som faktiskt finns, i praktiken två böcker av författaren Tim Jordan (2002 & med Paul A. Taylor 2004) där begreppet nämns. Det innebär alltså att all akademisk information om ”digitalt korrekt hacktivism” som jag kan basera uppsatsen på kommer från en källa. Självklart är detta något som skulle kunna generera kritik mot upplägget för uppsatsen, men samtidigt finns det inte några alternativ. Det måste exemplifieras i större utsträckning, och för varje nytt exempel kan teorierna stärkas. Således är bristen på material inget som underminerar uppsatsen utan snarare något som gör den än mer värdefull i både ett inom- och ett utomvetenskapligt perspektiv. Dock ska man vara medveten om att detta är en kandidatuppsats och som sådan är upptagningen begränsad. För att göra forskningen rätta och verkligen försöka att täcka igen luckor i tidigare forskning krävs en avsevärt mycket större uppsats och arbetsinsats.

2.5 Terminologi

DoS – *”Denial of Service”* – En attack mot ett nätverk, en server eller hemsidor som har som syfte att hindra åtkomsten till målet. Detta kan göras på många olika sätt. Det finns i huvudsak två övergripande kategorier, CDoS (C för Centralized) och DDoS (D för Distributed).

DDoS – ”*Distributed Denial of Service”* – En DoS-attack där många olika datorer samordnas för slå ut ett mål. Kräver oftast någon sorts aktiv handling från individen som äger en dator, till skillnad från CDoS där en enskild dator tar över många olika datorer med hjälp av virus för att attackera sina mål.

Tor – *Anonymiseringsnätverk* – En mjukvara som är till för att dölja användarens trafik och identitet från övervakningsförsök och trafikanalys. Man brukar illustrera Tor som virtuella tunnlar.

Proxyservrar – Servrar som agerar som mellanhänder när någon söker information eller liknande. Finns flera olika varianter, men den vanligaste är web proxys som används för att anonymisera internettrafik. Fungerar som en digital version av en langningskedja, där man skickar allt material via mellanhänder innan informationen når slutdestinationen, som i sin tur inte vet varifrån förfrågan kom ursprungligen, d.v.s anonymisering.

cDc – Cult of the Dead Cow – Ett av de äldsta hackernätverken, bildades redan 1984. Medlemmar i nätverket myntade begreppet hacktivism 1996, och har under sin existens varit väldigt viktiga dels för hacktivism världen över, smat den ideologiska debatten kring vad hacktivism borde vara.

Svärm – löst sammansatt gruppering – Många större hacktivistgrupper fungerar som svärmar. Det finns generellt sett ingen som styr individerna, men när ett gemensamt mål har etablerats arbetar alla tillsammans för att uppnå målet. Är också en bra liknelse då svärmar kan anses vara oförutsägbara för blott ögat i sitt beteende.

3 Hacktivismens begreppsliga bakgrund.

För att kunna definiera digitalt korrekt hacktivism och beskriva det i rätt kontext krävs det att jag redovisar den etablerade betydelsen av hacktivism i stort. Som jag tidigare påstått så har den relativt gamla versionen av begreppet fortfarande relevans och eftersom jag i större uträckning vill distansera ”digitalt korrekt hacktivism” från hacktivism i övrigt kräver det en längre redogörelse av begreppet.

Termen ”Hacktivist” skapades 1996 av Omega, en medlem i hackernätverket Cult of the Dead Cow (Ruffin 2010a). Därmed är det svårt att få något grepp om litteratur och forskning i ämnet före 1998. Likväl har det existerat som fenomen sedan sluten av 80-talet, och hacking generellt har sedan dess varit ett ord som dyker upp i media med jämna mellanrum. För företag och organisationer är hacking självfallet ett problem, skulle ens organisation vara involverad i något som kan anses kontroversiellt eller fel av någon part som besitter teknisk kompetens så kan man mycket väl bli utsatt för någon sorts hackerattack. Hacktivisterna är hackers med en politisk agenda, om man ska hårddra karakteriseringen något. Men den politiska agenda som driver hackers är inte alltid helt självklar. I vissa fall, som vi kommer se senare, finns uttalade policys från grupperingar, i andra fall är det enskilda individer som tar över ovetande människors datorer för att utföra attacker mot mål som individen inte tycker om. Och mellan de två punkterna finns en oerhörd variation ”politik” som hacktivister kan driva och det kommer att förtydligas i respektive del, vad för politik man ämnar föra.

Det finns ytterligare djup i begreppet ”hacktivism” som ofta verkar bli förbisett i litteraturen jag har gått igenom, över lag är väldigt få kritiska till användandet av ”hacktivism” som generellt begrepp för allt som har att göra med aktivism på nätet. Hacking kommer från ”hack” vilket innebär att man använder existerande teknologi på nya sätt. Tim Jordan ger ett klassiskt exempel: Du vill ha en kopp te men har ingen te-kokare, istället använder du kaffekokaren för att koka ditt tevatten. Användandet av kaffekokaren i detta sammanhanget är ett ”hack”. Hacking är alltså innovativ användning av tekniker. Det har dock blivit synonymt med att bryta sig in i datorer och förstöra hemsidor, något som bland tekniker brukar kallas ”cracking” istället (Jordan 2002:120).

