Robin Hood in Cyberspace

Hacken, Nationalisme en Digitale Politiek

> This is our world now. The world of the electron and the switch, the beauty of the baud. We exist without nationality, skin color, or religious bias. You wage wars, murder, cheat, lie to us and try to make us believe it's for our own good, yet we're the criminals. Yes, I am a criminal. My crime is that of curiosity. I am a hacker and this is my manifesto. (...)You may stop me, but you can't stop us all (Uit *Hackers*, Moreu 1995).

Virtuele Stenen

Op 7 mei 1999 werd de wereld opgeschrikt door een bombardement van de NATO op de Chinese ambassade in Belgrado waarbij drie Chinese journalisten omkwamen. De VS verklaarden al snel dat het om een ongeluk ging. Dat woord – ongeluk – werd in China tandenknarsend tussen ironische aanhalingstekens geplaatst. Noch de overheid, noch de Chinese bevolking waren overtuigd van de onschuld van de VS. Het bombardement bracht voor het eerst sinds de studentenopstanden van 4 juni 1989 weer massaal de studenten op de been. Veel lopen was er niet eens bij, de universiteiten hadden bussen geregeld voor de studenten. Ditmaal was dan ook niet de communistische partij, maar de Amerikaanse ambassade het doelwit van de studentenprotesten. Stenen vlogen op die bewuste zaterdag 8 mei 1999 door de lucht, stenen die volgens wantrouwende westerse journalisten door de partij waren klaargelegd. Anders dan tien jaar terug zagen de studenten zich ditmaal wel gesteund door de partij, getuige de diplomatieke conflicten die volgden op het bombardement. De geest van het anti-imperialisme, waarvan de geschiedenis minstens valt te herleiden tot de Opiumoorlog (1840-1842), toen het Verenigd Koninkrijk de Chinese keizer op zijn knieën wist te dwingen, leek opnieuw te zijn ontsnapt uit de fles.

Stenen vlogen er ook over en weer in cyberspace in mei 1999. Deze virtuele stenen waren weliswaar minder stoffelijk, maar des te efficiënter. Het vermoeden bestond dat, net als de werkelijke stenen waren klaargelegd door de partij,

enkele hackers zelfs in dienst waren van de overheid (Gertz 1999). Het Witte Huis, de Amerikaanse ambassade in China en andere Amerikaanse overheidsdiensten vormden het doel van de Chinese hackers. De hackers veranderden afbeeldingen op de Amerikaanse sites, voegden slogans als 'down with the barbarians' toe, en legden het systeem van de Amerikaanse overheid tijdelijk lam door e-mail spam (Gertz 1999). Amerikaanse hackers sloegen met soortgelijke aanvallen op Chinese websites en netwerken terug. De aanval in cyberspace veroorzaakte onrust in Amerika, met name omdat het de kwetsbaarheid van het overheidsnetwerk blootlegde. Angstaanjagende scenario's, bekend van Hollywoodfilms als *Hackers*, waarin een hacker door middel van de computer miljoenen weet te stelen en olietankers kan laten zinken, lijken door dergelijke aanvallen dichtbij de realiteit te komen.

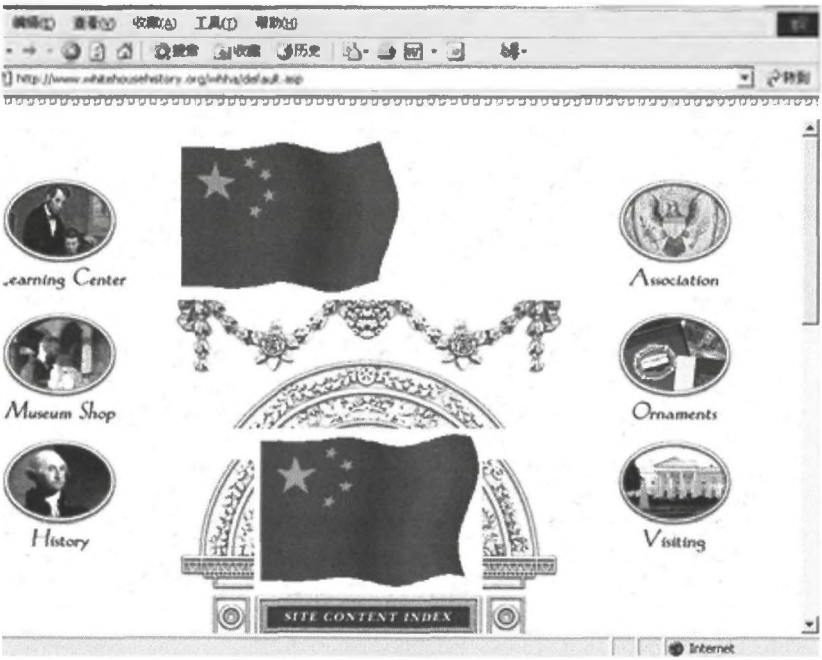
Twee jaar later herhaalde het gedroomde Hollywoodscenario zich wederom. In april 2001 botsten een verkenningsvliegtuig van Amerika en een Chinees vliegtuig tegen elkaar boven Chinees grondgebied, hetgeen de Chinese gemoederen danig beroerde. Naast de diplomatieke conflicten brak er wederom direct een oorlog uit op het web tussen Chinese en Amerikaanse hackers. Amerikaanse overheidssites hadden opeens de Chinese vlag, servers werden wederzijds geblokkeerd, en een wormvirus werd het web opgestuurd. De hacker Gao Jianfei maakte zich kwaad over het Amerikaanse imperialisme en verklaarde waarom hij, samen met de Red Hackers, mee heeft gevochten met de cyberoorlog (in Delio 2001):

> I am very angry. As a Chinese, I will not let anyone do this to my country. (...) This is a sign of American imperialism. Every Chinese who has any sense would not just sit there and watch this happen. And those of us who are capable of doing anything should do all we can. We stopped hacking activities against the Americans, but in the future we will rise up against anyone who dares to threaten our sovereignty.

