"Mikroskopiska händelser förändrar internets karaktär. En enda tunnel eller en enda koppling kan förändra ett händelseförlopp radikalt. En bild inifrån en diktatur, ett läckt handelsavtal från en korrupt regim, ett stycke programkod eller en vittnesbörd kan smitta och spridas som en löpeld mellan internets noder. Det främsta kännetecknet för det öppna nätet är att vi inte kan veta vad som kommer att hända imorgon."

Det nätpolitiska manifestet tar dig från Teherans gator till internets djupaste darknets, från tingsrätten i Stockholm till de surrande datorhallar där minsta rörelse på nätet registreras. Det är en svindlande text som visar hur internet skakat om vår politiska tillvaro i grunden och bundit oss vid en teknologi som inte går att skilja från våra liv. Internet erbjuder möjligheter till politisk kamp och frigörelse, men kan också tjäna som verktyg för övervakning och repression. Genom att analysera de senaste årens konflikter runt The Pirate Bay, FRA-lagen och Wikileaks, men även händelserna kring Ship to Gaza, visar Christopher Kullenberg vägen till ett kompromisslöst nätpolitiskt motstånd med räckvidd långt utöver fiberkablarna.

Det nätpolitiska manifestet är den tredje boken i serien Ink manifest.

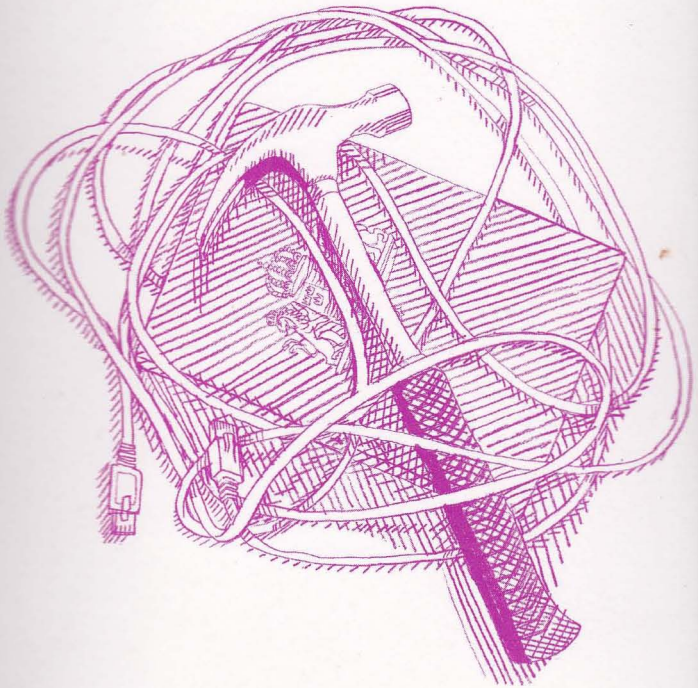
ISBN 978-91-978469-1-2

9789197846912

Ink bokförlag 2010

Christopher Kullenberg

DET NÄTPOLITISKA MANIFESTET



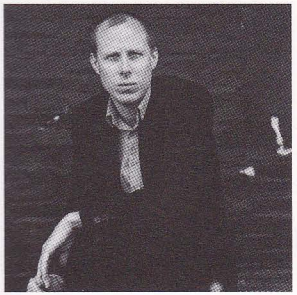
Ink bokförlag 2010

Ink bokförlag
www.inkbokforlag.com

Illustration: Gustaf von Arbin
Foto: Sannah Kvist
Tryck: Bulls Graphics, Halmstad 2010
ISBN: 978-91-978469-1-2

Ink manifest är en serie stridsskrifter författade av aktivister och kritiker. Manifesten skärskådar samtidens motsättningar, undersöker möjligheter till motstånd och pekar ut vägar framåt.

1. Rasmus Fleischer: *Det postdigitala manifestet*
2. Helena Granström: *Det barnsliga manifestet*
3. Christopher Kullenberg: *Det nätpolitiska manifestet*



Christopher Kullenberg (f. 1980) är aktivist, forskare och en ledande person i den nätpolitiska rörelse som vuxit fram i Sverige under de senaste åren. Kullenberg är bland annat engagerad i organisationerna Juliagruppen och Telecomix, som båda arbetar för ett öppet internet.

Tillsammans med sociologen Karl Palmås har Kullenberg skrivit en rad artiklar som berör maktutövning, övervakning och motståndsstrategier på internet. Vid sidan av att vara redaktör för den politiska tidskriften Resistance Studies Magazine driver han även bloggen Intensifier, som diskuterar hacktivism i Sverige och utomlands.

Sedan ett par år tillbaka arbetar Kullenberg som doktorand i vetenskapsteori vid Göteborgs universitet. Hans avhandling, som har arbetstiteln *Sociology in the making*, undersöker framväxten och produktionen av samhällsvetenskaplig kunskap och dess relation till moderniteten.

Det nätpolitiska manifestet är Kullenbergs debutbok.

Det nätpolitiska manifestet

1.

Det hotade nätet

I samband med presidentvalet 2009 slog den dåvarande iranska regimen ut en av de nyhetssatelliter som användes av BBC. Mobiltelefonnätet spärrades helt under vissa tider, Facebook och Youtube blockerades temporärt. Det iranska internet utsattes för en djupgående inskränkning.

När de traditionella kanalerna stängdes av riskerade händelserna i Teheran att falla i medieskugga. Den internationella opinionen var ju, sin välvilja till trots, helt beroende av att rapporter om vad som hände på gatorna strömmade in. Men det iranska internet blockerades aldrig fullständigt, åtminstone inte över någon längre tidsperiod. Direktrapporteringen letade sig sakta men säkert ut till Twitter, videofilmer laddades på omvägar upp på Youtube och förs ta-

handsinformation publicerades på bloggar och hemsidor. Endast ett fåtal länder, bland annat Nordkorea och Burma, hade tidigare klarat av att blockera internet helt och hållet, vilket varit möjligt främst på grund av att deras nationella datornätverk bara har ett fåtal fysiska anslutningar till omvärlden. Till regimens förtret höll sig dock nätet levande i Iran. Kommunikationen kunde upprätthållas trots censureringsförsöken. Ett fåtal iranska nätaktivister lyckades koppla upp sig mot datorer utanför Iran och kunde på så sätt sprida information som sedan kom att omsättas i förstasidesmaterial.

I många länder har internet blivit det primära kommunikationsmediet, inte minst för människor som av olika anledningar inte tillåts uttrycka sig fritt. Information på nätet både skickas och tas emot i en hastighet som inga tidigare medier kunnat åstadkomma. Det ger upphov till nya sätt att organisera handel, dela kunskaper och forma gemenskaper. Detta är en politisk angelägenhet i allra högsta grad.

Trots internets halvsekellånga historia är det först under de senaste två decennierna som människor över hela världen har börjat leva sina liv på och i anslutning till nätet. Detta har lett till uppkomsten av en ny form av närvaro, och därmed en påtaglig förändring i människors tillvaro. Det har gett upphov till en särskild existens – *nätvaron*. Att gå till näts – oavsett om det handlar om ett trivialt slösurfande på de stora webbplatserna eller om det resulterar i att information skickas förbi spärrar uppsatta av förtryckande regimer – innebär att man agerar på ett särskilt vis. Oavsett hur och varför vi kopplar upp oss mot internet är själva uppkopplandet alltid en politisk handling.

Nätpolitiken utmanar en hel uppsättning av etablerade makthierarkier; statliga diktaturer såväl som multinationella företag. Den kännetecknar vår samtid, men betecknar också en särskild politisk praktik.

Internet har förstärkt tidigare politiska kopplingar mellan människor, men framför allt har det skapat nya kopplingar vars möjligheter varken är utforskade till fullo eller utnyttjade maximalt. Vad internetbaserad kommunikation kan göra – med oss själva och med politiken överhuvudtaget – får vi reda på när vi bryter oss in i internet; i dess historia, teknologier och sociala sammansättningar.

Internet är idag hotat av ett flertal politiska processer som syftar till att begränsa och blockera det. Egyptiska bloggare arresteras för att de kritiserar regimen, länder som Kina och Frankrike tvingar nätanvändare att installera statliga spionprogram på sina datorer och i Sverige kopieras och övervakas all trafik till utlandet av Försvarets Radioanstalt. Samtidigt som dessa statliga interventioner präglar den samtida regleringen av internet strävar många stora företag, till exempel Apple, Google och Microsoft, efter att begränsa kommunikationen på internet så att den knyts närmare deras kommersiella tjänster. Internets infrastruktur designas allt mer efter principen att förmedla underhållning bunden till särskilda företagskonglomerat. Därmed ställer man sig i vägen för den neutrala rörelse av trafik som varit en förutsättning för datornätverkens framväxt.

Formeln för att försvara friheten på internet ligger inbäddad i själva infrastrukturen: vår nätvaro, och alla de kopplingar som den utgörs av, ger oss politisk kraft. Uppkomsten av internet medförde en sidoeffekt som idag har blivit dess viktigaste egenskap: förmågan att koppla samman människor i en nätvaro genom vilken motstånd kan utövas.

När nätvaron tvingas till självförsvar inträder en nätpolitik vars styrka vi endast har fått en försmak av. Det är en

politik som varken har ett givet mål eller en förutbestämd riktning; en politik vars potential ligger i att vi fortfarande inte exakt vet vad den förmår eller vilka krafter den kan sätta i rörelse. Nätpolitiken är en politik om internet, men dess omfattning är större än så: den drabbar alla som använder nätet för att framhärda som politiska varelser.

2.

De distribuerade nätverken

Den 29 oktober 1969 sändes det första paketförmedlade meddelandet mellan två datorer i ett amerikanskt militärprojekt som kallades för ARPANET. Paketförmedling innebär att ett digitalt meddelande delas upp i mindre enheter som sedan tillåts välja den mest framkomliga vägen till destinationen. Därutöver förses paketet med kontrollinformation som bland annat anger formatering, ursprung och slutmål. På det sättet utrustas varje meddelande med instruktioner för hur det ska skickas från en punkt till en annan, ungefär som informationen på ett kuvert talar om hur ett brev ska nå fram till rätt mottagare och med vilken prioritet. Dessutom innebär paketförmedling att meddelandena kan stuvas om på vägen, på samma sätt som ett kuvert

kan läggas i ett annat för att via nya delsträckor nå fram till mottagardestinationen.