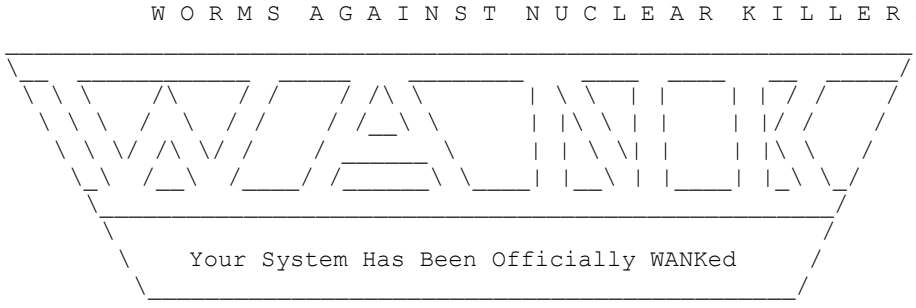
Det är min första definition, i hacktivism vill jag sammankoppla hacking och aktivism, alltså politiskt motiverad hacking. Cracking däremot, är inte en del av begreppet hacktivism då syftet med cracking eller cracktivism är att förstöra eller avbryta digital verksamhet. Det finns hacktivister som också sysslar med sabotage, så kallade mass action hacktivism, men det handlar då bara om att

tillfälligt avbryta kommunikation och anslutningar. Tar man det steget längre, att förstöra hemsidor och information, kan det inte längre anses vara hacktivism. Det jag tänkte visa i följande kapitel är hur begreppet hacktivism har utvecklats, så att jag senare kan ta fasta på historien när jag redovisar och problematisera digitalt korrekt hacktivism.

3.1 Hacktivismens grunder

”I know from personal experience that there is a difference between street and online protest. I have been chased down the street by a baton-wielding police office on horseback. Believe me, it takes a lot less courage to sit in front of a computer.” (Oxblood Ruffin citerad i Jordan, Taylor 2004:80)

Den tidigaste registrerade hacktivistiska aktionen skedde i oktober 1989 på datorer som ingick i NASAs och Department of Energy i USAs system blev infekterade av en internetmask, ett självkopierande virus, som visade följande meddelande på datorskärmen.



Det var ett aktivt politiskt budskap om att göra allvar av nedrustningsmålen och masken har spårats tillbaka till Australien. (Assange 2006)

Där börjar alltså historien om hacktivismen, före begreppet ens uppfunnits. Tim Jordan och Paul Taylor (2004) menar att hacktivismen som koncept egentligen inte skapades förrän i mitten av nittiotalet som en fusion av hackerfenomenet, den digitala informationssamhället och det Jordan kallar ”popular protest”, alltså allmänna protester. Jordan klassificerar hacktivismen som ”online direct action”, konkreta protesthandlingar överförda på en digital arena (Jordan, Taylor 2004:67). På detta sätt visar han att hacktivism är ett unikt fenomen som inte liknar något annat, men samtidigt är det påverkat av olika trender och fenomen runt om i världen. Med ”direct action” drar Jordan parallellerna till icke våldsamma protester vi kan se runt om i världen, sittstrejker, bojkotter, blockader och civil olydnad. Med andra ord verktyg som används för att konkret och direkt påverka samhället. Just den civila olydnaden är ett exempel som varit populärt att ta upp tidigare (Manion & Goodrum 2000:15), men det är inte det ickevåldsamma som är inspirationen för hacktivismen, utan det är snarare

den konkreta handlingen för att göra skillnad, inte minst för att 'våld' får absurda meningar om man talar om internet och digitala protester. (Jordan, Taylor 2004:68) Vidare delas begreppet hacktivism upp i två större grupperingar nämligen ”mass action hacktivism”, den traditionella hacktivismen som vi ska förklara nedan, och ”digitally correct hacktivism”, fokuset på denna uppsats som jag återkommer till senare.

Efter detta finns ett antal populära nedslag att göra i historien som går igen i nästan på samtliga böcker om ämnet. De viktigaste nedslagen som kan göras i sammanhanget är nätaktivismen kring Zapatistasrörelsen i Mexico. Zapatistas är en motståndsrörelse i Mexico som kämpar för indianernas rättigheter och även för att regionen Chiapas ska bli en autonom region (Ronfeldt and Arquilla 2001:172f). Under mitten av nittiotalet var de oerhört aktiva på nätet och blev snart uppmärksammade av en hackergrupp vid namn Electronic Disturbance Theatre (EDT) som började hjälpa Zapatisterna via direktaktioner på nätet. EDT skapade Floodnet, en mjukvara som genom att ständigt uppdatera en enskild hemsida från många datorer samtidigt, kunde sakta ner trafiken avsevärt och ibland till och med ta ner hemsidorna helt från nätet. Samtidigt ändrade Floodnet felmeddelandet på hemsidan så att om man försökte ansluta till mexikanska presidentens hemsida under en attack kunde man få meddelandet ”No democracy found on this server” istället för vanliga felmeddelande. (Jordan 2002: 120f)

3.2 En internationell säkerhetsfråga

Staters säkerhetstjänster har därmed av förklarliga skäl varit oroliga för hacktivism, främst i bemärkelsen mass action hacktivism, då all sorts militära interventioner riskerar att möta motstånd från civilbefolkning och andra, att nyttja datorer för detta motstånd sågs runt år 2000 som en reell risk i framtiden. Det är i detta scenario som antologin *Networks and Netwars* av John Arquilla och David Ronfeldt(2001) tar sin utgångspunkt. Att utvecklingen av hackers och den allt mer nätberoende världen kommer göra att framtidens krig riskerar att få en ny och oroväckande digital vinkling.

Det ska dock sägas att den inte enbart ser all hacking som brottslighet, i vissa artiklar, till exempel av Dorothy E. Denning görs en distinktion mellan vanlig aktivism på nätet, hacktivism och cyberterrorism. Aktivism är här icke hindrande användande av nätet för att uppnå någon sorts mål. Hacktivism ses som lätta ingrepp datorsystem och hemsidor, att skicka mass e-mail, skapa virus och att dämma upp trafik till särskilda webbsidor, utan att tillfoga verklig skada. Cyberterrorism är när man använder digitala medel för att uppnå politiska mål, det kan röra sig om att riskera liv eller orsaka allvarlig ekonomisk skada.(Denning 2001:241).