De naam van de groep – Red Hackers – is indicatief voor de identificatie van de hackers met het communistische China. Was het voorheen de Rode Garde die de communistische ideologie verdedigde, nu zijn het de Rode Hackers die de nationalistische ideologie verdedigen. De naam verwijst naar de communistische heroïek van de culturele revolutie, die nu mondiaal zou worden voortgezet in cyberspace.

De site afgebeeld op figuur 1 is van het Witte Huis, die, na te zijn gehackt door Chinese hackers, opgesierd wordt met de Chinese vlag.

FIGUUR 1
Website van het Witte Huis, na te zijn gehackt op 30 April 2001 (Qiu 2002)

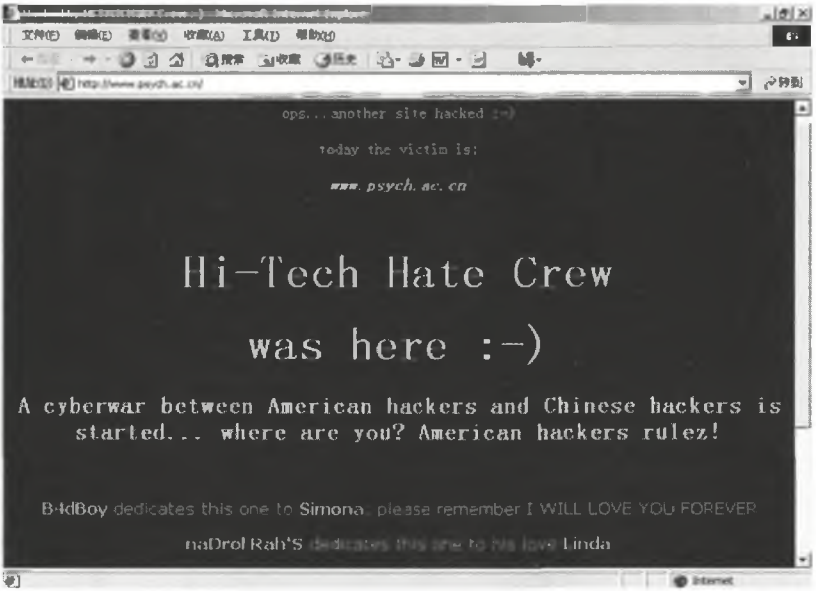


Het betreft hier een vrij onschuldig ogende actie, maar uit de woorden van hacker Xiao Yang blijkt dat de beoogde schade ernstiger kan zijn (Qiu 2002: 6):

> For [American] commercial sites, we only modify their webpages. But if they are public information networks that have wider influence, it's a rule that we have to erase some important documents like system files.

Figuur 2 laat het antwoord van Amerikaanse hackers zien. De tekst die ze geplaatst hebben op de site van de Chinese Academie voor Sociale Wetenschappen (de denktank van de Chinese communistische partij (CCP)) spreekt boekdelen: 'American hackers rulez.' Nationalisme vormt hier een cruciale voedingsbodem voor zowel de Chinese als Amerikaanse hackercultuur.

FIGUUR 2
Website van de Chinese Academie van Sociale Wetenschappen, na te zijn gehackt op 30 April 2001 (Qiu 2002).



Cyberspace wordt dikwijls geïnterpreteerd als een grenzeloze ruimte, waarin de politieke grenzen van de natiestaat oplossen in het Esperanto van de bits en bytes. Logischerwijs zullen degenen die het meest bedreven zijn in deze taal van de eenentwintigste eeuw – de hackers – zich het minst aantrekken van de oude grenzen. De quote uit *Hackers* aan het begin van dit artikel spreekt boekdelen: de hacker opereert buiten de gangbare kaders van nationaliteit, huidskleur of religie. De directeur van het Massachusetts Institute of Technology (MIT), Nicolas Negroponte, verwoordde zijn utopische visoen als volgt: 'Over twintig jaar zullen kinderen die het internet gebruiken niet meer weten wat nationalisme is' (De Wilde 2000: 9). Maar zowel Hollywood als de hoogleraar aan het MIT slaan de plank behoorlijk mis getuige het voorbeeld van de cyberoorlog tussen Chinese en Amerikaanse hackers. Chinese hackers identificeren zich juist sterk met China en trekken zich wel degelijk wat aan van nationaliteit. Het is deze frictie tussen de verbeelde grenzeloosheid van nieuwe technologie en de begrensde virtuele werkelijkheid die mij inspireert de hackercultuur onder de loep te nemen.

De lokalisering, en dan met name nationalisering, van de hackercultuur staat daarmee in dit artikel centraal. Ik zal me allereerst richten op de praktijk van het hacken, en de daaruit voortvloeiende identiteitspolitiek. Ik kijk daarbij met name naar de hackercultuur in China, en zal analyseren hoe deze zich verhoudt tot de hackercultuur van de VS – het land dat gezien wordt als het centrum van hacken. Hiertoe maak ik gebruik van studies over hacken alsmede van on linebronnen, met name de websites van hackergroepen en hun magazines. De culturele inbedding is cruciaal om de identiteitspolitiek van de Chinese hacker te begrijpen. Door de vermeende westerse wortels van nieuwe technologie in het algemeen en de hackercultuur in het bijzonder, zien de Chinese hackers zich gedwongen om op het Chinees aan het hacken te slaan. Daartoe putten zij uit de Chinese literaire geschiedenis. Ik maak hier ook een breder punt wat betreft de mondialisering van technologie: de imaginaire westerse origine van een technologische (sub-)cultuur dwingt mensen in 'niet-westerse' landen tot het ontwikkelen van lokale varianten. Dit punt sluit aan op het werk van Hannerz (1987), die in de context van Afrika spreekt over 'creolisering'. In een studie over de lokalisering (in zijn woorden: *indigenization*) van cricket laat Appadurai zien hoe de vermeende origine van een specifieke cultuur (in zijn studie het Engelse cricket, in mijn studie het Amerikaanse hacken) juist oproept tot een duidelijke culturele vertaalslag (Appadurai 1996: 89-113). In dit artikel geef ik voorbeelden van de Chinese vertaalslag van hacken (ofwel, de sinificatie) aan de hand van visuele en tekstuele componenten van websites en discussies die hierover in nieuwsgroepen worden gevoerd.