Det teknologiska tillvägagångssättet för paketförmedlingen hade utarbetats ett par år tidigare i samband med den pågående kärnvapenkapprustningen. På uppdrag av RAND Corporation skrev den amerikanske ingenjören och matematikern Paul Baran 1962 artikeln "On Distributed Communications Networks", där de grundläggande idéerna om det distribuerade nätverket presenterades. RAND, som var ett slags tankesmedja i nära samarbete med det amerikanska flygvapnet, tilldelades varje år stora ekonomiska bidrag av militären och kunde därmed föra en tillvaro oberoende av de konventionella ekonomierna.

Det amerikanska samhället präglades under 1950-talet av en tilltagande rädsla för kärnvapenkrig. För att förhindra totalt kaos vid ett eventuellt anfall var det avgörande att korrekt information kunde förmedlas mellan president, generaler och personal stationerad vid missilanläggningarna. Frågan var dock vilken typ av infrastruktur som överlevde längst vid ett militärt angrepp. Enligt Paul Baran var svaret de distribuerade nätverken.

Även Sovjetunionen byggde under denna period sina första datornätverk med utgångspunkt i ett högteknologiskt missilförsvar. Men där såg den teknologiska utvecklingen annorlunda ut. Det amerikanska ARPANET och arbetet på RAND Corporation ägde rum på en fullkomlig antimarknad; de militära kapitalflödena i USA gjorde att teknikforskningen aldrig behövde konkurrensutsättas. I den hierarkiska sovjetiska byråkratin pågick däremot en ständig kamp om vilka avdelningar som skulle tilldelas ekonomiska medel, och utvecklingen av datornätverk fick därmed konkurrera med andra militära och civila projekt.

När de sovjetiska vetenskapsmännen började intressera sig för hur den planekonomiska styrningen kunde dra nytta av datornätverken utgick de ifrån den samling av teorier som går under benämningen cybernetik. Ofta har cybernetiken, det vill säga läran om styrning och kommunikation, framställts som en amerikansk forskningstradition. Som tillämpad teoribildning inom ekonomi och samhällsplanering var den dock mest inflytelserik i Sovjet.

De sovjetiska datornätverken som med avstamp i de cybernetiska teorierna upprättades på 1960-talet var decentraliserade men samtidigt hierarkiska. Tanken var att en central dator i Moskva skulle fungera som toppen av en pyramid. Den skulle sedan kommunicera med andra städer i vilka mindre nätverk organiserades. Det paradoxala i detta upplägg var att noderna i datornätet i viss mån kunde kommunicera utan en central punkt, samtidigt som informationsflödet ändå alltid färdades uppåt i hierarkin. Parallellt med det militära nätverket byggde den sovjetiska staten även ett kommersiellt nät som syftade till att övervaka den planekonomiska produktionen. Genom att samla in så mycket information som möjligt sökte man bland annat förutsäga trender beträffande tillgång och efterfrågan på en viss råvara.

Det distribuerade nätverk som Paul Baran hade skisserat i sin artikel skiljde sig radikalt från Sovjetunionens motsvarighet. Barans system förutsatte inte en "supernod" på toppen av informationsflödet, utan likställde statusen för nätverkets alla noder. Till skillnad från de sovjetiska nätverkens arkitektur, som i första hand syftade till *styrning* och *kontroll* av en helhet, var Barans grundläggande mål *överlevnad*, vilket ledde till konstruktionen av den distribuerade nätverksstrukturen.

Vilket datornätverk är bäst lämpat för militära syften – ett distribuerat eller ett hierarkiskt? Frågan blev allt mindre relevant ju mer kalla kriget tinade upp. Det som istället blev avgörande var vad som hände med teknologierna när de började tillämpas i civila sammanhang. Det sovjetiska datornätverket var inte bara hierarkiskt på ett teknologiskt plan; även i sin vidareutveckling var det insnärjt i den byråkratiska visionen om en cybernetiskt kontrollerbar stat. I USA hände däremot något ganska oväntat: Paul Baran registrerade huvuddelen av sitt arbete som public domain, det vill säga allmän egendom tillgänglig för vem som helst. Detta offentliggörande av de distribuerade nätverken skulle leda till att internet tog sina första stapplande steg i USA.

I början av 1980-talet gick ARPANET successivt över till den så kallade TCP/IP-arkitekturen. Den bestod av ett flertal protokoll som angav regler för hur datorer skulle kommunicera med varandra på ett enhetligt sätt. Datapaket kunde tidigare färdas globalt i specialdesignade nätverk, men med TCP/IP-arkitekturen blev det även möjligt för mindre nätverk att anslutas till större i kraft av en gemensam standard. Från och med nu kunde man koppla samman miljöer som såg mycket olika ut, vilket gjorde att den globala datorkommunikationen kom igång på allvar. Under 1980-talet steg antalet uppkopplade datorer från ett par hundra till cirka 300 000. Användarna var framför allt människor knutna till företag och universitet, men ett litet antal pionjärer använde nätet för privat bruk.

Under samma decennium gjordes även ett antal försök att skapa centraliserade nätverk, men de blev ganska snart omsprungna av de TCP/IP-baserade motsvarigheterna. Dessa hade en avgörande fördel gentemot de hierarkiska och slutna systemen – de innehöll ett antal öppna och standardiserade protokoll som än idag utgör några av internets grundteknologier – exempelvis e-post, filöverföringar (FTP), chat (IRC) och fjärrterminaler.

Omkring 1990 togs de första stegen mot world wide web och hypertext-protokollet, vilket gav upphov till den slutliga populariseringen av internet. Nu kunde människor snabbt och enkelt navigera sig fram över nätet genom ett växande antal hemsidor. Till en början bildade dessa en väv av enkla textdokument, men successivt fylldes de på med bilder och ljudfiler. Från de 300 000 användarna i början av 1990-talet skulle decenniet klocka in på runt sjuttio miljoner uppkopplade datorer.

I och med den användarexplosion som följde i spåren av world wide web skapades en ny ekonomi kring internet. Datornätverken byggdes ut och fick allt större kapacitet, de statliga europeiska telekom-monopolen avreglerades och nya affärsmodeller växte fram. Internet var förhållandevis billigt att investera i, vilket ledde till att börsnoterade företags aktiekurser kunde skjuta i höjden utan att bolagen hade tillgång till mer än en uppsättning vågade idéer och en hemsida. Många privata internetanvändare hade samma teknologiska förutsättningar. Att sätta upp en hemsida eller en blogg var i många fall gratis eller ingick i internetabonnemanget, och med den nya RSS-teknologin kunde bloggar få prenumererande läsare. Rent tekniskt skapades RSS och bloggar redan före millennieskiftet, men det var först några år efter IT-bubblan som de blev tillgängliga som allmänna tjänster.

Idag har vi ett distribuerat och paketförmedlat internet, en djungel av kablar och servrar, en flodvåg av datatrafik, protokoll och meddelanden. Det är en infrastruktur som är byggd för att kunna skyffla datapaket runt om i världen utan att ta hänsyn till om innehållet är en finansiell

transaktion, en chatkonversation eller en forskningsrapport. Den snabba tillväxten av internetuppkopplade mobiltelefoner och mobila bredband gör att den version av TCP/IP-protokollet som gällt sedan början av 1980-talet, IPV4, beräknas få slut på nummer inom ett par år. Det innebär att vi då passerar fyra miljarder direktanslutna enheter.

3.

Att gå till näts

Om e-post i början av 1990-talet användes av ett fåtal akademiker i syfte att upphäva distansen mellan olika forskargrupper har de sociala medierna idag sjunkit in i våra liv så djupt att människor på samma arbetsplats skickar meddelanden till varandra – inte för att något geografiskt avstånd behöver överbryggas, utan för att det har blivit ett konventionellt sätt att umgås på.

Allt fler sammanhang har med andra ord *blivit internet* – ibland under vår medvetna uppsikt, ibland utan att vi kunnat kontrollera det. Detta internetblivande kan inte förstås som rent tekniska processer. Att fiberkablar i marken, radiosignaler riktade mot satelliter och datorhallar fulla av servrar konstant skickar paketförmedlade meddelanden

är bara en sida av myntet. Ur denna tekniska infrastruktur uppstår dessutom någonting annat, en mångfald av nya sociala relationer som inte var möjliga tidigare.

Att bli internet innebär att människor går in och ut genom olika sammanhang som existerar genom nätet – sammanhang som kan vara allt från en mejlinglista till en chatkanal eller ett forum som helt eller delvis sammankopplas över internet. De sakfrågor som nätpolitiken tar upp är beroende av det faktum att människor har blivit en del av internet, och vid givna tillfällen investerar stora mängder energi i att försvara sin gemensamma nätvaro. Nätpolitiken är således inte en individualiserad politik – tvärtom är det alltid en kollektiv företeelse.

Eftersom det paketförmedlade internets grundstruktur tillåter varje digitalt meddelande att nå vilken annan nod i nätverket som helst uppstår nätvarons möjliga sammanhang som begränsningar sprungna ur ett överflöd. Om en miljard människor skulle tala i en och samma chatkanal, om varje e-postmeddelande skulle gå ut till alla adresser som finns eller om vi skulle få för oss att prenumerera på alla bloggar som skrivs, skulle nätblivandet förvandlas till ett enda vitt brus. Således har begränsandet av det potentiella informationsöverflödet en navigerande funktion. Vi måste hitta sammanhang som är tillräckligt avgränsade för att de överhuvudtaget ska vara meningsfulla. Det sker genom att vi gör bruk av en viss tjänst, exempelvis Facebook, läser vissa bloggar eller deltar i ett ämnesspecifikt forum.

Internet har lett till att idéer och innovationer i allt högre grad och med allt högre hastigheter *smittar*. Att gå till näts innebär att man drabbas av, och bär vidare, fragment av den strida informationsflod som utgör internet. Ett kollaborativt projekt som Wikipedia kräver att tusentals människor samarbetar i enlighet med ett regelverk, samtidigt som lusten att bidra hålls uppe. Öppna mjukvaror, med vars hjälp hela operativsystem skapas, kräver likaså delaktighet och en kultur som premierar att man delar med sig av sina kunskaper.

