

Karatzogianni, Athina (2005) The politics of cyberconflict: ethnoreligious conflicts in computer mediated environments. PhD thesis, University of Nottingham.

**Access from the University of Nottingham repository:**  
<http://eprints.nottingham.ac.uk/12112/1/423635.pdf>

**Copyright and reuse:**

The Nottingham ePrints service makes this work by researchers of the University of Nottingham available open access under the following conditions.

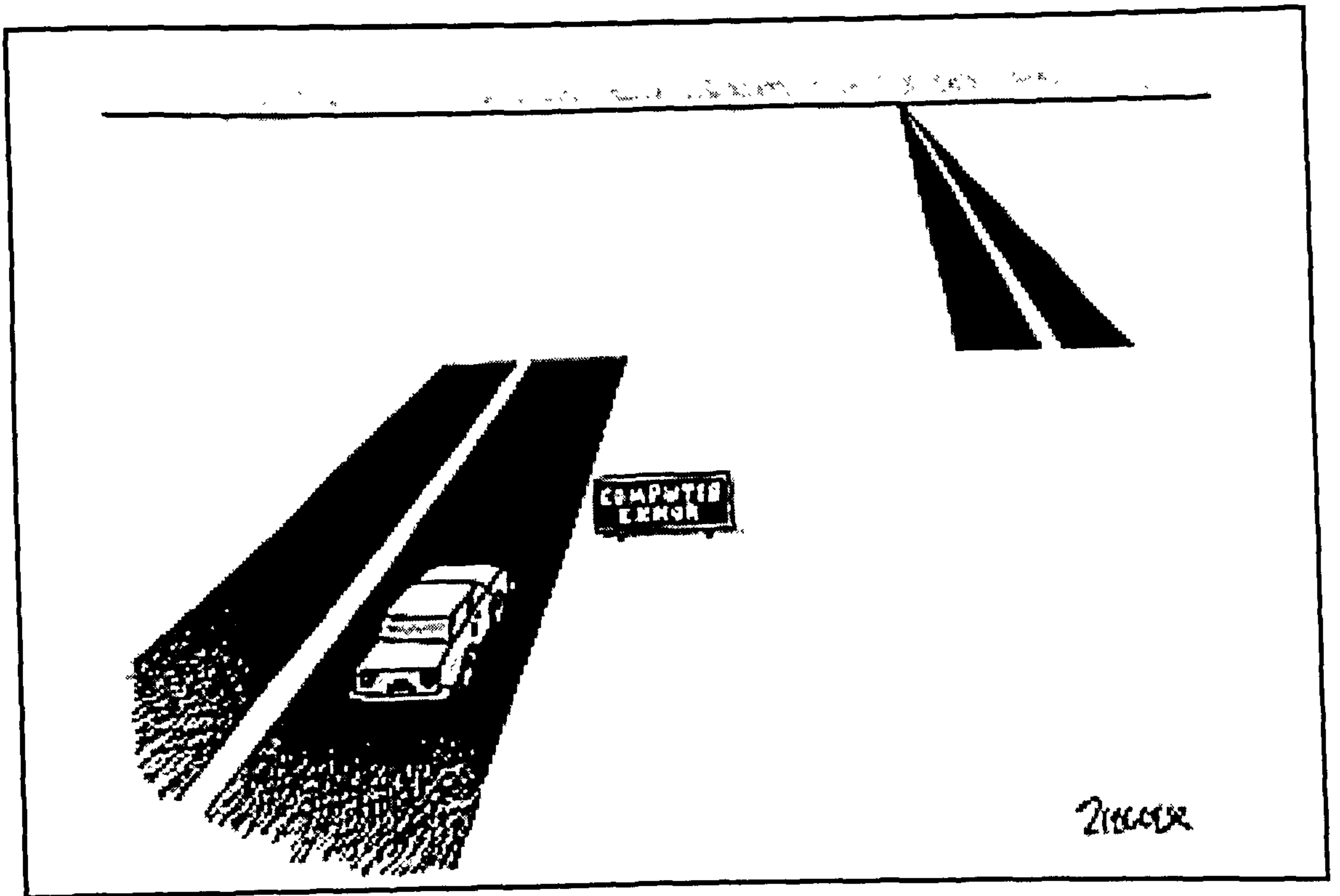
- Copyright and all moral rights to the version of the paper presented here belong to the individual author(s) and/or other copyright owners.
- To the extent reasonable and practicable the material made available in Nottingham ePrints has been checked for eligibility before being made available.
- Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.
- Quotations or similar reproductions must be sufficiently acknowledged.