De cyberoorlogen tussen Chinese en Amerikaanse hackers zoals besproken laten zien dat met name de nationalisering van de technocultuur van hackers wel degelijk directe politieke gevolgen heeft. In het laatste deel van dit artikel zal ik trachten een kort overzicht te geven van de politieke implicaties van het hacken, die niet per definitie zijn gericht op de natiestaat. Het is mijn stelling dat de nationalistische cyberpolitiek van Chinese hackers voortkomt uit enerzijds hun grensoverschrijdende identiteitspolitiek, en anderzijds uit de drang en dwang tot lokalisering.

> Look, you wanna be elite? You gotta do a righteous hack. None of this accidental shit (*Phreak* in *Hackers*, Moreu 1995).

In teksten over nieuwe techniek en de opkomst van de informatie- of netwerksamenleving worden hackers meestal opgevoerd als technologische pioniers, whizzkids die met een pizzapunt in hun hand inbreken op een computernetwerk (de netwerkhacker) of een software programma herschrijven (de softwarehacker). Manuel Castells betoogt dat 'the theoretical understanding of [hacker] culture and its role as the source of innovation and creativity in informationalism is the cornerstone in our understanding of the genesis of the network society' (Castells 2001: 178). Zelf beschrijft Castells kort het belang van hackers gedurende de ontstaansgeschiedenis van het internet, maar de rol die hackers momenteel spelen blijft in zijn werk onderbelicht. Toch blijven hackers, zoals blijkt uit de introductie, actief, en keren zij telkens terug in zowel het nieuws (bijvoorbeeld wanneer een nieuw virus het web weer onveilig maakt) als in de populaire verbeelding (bijvoorbeeld in de Hollywoodproducties *War Games* (1983), *The Net* (1995), *Hackers* (1995) en *The Matrix* (1999)).

In teksten over de geschiedenis van hacking worden de eerste computerhackers getraceerd aan het MIT in de jaren zestig van de vorige eeuw. Teneinde de logge, grote en trage computers te verbeteren creëerden de programmeurs shortcuts (ofwel, hacks) die dikwijls het systeem verbeterden (Slatalla 2002). Er zijn bij deze groep 'hackers' nog geen duidelijke criminele connotaties, al speelt het belang van vrije informatievoorziening – en daaraan gekoppeld de kritiek op copyright – al wel een rol. Met de komst van de personal computer in de jaren tachtig heeft de hackercultuur een grote vlucht genomen. In die jaren beginnen de hackers zich te verenigen in collectieven, zoals bijvoorbeeld de Sherwood Forest, de Legion of Doom in de VS en Chaos Computer Club in Duitsland. Tot op de dag van vandaag zijn er over de hele wereld talrijke hackercollectieven, in China zijn er onder meer The Red Hackers en The Hackers Union of Hakka en in de VS de Cult of the Dead Cow en '2600'.

Wie zijn hackers en wat doen ze? Het plezier in technologie, en de wens deze naar je eigen hand te zetten is de eerste van een zestal indicatoren waar het volgens Jordan en Taylor (1998) bij het hacken om draait. De overige vijf indicatoren die zij onderscheiden zijn: geheimhouding (een ambivalent punt, je moet in het geheim hacken maar wil toch vooral gezien worden), anonimiteit (terugkomend in het gebruik van prozaïsche (groeps-) bijnamen (handles)), fluïditeit (het is een informele cultuur waar je soms wel en soms niet bij hoort),

masculien (de vrouwelijke hacker is moeilijk te vinden (zie ook Nordli 2002)) en, ten slotte, de voortdurende expliciete reflectie op de motivatie van het hacken, welke steeds ter discussie wordt gesteld op hun websites (samenhangend met het belang van de ethiek van het hacken). Thomas (2002) benadrukt in zijn boek over hackercultuur met name het subculturele aspect van hackers, en analyseert de grenzen die hackers trekken tussen hun eigen *boy culture* en *mainstream society*.

In deze studies komen de demografische indicatoren van de hacker naar voren: jong, mannelijk, stedelijk en intelligent; indicatoren die gemakkelijk, en dikwijls, worden vertaald in een beeld van de eenzame, sociaal incapabele *nerd* (Verton 2002). Thomas (2002: xiii) vat de dominante verbeelding van de hacker als volgt samen: 'The typical hacker is a white, suburban, middle-class boy, most likely in high school. He is also very likely self-motivated, technologically proficient, and easily bored.' Het is te verwachten dat de hacker ook jonger is geworden over de jaren heen, en dat het met name in China gaat om jongeren (volgens Qiu (2002: 2) voornamelijk studenten) uit de hogere lagen van de samenleving, gezien de benodigde financiële investeringen. Echter, belangrijker dan zulke indicatoren is de strijd over identiteit, en de voortvarendheid waarmee hackers van positie veranderen – een verandering die samenhangt met de onder hackers veelbesproken ethiek van het hacken.

Wat een hacker tot een echte hacker maakt is daarmee voortdurend onderwerp van discussie:

> The very definition of the term 'hacker' is widely and fiercely disputed by both critics of and participants in the computer underground. Indeed, because the term is so highly contested, it gives a clue to both the significance and the mercurial nature of the subculture itself. Moreover, there seems to be little agreement within the academic literature on what constitues hacking."(Thomas 2002: ix-x)

---

1 In een curieus artikel seksualiseert Risan de masculiniteit van hackers: 'Hacking is *really* a kind of sexual courtship. The identity games of hacking is a matter of producing sexual identities. (...) Hacking is a sublimated sexuality' (Risan 2002, cursief in origineel).

2 Voor een politieke versie van de ethiek van het hacken zie de website van Hacktivismo – het internationale karakter van de hackerbeweging blijkt uit het feit dat dit manifest beschikbaar is in diverse talen, waaronder Nederlands en Chinees. http://www.hacktivismo.com/news/modules.php?name=Content&pa=showpage&pid=17.