Före internet spred sig smittor med låga hastigheter. När de mediala infrastrukturerna var centraliserade kunde de inte mutera och utvecklas i flera led. När något visades på tv fanns det inget sätt att omedelbart återsända information tillbaka till källan, utan diskussionen begränsades fysiskt till tv-soffan. Etermedierna producerade såtillvida en *sekundär oralitet*, vilket innebar att deras sändningar gav upphov till lokala härdar av samtal som en reaktion på den ursprungliga utsändningen. Nyheter och allmänna angelägenheter diskuterades sedan på caféer, i föreningar eller på arbetsplatser. För att kommunicera vidare informationen till en större publik krävdes emellertid att den återfördes och koncentrerades till en central punkt, exempelvis redaktionen på en tidning eller en tv-station. Dessa punkter fungerade, och fungerar än idag, som trösklar i informationsflödet. Att sända ett radioprogram, trycka en tidning eller sprida flygblad krävde en organisation och resurser som gjorde att den politiska kommunikationen fråntogs den spontanitet som präglar det direkta samtalet.

I och med internet har dessa krav blivit allt mer svårmotiverade. Ett budskap eller meddelande på nätet kan nå alla noder i nätverket, och man kan genast återsända kommunikation till den ursprungliga källan. Med nätblivandet uppstår en *primär oralitet*, det vill säga möjligheten för en enskild person att själv agera smittokälla. Istället för att ett meddelande måste centraliseras för att komma över de kommunikativa trösklar som tidigare präglade medielandskapet kan det nu genast återinträda på en global nivå.

Konstitutivt för nätvaron är alltså att varje nod i nätverket kan bära vidare smittor på samma villkor som de andra noderna, vilket innebär att varje dator har möjlighet att omedelbart kommunicera med hela internet. Detta förhållande, som tydligast kommer till uttryck i peer-2-peer-teknologierna, innebär att helt nya kunskapsprocesser blir möjliga och helt nya kontaktytor uppstår mellan människor och maskiner. Det gör även att konflikter och problem som tidigare kunde hållas borta från etern och tryckpressarna kommer upp till ytan – på gott och på ont. Samtidigt som läckta dokument kan spridas i syfte att avslöja maktmissbruk, kan exempelvis främlingsfientliga grupper komma till tals på ett sätt som inte var möjligt tidigare.

Smittor affekterar oss på olika sätt. Ett datorvirus har kapacitet att infektera miljontals datorer inom loppet av någon timme. Spridningen av viruset syftar ofta till att få de infekterade datorerna att utföra en viss uppgift, och om vi användare överhuvudtaget märker av det beror det på att våra datorer börjar bete sig konstigt eller att systemadministratören stänger av oss från nätverket. Ett annat sätt som smittor påverkar oss på är när datorkod utväxlas mellan programmerare. Delningen av programmeringskod pågick i begränsad skala före internet. När det blev möjligt att skicka program över internet uppstod den öppna mjukvaran. Plötsligt kunde man genom att dela med sig bitar av kod skapa avancerade operativsystem.

När world wide web lanserades under 1990-talet uppstod en gigantisk smittohärd av information. Bild, video, text, ljud – allt som kunde pressas genom infrastrukturen blev plötsligt tillgängligt inte bara för spridning, utan även som muterande smittohärdar. Filer kunde förändras, remixas och flyttas in och ut genom olika sammanhang i en

rasande fart. Över en natt hade world wide web skapat en höghastighetsterräng vars expansion möjliggjordes med hjälp av kommandona copy och paste.

Smittohärdarna är av avgörande betydelse för att nätpolitiken ska kunna premiera deltagande framför basunerande budskap. Kraften att påverka ett händelseförlopp på internet avgörs inte av hur högt man skriker, utan av hur smittsamt ens ärende kan bli. De mest lyckade kampanjerna på nätet tycks vara sådana som inte har ett tydligt budskap, vilket annars betraktas som ett ideal för den traditionella partipolitiken. Smittsam politik sätter igång en form av opinionsbildning som snarare är *bildande* i bemärkelsen att det rör sig om en kunskapsprocess. Till denna kategori hör kollaborativa mjukvaruprojekt, exempelvis I2P (Invisible Internet Project), som genom att skapa krypterade nätverk underlättar för den anonyma kommunikationen på nätet, men även aktivistgrupper som La Quadrature du Net, som genom att sprida information om EU:s lagstiftning söker påverka den europeiska politiken.

Ju mer en smitta muterar desto livskraftigare blir den; det öppna internet gynnar just föränderliga budskap. En upprörd universitetsprofessor kallade häromåret bloggar för "kloaker". Vissa krävde upprättelse och ursäkter från professorn, andra menade att ordvalet var träffande – i kloaker frodas nämligen smittohärdar i vilka vi inte riktigt kan veta vad för slags liv som lever. Denna osäkerhet präglar nätblivandet som process, och ligger till grund för nätpolitikens öppna karaktär. Avsaknaden av uniforma normkällor och enkelriktade massmediers monopol gör att det enhetliga budskapet aldrig kan få samma genomslagskraft som när smittorna sprids från människa till människa via miljontals datorer som alla är del av internet.

Att sprida information utan att varken behöva ta hänsyn

till de teknologiska hinder som tidigare fanns – exempelvis behovet av tryckpressar – eller de sociala funktioner som kontrollerade spridningen – exempelvis redaktörer och nyhetsbyråer – gör att nya sätt att värdera informations- och kommunikationsflödena blir nödvändiga. Därmed möjliggörs inget mindre än en radikal demokratiform oberoende av massans opinion, ledares representerande makt och byråkratiska beslutsordningar. Denna internets grundstruktur reflekteras dock sällan i det individuella användandet. Istället förmedlar centrala noder ofta ett mycket stort antal användares information. Ett blogghotell kan ha hundratusentals användare, mikrobloggen Twitter och de stora e-postleverantörerna har miljoner. De flesta av oss väljer med andra ord att överlåta kontrollen över våra digitala liv till ett fåtal stora aktörer. Vi programmerar inte våra egna sökalgoritmer, utan använder Google. Vi kodar inte egna hemsidor, utan skapar en Facebook-profil eller en blogg i ett blogghotell. Vi låter inte våra hemdatorer agera chatservrar, utan använder färdiga tjänster som Microsofts MSN Messenger.

I praktiken innebär detta att informationen på internet centraliseras och färdas uppåt i en hierarki där den som driver tjänsten har den slutgiltiga makten att släppa fram eller bryta kommunikationsflödet. När en centralnod tar över distributionen blir nätet mer sårbart, och informationsöverflödet koncentreras kring en enskild aktör. Om de tidigare massmedierna kontrollerades genom statliga monopol och licenser för etersändningar gör centraliseringen av de sociala medierna på internet att ett fåtal aktörer får kontroll över hur information smittar. Sökmotorer anpassar sina resultat efter exempelvis den kinesiska regeringens lista över godkända hemsidor. E-postleverantörer i USA låter sina integritetsföreskrifter underordnas Patriot Act och lämnar gladeligen ut användaruppgifter när begreppet nationell säkerhet åberopas. Om man länkar till en fildelningssida på Facebook händer det ofta att länken automatiskt raderas eftersom film- och musikindustrin mer än gärna ställer sig i vägen med hot om stämningar. Smittan stoppas och kommunikationen bryts av.

Med tanke på att informationen som smittorna består av förmedlas med ljusets hastighet, samtidigt som tröskeln som måste överstigas för att kunna nå ut med denna information är låg, kännetecknas nätvaron av ett korttidsminne. Detta får påtagliga följder för den nätpolitiska praktiken. Eftersom en myriad händelser och fenomen befinner sig i ständigt omlopp på internet försvåras upprätthållandet av en politisk kontinuitet. En kollektiv glömska infaller varje gång trycket kring en given fråga klingar av. Detta är en konsekvens av överflödet självt.

Korttidsminnet kompletteras emellertid av ett annat slags minne, nämligen det gigantiska arkiv som internet utgör. Att avlägsna något från nätet kan ofta vara svårare än att göra det tillgängligt. Arkivet är dock inte helt lätt att få tillgång till; sökmotorer och indexeringstjänster kopierar all information de kan komma över och lagrar ofta denna utom räckhåll för användarna. Eftersom arkivet genereras av maskiner och automatiska index tenderar det att förbli passivt. För att vinna kraft och skapa engagemang måste de nätpolitiska kollektiven i någon mån förvalta arkivet. Vad som hände förra veckan, eller vad som hände för tio år sedan, är historier som måste skrivas, kommuniceras och infogas i det nätpolitiska tänkandet.

Korttidsminnet låter sig påverkas av aktuella händelseförlopp, av det som är på tal för stunden. En demonstration på gatan, ett lagförslag i ett parlament eller en läcka av hemlig information bygger upp ett tryck som genast kan smitta och spridas. När politisk information går från nod till nod, från en människa till en annan utan att passera en redak-

tion som granskar den, bildas snabbt nya gemenskaper. Nätvarons korttidsminne gör emellertid att dessa gemenskaper inte nödvändigtvis utgår ifrån tidigare politiska distinktioner. När FRA-lagen röstades igenom i Sverige enades bloggare med olika ideologiska grunduppfattningar i ett försök att bilda motopinion, när sajten Wikileaks publicerade hemligstämplade dokument om USAs krigföring i Afghanistan krävde såväl liberaler som socialister att kriget skulle ta slut, när telekom-marknaden regleras i EU går marknadsivrare och marxister samman och organiserar motaktioner. Samarbeten på nätet uppstår alltså ofta mellan politiska aktörer som tillfälligt blundat för det som skiljer dem åt. Denna pragmatism beror inte på att politiska skiljelinjer utraderats, utan är en följd av nätvarons förmåga att skapa nya politiska gemenskaper. Dessa gemenskaper kan i sin enklaste form bestå av en grupp på ett nätforum eller en mejlinglista som använder den nätmedierade kommunikationen som ett verktyg för att organisera sig. Men det kan också handla om politiska gemenskaper som överhuvudtaget inte var möjliga före internet, och som har nätet i sig som politiskt objekt.

Korttidsminnet på internet är en flykt bort från en institutionalisering av det politiska – i sin mest extrema form övergår denna flykt i en knapptryckningens politik, ett engagemang för en viss fråga som varar några sekunder för att strax skifta fokus till en annan. Samtidigt som denna politiska praktik ter sig fragmenterad är det just i förmågan till glömska som nätvaron har möjlighet att etablera en annan typ av demokrati. Nätvaron och nätpolitiken sammanfaller, och en nätets politik blir en gemenskapens politik.

4.

Nätpolitik

De stora flödena av internettrafik följer med slående likhet de globala flödena av pengar, varor och energi. Detta innebär dock inte att nätpolitiken på ett simpelt sätt kan förklaras utifrån exempelvis kapitalackumulation eller ideologiska regeringskonster.