Denning använder kriget i Kosovo som exempel för att illustrera hur man kan använda nätet vid krig. Båda sidor använde nätet som ett verktyg för att sprida både information och desinformation för att påverka motståndarsidans opinion. Spam, DoS-attacker, virtuella sittstrejker och manipulerade hemsidor användes

flitigt under konflikten av myndigheter, privatpersoner, icke statliga organisationer och andra intressenter. Men exemplen är fler än bara Kosovo. Zapatisterna i Mexico, Cult of the Dead Cow och Legion of the Underground är andra organisationer som har använt hacking för att få fram sina politiska åsikter, vilket då gör dem till hacktivister.

I hela *Networks and Netwars* är temat att hacking och cyberkrig mycket väl kan komma att utvecklas i framtiden och få verkliga konsekvenser för medborgare och organisationer. Tyvärr är attacker på nätet något som man inte kan veta omfattningen av: Där väpnade konflikter är ganska tydliga, är nätattacker osynliga för de flesta utom de drabbade. Spekulationerna i boken ger till viss del intrycket av att cyberkrigföring redan existerar som fenomen, men kanske inte i någon fullt utvecklad skala, då gränsdragningen till de andra kategorierna av digital aktivism är så vaga. Till exempel har hackers som stödjer al-Aqsa intifadan DoS-attackerat israeliska statliga och kommersiella mål, och Israel har i sin tur återgäldat attackerna med att DoS:a runt 15 olika palestinska mål, inklusive Hizbollah, Hamas och Palestinian National Authority (Zanaini & Edwards 2001:48f). Och trots att det har eskalerat på sina håll har liknande attacker inte använts i så pass stor skala att tredje part blir påverkad eller att man har kunnat tala om ett nätkrig.

Men samtidigt som jag skriver denna text så pågår faktiskt något som internetaktivister kallar ”det första infokriget” i svallvågorna av Wikileaks publicering av en stor mängd amerikansk diplomatkorrespondens. Tidigt efter publiceringen togs Wikileaks hemsida ner av Amazon.com efter påtryckningar från den amerikanska administration. Därefter började olika aktivister sätta upp speglar så att man kunde komma in på Wikileaks med andra domännamn. Kort därefter stängde PayPal (som förmedlar ekonomiska transaktioner på nätet) ned alla transaktioner till Wikileaks, varpå en ökänd hackinggrupp kallad Anonymous riktade en stor DoS-attack mot PayPal som tidvis gick ner helt. Även stora kreditkortsbolag som Mastercard och Visa har stängt ner transaktioner till Wikileaks av, i skrivande stund, oklara anledningar. Under tiden har flera av organisationerna som satt upp egna Wikileaksspeglar råkat ut för DoS-attacker från okända aktörer bland annat har politiska partier som uttryckt stöd för Wikileaks fått se sina hemsidor och administrativa system inkapaciterade. På den ena sidan i konflikten finns otaliga individer som stödjer Wikileaks, på andra sidan finns en okänd aktör som gör allt i sin makt för att stänga ner Wikileaks verksamhet på nätet.

Det är en utveckling som trasade sönder de tidiga funderingarna jag hade om den här uppsatsen. Jag ville visa på hur själva begreppet hacktivism har förändrats mot en mer solidarisk, humanitär och informationsfrihetlig inriktning. Istället märker jag tydligare än vad man kunnat se tidigare, hur begreppet verkligen är tudelat och att skillnaderna mellan ”mass action hacktivism” och ”digitally correct hacktivism” är värdefulla att studera och redovisa i en studie som denna. För att kunna göra denna distinktion tydligare kommer jag att ta upp ett sentida exempel och även försöka karakterisera några av de grupperingar som har varit involverade och tongivande i de senaste årens nätdrivna protester och aktioner. Därefter kommer jag att ge en utförligare beskrivning av den digitalt korrekta hacktivismen utifrån mitt exempel och tidigare litteratur.

4 Iran

”Denial of Service attacks are a violation of the First Amendment and of the freedoms of expression and assembly. No rationale, even in the service of the highest ideals, make them anything other than what they are – illegal, unethical and uncivil” (Cult of the Dead Cow i Jordan, Taylor 2004:98)

Valet i Iran ägde rum den 12:e juni 2009. De två huvudkandidaterna var den sittande presidenten Mahmoud Ahmadinejhad och oppositionens ledare Mir-Hossein Mousavi och utgången i valet följdes av intresserade ögon världen över. På morgonen den 13:e juni meddelades det att Ahmadinejad hade vunnit en jordskredsseger med 62,46% mot Mousavis 33,87%. Arga och besvikna Mousavianhängare började protestera på gatorna och anklagade Ahmadinehad för valfusk.

Redan den 14:e rapporterade en journalist från *The Telegraph* att iranska regimen gjorde allt i sin förmåga för att försöka strypa flödet av nyheter från Iran till omvärlden. (Blair 2009) Eftersom Iran är ett land med tämligen hög grad av internetanvändning och framför allt en mycket aktiv bloggosfär och twittersfär så blev nätet en naturlig väg för medborgare att sprida information om vad som hände på gatorna i Teheran och resten av Iran, samt samordna varandra. Detta i sin tur gjorde att regimen försökte strypa åtkomsten till nätet genom att sänka mängden trafik som kunde gå genom kablarna. Detta, tillsammans med en stor aktivitet gjorde att nätet knappt gick att använda.