Parallel aan de voortdurende discussie over wie nu wel of niet een hacker is, loopt een uitgebreide typologie van soorten, met naast de hackers ook de *crackers* (degenen die moedwillig systemen vernielen), de ontwikkelaars van virussen en de *phreaks* (die inbreken in telefoonsystemen). Thomas (2002: 42-43) maakt onderscheid tussen de *white hat*- en *black hat*-hackers, de eersten streven naar verbetering van netwerkveiligheid, de tweeden zoeken naar de gaten in een systeem om daar vervolgens munt uit te slaan. Ook zijn er de *script kiddies*, degenen die de middelen kopiëren van andere hackers zonder echt te weten wat ze doen. Onder hackers geldt dit niet als een 'echte hack'. Ten slotte (maar dit overzicht van identiteiten is allesbehalve uitputtend) is er nog het al eerder genoemde onderscheid tussen de netwerk- en de softwarehacker.

Posities van hackers veranderen, en buitenstaanders noemen een hacker dikwijls een cracker, hetgeen onder meer blijkt uit het volgende citaat van de Hacktivismo website – een internationaal netwerk van hackers dat claimt te hacken uit politieke overtuiging (www.hacktivismo.com, bezocht op 29 januari 2003):

> One so-called Internet intelligence group [surely not those morons at iDefense?] referred to us as 'Black hat' hackers attempting to upgrade our public image. If we were Black hats we wouldn't need spin doctors, we'd need criminal attorneys. The cDc [Cult of the Dead Cow] and Hacktivismo aren't to everyone's taste. But attempting to vilify us because we defy simple categories is judgmental at best, and irresponsible at worst.

De opmerking dat hackers zich onttrekken aan simpele categorieën duidt al op een cruciaal kenmerk van de hackeridentiteit: het is een grensoverschrijdende identiteit. Niet alleen verschuiven identificaties, en kan een hacker op zondag de dag erop een cracker zijn, de verschuivingen gaan ook verder, de hacker ontwerpt overdag software voor, bijvoorbeeld, Microsoft, en hackt in de nacht een netwerk. De identificaties van hackers en de praktijken van het hacken zijn daarom permanent instabiel, hetgeen ook blijkt uit de volgende woorden van Plague in *Hackers* (Moreu 1995):

> Dade, I know how you might feel about narking on your friends, but, we're hackers. For us, there's no such thing as family and friends. We're each our own country, with temporary allies and enemies. I'd like to take a treaty with you.

Hackerculturen kenmerken zich door onvoorspelbaarheid en ongrijpbaarheid. Soms keren hackers zich tegen hun overheid, even later scharen zij zich weer achter diezelfde overheid en vechten ze over de grenzen van de natiestaat heen tegen hun Amerikaanse collega's. Dikwijls, maar niet per definitie, betreft het hier eenzelfde hacker. 'De hacker' lijkt daarmee op een technologische nomade, die tijdelijke verbanden aangaat die hem uitkomen, om vervolgens weer de overstap te maken naar wat voorheen als de vijand werd gezien. Om te spreken in de woorden van agent Smith, die hacker Neo in *The Matrix* (1999) verwijt twee levens te leiden (Wachowski & Wachowski 1997):

> It seems that you have been living two lives. In one life you are Thomas A. Anderson, program writer for a respectable software company. (...) The other life is lived in computers where you go by the hacker alias Neo, and are guilty of virtually every computer crime we have a law for.

Het grensoverschrijdende van hackers heeft niet alleen betrekking op de grenzen die worden getrokken (en bevochten) tussen, bijvoorbeeld, hackers en *crackers*, maar behelst tevens een letterlijke verwijzing: soms speelt de grens van de natiestaat geen rol, soms symboliseert die grens het doelwit van hackers (wanneer die inbreken op het netwerk van de overheid), en soms motiveert die grens de hacker tot het hacken van een andere natiestaat, over de 'eigen' grenzen heen.

De bindende elementen in het hackersvertoog zijn geheimhouding en vrije informatie, volgens Thomas (2002) zitten hackers als het ware gevangen in de frictie die tussen beide concepten bestaat. Geheimhouding door middel van codes en passwords is onderdeel van de ontwikkeling van de computer, een ontwikkeling waar hackers een belangrijke rol in spelen. In de woorden van Thomas (2002: 3): hackers 'are caught halfway between these two worlds. They acknowledge, but refuse to accept, the manner in which secrecy has become part of our daily routine. They are interested in the ways that technology and secrecy interface and how that combination can be explored, exploited, and manipulated to their own advantage.' Wat Thomas hier onderbelicht laat, en wat door een term als fluïditeit zoals voorgesteld door Jordan en Taylor (1998) eveneens aan het zicht ontsnapt, is dat hackers niet zozeer halverwege gevangen zitten tussen twee posities, maar juist dat ze zo makkelijk de grenzen overschrijden. Daarmee verdwijnt het belang van die grens niet, integendeel, maar de noodzaak tot een eenduidige keuze heeft plaatsgemaakt voor een meer flexibele identiteitspolitiek.

Deze politiek en de bijbehorende classificaties heeft zijn wortels in de expliciet in allerlei hackermanifesten terugkerende ethiek van het hacken. De ideologie van vrije informatievoorziening staat in deze ethiek centraal. Een studie van de Chinese hackers somt het als volgt op (Chen 2001):

> Although hackers today have different means, they have at least one thing in common: their purpose is accessing computers of others illegally, some of them keeping in mind the motto of their originators: Access to computers and hardware should be complete and total. Information wants to be free. Mistrust authority. You can create truth and beauty on a computer.

In een standaardwerk over hackers uit 1985 van Steven Levy (*Hackers – Heroes of the Computer Revolution*) vormt vrije toegang tot informatie, een wantrouwen jegens autoriteit en het plezier dat computers kunnen brengen de kern van de hackersethiek. Chinese hackers scharen zich, als we de teksten op de websites mogen geloven, vrijwel unaniem achter de mondiale ethiek van het hacken. Bij een opsomming van de ethiek staat weliswaar dat je vooral geen overheidscomputers moet hacken, een waarschuwing die in de Chinese context meer nadruk behoeft dan in het meer liberale VS, in het algemeen zijn Chinese hackers het erover eens dat hun ethiek toch gelijk is aan de Amerikaanse collega's (citaten van www.cnredmay.com, bezocht op 14 september 2002):

> In China, our *guoqing* (national spirit) is different from that of the US or other places. But, however different our nationalities or ethnic origins are, the ethics hackers observe should not differ too much.