En av de nätpolitiska grundfrågorna rör begränsandet av det överflödets tillstånd som karakteriserar internet. Hur ska gränserna dras och vem ska ansvara för gränsdragningen? Trots den teknologiska utgångspunkten – att varje nod i nätverket kan kopplas samman med alla andra noder – består internet i praktiken av en mängd artificiella spärrar. Det kinesiska internet begränsas av en gigantisk brandvägg som hindrar användare från att kommunicera med varandra, det

iranska internet är inte bara begränsat utan starkt övervakat – varje meddelande som innehåller regimkritik är en möjlig väg till fängelse och tortyr. I Italien pågår en ständig kamp mellan statlig blockering av webbsidor och användare som kringgår spärrarna. I Turkiet blockeras Youtube eftersom regimen anser att sajten sanktionerar uttryck som skändar landsfadern Atatürk.

Samtidigt som internet möjliggör sammankopplandet av en mångfald användare tillåter det likväl att infrastrukturen spärras och övervakas. Internets potentiella frihet, som ur en demokratisk synvinkel ter sig hisnande, är i praktiken alltid inskränkt. Gränsdragningarna innebär med nödvändighet ett maktutövande, som i nätpolitikens fall aktualiserar en rad frågor: Vem är det som blockerar en viss nod på internet? Vem privilegierar en viss typ av trafik framför en annan? Vem kontrollerar fiberkablarna i marken?

När en begränsning på internet upplevs som repressiv uppstår motstånd i form av nätpolitisk aktivism. Huruvida en stats inskränkning av medborgarnas internettillgång är att betrakta som legitim eller repressiv går dock inte att fastslå a priori, utan måste alltid bedömas mot bakgrund av den specifika kontexten. Varje försök att uttrycka internetrelaterade rättigheter i universella termer riskerar att fastna i ett ahistoriskt resonemang som inte tar hänsyn till mediets sociotekniska historia. Att formulera en nätpolitik enbart med utgångspunkt i universella rättigheter vore detsamma som att befria den från reell politisk handlingskraft. En sådan kraft bör snarare sökas i det specifika sätt varigenom nätvaron svarar på gränsdragningar i form av exempelvis blockeringar och övervakningsförsök.

Varje sökande efter nätpolitiska strategier måste alltså relateras till de konkreta situationer och sammanhang som har

gjorts möjliga genom internet snarare än till de transcendenta och ideala principer som karakteriserar den lagstiftande politiken. Detta förhållningssätt innebär ett tillbakavisande av kraven på att samma lagar och regler som gäller i samhället även ska tillämpas på internet. När det exempelvis gäller meddelarskyddet – som fastslår att anonyma källor som ger uppgifter till pressen inte får eftersökas av en myndighet – eller brevhemligheten – som innebär att brev som skickas med posten inte får läsas på väg till mottagaren – föreställer man sig att dessa rättigheter ska "översättas" så att de kan bli giltiga i det nya mediet internet. Abstraktionen och principen tillåts med andra ord att föregripa situationen och händelsen. Det är ohållbart. Man kan exempelvis inte införa en förhandscensur på internet, eftersom varje nod kan ansluta direkt till andra noder utan att passera en myndighet som granskar informationen. Det finns inte heller någon stat som kan garantera meddelarskydd för människor som via internet kontaktar tidningsredaktioner, eftersom de servrar som används kan befinna sig i princip var som helst på jordklotet. En majoritet av Norges internettrafik går genom Sverige, och övervakas därmed av Försvarets Radioanstalt som när som helst kan lämna vidare informationen till en tredje part. Att Norge skulle kunna garantera sina medborgare frihet från övervakning framstår därmed som en omöjlighet.

Nätpolitiken står i direkt förhållande till de hastigheter som internet möjliggjort. En demonstration med tusentals människor kan arrangeras på några timmar, varenda parlamentsledamot i en nation kan kontaktas på några minuter, hela ekonomier kan påverkas genom den blixtsnabba börshandeln. Man skulle kunna jämföra en mikroblogg med en samling människor som står förberedda på ett torg med ett plakat i ena handen och en tuschpenna i den andra – skill-

naden är att mikrobloggar inte har någon övre gräns för hur många som kan se meddelandet, och att kostnaden för att nedteckna ett budskap på internet i princip är obefintlig. Nätpolitikens trösklar är med andra ord ytterst låga. Att engagera sig är oerhört enkelt, men det kan vara desto svårare att uppnå en kontinuitet i det politiska arbetet. Utan de traditionella institutionernas tröghet måste nätpolitiken finna nya sätt att skapa politiska sammanhang.

Den immanens som kännetecknar nätpolitiken går på många sätt stick i stäv med den politik som präglat den västerländska moderniteten. Nätvarons *nomos* står i kontrast till den traditionella politik som syftat till att skapa generella lagar, principer och sanningar. Nätpolitiken upprättar sammanhang där människor utvecklar en praxis genom samvaro snarare än genom fastställandet av politiska program eller ideologiska manualer. Det innebär att den nästan alltid undflyr den allmänpolitiska matrisen, vars dikotomier – höger/vänster, individualistisk/kollektivistisk, tillväxtorienterad/grön och så vidare – upplevs som klumpiga analysverktyg. Det innebär dock inte att mer övergripande ideal och föreställningar är helt överflödiga. Snarare existerar de som en passiv bakgrund till den aktiva nätpolitiken.

Skillnaderna mellan nätpolitiken och den traditionella parlamentarismen visar sig inte minst när den förra nästlar sig in i den senare. Under våren 2009 vände sig några nätpolitiska kollektiv mot EU i samband med att det så kallade telekompaketet, som innefattar ett antal direktiv för regleringen av telekom-marknaderna i Europa, behandlades i EU-parlamentet. I två av de föreslagna tilläggspropositionerna såg aktivisterna en möjlighet att garantera nätneutralitet och rätt till domstolsprövning för personer som riskerade att stängas av från internet. En chatkanal

fylldes med bekymrade aktivister som ville skydda internet i lagstiftningen. Vissa kände varandra sedan tidigare, andra inte. Några kände aktivister i andra nätverk och några trillade in av ren nyfikenhet för att snabbt sugas in i aktiviteterna. Den traditionella lagstiftande processen blev utsatt för en internetbaserad direktaktion.

En chatkanal är i huvudsak inte en plats, utan en händelse. Denna händelse kan pågå under en kväll eller i flera år. Den är visserligen alltid rent fysiskt placerad på en eller flera servrar, men dess rumslighet ger sig inte sällan tillkänna någon annanstans, exempelvis där de politiska processerna utspelas för tillfället. Chatkanalen kan befinna sig lika mycket i lägenhetsfester, på krogar och dansgolv som i parlamentens Bryssel och Stockholm. Genom sin koordinerande funktion kan själva kanalen utgöra en kontaktyta mellan alla dessa platser.

I slutet av 1990-talet fann företagen sina konsumenter på internet, och idag har politikerna funnit sina väljare där. Inget parlament består enbart av en insida, utan är alltid kopplat till en mängd grupper, institutioner och individer utanför. Genom att en mängd kontaktytor mycket snabbt har digitaliserats, exempelvis genom just chatkanaler, bloggar och nätcommunities, har den parlamentariska politiken blivit en del av internet. Ett affektdrivet nätpolitiskt kollektiv som vid givna intensitetspunkter drabbar politiken går dock inte riktigt att underordna ett parlamentariskt, representativt demokratiideal. Om det parlamentariska systemet är territoriellt och medierar en genomsnittlig folkvilja pekar det affektdrivna kollektivet mot partikulära sakfrågor som politiseras i små, direktförmedlade gemenskaper.

Trots dessa skillnader behöver nätpolitiken inte stå i opposition till parlamentarismen, utan kan tvärtom inter-

agera med det. Genom viljan att ifrågasätta hur traditionell politik bedrivs ges möjligheten att hacka systemet. En politisk process kan öppnas upp, och när dess beståndsdelar ligger på bordet och ett aktivistkluster ser hur komponenterna fungerar går de att förändra. Det blir då möjligt att ta sig an ett politiskt skeende och styra det i en annan riktning, överraska det och drabba det med kraft. Alternativen, som skulle vara att antingen ge sig in i politiken på dess förutbestämda villkor eller att helt och hållet negera systemet genom isolering eller våld, ter sig i ljuset av detta som återvändsgränder.

Ett system som består som en intakt enhet trots yttre påverkan, som förmår reglera sig självt likt ett element ökar eller minskar värmen vid temperaturfluktuationer – detta var den cybernetiska drömmen. Det är också en dröm som i viss mån genomsyrar den parlamentariska politiken, där folkviljan i sin genomsnittlighet ska komma till uttryck i syfte att påverka hur ett givet territorium regleras och domineras. Men internet och nätpolitiken accepterar inte en sådan praxis, i synnerhet inte när den försöker begränsa och ta kontroll över själva nätvaron. Såtillvida är nätpolitiken varken parlamentarisk eller utomparlamentarisk. Den är snarare driven av en vilja att plocka upp delarna av ett givet politiskt system och bygga om det.

5.

Från cyberrymden till Spectrial

Under internets tidiga historia var det vanligt att i filosofiska, sociologiska och politiska termer tala om den virtuella världen som en entitet som var helt separerad från den fysiska. Det nätverk av datorer som under 1980-talet bland annat hade beskrivits av cyberpunkförfattaren William Gibson, framför allt i genombrottsromanen *Neuromancer*, var en okroppslig och kall värld där information ägdes av företag som var större och mäktigare än nationalstater. Dessa kommersiella nät, som gick under beteckningen ”matrisen” och huvudsakligen var till för finansiella transaktioner, blev då och då utsatta för angrepp av ”tangentbordsjockeys” som tack vare sina datorkunskaper kunde stjäla information och pengar. Motsatsen till matrisen var ”köttvärlden”, en plats där den

rena tanken besudlades av människokroppens oberäkneliga drifter och begränsningar.

En liknande dualism låg till grund för den amerikanske författaren och aktivisten John Perry Barlows manifest *A Declaration of the Independence of Cyberspace* från 1996. Barlow menade att cyberrymden varken borde eller kunde regleras utifrån av en juridisk kropp som inte själv befann sig på internet. Nätet utgjorde enligt Barlow en väsensskild verklighet som i grund och botten var separerad från, och borde förhålla sig autonomt till, den analoga världen.

Barlows självständighetsförklaring må ha fungerat 1996, men ett drygt decennium senare ter sig tanken om en autonom värld som överskrider sociala, ekonomiska och framför allt mellanmänskliga villkor som utopisk, på gränsen till naiv. I och med att internet blev en viktig ekonomisk och infrastrukturell realitet i slutet av 1990-talet förvandlades cyberrymden till en plats för reella politiska kontroverser. Men ännu viktigare än det faktum att den lagstiftande makten blev tvungen att hantera denna teknologiska revolution var att människor hade *blivit* internet.