När olika nätaktivistgrupper insåg vad som hände i Iran var deras första reaktion att försöka skada den iranska regimen på samma sätt som man skadar andra som försöker hindra åtkomsten till internet. Den normala reaktionen från nätaktivistgrupper när någon försöker ge sig på internet, är att sabotera statens/organisationens/företagets åtkomst till nätet genom att överbelasta deras servrar och hemsidor med DDoS-attacker, ändra innehåll på hemsidor eller ta sig in i nätverken och förstöra information där (hacking). Detta var vad hackers började göra även vid detta tillfälle för att försöka förstöra för regimen, och enligt vissa källor lyckades de även i stor utsträckning. Enligt Josh Shahryar (2010), journalist och människorättsaktivist, gick delar av attackerna ut på att störa interna kommunikationen inom iranska myndigheter och även kommunikationen mellan myndigheterna för att hindra dem att samordna arresteringar av demonstranter. Detta ska ha räddat livet på ett flertal demonstranter som var ute på gatorna utan maskering. Mycket av den DDoS:ing som uträttades gjorde att det iranska nätet helt och hållet fylldes upp av överbelastningsattacker och att ingen legitim trafik kunde ansluta och sprida livsnödvändig information till meddemonstranter och omvärlden.

4.1 Aktivismen på nätet

Den 16:e juni publicerades dock en guide för hur aktivisterna kunde sätta upp Tor-noder och proxyservrar för att hjälpa aktivisterna i Iran att få tillgång till nätet. Anledningarna som angavs var att det redan överbelastade iranska nätet inte skulle klara av en attack från hackersvärmar utan att kollapsa helt och på så sätt förstöra för de iranska demonstranterna. Med Tor-noder och proxyservrar kunde man istället sätta upp vägar kring det överbelastade nätet genom att individer i Iran kunde ansluta genom datorer i andra länder. I de största och mest aktiva hackersvärmarna började man nu propagera för att aktivisterna skulle sätta upp Tor-noder och proxyservrar, och de fick stort gehör i hacktivistkretsar. (Anonym 2010)

Det blev en kamp mellan regimen och hacktivisterna över vem som skulle kunna få tillgång till nätet. Enligt Lissnup (2010), en person som agerar som aktivistnav på Twitter, bloggar och liknande, blockerade regimen tillgången till ungefär 5 miljoner olika URL:er. Av de tre stora näthubbarna i Iran stängdes en ner permanent och mängden trafik i de andra två begränsades avsevärt, samtidigt som övervakning av all trafik därigenom implementerades. Enligt en anonym källa blockerades de största siterna, Facebook, Twitter och Youtube, samtidigt som Tor-projektets hemsida och flera hemsidor med ordet”proxy” blockerades för att hindra aktivisterna i Iran att upprätta kontakter utanför Iran. På grund av detta började grupper som WhyWeProtest och Telecomix sätta upp speglar av Tor-projektets hemsida förutom att de satte upp noder och proxyservrar själva, allt för att se till att människor i Iran fick tillgång till information utanför gränserna, och kunde sprida information från insidan. Josh Shahryar var en av dem som tog emot information från Iran och sedan spred den vidare till intresserade personer. Han beskriver i fyra, tämligen simplistiska, steg hur informationen spreds;

1. Vanliga personer bevittnar en händelse och berättar för bekanta
2. Någon med mycket sådan information sprider det till andra aktivister inom Iran via telefon
3. Aktivisterna för vidare informationen via kanaler på nätet till aktivister utanför Iran
4. Aktivister utanför Iran sprider informationen vidare. (Josh Shahryar 2010)

Den största censureringen skedde mellan tredje och fjärde steget. Och det var också här Tor-noder och proxyservrarna gjorde nytta. Visserligen går det inte att säga exakt hur mycket de hjälpte eftersom att viss information gick genom andra kanaler, men Shahryar påstår att ungefär hälften av all information som kom ut ur Iran sommaren 2009 skickades genom de kanaler som hacktivisterna satt upp. Det viktigaste var dock inte vilken kanal som användes menar Shahryar, istället var det att aktivisterna direkt kunde se att informationen de skickade ut blev

publicerad och togs om hand. ”As you know, all opposition websites are inaccessible in Iran. So when activists send data abroad, they cannot access websites with normal internet to see if their work as made an impact. However, with Tor and other devices, people were able to instantly see their contribution, the responses to it and the support generated by it, giving them more courage and determinism to continue sending information out” (Josh Shahryar 2010)

4.2 Hacktivisternas bakslag

Viss DDoS-ning fortgick, även efter att WhyWeProtest hade börjat uppmana till andra sorts aktioner, riktad mot Iranska myndigheter för att fortsätta störa dem i deras försök att arrestera demonstranter. Varför stoppades inte dessa attacker samtidigt som de andra? Här måste vi ge oss in på ett kort sidospår om olika sätt att utföra DDoS-attacker. Standardprogram att använda för DDoS-attacker är, åtminstone för aktivistgruppen Anonymous som jag förklarar mer om senare, mjukvara som LOIC (Low Orbit Ion Cannon) eller Bwraep. LOIC, den mjukvara som används i de aktioner som kretsar kring konflikten om Wikileaks, överbelastar både nätverksutrustning och bandbredd genom att skicka en enorm mängd trafik till en enskild hemsida eller server, det fungerar i princip som att man skulle gå in på en hemsida och trycka på ”uppdatera” konstant, om tillräckligt många datorer riktar sina LOIC mot samma sida kommer den slutligen gå så långsamt att den går ner. Bwraep laddar istället ner stora paket information från en hemsida och överbelastar på så vis också nätverk och blockerar bandbredden. När man ville hålla nätet i Iran så öppet som möjligt kunde man inte använda de ganska så buffliga och kraftfulla metoderna, utan var istället tvungna att ha riktade attacker mot enskilda servrar och datorer utan att överbelasta nätverket. Den 17:e juni 2009 lanserades SlowLoris som är en mer kirurgisk DDoS-mjukvara. Här gör man istället så att SlowLoris börjar fråga efter information från en server, men avslutar inte frågan, utan håller istället uppe en kanal till servern utan att någon information passerar igenom just den kanalen. Genom att göra flera förfrågningar från många olika datorer kan man till slut ockupera samtliga anslutningar till servern, och därmed effektivt hindra någon annan från att ansluta. På så vis kunde man attackera iranska staten samtidigt som man hjälpte iranska medborgare att kommunicera via Tor-noderna och proxyservrarna. (Intervjuer med Josh Shahryar och Anonym 2010)

Tack vare att demonstrationerna i Iran dominerade nyhetsflödet i media blev stödet på sociala medier för den gröna vågen i Iran massivt. Detta, hävdar Lissnup, var en självklar faktor för varför så många Tor-noder och proxyservrar sattes upp (Intervju med Lissnup). Anonym påpekar att sommaren 2009 var första gången man så tydligt kunde se hur en regim förtryckte dissidenter samtidigt som det hände. I andra fall tenderar man enbart att få reda på förtryck i efterhand (Anonym 2010). Detta, tillsammans med starka bilder och videor som när iranska Neda blir skjuten och dödad, skapade en enorm våg av sympati och aktivism för demonstranterna i Iran.