Please see our full end user licence at:  
[http://eprints.nottingham.ac.uk/end\\_user\\_agreement.pdf](http://eprints.nottingham.ac.uk/end_user_agreement.pdf)

**A note on versions:**

The version presented here may differ from the published version or from the version of record. If you wish to cite this item you are advised to consult the publisher's version. Please see the repository url above for details on accessing the published version and note that access may require a subscription.

For more information, please contact [eprints@nottingham.ac.uk](mailto:eprints@nottingham.ac.uk)



**'The Politics of Cyberconflict: Ethnoreligious and Sociopolitical Conflicts in Computer Mediated Environments'**

by Athina Karatzogianni

Thesis submitted to the University of Nottingham for the degree of Doctor of Philosophy, last revised October 2005



## Table of Contents

<b>‘THE POLITICS OF CYBERCONFLICT: ETHNORELIGIOUS AND SOCIOPOLITICAL CONFLICTS IN COMPUTER MEDIATED ENVIRONMENTS’ .....</b>	<b>1</b>
<i>Table of Contents</i> .....	2
<b>ACKNOWLEDGEMENTS .....</b>	<b>6</b>
<b>GLOSSARY .....</b>	<b>7</b>
<b>INTRODUCTION .....</b>	<b>14</b>
<b>CHAPTER 1: HOW TRADITIONAL CONCEPTS AND ISSUES FIT INTO A GLOBAL POSTMODERN MEDIUM. ....</b>	<b>17</b>
1.1 POLITICAL MOVEMENTS AND THEIR USE OF THE INTERNET .....	19
1.2 INTERNET POLITICS: DEMOCRACY, PARTICIPATION, POWER .....	28
1.3 THE GLOBALISATION-INTERNET CONNECTION.....	85
1.4 A POSTMODERN MEDIUM? .....	95
<b>CHAPTER 2: THE THREE THEORIES.....</b>	<b>122</b>
2.1 SOCIAL MOVEMENT THEORY.....	122
2.2 CONFLICT THEORY.....	163
2.3 MEDIA THEORY. ....	179
2.4 DERIVING AN INTEGRATED FRAMEWORK FOR CYBERCONFLICT .....	196
<b>CHAPTER 3: THE ENVIRONMENT OF CYBERCONFLICT .....</b>	<b>210</b>
3.1 INFORMATION WARFARE .....	214
3.2 INTERNET SECURITY ANALYSIS: INCIDENTS AND RESPONSES .....	243
3.3 SOCIOPOLITICAL IMPLICATIONS.....	257
<b>CHAPTER 4: SOCIOPOLITICAL CYBERCONFLICTS .....</b>	<b>270</b>
4.1 SOCIOPOLITICAL CYBERCONFLICTS.....	270
4.2 CHINESE DISSIDENTS .....	284
4.3 INTERNET CENSORSHIP INTERNATIONALLY .....	317
<b>CHAPTER 5: ETHNORELIGIOUS CYBERCONFLICT.....</b>	<b>340</b>
5.1 ETHNORELIGIOUS CYBERCONFLICTS .....	340
5.2 ETHNIC CYBERCONFLICTS .....	364
5.3 IS THE INTERNET A TOOL FOR CONFLICT RESOLUTION OR AN ESCALATING FACTOR? ...	369
<b>CHAPTER 6: THE EFFECTS OF THE INTERNET ON THE 2003 IRAQ WAR .....</b>	<b>383</b>
6.1 THE INTERNET’S ROLE IN THE ORGANISATION OF ANTI-WAR PROTESTS .....	386
6.2 THE INTERNET’S EFFECT ON MEDIA COVERAGE.....	394
6.3 THE IMPACT OF THE WAR ON THE INTERNET ITSELF.....	414
<b>CONCLUSION .....</b>	<b>425</b>
<b>BIBLIOGRAPHY.....</b>	<b>440</b>
<b>WEB SOURCES:.....</b>	<b>468</b>