Internet är varken en cyberrymd eller mindre affekterande än en föreställd köttvärld. Nätet är inte en separat verklighetssfär som följer sina egna naturlagar, utan en domän som hela tiden hakar i och kopplar samman en mångfald av situationer och processer utanför datornätverken. På samma sätt som den cybernetiska visionen om styrning av virtuella system i Sovjetunionen var dömd att gå i kras ter sig varje försök att isolera internet i form av ett egenmäktigt system som en återvändsgränd.

Vid millennieskiftet fanns 70 miljoner datorer med egna IP-nummer anslutna till internet. Tio år senare finns fler än en miljard anslutna datorer. Internet är såtillvida varken en

kall maskintriumf eller en köttig röra av oförändrade individer – det är något som uppstår i kopplingarna mellan människa och maskin, mellan det analoga och det digitala. Om den tidiga cyberpunken gjorde en tydlig distinktion mellan cyberrymden och köttvärlden, och 1990-talets nätaktivism koncentrerade sig på att ifrågasätta hur "världsliga" lagar och regleringar förhöll sig till internet, kommer 2010-talet präglas av en nätpolitik där detta glapp har förlorat sin relevans. Detta kommer till uttryck både i hur internet regleras och diskuteras i den generella offentligheten, i hur våra ekonomier har förvandlats, och framför allt i hur vi hanterar vår nätvaro som en fullt integrerad del i våra vardagsaktiviteter.

Det kanske tydligaste tecknet på denna utveckling är den världsomspännande nätpolitiska händelse som vintern 2009 kom att öppna upp helt nya politiska arenor. Den 16 februari bevakade ett flertal internationella medier tingsrätten i Stockholm, där tre personer stod anklagade för att ha drivit fildelningssidan The Pirate Bay. Rättegången måste betecknas som den största fildelningshändelsen sedan Napster stämdes 1999. Det som stod på spel var inte bara upphovsrättens eller fildelningens framtid. Rättegången var även ett uppvisande av nätvaron som politisk kraft, eftersom den innebar att åtskilliga nätaktivister korsade varandras vägar och ett antal viktiga projekt föddes.

I Sverige hade den föregående sommaren och hösten präglats av en hård debatt om den så kallade FRA-lagen, som skulle ge Försvarets Radioanstalt rätten att övervaka kabelburen kommunikation, vilken till stor del består av internettrafik. Dessutom hade det så kallade Ipred-direktivet, som tillät upphovsrättsinnehavare att begära ut nätanvändares identiteter från internetoperatörerna, genomdrivits under stark kritik. Ironiskt nog sammanföll klubbandet av Ipred-

direktivet med rättegången mot The Pirate Bay, och händelserna gav upphov till stora politiska manifestationer.

Det unika med *Spectrial* – som rättegången mot The Pirate Bay kom att kallas – var dock inte faktumet att hundratals nätaktivister fyllde tingsrättens salar till brädden samtidigt som internets chatkanaler i princip blev oläsliga då varje minut av den utsända rättegången diskuterades i detalj. Det unika var att rättegången etablerade ett nytt gränssnitt för social interaktion som tidigare hade varit nästan uteslutande internetbaserad, och därmed kopplade samman heterogena grupper av människor på ett nytt sätt. Den svenska nätaktivism som hade orsakat den så kallade bloggbävningen kring FRA-lagen och ihärdigt kritiserat införandet av Ipred-direktivet hade i huvudsak varit nätbaserad. Spectrial utspelade sig istället på en fysisk plats och utgjorde därmed en mötespunkt för människor som flödade in och ut ur stadsrummet. I tingsrätten bildades små öar av människor som planerade framtida aktiviteter, utanför trotsade aktivister vinterkylan i Piratbyråns buss, ett par kvarter bort samlades folk på caféer för att blogga om vad som hade hänt under dagen och på pubar och klubbar arrangerades fester mer eller mindre anslutna till dramat i tingsrätten. Spectrial var, som händelse betraktat, lika mycket en ockupation av en mängd lokala platser som en tre veckor lång juridisk process. Samtidigt som rättegången ägde rum i Stockholm arrangerades gatufester i Moskva till hyllning av The Pirate Bay. I de djupaste anonyma chatnätverken anfölls den målsägande organisationen IFPI (International Federation of the Phonographic Industry) och Maqs advokatbyrå, som företrädde musik- och filmbolagen, genom överbelastningsattacker mot deras hemsidor.

Spectrial handlade på ett sätt mer om internet som infrastruktur än om frågan om upphovsrätt. I lagens namn

skulle de skyldiga utpekas, men det var inte helt enkelt eftersom The Pirate Bay hade drivits som ett distribuerat projekt bestående av ett stort kluster av människor snarare än en tydlig organisation. Att bittorrent-tekniken som sidan byggde på utgörs av ett protokoll som sprider ut delar av filerna över ett mycket stort antal datorer gjorde inte saken enklare. I en bemärkelse *är* The Pirate Bay sina användare, eftersom infrastrukturen är distribuerad mellan de deltagande noderna i bittorrent-svärmarna.

Bittorrent förmedlar trafik fördelad över ett stort antal datorer istället för att förlita sig på en central punkt i nätverket. Det innebär att maktpositioner förskjuts till den grad att de enskilda användarna kan bestämma över vad som skickas mellan datorerna. Att förskjuta maktpositioner genom direkt handling innebär att omdefiniera hur internet bör se ut, vilket var precis vad The Pirate Bay gjorde. De branscher som bygger på centraliserad exemplarförsäljning kunde på grund av The Pirate Bay och andra bittorrentsidor inte längre upprätthålla ett materiellt övertag – möjligheten till kontroll försvann. Fördämningarna brast och filerna spreds med en teknologi som vävdes in i miljoner datorer och idag står för mellan en fjärdedel och hälften av all internettrafik. Den går inte att stoppa med mindre än att nätet stängs av helt eller övervakas ned till minsta paket.

Bittorrent skapar en värld där information kan förmedlas enligt en helt platt organisationsform, där varje nod i nätverket bidrar till att optimera upp- och nedladdningar. Detta gör det möjligt för en helt vanlig persondator att sprida stora filer till hela den internetanslutna världen. Även om kalla krigets skisser över det distribuerade nätverket aldrig var i närheten av att förutsäga att tunga filer skulle överföras i datornätverken på detta sätt är parallellerna på en nivå

ändå slående. Genom att minimera funktionen för en central punkt i nätverket och sprida ut trafiken utan att fastslå någon förutbestämd väg bygger man in överlevnad i det tekniska systemet. Det faktum att The Pirate Bay trots ihärdiga försök inte har kunnat stängas ned är en tydlig manifestation av detta. Så länge det finns ytterligare en nod i nätverket som är beredd att bistå med utrymme kommer sidan att finnas kvar.

Bittorrent är såtillvida ett av de mest radikala sätten att nyttja de distribuerade nätverken på. Rättegången mot The Pirate Bay tvingade in såväl domstolar som nyhetsmedier i en diskussion som fördjupade förståelsen av internet som infrastruktur, och fick även aktivister att engagera sig i frågor som gick bortom upphovsrätt och piratverksamhet.

Att gå till näts innebär att man gör nätet till sitt eget, till en del av sin egen existens. Detta är den främsta anledningen till att Spectrial samlade en offentlighet som i förlängningen till och med kunde betraktas som en opinion att räkna med i parlamentariska val. Men Spectrials förmåga att bilda gemenskaper överskred samtidigt den traditionella politiska opinionsbildningen; det som skapades var en tekno-social kropp av människor, datorer och nätverksprotokoll som uttryckte ett slags gemensamt självförsvar. Nätvaron var under angrepp av en industri som bara något decennium tidigare hade sett sin guldålder och levererat populärkultur till förhållandevis passiva konsumenter. Bittorrent, med The Pirate Bay i spetsen, hade kastat om en grundläggande relation i förhållandet mellan kultur och människa – protokollet hade skapat en möjlighet för människor att själva sätta villkoren för kulturprodukternas distribution och spridning.

Månaderna efter Spectrial hade vissa av de nätpolitiska grupperingar som deltog vid rättegången förändrat sin

praktik. Om tidigare sakfrågor i huvudsak hade hanterats på ett ganska traditionellt sätt skedde ett nätpolitiskt taktikskifte mot mer direkta former av aktioner. Istället för att protestera mot makten hade det blivit dags att skruva isär den för att få reda på hur den fungerade. Komplicerade politiska processer kartlades, och det visade sig att man kunde hitta många olika möjligheter att påverka dem. För att utmana lobbyister i EU skapades en egen lobbyorganisation. För att konkurrera med industrins utredningar och siffror författade en aktivistgrupp en egen utredning och presenterade den för den svenska regeringen under hösten 2009. När mediernas agenda inte överensstämde med aktivisternas upprättades en egen nyhetsbyrå vid namn Telecomix News Agency. När det saknades en stab av jurister som kunde jämföra lagförslag byggdes ett datorprogram som gjorde det automatiskt. Med hjälp av de verktyg för samarbete som internet erbjuder kan man med mycket små ekonomiska medel intervenera i den traditionella politiken.

6.

Panspektron

Parallellt med framväxten av de distribuerade nätverken skedde en utveckling inom underrättelseverksamheter världen över som långt senare skulle få konsekvenser för det vi idag kallar för nätpolitik.

Under första hälften av 1900-talet hade den militära signalspaningen skett med hjälp av radiosignaler. Underrättelser om exempelvis truppförflyttningar skickades delvis genom etern, oftast i form av krypterad information som behövde dekrypteras för att kunna tydas. För att avgöra vad som var relevant information började militär och underrättelsetjänster använda datorer för att känna igen mönster och sökord i de analoga utsändningarna. Dessa sändningar underställdes digital metadata, ett slags sök-

och indexeringssystem. För att hitta rätt i den polyfoni av röster och morsekod som färdades genom etern var man tvungen att tillföra information som gjorde själva innehållet sökbart och därmed meningsfullt.