Men den 25:e juni uppvisade internet en gång för alla bevis för den oerhörda nyckfullhet som finns bland de mindre aktiva nätaktivisterna och allmänhetens sensationsbegär. Aktivismen kring Iran avtog kraftigt när nyheten om Michael Jacksons död började sprida sig. ”Det nya heta” var inte längre i Iran och en stor del av de som drev på informationsflödet via sociala nätverk försvann, statusrader på Twitter och Facebook handlade i större utsträckning om vilken låt med Michael Jackson man fick flest nostalgitrippar av, än om några demonstranter i Teheran hade fängslats eller dödats. De som faktiskt fortsatte sin aktivism var de mer dedikerade hacktivistnätverken. På många håll finns det fortfarande TOR-noder uppe som hjälper personer i Iran, liksom proxyservrar och andra tekniska hjälpmedel som utvecklats efter hand. För att lättare kunna förstå den digitalt korrekta hacktivism som fortsatt efter att uppmärksamheten kring Iran dött ut medialt och socialt, men även under den, krävs det en introduktion till dessa hackernätverk.

5 Hackernätverken

5.1 Anonymous / WWP

Ett av de absolut mest ökända hackersvärmarna i världen är Anonymous. En ganska sen efterlöpare till sammanslutningar så som Cult of the Dead Cow och liknande, har Anonymous (eller Anon) gjort sig kända för sitt passionerade motstånd mot Scientologikyrkan och på senare tid ett ihärdigt förfäktande av ett fritt internet, där alla företag och stater som försöker begränsa information får Anon emot sig. ”Many are teenagers, male and besides being fueled by their hormone induced anger, [they] lack life experience and reflection. (Anonym 2010). Ett exempel på detta är när Australiens parlament förbjöd all pornografi som avbildade kvinnor med små bröst eller kvinnliga ejakulationer så DDoS:ade Anonymous Australiens statliga servrar. Detta fick till följd att statligt anställda samt privatpersoner inte kunde komma åt information som låg på statliga servrar under nästan ett helt dygn. Vidare sände aktivisterna i Anonymous mängder med fax- och emailspam innehållande bilder på kvinnor med små bröst till parlamentsledamöter för att de skulle häva beslutet som Anon ansåg begränsade möjligheten till fri information på nätet.

Det kan tyckas vara ett barnsligt svar på ett beslut som föranletts av domslut där det har varit svårt att urskilja om bilder på unga kvinnor ska klassas som barnpornografi eller inte, och det är ett beteende som går igen i flera av de nätverk som sysslar med hacktivism av denna sort. En källa med god insyn och flera års aktivitet kring Anonymous bekräftar vad det är som driver personerna i liknande nätverk, och varför de inte tvekar till att ta ner något så viktigt som ett lands datorsystem bara för att informationsfriheten har begränsats minimalt jämfört med tidigare.

Svärmar som Anonymous är inte organiserade, de har inga ledare och det finns ingen enskild person att hålla ansvarig för deras verksamhet. De brukar liknas vid en svärm, där det är frivilligt att delta och att lämna om man så önskar. Däremot finns det mer organiserade grupper i anslutning till Anon som har en tydligare agenda och framför allt ett tydligare sätt att agera. En av dessa, och den troligtvis viktigaste i protesterna mot Scientologikyrkan och operationerna kring Iran, är WhyWeProtest, eller WWP. I ett pressmeddelande som skickades ut med anledning av protesterna kring Wikileaks i december 2010 för klarade man att ”WhyWeProtest supports reform, not coercion. We take no position regarding the actions of others, however we explicitly do not promote or endorse strategies such as the Anonymous Denial of Service attacks. Instead, we serve as a thinktank and conduit for legal alternatives” (Anonym 2010). WWP försöker alltså med lagliga medel att förändra samhället. De är fortfarande hacktivister i den bemärkelsen att

de använder nätet och sådan teknik som jag talat om tidigare för att driva sin politik, men de har tagit avstånd från all destruktiv och olaglig hacktivism och är därmed att se som digitalt korrekta hacktivister.

Precis som andra digitalt korrekta hacktivister är det informationsfriheten som är WWPs högsta mål, inte att straffa de som bråkar med nätet: ”Our over-arching mission is to ensure and promote the right of any person to speak and act freely and conscientiously.” (Anonym 2010). Under, den i skrivande stund pågående, kampanjen kring Iran använde WWP inte bara tekniska hjälpmedel för att se till att iranska medborgare kunde komma åt information, de etablerade också kontakter i Iran för att kunna få in och ut information på regelbunden basis som andra inte hade eller kunde få tillgång till. På så vis blev WWP inte bara en aktivistgrupp som hjälpe medborgarna, utan blev också en kanal för information att flöda ut ur, och in i, Iran.

5.2 Telecomix / HWB

Samma gäller en aktivistgrupp vid namn Telecomix. Denna grupp startade när debatten kring telekompaketet gick het i EU, och nätaktivister sökte ett sätt att samordna sina krafter för att hindra paketet, som fortfarande är kontroversiellt, att bli lagstiftning i unionen. Under aktionerna kring Iran var de också aktiva med att sätta upp TOR-noder och proxyservrar samt distribuera information och samordna hacktivister.