> The aims of hackers are: there are more ways to computing, all information should be shared, free of charge; computing monopoly should be broken up. These are the guiding principles shared by all hackers.

De ethiek gaat samen met eerdergenoemde specifieke classificaties, de hacker is vooral geen *cracker*, de hackers zijn nobele helden die het netwerk beschermen, terwijl de *crackers* de schurken zijn die uit plezier vernietigen (citaat van www.cnredmay.com, bezocht op 14 september 2002):

> Everyone wants to be a hero. Gradually some people, under the banner of hacker, did some infamous things. Hackers call them crackers. They are ashamed of crackers. They refuse to be friends of crackers.

Echter, zoals de cyberoorlogen laten zien, ontpoppen hackers zich wel degelijk tot crackers, noch het lamleggen van een overheidsnetwerk noch het rondsturen van een virus passen in de 'echte' ethiek van het hacken. De heroïek van de hacker is allesbehalve statisch en eenduidig. De grens die de 'echte' van de 'niet-echte' hacker onderscheidt is weliswaar scherp getrokken, hij wordt alleen minder serieus genomen dan op het eerste gezicht lijkt.

Robin Hood en *Xiake*

De ethiek van het hacken heeft zijn (verbeelde) wortels in het westen, het is een ethiek die net als de BigMac van McDonalds moeiteloos lijkt te globaliseren. Maar hoe ver gaat die mondialisering van de hackercultuur? Met de snelle opkomst van computertechnologie in China gedurende de jaren negentig – inmiddels staat China met 46 miljoen gebruikers derde in de wereld wat betreft internetgebruik, na de VS en Japan (*The Economist* 2003) – heeft de hacker zijn intrede in China gedaan. Een reflectie op de vertaling van het woord hacker maakt duidelijk hoe Chinees de Chinese hacker is. De Chinese hacker heet *heike*, hetgeen ten eerste een monofoon is. Tegelijkertijd staat *Hei* voor zwart, en *ke* voor gast, een zwarte gast dus, hetgeen de illegaliteit van de hacker benadrukt. Maar dit gaat gepaard met een flinke dosis romantiek, nationale trots en literaire geschiedenis. Het karakter *ke* komt van het literaire genre *xiake*: de ridderlijke verhalen vol heldendom. Ridderlijk is een term die niet geheel de lading dekt – een van de weinige *xiake* adepten die het westen heeft gehaald is de film *Croaching Tiger Hidden Dragon*. Indicatief is de volgende beschrijving van de Chinese hacker (citaat van www.cnredmay.com, bezocht op 14 september 2002):

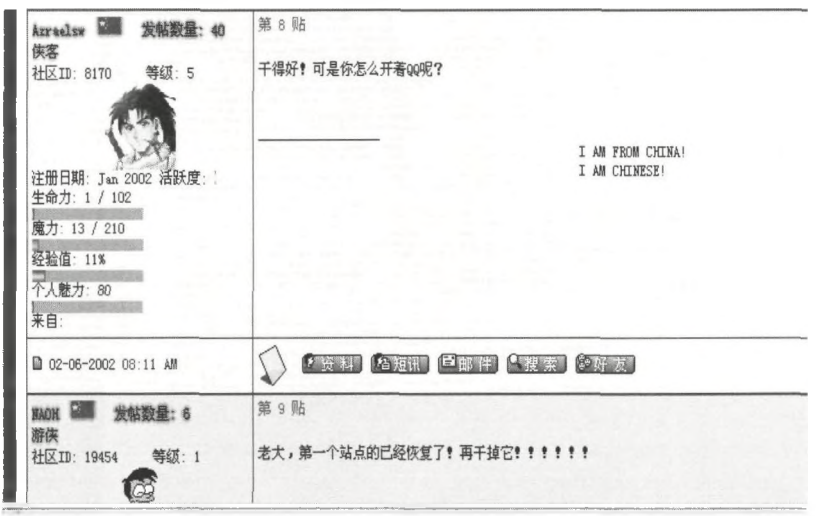
> Hackers (...) are holding their swords, travelling thousands of miles, accomplishing swordsman's deeds in *jiangwu* (*hengxia jiangwu*). They are beyond regulations, making fun of the net, offering the cold, stringent cyberspace a touch of carefree and playful spirit.

---

3 Er is hier duidelijk sprake van wat binnen technologiestudies aangeduid wordt als *leapfrogging*: juist door het overslaan van de beginstadia van technologieontwikkeling is het mogelijk om opeens een voorsprong te nemen op degenen die nog werken op verouderde apparatuur.

De Chinese hacker is als een moderne Robin Hood, ontdaan van zijn Engelse kledij, om te verschijnen in een respectabele Chinese outfit. De ridderlijke verwijzingen zijn niet specifiek Chinees, de naam van de eerder genoemde Sherwood hackersgroep verwijst naar het bos waar Robin Hood opereerde, net zoals hackers ook veelvuldig verwijzen naar de fantasiewereld van *In de Ban van de Ring* (Turkle (2002) spreekt over 'Lord of the Hackers').[4] Echter, deze mondiale articulatie van ridderlijke heroïek wordt ingepast in een specifiek Chinees genre. Een blik op de website van de Cnhacker.com (figuur 3) laat zien hoe de hackers de verwijzingen naar de *xiake*-romans die al besloten liggen in het woord *Heike* waar maken, en daar ook nog een contemporaine nationalistische laag aan toevoegen. De site betreft een discussie over een Japanse site die na te zijn gehackt weer is gerepareerd en laat ook een oproep zien om hem weer snel terug te hacken.

FIGUUR 3
Website CN.hacker (bezocht op 15 september 2002)



4 Nederland mist dergelijke ridderlijke helden, hacker en oprichter van XS4ALL Rob Gonggrijp noemt hackers de Pietje Bells van Cyberspace (Poppe 2002).