När internet kom att användas som ett transkontinentalt kommunikationsmedium fick de signalspanande myndigheterna ett nytt territorium att övervaka. I motsats till radiosignaler är all internettrafik digital och kan därmed sorteras och genomsökas på ett mycket effektivt sätt. Paketen är redan utrustade med metadata i form av information om deras destinationer. Ju fler saker i vår omvärld som digitaliseras, desto större blir det spektrum (oavsett om det rör sig om ljud, ljus eller radiovågor) som är möjligt att mäta, beräkna och behandla. Vid internets födelse var digitaliseringen småskalig – dåtidens datorer var stora, klumpiga och dyra. Idag kan mobiltelefonerna i våra fickor digitalisera ljudvågor i form av samtal, ljus med hjälp av kameror och position genom GPS-mottagare. En dator eller en mobiltelefon är ur ett militärt perspektiv en spårsändare som kan lokaliseras, avlyssnas och loggföras. De servrar som bygger upp internets infrastruktur sparar automatiskt en ofantlig mängd loggfiler som kan generera mycket detaljerad information om varje användare.

Den *panspektriska* övervakning som möjliggjorts av internet utvecklades alltså ursprungligen som en militär metod för signalspaning, men precis som det distribuerade nätverket skulle den inte få sitt största användningsområde inom krigföringen. Istället flyttade panspektron in i internetanvändarnas hem och fickor. Genom ett mycket snabbt teknikskifte kunde helt vardagliga situationer plötsligt digitaliseras, genomsökas och övervakas.

Panspektron anspelar på begreppet *panoptikon*, som myntades av den brittiske filosofen Jeremy Bentham i slutet

av 1700-talet. Med panoptikon avsåg Bentham en praktik för social kontroll som innebar att människors beteenden gjordes synliga, vilket ledde till att de anpassade sitt agerande till denna visibilitet. Panoptikon kunde användas som modell för fängelser där cellernas gallerdörrar gjorde att fångarna ständigt kunde betraktas av fångvakterna, i skolor där eleverna alltid var synliga för lärarna eller på fabriksgolvens löpande band som kunde inspekteras av förmännen.

I takt med att allt mer avancerade informationsteknologier såg dagens ljus förvandlades emellertid panoptikon till en otidsenlig form av kontroll. I vår samtid är det inte längre den optiska blicken som övervakar oss, utan istället databaser och loggfiler, datorer och mobiltelefoner. De skapar en ny form av visibilitet bortom det mänskliga ögat. Panspektron markerar således de nya frontlinjer inom vilka breda spektra av analoga signaler kan göras digitala, och därmed synliga, på ett mycket mer omfattande sätt än tidigare.

Den panspektriska tidsålderns övervakningsstrategier manifesteras i två huvudsakliga former. Å ena sidan visar de sig som inbäddade verktyg i vår vardag i form av sökmotorer, communities, databaser och kortbetalningar. De får kort sagt vardagen att fungera på ett smidigt sätt. Å andra sidan kommer panspektrismen till stånd i lagar och regleringar instiftade av övervakande myndigheter och i viss mån även av de företag som hanterar informationen på nätet. Den panspektriska övervakningen är således en produktiv process som innebär att resultatet av den både kan vara ekonomisk vinning för företag och social lydnad inför olika former av polisiär verksamhet.

När internet under millennieskiftet expanderade dramatiskt dröjde det inte länge förrän mycket restriktiva lagar som begränsade friheten på nätet kom till stånd. 2001

instiftades Patriot Act i USA, som på ett direkt sätt gav myndigheter möjlighet att övervaka internet. 2006 trädde datalagringsdirektivet i kraft i EU, vilket förpliktigade medlemsländerna att spara elektronisk trafikdata för internetanslutningar, telefoner samt e-post. I Sverige och många andra länder fick signalspanande myndigheter uppgiften att bevaka internettrafiken, vilket stadfästes i och med 2008 års införande av FRA-lagen. Även privata aktörer fick allt större befogenheter att tillse internet i syfte att ställa människor till svars för upphovsrättsöverträdelser. I EU implementerades Ipred-direktivet första gången 2006, vilket gav upphovsrättsindustrin tillåtelse att begära ut privatpersoners IP-nummer från deras internetoperatörer. Idag diskuteras det globala handelsavtalet ACTA (Anti-Counterfeit Trade Agreement), som mycket väl kan komma att ge ännu större möjligheter för upphovsrättsinnehavare att övervaka och blockera trafik på internet.

Gemensamt för den militära och polisiära övervakningen av internet är att den är elektronisk, och därmed kan möjliggöra föregripande insatser. Militären har alltid försökt förutse truppförflyttningar och förutspå försvarsstrategier. Polismakterna har däremot i huvudsak arbetat med att utreda brott genom att säkra bevis i efterhand. Genom en allt mer påtaglig digitalisering av människors liv har emellertid även polismakterna fått möjligheter att arbeta med föregripande metoder. Så kallade intelligenta övervakningskameror, som inte bara spelar in video utan även känner igen ansikten, installeras för att förhindra terrordåd i Londons tunnelbana. Trafikavgiftskameror som är direktkopplade till bilskatteregistret används över hela Storbritannien för att kunna visitera bilister i syfte att upptäcka droger (utifrån antagandet att det finns ett samband

mellan människor som inte betalar skatt och använder narkotika). Fingeravtrycksläsarna på amerikanska flygplatser är direktkopplade till straffregister och listor över misstänkta terrorister. Trafikmönster på internet, det vill säga den typ av information som avslöjar vem som kommunicerar med vem, antas kunna användas för att kartlägga kriminella nätverk och terroristceller. Ju mer data vi kan utvinna ur en människas liv, desto fler samband kan vi konstruera mellan olika variabler. På så sätt förskjuts övervakningens blick från att fokusera på en individ till att leta efter mönster, sannolikheter och tröskelvärden för när ett brott kan tänkas komma att begås i framtiden.

Den panspektriska övervakningen ser saker som den panoptiska övervakningen inte gjorde. Google eller Facebook kan idag sammanställa datamängder som säger saker om våra liv som vi inte ens själva är medvetna om. Google minns dina sökord i exakt detalj för flera år tillbaka i tiden. Facebook vet vilka som är dina vänner och vilka dina vänners vänner är, och vilken konstellation av människor som har besökt en viss plats vid ett visst tillfälle. Om man föreställer sig den arbetsmängd som en sådan sammanställning skulle ha motsvarat innan vi började omge oss av elektroniska övervakningsteknologier, en sammanställning som idag utförs automatiskt av databaser och datorer, inser man att nätvaron resulterar i en typ av övervakning – och därmed ett visst vetande – som inte var möjligt tidigare.

För vissa företag är denna form av övervakning en kärnverksamhet. Att samla på sig data om mänskligt beteende har blivit en affärsidé för detaljhandels- och reseföretag, sökmotorer och internetcommunities. Paradexemplet är Google, som tidigt började övervaka sökord i syfte att fånga konsumenter som var på väg att göra ett inköp och

sedan rikta specifik reklam mot dem. Ett annat exempel är Facebook, som genom att dra nytta av användarnas sociala nätverk, deras "sociogram", matchar produkter med specifika konsumentgrupper. Att länka samman de spår som användare lämnar ifrån sig på internet har gett upphov till en hel politisk ekonomi, som inte bygger på att hålla arbetare instängda i fabriker där deras kroppar skapar värde genom arbete, utan istället placerar människor i värdeskapande arbetsprocesser genom att övervaka deras beteende. Att söka på internet, skicka e-post eller interagera med sina vänner på communities är big business eftersom det genererar det sista ledet i den logistik som garanterar att konsumentprodukter når sina konsumenter. Såtillvida utgör de panspektriska företagen ett symptom på en ultrasnabb global kapitalism. Varje dag arbetar vi för dessa företag. Vi behöver inte ens gå till arbetet eller genomföra en transaktion, varje klick och varje sökning vi gör är redan del i en värdeskapande process. Således utgör gratistjänsterna på internet, från sökmotorer till nätcommunities, den primitiva ackumulation av arbetskraft som krävs för att upprätthålla de internetbaserade ekonomierna.

I skärningspunkten mellan de panspektriska ekonomierna och den statliga viljan till kontroll över internet uppstår ett speciellt subjekt som synliggörs med hjälp av digitalt genererade datamönster. Detta subjekt underordnar sig dem som besitter de datamönster som beskriver dess vanor, beteenden och preferenser, eftersom dessa mönster ligger till grund för beslut tagna bortom subjektets medvetenhet därom. Att befinna sig i ett kundregister eller att överlåta information om sina vänner på ett community som Facebook innebär att man sätter igång processer som i sin tur återverkar på den materiella vardagen.

De register som tidigare fördes över medborgarna i en nationalstat var primitiva. Folkbokföring, sjukjournaler, skatteregister och telefonkataloger hade alla som mål att förvandla individen till en del i en större helhet – populationen. I den panspektriska övervakningens tidevarv är populationen inte längre intressant. Varken militären eller företagen är längre intresserade av nationalstaternas gamla gränser. För att upptäcka det som idag upplevs som hot mot samhällsordningen vänder sig övervakaren inåt och fokuserar blicken på avvikande beteendemönster i den egna samhällskroppen.

Det panspektriska subjektet görs alltså synligt av en mängd mönster som samlas i olika databanker. På samma sätt som företag letar efter vissa mönster som signalerar ett potentiellt konsumtionsögonblick söker underrättelsetjänster efter de mönster som uppvisar ett beteende som skulle kunna leda till en krigshandling. Detta återspeglas i de lagstiftande processer som genomdrivits under de senaste två decennierna. I Europa har underrättelseverksamheterna getts tillstånd att övervaka den elektroniska kommunikationen, samtidigt som den polisiära makten genom EU:s datalagringsdirektiv fått befogenhet att genomsöka loggfiler för i princip all elektronisk kommunikation.

På samma sätt som Google vill samla in all data på internet vill FRA ha tillgång till de trafikmönster som genereras när en dator ansluter till en annan. Följden av detta blir att internet hamnar under ständig övervakning. Panspektron påbjuder å ena sidan en medvetenhet om att vi ständigt är övervakade. Å andra sidan ger den upphov till en nätaktivism som motsätter sig hur makten över den elektroniska kommunikationen förskjuts till en övervakande kropp. Datorerna, myndigheterna och företagen vet mer om dina digitala spår än du själv någonsin kan veta. Det panspektriska

maktdiagrammet är dock inte befriat från friktionspunkter. De nätpolitiska aktivisterna finner hela tiden möjligheter till motstånd inne i datornätverken.

7.

Cipherspace

De distribuerade nätverken skapar nya former för social kontroll genom panspektron, som intensifierar och sammanfaller med andra former av ordningsskapande. Detta visar sig som tydligast i despotiska stater, där internetövervakningen i förlängningen leder till fängelsestraff och tortyr, men går även att skönja i demokratiska regimers mjukare men likväl effektiva sätt att hos människor ingjuta känslan av att ständigt vara övervakad.