Ett av initiativen de startade ger under namnet Hackers Without Borders, eller HWB, en hacktivistvariant av *Médecins sans frontières (*Läkare utan gränser). Ett samarbetsorgan tänkt att samordna aktivister kring Iran. En av Telecomix administratörer, Jaywalk, berättar att ”målet var väldigt brett, det var mer en gemensam vilja om att hjälpa alla som av en eller annan anledning hade skadade kommunkationsmöjligheter (sic), så långt som det går” (Intervju med Jaywalk) På frågan om projektet uppnått de mål man satte upp svarade Jaywalk ”det var mycket ideer (sic) som byttes, och jag tycker att det var mycket lyckat.:) det är dock svårt att se definitiva produkter, det var mer av ett utbyte som förhoppningsvis hjälpte alla” (Intervju med Jaywalk)

På hemsidan för HWB står några av målen, först och främst bör märkas att de anser kommunikation vara en mänsklig rättighet och att man alltid tar sida i konflikter och värnar enbart om att individer ska få tillgång till kommunikation. Och framför allt skriver de att HWB aldrig ska förstöra kommunikation för något, till exempel genom att DDoSa servrar. De lägger stor emfas på att DDoS av servrar i Iran skadar medborgarna i Iran mycket mer än vad det skadar staten. Av hemsidan märker man också att hacktivistgrupperna inte är själva på arenan, de stöter hela tiden på motstånd från, i detta fallet, iranska staten som ständigt skickar ut desinformation och försöker stänga ner användarkonto som tillhör iranska aktivister på populära webbsidor som Twitter och Facebook. Som jag skriver ovan så försökte de också blockera hemsidor om Tor-servrar och som nämnde proxyservrar, och i dessa fallen kunde hacktivisterna sätta upp speglade

sidor så att de fortfarande gick att komma åt. Detta gick inte att göra med Twitter och Facebook, vilket gjorde det än viktigare att de iranska näten var fria från DDoS attacker så att de som fortfarande hade möjlighet att kommunicera kunde göra det..

6 Digitalt korrekt hacktivism.

”They were asserting a different set of human rights; not rights *for* networked computers but the right *of* humans to free flows of information; not of conferring rights on inanimate objects but on what those objects offer humans.” (Jordan, Taylor 2004:91)

6.1 Hacktivismens samvete

WWPs och HWBs verksamhet visar alltså på en utveckling och förändring i hacktivismen. Det är en utveckling som gör begreppet mer diversifierat och som ligger i linje med den stora spridning det finns i vanlig politisk aktivism där man kan tala om allt från att skriva på protestlistor till att begå våldsamma handlingar som hotar människors liv och lem. På samma sätt som i den fysiska världen så finns det online de som försöker få fram sina politiska mål genom att attackera företag eller stater. Och så finns det de som istället arbetar till fördel för medborgarna i stater som begränsar informationen och försöker hjälpa människor att kommunicera. Det kan tyckas att jag lägger värderingar i dessa båda företeelser, men båda har sina syften och kan användas för att nå politiska mål. Detta såg vi inte minst i de riktade SlowLoris-attackerna mot iranska staten. Skulle det vara så att dessa uppgifter verkligen är samma så användes troligen DDoS för att rädda liv, medan de andra verktygen ”enbart” hjälper individer att kommunicera.

Så vad är den digitalt korrekta hacktivismen, vad är det som gör detta fenomenet så värdefullt att utreda och förklara ur en statsvetenskaplig synvinkel. För mig personligen så handlar det om man kan se ett trendbrott från vad den anonyma källan kallade de ”hormonstinna” tonåringarna och unga männen som samlas i hacktivistgrupperna för att göra det de gör bäst. Den främsta forskaren på området ”digitalt korrekt hacktivism”, och en av väldigt få som skrivit om hacktivism över huvud taget sedan 2000, är Tim Jordan. I *Activism! - Direct Action, Hacktivism and the Future of Society* och *Hacktivism and Cyberwars - Rebels with a Cause*, skriven tillsammans med Paul A. Taylor, använder han begreppet för att särskilja de hacktivistaktioner där tidigare schabloner med förstörande, störande och i allmänhet ganska oberäknelig aktivism istället blev medveten, byggde på en vilja att låta all information vara fri samt att kringgå spärrar så att människor i utsatta situationer och i länder utan fri tillgång till nätet, också kunde njuta av informationsfrihet. Stefan Wray (1998) menar att detta ”can be said to be a digitally correct position” och med det blev han också den som först använde ”digitalt korrekt” för att beskriva den nya utvecklingen.

Grunden för den politiskt korrekta hacktivismen är synen på information och kommunikationen som mänskliga rättigheter. Från att Stefan Wray och hans dåvarande kollega Ricardo Dominguez blev närmade av hacktivister på en Ars Electronica konferens i Österrike 1998 – som påpekade att vad de och Zapatisterna gjorde var ett oacceptabelt sätt att använda nätverken, som mail-spam, om inte värre (Jordan, Taylor 2004:91) – till WWPs och andras arbete för att värna informationsfriheten i Iran och i andra delar av världen. Det är fundamentalt för förståelsen av dessa rörelser att det är rätten till information, rätten till internet, som är motivationen bakom alla aktioner som klassificeras som digitalt korrekta. Det handlar inte om en motståndsrörelse mot regimen i Iran, så som Zapatisterna aktivt motarbetade den mexikanska staten. Det är en aktivism som har en mottagare, inte ett offer, och den bygger alltid på samma grundläggande ideal.