De cartooneske avatars die de hackers gebruiken dragen namen die verwijzen naar karakters uit de Chinese ridderromans. De communistische vlag komt voor bij iedere posting, en de slogan in het Engels 'I am from China! I am Chinese!' maakt duidelijk hoe belangrijk de Chinese identiteit is voor de hackers. Websites zijn vaak donker, hebben een wat duistere sfeer, als een fantasiewereld die past bij het *xiake*-genre. Deze fantasiewereld heet *Jianghu* in het Chinees. Net zoals Deng Xiaoping sprak over een socialisme met Chinese karaktertrekken, zo zien we hier de wens te hacken met Chinese karaktertrekken. Op de site van de China-eaglegroep zijn forums gericht op geschiedenis, cultuur en het leger – drie domeinen die het hacken niet alleen sinificeren, maar ook nog eens de nationalistische connotaties onderstrepen. De slogan van de China-eaglegroep spreekt boekdelen (Qiu 2002: 4):

> We are the eagles of China
> We are China's elite
> Hard as it is, the enemy's shield
> We will show them our sharpness

Ten slotte, op de site van de China-hackergroep (www.chinahacker.net, figuur 4) zien we in klassieke archaïsche Chinese karakters (de stijl van de karakters kan gezien worden als een directe verwijzing naar de vermeende oude en rijke cultuur van China) de tekst 'Chinese drakengroep netwerkveiligheid unie' (*Zhongguo long pai wangluo anquan lianmeng*).

Niet alleen positioneert de groep zich hiermee als nobele, *white hat*-hackers, zowel de stijl van de karakters als de verwijzing naar de draak – het klassieke Chinese symbool – onderstrepen wederom dat hier om *Chinese* hackers gaat.

Aldus, om een echte hacker te zijn in China moet je er een Chinese kleur aan geven. Om echt te zijn – en het discours van authenticiteit is cruciaal hier – om niet een domme copycat van Amerika te worden moet je hacken op zijn Chinees. Dit komt niet alleen terug in de visuele aspecten van de websites, maar vormt ook een onderwerp van discussie onder de Chinese hackers. De volgende quotes zijn illustratief (citaten van de website van de patriottische rode hackers www.cnhunker.com, bezocht op 15 september 2002):

> Hacking culture originated from the States and Europe, bearing their specific historic and social backgrounds. It's definitely not only a technological issue. Our *guoqing* (national spirit) is different from the States.

> If we want to create our hacking culture, inevitably we have to incorporate certain non-technological factors such as nationalism.

De slogan onder aan de site van de CNHUH (Hacker Union of Hakka (de Hakka zijn een minderheidsgroep in China)) stelt: 'Aan alle hackers van de wereld, laten we samen een netwerk – grote muur bouwen' (www.cnhuh.com, bezocht op 15 september 2002).

FIGUUR 4
Website China Hackergroep (bezocht op 15 september 2002)

Deze slogan is indicatief voor de paradox van het Chinese hacken: Het betreft hier een mondiale cultuur die haar verbeelde wortels in het westen heeft, en precies daarom is er de drang tot lokaliseren. Vandaar de referentie naar de grote muur, een symbool dat staat voor China als de tulp en de molen staan voor Nederland. Dit alles wijst op een belangrijk punt betreffende de mondialisering van technologie: de harde taal van de bits en bytes mag dan wel dezelfde zijn in Beijing als in New York, de context waarin deze taal wordt gehanteerd is niet identiek. Dit leidt ertoe dat de Chinese hacker een ander

visueel en tekstueel idioom gebruikt om zijn identiteit (on-line) vorm te geven. De drijvende kracht achter de lokalisering van de Chinese hackercultuur vormt de vermeende origine van het hacken: het westen (of, meer specifiek, de Verenigde Staten). Om te voorkomen dat je slechts een goedkope kopie bent van de 'echte' – en dus Amerikaanse – hacker, is het van belang om op zijn Chinees te hacken. Deze drang (en dwang onder het toeziend oog van het westen) tot lokalisering speelt veel minder in niet-Amerikaanse westerse hackerculturen. Op de Nederlandse websites van hackers, bijvoorbeeld, is er geen discussie over wat nu de Nederlandse elementen van het hacken zijn, terwijl zo'n discussie wel prominent aanwezig is bij de Chinese hackers. De Nederlandse hacker kan zich zonder problemen spiegelen aan zijn Amerikaanse collega, dat maakt hem niet tot een goedkope copycat. De Chinese hacker ziet zich geplaatst voor een groter dilemma, teneinde zijn authenticiteit te waarborgen kan hij zich niet straffeloos onderdompelen in een mondiale ideologie van vrijheid en anarchisme. Natuurlijk hangt het belang van de nationale identiteit ook samen met de rol die het desbetreffende land speelt op het wereldtoneel, China is immers een veel groter en machtiger land dan Nederland. Echter, de westen versus niet-westen tegenstelling speelt een cruciale rol in de globalisering van cultuur, het is te verwachten dat ook in de hackerculturen van, bijvoorbeeld, Duitsland en Frankrijk, de drang tot lokalisering aanmerkelijk zwakker zal zijn (zie ook De Kloet 2001). De vermeende westerse origine van hacken noopt tot een Chinese vertaalslag, zoals ik heb laten zien. Deze vertaalslag kan soms, ten tijde van politieke conflicten, wel degelijk leiden tot oorlogen op het www.

Digitale Politiek

> Quark: The Matrix is a euphemism for the government.
> SUPERASTIC: No, The Matrix is the system controlling our lives.
> TIMAXE: You mean MTV.
> SUPERASTIC: I mean Sega.
> FOS4: ALL HAIL SEGA!!!
> Uit het script van *The Matrix* (Wachowski & Wachowski 1997).

Aan het begin van dit artikel ben ik reeds ingegaan op een belangrijke politieke component van het hacken: de cyberoorlogen tussen Amerikaanse en Chinese hackers. Naast de vs zijn ook Indonesië, Taiwan en Japan het doelwit geweest van Chinese hackers. Op deze momenten scharen desbetreffende hackers zich

achter de ideologie van de natiestaat, en handelen als een illegale handlanger van de overheid. Hardnekkige geruchten gaan dat hackers ook door de overheid worden ingezet om de diplomatieke conflicten in cyberspace te ondersteunen, door bijvoorbeeld de Free Tibetgroep te hacken (Leyden 2002). De Chinese overheid ontkent dit, en stelt dat ze ten alle tijde de activiteiten van hackers afkeurt. Zeker is dat de meeste Chinese hackers onafhankelijk van, en bij tijd en wijle tegen, de overheid opereren. Terwijl Qiu (2002) Chinese hackers voornamelijk in een nationalistisch kader plaatst (en de voorbeelden die ik tot dusver heb gegeven sluiten daar goed bij aan), ziet de auteur van een artikel in *The Economist* (23 januari 2003) Chinese hackers juist als digitale strijders voor vrijheid en democratie. Het gemak waarmee hackers van positie veranderen maakt beide interpretaties van Chinese hackers valide. Teneinde duidelijker zicht te krijgen op de politieke implicaties van de hackercultuur is het van belang om de diverse politieke arena's waarin hackers opereren beknopt in kaart te brengen.