Den panspektriska övervakningen har två teknologiska förutsättningar. Den första är att trafik ofta skickas i klartext över datornätverken, det vill säga i okrypterad form som kan läsas av vem som helst. Den andra är TCP/IP-protokollet, som innebär att varje dator som kopplar di-

rekt till internet har ett unikt nummer. Genom att loggföra detta nummer går det att se vem som gör vad.

Insikten om att de distribuerade nätverken var sårbara för övervakning drabbade både de militära och civila ingenjörerna under 1970-talet, och ledde till att ARPANET 1983 separerades i en militär och en civil del. Endast ett fåtal så kallade gateways gjorde att e-post kunde skickas dem emellan. Men vetskapen om övervakningsmöjligheterna ledde även till att kommersiella företag började efterfråga ett säkert sätt att överföra företagsinformation på. 1974 anlitades IBM av den nationella standardiseringsbyrån i USA för att utveckla Data Encryption Standard (DES), en krypteringslösning som kunde användas av alla företag som investerade i datorsystem. Den byggde på att man med hjälp av komplicerade algoritmer förvandlade den sårbara klartexten på internet till chiffertext (ciphertext). Eftersom DES var tänkt att fungera som en standard på det civila internet började allt fler intressera sig för kryptoanalys, som därmed kom att studeras öppet på universiteten och inte enbart under strikt militär sekretess.

Tack vare sina enorma ekonomiska resurser kunde den amerikanska militären bygga egna och autonoma nätverk i syfte att undvika övervakning. För civila internetanvändare har detta givetvis aldrig varit någon möjlighet – trots att det är just de som i störst utsträckning drabbas av övervakningen. Under sent 1980-tal började därför ett fåtal pionjärer att experimentera med ett annat koncept, så kallade *darknets*. Darknets är ett system av tunnlar som upprättas i samma infrastruktur som det vanliga nätet. Det görs genom att man skapar en krypterad anslutning från en dator till en annan, eller mer exakt: från en host till en annan. En dator i Kina kan alltså upprätta en tunnel till en dator i Sverige och sedan använda den svenska datorn för att nå ut på internet. På det viset kringgås de kinesiska spärrarna och det blir svårt att övervaka den respektive användarens aktiviteter.

Samma metoder som brukas för att kryptera företagshemligheter och finansiella transaktioner kan således användas – och används dagligen – av nätaktivister som behöver skydda den information de vill sprida. All innehållsdata på internet kan krypteras till oigenkännlighet – en text-, ljud- eller bildfil blir då oläslig även om den kopieras. Även trafikdata görs meningslös när trafiken inte går direkt från användarens dator, utan via en eller flera andra datorer på internet. Eftersom internettrafiken är paketförmedlad kan den ta flera omvägar fram till destinationen, vilket innebär att den blir allt svårare att spåra till den ursprungliga avsändaren.

Kombinationen av dessa två teknologier, kryptering och paketförmedling, ger upphov till ständigt nya darknets. Cyberspace blir *cipherspace* – ett krypterat internet inuti internet där det är nästintill omöjligt att röja en användares identitet. Följden av denna identitetslöshet blir att inga lagar kan verkställas och inga straff utdömas; cipherspace är ett tillstånd av teknologisk anarki. De tidigmoderna samhällskontraktsteoretikerna tänkte sig att ett sådant tillstånd skulle vara en tygellös och otrygg situation. I linje med detta menade kritikerna under 1990-talet att kryptering av internet skulle leda till fullständigt kaos. De föreslog till och med att krypteringsmjukvara borde klassificeras som "ammunition" och beläggas med förbud – vilket också blev fallet i USA.

Med tanke på att cipherspace uppstod som en reaktion mot lagar som kränkte individers frihet bör man emellertid inte förstå det i termer av ett nihilistiskt kaos. Utvecklingen av darknets är en aktiv lösning på övervakningens problem.

Det är ett tecken på nätvarons vilja till självförsvar, en direktaktion riktad mot de panspektriska samhällena.

Idag växer intresset för dessa tunnlar, som i allt högre utsträckning fyller fiberkablarna med krypterad trafik. När Ipred-direktivet drevs igenom i Sverige skapades Ipredator, en tjänst som upprättar en krypterad tunnel ut mot internet och som med enkla medel kringskär den trafikdata som behövs för att anmäla en misstänkt fildelare. I Frankrike har den så kallade Hadopi-lagen från 2009, som ger upphovsrättsinnehavare möjligheten att stänga av misstänkta fildelare från sina internetabonnemang, lett till ett stort uppsving för mjukvaror som skapar darknets.

Nätpolitiken flyttar in i cipherspace i syfte att återta kontrollen och undvika den panspektriska övervakningen. Att kringgå övervakning är en direktpolitisk handling som ställer den långsamma parlamentariska processen frågande inför nästa möjliga reglering. Att förvandla de distribuerade nätverken till cipherspace är bara en fråga om kunskap, och teknologin ligger redan i händerna på användarna.

8.

Till försvar för det öppna internet

Det har aldrig funnits någon given utvecklingslinje som visat hur den amerikanska militärens distribuerade datornätverk skulle komma att bli det brokiga landskap som vi idag kallar internet. Nätet omformas hela tiden; en fiberkabel kopplar plötsligt samman en fysisk plats med miljarder punkter på internet, ett globalt protokoll som TCP/IP får kontinenter att kommunicera med varandra, ett kulturellt uttryck förvandlas till ett globalt fenomen över en natt eller försvinner i översvämmande floder av data.

Vi lever i en tid då inte bara stora aktörer som politiker, företag eller framgångsrika aktivistgrupper står för omformandet av nätet, utan även de miljontals användare som går till näts och därmed intensifierar nätvaron. Mikroskopiska

händelser förändrar internets karaktär. En enda tunnel eller en enda koppling kan förändra ett händelseförlopp radikalt. En bild inifrån en diktatur, ett läckt handelsavtal från en korrupt regim, ett stycke programkod eller en vittnesbörd kan smitta och spridas som en löpeld mellan internets noder. Det främsta kännetecknet för det öppna nätet är att vi inte kan veta vad som kommer att hända imorgon.

Samtidigt finns det idag ett flertal processer som verkar i motsatt riktning. Man bygger murar i näten som effektivt stänger ute majoriteter av användarna. I öst och väst, nord och syd, införs ständiga regleringar av internet i form av direkta blockeringar riktade mot vad som kan tänkas vara samhällets fiender. Vilka dessa fiender sägs vara varierar givetvis kraftigt, men de fungerar i samtliga fall som en legitimerande grund utifrån vilken man söker rensa upp i det vildvuxna nätet. Eftersom internet hela tiden överskrider de lokala regimerna uppstår en chockartad paradox; den som betraktas som en fiende på ena sidan jordklotet är en frihetskämpe på den andra.

När människor möts och utbyter erfarenheter på internet skapar de en gemenskap som inte tidigare fanns, en solidariserande nätvaro. När gemenskapen plötsligt bryts upp av en utomstående kraft omvandlas nätvaron till aktivism.

De distribuerade nätverken utgör på ett grundläggande plan motsatsen till två av de dominerande maktformerna i de moderna samhällena: å ena sidan den territoriella och nationsbaserade staten, å andra sidan den industrikapitalism som bygger på produktion och konsumtion av slutprodukter. Nätverken överskrider de lagstiftande kropparnas territorier, men även deras hastigheter. När information kan förflyttas över jordens yta med ljusets hastighet låter den sig inte kontrolleras med mindre än att datornätverken

helt stängs av. Stater läcker; på ett konkret sätt i och med att filmer, bilder, texter och hemliga dokument kan leta sig ut och spridas, men även i form av kulturella utbyten och vänskapsrelationer. Det finns strikt sett inget svenskt internet – bara kopplingar från ett nät till ett annat – och det finns inte mycket den svenska nationalstaten kan göra åt det. Detta visar sig kanske som tydligast i sajten Wikileaks, som till både staters och företags förtret läcker ut tusentals politiska och juridiska dokument utan att röja sina källor – allt med hjälp av krypterade tunnlar i cipherspace.

De ekonomier vars slutprodukter är möjliga att digitalisera och försätta i ett fritt flöde i de distribuerade nätverken försöker just nu med lagstiftande medel begränsa dessa nätverk. Efter att branscherna i princip misslyckats med att ingripa mot de individer som kopierat filer, men även med att slå till mot dem som tillhandahållit länkar, söktjänster och nedladdningssajter, äger nu en process rum som syftar till att designa om nätverkens själva infrastruktur. Med globala handelsavtal, exempelvis ACTA och immaterialrättslig lagstiftning, försöker man återskapa en envägskommunikation ovanpå de distribuerade nätverken. Aktivister har kallat detta för "kabel-tv-internet", och avser med detta ett nätverk där konsument och producent separeras så att vissa protokoll – exempelvis bittorrent och IP-telefoni – stryps, och själva slutprodukterna – framför allt musik, film och mjukvara – förses med kopieringsskydd så att de endast kan konsumeras av en betalande och prenumererande kund. I förlängningen kan man tänka sig att hårdvaran, alltså själva datorn, börjar byggas om i syfte att efterlikna en simpel "mottagare" av information istället för en neutral paketförmedlande nod i nätverket.

Mot båda dessa processer uppbådar de distribuerade nätverken en stark motståndskraft. Men för att skapa ett

öppet internet räcker det inte med nätpolitisk gerillakrigföring. Nätverkens öppenhet måste även försvaras i mer generella termer i de arenor där andra gemensamma angelägenheter diskuteras. Såtillvida råder det ingen motsättning mellan teknoaktivism och andra politiska strategier. På samma sätt som teknologiska system kan hackas går det att intervenera i politiska processer varhelst de äger rum. Ett parlament, ett företag, en sakfråga eller en lokal angelägenhet – genom att gå in och ut genom det snabbaste kommunikationsmedium som världen hittills har skådat finns alltid möjligheten att göra ett ingrepp, öppna upp politikens svarta låda och förändra den.

När den amerikanska militärens distribuerade nätverk förenades med en annan banbrytande teknologisk innovation – persondatorn – skapades ett handlingsutrymme som gav människor politisk kraft. Det finns fortfarande aktörer som önskar att dessa två teknologier aldrig skulle ha fallit i händerna på en allt större del av mänskligheten. Vissa stater och företag skulle helst av allt vilja invertera utvecklingen och skapa enkelriktade datornätverk och maskiner som bara utförde speciella uppgifter, exempelvis spelade upp musik och film eller levererade redaktionell skrift.