6.2 Ett ”korrekt” kräver ett ”felaktigt”

Men detta grundläggande ideal är inte utan problem. HWB hävdade själva att de aldrig tar någons sida i en konflikt, de förhåller sig neutrala till konflikten. Det finns dock fler konfliktlinjer än vad hacktivisterna i HWB och WWP verkar vilja se. Hacktivisterna står på barrikaderna i en konflikt som de i mångt och mycket kan anses konstruera själva. Det är konflikten mellan det fria och oreglerade nätet och staters samt företags vilja att reglera eller i viss mån strukturera nätet för medborgarnas bästa eller vinstintressen. Konflikten mellan det digitala och det politiska. Att värna det digitala är dock inte okontroversiellt, precis som att värna ”det politiska” kan skapa stor kontrovers så går åsikter isär på både politiska och digitala arenor. Det innebär också att det ”digitalt korrekta” inte är korrekt för alla utan bygger på vissa värderingar som vi har talat om här ovan. Det måste man bära med sig när man talar om ”digitalt korrekt hacktivism”, att det enbart är korrekt enligt somliga moraliska referensramar. Vissa forskare menar till exempel att de som är extremt tekniskt kunniga och kompetenta programerare fördjupar sig så pass mycket i kod och programmering att de höjer kodens, alltså det digitalas, ideal över andra ideal i samhället. (Taylor 2005:631)

Begreppet är kontroversiellt på fler sätt. Vissa hacktivister anser att det jag och tidigare författare benämner som ”digitalt korrekt hacktivism” egentligen är vad hacktivismen borde vara, att tekniker som SlowLoris, LOIC och liknande är en skymf mot andra hacktivister: ”These are essentially censorship technologies, so I don't consider them to be appropriate for anyone calling themselves a hacktivist. Hacktivism is all about using technology to improve human rights. And since access to information is a basic human right then shutting down someone's right to speak, even if it's offensive speech, is nothing that we'd endorse.” (Oxblood Ruffin 2010).

Oxblood hänvisar till artikel 19 i FN:s deklaration om de mänskliga rättigheterna när han säger att tillgång till information är en mänsklig rättighet; ”Var och en har rätt till åsiktsfrihet och yttrandefrihet. Denna rätt innefattar frihet

att utan ingripande hysa åsikter samt söka, ta emot och sprida information och idéer med hjälp av alla uttrycksmedel och oberoende av gränser”. Oxblood var mottagaren av det mail från Omega, där den senare myntade begreppet Hacktvisim, och kan således anses vara något av en auktoritet på området. Han har sedan slutet av 80-talet varit talesperson för Cult of the Dead Cow, ett av de första hackernätverken. Oxblood anser att, med grund i det tidigare påståendet, företeelser som DoS och annan förstörande hacktivism istället borde kallas ”social netwar”. Många utger sig enligt Oxblood att vara hacktivister trots att de inte följer vad Culd of the Dead Cow anser är rätt definition (Ruffin 2002)

Den digitalt korrekta hacktivismen är alltså också kontroversiell på sitt eget sätt. Det finns betänkligheter med det ”digitala”, det finns betänkligheter med det ”korrekta” och det finns betänkligheter med ”hacktivismen”. Likväl anser jag att de begreppsliga definitioner som Jordan gjort är en lämplig och väl motiverad indelning av en svåröverskådligt fenomen; ”Digitally correct hacktivism – is the political application of hacking to the infrastructure of cyberspace. It is an attempt to use the lack of physicality online life to amplify a political message. Digitally correct hacktivism flows within the structure of online life and uses its power.” (Jordan, Taylor 2004:69). Vad Jordan menar är att begreppet är politisk hacking, användande av existerande teknologi på ett nytt sätt, på nätet. Genom att utnyttja bristen på fysisk närvaro på nätet kan man förstärka politiska budskap. Detta till skillnad från ”mass action hacktivism” där man försöker trotsa bristen på fysisk närvaro genom att samla mängder med virtuella kroppar för att föra fram ett budskap. (Jordan, Taylor 2004:69)

7 Analys och slutsats

Politisk aktivism är den lilla människans röst mot den stora politiska makten. På nätet kan dock den lilla människan förstärka sin röst med tämligen små medel. Den politiska aktivismen på nätet kan ta många olika former, från digitala listinsamlingar till att bryta sig in i statliga nätverk. I detta arbete har begreppet hacktivism utvecklats, problematiserats, uppdelats och analyserats. Stora delar av begreppet finns beskrivet sen tidigare, men några delar som är av stor vikt för förståelsen av den politiska aktivismen online, saknas i stor utsträckning. Den digitalt korrekta hacktivismen är hacktivismens samvete. Det är aktivister som baserar sin agenda på deklarationen om de mänskliga rättigheterna. De försöker aldrig förstöra eller begränsa åtkomsten till internet för någon part, deras mål är att individer som är instängda bakom brandväggar ska få kommunicera fritt.

Jordan hävdar att skillnaden mellan hacktivismens två delar, mass action hacktivism och digitalt korrekt hacktivism inte handlar så mycket om absolut distinktion som var man väljer att lägga emfas, på hacking, protester eller informationssamhället (Jordan, Taylor 2004:68). På så vis kan Jordan ge en definition som inte ger några klara svar på frågan om vad digitalt korrekt hacktivism är för något. Jag skulle dock påstå att det finns större element av distinktion än vad Jordan hävdar. De hacktivister som sysslar med mass action hacktivism har inte samma inställning till politisk påverkan som de digitalt korrekta hacktivisterna har. När det gäller den första gruppen karakteriseras deras aktivism ofta som urskiljningslös då de attackerar mål som de för stunden anser vara fienden, ofta utan att ta hänsyn till de konsekvenser detta får andra nätanvändare. Deras lasrar, vad Anonymous brukar säga att de avfyrar när de inleder in attack, träffar diktaturer, onda företag och medier. Den digitalt korrekta hacktivisten styrs oftast av en agenda och en idealbild av hur världen bör se ut. De tenderar vara noggrannare när de väljer i vilka områden de ska engagera sig i. De riktar sig inte mot stater, inte mot onda företag, utan mot de som får sina informationsflöden strypta.