Soms is de overheid het doelwit van de activiteiten van hackers. Maar dezelfde hackers zijn dikwijls evengoed actief in de internationale digitale gevechten. Wan Qun, bijvoorbeeld, had dertig Amerikaanse sites gehackt in de cyberoorlog van het voorjaar in 2001 voordat hij de bakens verzette om zich te richten op de lokale overheid in de provincies *Hubei* en *Fujian*. Hij verving de namen van partijbonzen op websites in, bijvoorbeeld, 'idioot', en veranderde communistische afbeeldingen in pornoplaatjes. De politie kwam Wang op het spoor en arresteerde hem (Qiu 2002: 6). De flexibele identiteitspolitiek van Wan Qun is duidelijk: we zien hier hoe eenzelfde hacker eerst een cyberridder was die de grenzen van de natiestaat verdedigde, om zich vervolgens te ontpoppen als een politieke dissident op eigen bodem.

In hun gevecht tegen de Chinese overheid hebben de *Hong Kong Blondes* technische ondersteuning gekregen van de Amerikaanse *Cult of the Dead Cow*. Oxblood Ruffin van de *Cult of the Dead Cow* beschrijft de *Blondes* als volgt (in Thomas 2002: 97):

> The Blondes are currently monitoring government networks and gathering data to be shared with other activists .(...) They would also be prepared to disrupt government/military networks in retaliation of any egregious human rights violation. (...) As to the risks involved, they are rather apparent: death, relocation, and loss of employment for family members, etc.

Lemon Li, een hacker van de *Blondes* is inderdaad opgepakt in China. Dit voorbeeld laat zien hoe hackergroepen wereldwijde allianties aangaan.

Hackers richten zich lang niet altijd op de overheid, met name in het westen zijn hackers actief in gevechten tegen, bijvoorbeeld, multinationals (door bijvoorbeeld het Shell-logo te vervangen) en softwarebedrijven als Microsoft (om de website www.hacktivismo.com (bezocht 29 januari 2003) te citeren: 'What do you call a software company that does business with the worlds largest sponsors of terrorism and human rights abuse? Profitable'). De collagemethode van hackers, waarbij afbeeldingen op websites worden aangepast, wordt ook wel culture-jamming genoemd en reflecteert een bredere trend in populaire cultuur waarin massamediale visualisering steeds belangrijker wordt (Kuipers 2002). Ook instanties als de wereldbank en de World Trade Organisation vormen vaak het doelwit van hackers. De laatste is door de hackergroep de *ehippies* aangevallen tijdens de Seattle bijeenkomst in 1999. Door middel van e-mail spam werd het netwerk van de WTO tweemaal lamgelegd en gedurende de hele conferentie werd het netwerk ernstig vertraagd (Jordan 2002: 122). Ten slotte strijden hackers vaak voor digitale vrijheid. De *Cult of the Dead Cow* heeft bijvoorbeeld *Peekabooty* ontwikkeld, een groep die, met de verklaring van de rechten van de mens in haar hand, strijdt tegen censuur op het internet. Met name China, waar de overheid door middel van zogenaamde *fire walls* niet gewenste informatie weert van het nationale web, wordt bekritiseerd door *Peekabooty*. Daartoe is een netwerk opgezet dat wars van firewalls gebruikt kan worden en waarmee, bijvoorbeeld, Chinese internetgebruikers toch de gewenste CNN-site kunnen bezoeken. *Peekabooty* tracht zodoende nationale grenzen in cyberspace te ondermijnen (Jordan 2002: 128-130).

Jordan (2002: 119) schaart deze activiteiten tegen instanties en bedrijven onder de noemer hacktivisme, dat hij definieert als: 'Politically motivated hacking. Hacktivism is activism! (sic.) running free in the electronic veins that enliven our 21st-century, global socio-economies.' Terwijl de strijd tegen de eigen overheid eveneens onder hacktivisme geschaard wordt, zijn de nationalistische digitale riders opmerkelijk afwezig in studies over hacktivisme, hetgeen duidt op een zekere romantische, utopische lezing van de hackercultuur.

Het beeld dat naar voren komt uit deze beknopte en onvolledige opsomming van de politiek van hackers is gefragmenteerd en veelzijdig. Hackers opereren, dikwijls parallel, in diverse politieke arena's. Van belang in de context van dit artikel is niet zozeer de observatie dat hacken een sterke politieke dimensie heeft, duidelijk is in ieder geval dat een idyllisch subcultureel verhaal van macht en verzet waarin de hackers de nobele ridders van cyberspace zijn een te romantisch beeld geeft van hackerculturen. Interessanter is de verwarrende identiteitspolitiek die naar voren komt in dit verhaal. Op het ene moment strijdt de Chinese hacker tegen zijn Amerikaanse collega, op het

volgende moment helpt die collega hem de Chinese overheid te hacken. De Chinese hacker breekt in bij het softwarebedrijf waar hij even later zal werken. Het is deze instabiele identiteit die de politiek van het hacken voedt. De nationalistische dimensie van hacken komt precies daar tot uiting waar de grensoverschrijding van de hacker overlapt met de drang en dwang tot lokalisering.