Försvaret för de öppna näten skulle kunna ske med hänvisning till universella rättigheter. Dessa rättigheter må vara väl avvägda, kanske till och med sanna. Men rättigheter kan köras över lika lätt som de en gång formulerats. Därför måste de öppna näten praktiseras, vilket sker genom att vi blir en del av dem – vi blir nätvarande.

Denna praktik har inget att göra med bandbredden på ens uppkoppling eller antalet timmar man tillbringar framför datorn. I Xinjiang-provinsen i Kina har internet nästan stängts ned helt och hållet av regimen, som fruktar att

Twitter-meddelanden kommer att orsaka än mer politisk instabilitet i regionen. Människor tvingas resa i flera timmar för att skicka e-post på långsamma och delvis blockerade uppkopplingar. Dessa människor är minst lika nätvarande som de bredbandsanvändare i USA som distribuerar de senaste Hollywoodfilmerna till hundratals användare i en bittorrentsvärm. De sätts alla i rörelse och vinner politisk kraft med hjälp av internet.

När de öppna näten inte räcker till, när de begränsas av de upphovsrättsbaserade industriernas jakt på ”illegala fildelare” eller regimers jakt på politiska dissidenter, gräver nätaktivister tunnlar i nätverken och gör sig osynliga för den panspektriska blicken. Tunnlarna skapar veck mellan två punkter som gör att den som står mittemellan tappar kontrollen. Den mur som byggts för att förhindra informationsflödet faller samman. Nätvaron fortsätter i cipherspace, ett rum som sakta växer och förgrenas i nya världar.

De öppna nätverken måste försvaras genom nätpolitik i alla dess former. Internets fiender kan gå nätvaron till mötes på ytan eller i tunnlar, i domstolar eller i parlament, i mikroskopiskt lokala delar av nätverket eller i försök att reglera globala avtal mellan stater. Men internet går inte att stänga av, lika lite som människor går att stänga av. Varje övervakningsförsök kommer att bemötas med allt starkare kryptering. Varje avstängd nod kommer att leda till att noder multipliceras. Varje angrepp kommer att leda till att de nätvarande gör motstånd – med eller utan lagens godkännande.

9.

Epilog: Informationskrigets hastigheter

Internet uppstod inom ramen för det militärindustriella komplexet. Ironiskt nog är det just när de öppna nätverken ställs mot arméers informationskrig som själva tekniken och infrastrukturen blir föremål för diskussion. De distribuerade nätverkens yttersta intensitetspunkt vecklar ut sig precis i det moment då de är i färd att angripas. Bortom de annars så välfungerande tjänsterna och hemsidorna framträder protokoll, kablar och paranoida säkerhetsrutiner. Det är som om internets närvaro har integrerats i vår vardag till den grad att vi inte längre ser det som en teknologi – förutom när nätet kollapsar, och i synnerhet när någon försöker stänga ned det.

I slutet av maj 2010 styrde en konvoj bestående av sex skepp mot Gaza City, däribland det svensk-grekiska initia-

tivet Ship to Gaza. Syftet med flottiljen var att skicka förnödenheter och humanitär hjälp till de palestinier som försatts i blockad av Israel. Skeppen var med konventionella mått mätt obeväpnade, men ständigt uppkopplade mot internet via satelliter. Ju närmare Gazas stränder de kom, desto fler följde deras Twitter-meddelanden, bloggar och videoutsändningar. Fartygen hade blivit internet, och deras nätvaro delades av aktivister, underrättelsetjänster och journalister som analyserade varje meddelande som sändes ut.

***

Några månader tidigare hade Wikileaks, en sajt grundad av hackers och människorättsaktivister, släppt en videofilm från en amerikansk Apache-helikopter som visade hur obeväpnade Reuters-journalister dödades och två barn skadades allvarligt i Bagdad. Trots att den amerikanska militären hade krypterat videofilmen, och trots den rigorösa säkerhet som omger de militära datornätverken, hade videon läckt ut och Wikileaks lyckats dekryptera den. Dagarna innan den släpptes förberedde sig nätaktivister runt om i världen för att kunna bistå med ytterligare datorkapacitet i det fall att volontärerna som drev Wikileaks skulle gripas av de amerikanska myndigheterna. När videon lades upp på Youtube blev den dock omöjlig att avlägsna från internet. En hel svärm av datorer stod redan beredda att flytta ettor och nollor längs de distribuerade nätverken. Med endast några månaders mellanrum hade både aktivisterna på Gaza-konvojen och aktivisterna kring Wikileaks ställts ansikte mot ansikte med den militära informationskrigföringen.

***

Natten den 30 maj 2010 kokade Twitter av meddelanden med hashtaggarna #flottilla och #ShiptoGaza. Genom att Twitter-meddelanden från konvojen återpublicerades av nätvarande människor som följde händelseförloppet smittade varje uppdatering mycket snabbt, och själva rapporteringen på Twitter kunde på så sätt ligga flera timmar före de konventionella nyhetsmedierna. Detta skedde på vinst och förlust – varje hashtagg på Twitter kan genast infiltreras med desinformation som smittar lika snabbt. Erfarenheterna från valet i Iran och hashtaggen #IranElection hade i vissa fall varit brutala. Desinformation ledde till att de som protesterade på gatan hade försetts med instruktioner som vid tillfällen försatte dem i livshotande situationer.

Så länge det fanns en koppling till satelliterna 35 000 kilometer upp i rymden kunde nyheterna från skeppen förmedlas till internet i ett konstant flöde. Men plötsligt bröts signalerna. I efterhand rapporterade aktivisterna att deras satellitsignaler hade blivit utstörda av den israeliska militären, ett rimligt men obekräftat påstående. Den knapphändiga information som letade sig ut till nyhetsbyråerna måndagen den 31 maj gjorde gällande att mellan tio och tjugo personer hade dödats ombord det turkiska fartyget Mavi Marmara. Aktivisternas internetuppkoppling var bruten.

På bara några timmar hade demonstrationer anordnats i ett flertal städer, bland annat i Stockholm, Istanbul och London. Via Facebook, Twitter, sms och e-post spreds snabbt tid och plats för demonstrationerna. Internet hade stängts av ombord på båtarna, men omvärlden kunde fortsätta att kommunicera och mobilisera.

Vem som skulle bli den första att förmedla berättelsen

om vad som hände ombord på Mavi Marmara förvandlades till en fråga om att ta kontrollen över kommunikationsmedierna. Med satellitsändningarna utslagna och mobiltelefoner och videokameror beslagtagna kunde den israeliska armén göra sig till den enda aktör som förmedlade bilder och videoklipp från bordningen av skeppen. På samma sätt som aktivisternas Twitter-meddelanden hade återpublicerats av de traditionella medierna blev nu den israeliska arméns Youtube-kanal den primära källan för videofilmer, vars redaktionella kontroll togs om hand av militären.

***

Den som har de snabbaste vapnen skaffar sig ett omedelbart övertag i krig. Detsamma gäller informationskrig. Dagens öppna internet kan sända video i realtid till alla andra noder i nätverket. Men satelliter är känsliga på grund av att de sänder på särskilda radiofrekvenser och enkelt kan störas ut av en högteknologisk krigsmakt. Enskilda centraliserade tjänster är ömtåliga eftersom de enkelt kan blockeras eller beslagtas. För att internet ska kunna fungera i kritiska situationer måste kontrollen av tjänsterna återtas av användarna. Varje beroende av en central punkt gör kommunikationen sårbar.

Samtidigt som internets hastigheter ger oss möjligheten att mycket snabbt organisera demonstrationer och politiska möten, innebär vår nätvaro att vi medvetet eller omedvetet ger upphov till en databas och en övervakningsapparat som inte tidigare har existerat. På Facebook ger vi detaljerade personuppgifter till ett amerikanskt företag när vi organiserar demonstrationer, med datalagringsdirektivets implementering i Europa tillhandahålls exakt

positionering för alla mobiltelefoner som befinner sig på ett torg eller ett möte i ett hus. Panspektron drar nytta av relationen mellan nätpolitikens korttidsminne och arkivets beständighet; vi klickar i att vi kommer att närvara på en demonstration och glömmer genast bort vilka uppgifter som samtidigt lagras om oss. Men uppgifterna försvinner inte; Facebook, Twitter och din mobiloperatör kan, på eget bevåg eller under lagligt tvång, lagra databasen i princip hur länge som helst. Därmed upplåter vi vårt nätpolitiska liv till framtida aktörer.

Hur dessa aktörer kommer att behandla loggfilerna om tio år är det ingen som vet. På flygplatsen i Teheran har gränspolisen, enligt rapporter från exiliranier på besök, datorer för att söka i Facebook i syfte att ta reda på vem som har en vänskapsrelation med vem. I Egypten har de som organiserat och deltagit i demonstrationer via Facebook kunnat gripas eftersom de släppt ifrån sig detaljerad information.

***

I en tid när allt fler stater driver igenom lagar i syfte att övervaka internet finns dock ett undantag. Under bankkrisen på Island 2009 insåg ett antal medborgare att yttrande- och informationsfrihet var viktiga komponenter i avslöjandet av olika former av maktmissbruk. Tillsammans med bland annat Wikileaks utformade 19 isländska parlamentsledamöter lagförslaget Icelandic Modern Media Initiative, vilket röstades igenom den 15 juni 2010. Detta lagpaket går på tvärs med det som sker i de flesta demokratier i västvärlden. Det utgör troligtvis den starkaste lagstiftningen i världen gällande informationsfrihet. Bland annat garanterar den källors anonymitet, skyddar mot för-

handscensur och gör internetoperatörer fria från ansvar *för vad som skickas i deras nätverk. Det meddelarskydd* som i praktiken avskaffades i Sverige i och med FRA-lagen kan kanske komma att restaureras på Island, givet att lagen tas på allvar.

Händelserna utanför Gazas kust och i Reykjavik, Bagdad och Bryssel är alla sammankopplade. Internets hastigheter har gjort det möjligt för nätvarande människor att ta sig an politiska händelser och konflikter. Med eller utan staters godkännande kommer internet att fortsätta koppla ihop människor och förändra formerna för politiska motståndspraktiker. Förhoppningsvis kommer detta att underminera legitimiteten för blockering av sajter och övervakning av användarna till den grad att allt fler följer Islands exempel. En stat som inte kan hantera att människor kommunicerar fritt med varandra är inte en demokrati värd namnet.