Men visst finns det överlappning. Det finns mass action hacktivister som kan göra stor nytta utan att förstöra åtkomsten till nätet, och den digitalt korrekta hacktivismen sätter ibland liv på spel då dissidenter som gör sin röst hörd kan bli upptäckta av regimer. Det digitalt korrekta kan vara lika kontroversiellt som mass aktionerna eftersom att det vissa anser vara ”korrekt” är olagligt eller moraliskt förkastligt i andra kulturer. Och det digitala kan ibland stå i motsättning till det politiska.

Jag har under arbetet med denna uppsats intervjuat flera oerhört intressanta och kompetenta människor med stor insyn i hacktivism och de nätaktioner som skedde kring Iran sommaren 2009 och läst igenom den litteratur som finns att tillgå i ämnet. Likväl slås jag av känslan att det inte går att säga något säkert om

mina forskningsfrågor i inledningen. En viktig anledning är att det under hela arbetets gång har förekommit exempel på både mass action hacktivism och digitalt korrekt hacktivism i medier och på nätet i övrigt. De grupper jag har skrivit om, Anonymous och Telecomix, har lanserat nya projekt och nya konfliktområden har blossat upp. I syftet angavs att uppsatsens mål var att bygga på den induktiva forsknings som tidigare gjorts för att kunna specificera begreppet ytterligare. Ju djupare man läser in sig i ämnet desto mer inser man hur mycket det finns kvar att skriva om, och med de fortgående exemplen av hacktivism som finns runt om i världen ser man att ämnet är högaktuellt.

Hacktivism är något som allmänheten vet otroligt lite om, och statsvetenskapen är i stor utsträckning lika ovetande. Men det är en sorts aktivism som redan har påverkat, upprört och engagerat på flera olika arenor. Och när nätet når än fler människor världen över och makthavare kommer att försöka styra nätet i vissa riktningar kommer hacktivismen att skapa nya rubriker och kontroverser. Med största sannolikhet kommer det både hyllas och fördömas. Men det kräver att statsvetenskapen och politiker kan se på fenomenet ur en både aktuell och underbyggd kontext. Detta är mitt bidrag för att öka förståelsen, den begreppsliga integriteten och intresset för hacktivism i allmänhet och digitalt korrekt hacktivism i synnerhet.

8 Referenser

Assange, Julian 2006. ”The Curious Origins of Political Hacktivism”, i *Counterpunch* Weekend Edition 25-26 november 2006. Hämtad online 2011-01-03. http://www.counterpunch.org/assange11252006.html

Blair, David, 2009. ”Iran Struggles to Censor News of Protests”, *The Telegraph* 2009-06-15. Hämtad online 2011-01-03. http://www.telegraph.co.uk/news/worldnews/middleeast/iran/5543145/Iran-struggles-to-censor-news-of-protests.html

Denning, Dorothy E, 2001. “Activism, Hacktivism, And Cyberterrorism: The Internet as a Tool for Influencing”, sid 239-288 i Arquilla, John – Ronfeldt David (red) *Networks and Netwars : The Future of Terror Crime, and Militancy*. USA : RAND.

Essiansson, Peter – Gilljam, Mikael – Oscarsson, Henrik – Wägnerud, Lena, 2007. *Metodpraktikan : Konsten att studera samhälle, individ och marknad*. Vällingby : Norstedts Juridik.

Jordan, Tim, 2002. *Activism! Direct Action, Hacktivism and the Future of Society*. London : Reaktion Books Ltd.

Jordan, Tim – Taylor, Paul A. 2004. *Hacktivism and Cyberwars : Rebels with a Cause*. London : Routledge.

Manion, Mark – Goodrum, Abby, 2000. “Terrorism or Civil Disobedience : Toward a Hacktivist Ethic” sid 14-19 i *Computers and Society* Juni 2000.

Ronfeldt, David – Arquilla, John, 2001. “Emergence and Influence of the Zapatista Social Netwar” sid 171-200 i Arquilla, John – Ronfeldt David (red) *Networks and Netwars : The Future of Terror Crime, and Militancy*. USA : RAND.

Ruffin, Oxblood, 2002. “Waging Peace on the Internet” i *The Register* 2002-04-19. Hämtad online 2011-01-03. http://www.theregister.co.uk/2002/04/19/waging_peace_on_the_internet/

Ruffin, Oxblood, 2010a. “Hacktivism: From Here to There”, *Threatpost* 2010-12-09. Hämtad online 2011-01-03. http://threatpost.com/en_us/blogs/hacktivism-here-there-120910

Taylor, Paul A. 2005. ”From hackers to hacktivists : speed bumps on the global superhighway?”, sid 625-646 i *New Media & Society* nr 7-2005.

Wray, Stefan, 1998. “Electronic Civil Disobedience and the World Wide Web of Hacktivism”. Publicerad på olika platser. Hämtad 2011-01-03 http://switch.sjsu.edu/web/v4n2/stefan/

Zanini, Michele – Edwards, Sean J.A. 2001. “The Networking of Terror in the Information Age”, sid 29-60 i Arquilla, John – Ronfeldt David (red) *Networks and Netwars : The Future of Terror Crime, and Militancy*. USA : RAND.

8.1 Intervjuer

Anonym, 2010. Samordnare för WhyWeProtest och aktiv kring Iran.

Lissnup, 2010. Twitteraktivist och ett nav för aktivister som vill sprida information från och om Iran.

Ruffin, Oxblood, 2010b. Grundare till Cult of the Dead Cow, hacktivistevangelist.

Shahryar, Josh, 2010. Journalist och människorättsaktivist.

Walck, Jonathan 2010. Aktivist och delvis tekniskt ansvarig för Telecomix.