Conclusie

Juist omdat hackers in China – een opkomende politieke en economische macht – zich geplaatst zien buiten het centrum van moderne technologie (het westen, en dan met name de VS), bestaat er, zoals ik heb beargumenteerd, de drang (en dwang) tot lokalisering. Dit geldt in veel mindere mate voor hackers in, bijvoorbeeld, Europa, die immers nog altijd westers zijn, net als de technologie waarop zij hun identiteit bouwen. De Chinese hacker is telkens weer op zoek naar een Chinese hackerstijl. En juist op het moment dat de hacker de grenzen van de natiestaat overschrijdt, wanneer hij zijn pijlen richt op zijn collega's in de VS of Japan, dan krijgt zijn hacktivisme een sterke nationalistische lading. Om een eerder citaat te herhalen: 'We're each our own country, with temporary allies and enemies.' Op momenten dat de Amerikaanse hacker het doelwit vormt, trekt de Chinese hacker zich terug achter de veilige grenzen van de nationale identiteit, hij is dan voor even boven alles een *Chinese* hacker. Om zich wat later niets van China aan te trekken en zich te verliezen in technologisch spel. Dat spel is niet grenzeloos, net zomin als techniek onafhankelijk opereert van de culturele context. Het spel is wel grensoverschrijdend, en juist dat maakt de hacker ongrijpbaar, angstaanjagend en daarmee een dankbare bron voor de verbeelding, getuige de rol die hackers spelen in het nieuws: Cyberterroristen die enge virussen rondsturen (de toenemende onrust over de mogelijke subversieve politieke rol van hackers blijkt ondermeer uit het Amerikaanse rapport van Arquilla & Ronfeldt (2001)); en in Hollywood: Cyberschurken die banken leegroven dan wel helden die ons bevrijden van de allesoverheersende nieuwe technologie.

Wat mijn studie naar hackers uiteindelijk laat zien is dat techniek allesbehalve koud en abstract is, integendeel, fervente gebruikers als hackers eigenen zich de taal van de bits en bytes toe, transformeren haar naar de eigen specifieke culturele context en spelen ermee, om van hacker te verworden tot cracker, tot dissident, of tot digitale nationalist. De drang en dwang tot lokalisering van nieuwe technologie in China, welke te herleiden valt naar de imaginaire

Amerikaanse origine, gekoppeld aan de grensoverschrijdende identiteitspolitiek van hackers voeden een specifieke, nationalistische stijl van hacken. De hacker is een technologische nomade die als een spiderman het world wide web afreist, maar ondanks het imago van digitale vrijbuiter is hij wel degelijk met handen en voeten gebonden aan de grenzen van de natiestaat. De nieuwe technologie is niet in alle opzichten grenzeloos, net zomin als de taal van de bits en bytes het Esperanto van deze eeuw is.

Literatuur

Appadurai, A. (1996) *Modernity at Large. Cultural Dimensions of Globalization*, Minneapolis: University of Minnesota Press.

Arquilla, J. & D. Ronfeldt (eds.) (2001) *Networks and Netwars. The Future of Terror, Crime and Militancy*, RAND Netwars Series. Santa Monica: RAND.

Castells, M. (2001) 'Informationalism and the network society', epiloog in P. Himanen, *The Hacker Ethic*, pp. 155-178, New York: Random House.

Chen, X. (2001) *Zhongguo Heike (Chinese Hacker)*, Beijing: *Minzhu Yu Jianxie Chubanshe.*

Delio, M. (2001) 'Is this World War III?', *Wired* (29 August), at www.wired.com/news/, retrieved 29 August 2001.

Economist, The (23 January 2003) *Caught in the Net*, At www.economist.com, retrieved 29 January 2003.

Gertz, B. (May 16, 1999) 'Chinese Hackers raid U.S. computers', *The Washington Times.*

Hannerz, U. (1987) 'The World in Creolisation', *Africa*, 57 (4): 546-559.

Jordan, T. & P. Taylor (1998) 'A Sociology of Hackers', *The Sociological Review*, 46 (4): 757-780.

Jordan, T. (2002) *Activism! Direct Action, Hacktivism and the Future of Society*, London: Reaktion Books.

Kloet, J. de (2001) *Red Sonic Trajectories. Popular Music and Youth in Urban China*, Unpublished PhD Thesis, Amsterdam: University of Amsterdam.

Kuipers, G. (2002) 'Media culture and internet disaster jokes – Bin Laden and the attack on the World Trade Center', *European Journal of Cultural Studies*, 5 (4): 450-470.

Leyden, J. (25 September 2002) 'China implicated in Dalai Lama hack plot', *The Register USA*, at www.theregus.com/content/6/26433.html, retrieved 17 October 2002.

Levy, S. (1984) *Hackers. Heroes of the Computer Revolution*, New York: Anchor Press.

LoBaido, A. (1999) 'The Beijing hack attack. Hong Kong based cyber warriors build anti-China techno army , *Worldnetdaily.com*, retrieved 7 January 2003 at http://www.worldnetdaily.com/news.

Moreu, R. (1995) *Hackers*, Film script, New York: United Artists. At www.tempt.gts.nsk.su/scripts/hackers.html, retrieved 15 January 2003.

Nordli, H. (2002) *The Net is Not Enough. Searching for the Female Hacker*, Unpublished PhD Thesis. Oslo: NUST.

Poppe, I. (2002) *Hippies from Hell*, Documentary, Amsterdam.

Qiu, J. (2002) *Chinese Hackerism in Retrospect. The Legend of a New Revolution Army*, retrieved 30 October 2002 at http://www.mfcinsight.com/products/iframe/article/020917/oped2.pdf.

Risan, L. (2002) *Hackers Produce More than Software, They Produce Hackers*, At http://folk.uio.no/lrisan/linux/identity_games, retrieved 2 December 2002.

Slatalla, M. (2002) *A Brief History of Hacking*. At http://tlc.discovery.com/convergence/hackers/articles/history_print.html, retrieved 15 January 2003.

Thomas, D. (2002) *Hacker Culture*, Minneapolis: University of Minnesota Press.

Turkle, S. (2002) 'Lord of the Hackers', *The New York Times*, March 7.

Verton, D. (2002) *The Hacker Diary. Confessions of Teenage Hackers*, Berkeley: McGraw-Hill.

Wachowski, A. & L. Wachowski (1999) *The Matrix*, Film script, Burbank: Warner Bros.

Wilde, R. de (2000) *De voorspellers. Een kritiek op de toekomstindustrie*, Amsterdam: De Balie.