**Paginated  
blank pages  
are scanned  
as found in  
original thesis**

**No information  
is missing**





## **Abstract**

This thesis argues that it is important to distinguish between two different phenomena in cyberpolitical spaces: First of all, between ethnic or religious groups fighting over in cyberspace, as they do in real life (Ethnoreligious cyberconflict) and second, between a social movement and its antagonistic institution (Sociopolitical cyberconflict). These different kinds of cyberconflict can be explained in the context of international conflict analysis for ethnoreligious cyberconflict and social movement theory for sociopolitical cyberconflict, while keeping in mind that this takes place in a media environment by using media theory. By combining elements of these approaches and justifying the link to cyberconflict, it is possible to use them as a theoretical light to look at the environment of Cyberconflict (CC) and analysis of incidents of CC. Consequently, this work looks at the leading groups using the internet either as weapon or a resource against governments, while also looking at networks, international organisations and new social movements. Searching for a satisfactory theoretical framework, I propose the following parameters to be looked at while analysing cyberconflicts:

1. Environment of Conflict and Conflict Mapping (real and virtual). The world system generates an arborescent apparatus, which is haunted by lines of flight, emerging through underground networks connected horizontally and lacking a

hierarchic centre (Deleuze and Guattari). The structure of the internet is ideal for network groups, (a global network with no central authority) has offered another experience of governance (no governance), time and space (compression), ideology (freedom of information and access to it), identity (multiplicity) and fundamentally an opposition to surveillance and control, boundaries and apparatuses.

2. Sociopolitical Cyberconflicts: The impact of ICTs on: a. Mobilising structures (network style of movements using the internet, participation, recruitment, tactics, goals), b. Framing Processes (issues, strategy, identity, the effect of the internet on these processes), c. Political opportunity structure (the internet as a component of this structure), d. hacktivism.
3. Ethnoreligious Cyberconflicts: a. Ethnic/religious affiliation, chauvinism, national identity, b. Discourses of inclusion and exclusion, c. Information warfare, the use of the internet as a weapon, propaganda and mobilisational resource d. Conflict resolution depends on legal, organisational framework, number of parties issues, distribution of power, values and beliefs.
4. The internet as a medium: a. Analysing discourses (representations of the world, constructions of social identities and social relations), b. Control of information, level of censorship, alternative sources, c. Wolsfeld: Political contest model among antagonists: the ability to initiate and control events, dominate political discourse, mobilise supporters, d. Media effects on policy (strategic, tactical, and representational).

## **Acknowledgements**

First and foremost, I am utterly indebted to my family Magdalene, George and Manos whose persistence, confidence and character, I attempted to breathe into this work.

I would especially like to thank my supervisor Prof. Ian Forbes, for motivating me to pursue my passion for the subject and for showing patience, encouragement and understanding.

I am also grateful to the School of Politics and its people at the University of Nottingham and above all my friends in the A1 research room, for swapping ideas and critiques with me over the past three years. This cannot but include my students and their fresh and intimate way of looking at global politics.

Lastly, this work would have been far less enjoyable without the help and hindrance of virtual, real and imaginary friends, mentors and co-travellers. This thesis is dedicated to them.



## **Glossary**

*Avatar:* Among people working on virtual reality and cyberspace interfaces, an avatar is an icon or representation of a user in a shared virtual reality.

*Authentication:* Verifying that a person is known to you.

*BBS:* Bulletin Board Systems

*Blogs:* Short for a weblog, an online journal that can turn anyone with Internet connection into a mini-media outlet.

*CMC:* Computer Mediated Communication

*Cracker:* One who breaks security of a system. Coined in 1985 by hackers in defence against journalistic misuse of hacker.\*

*Cyberattacks:* Attacks in cyberspace like defacements, worms and viruses.

*Cyberconflict:* Political conflict in computer mediated environments. Takes two forms: ethnoreligious (two ethnic or religious groups fighting it out in cyberspace

as they do in real life) and sociopolitical (social movements against antagonistic institutions).

*Cyberdemocracy:* The promise of nearly unlimited information delivered to your monitor in mere seconds is the promise of a better democracy.

*Cyberdissidents:* Dissidents fighting against authoritarian governments online using emails, file-trading, BBS and spamming e-magazines.

*Cyberjihad or e-jihad:* The online equivalent of Islamic fundamentalist jihad.

*Cybernation:* A nation whose communication of commonly held beliefs and philosophies is affected by the Internet or similar mechanisms.

*Cyberpower:* It is the form of power that structures culture and politics in cyberspace.

*Cyberpunks:* A movement or fashion trend associated especially with the rave/techno subculture.\*

*Cyberspace:* Notional 'information space' loaded with visual cues and navigable with brain computer-interfaces.\*

*Cyberterrorism:* Computer-based attacks intended to intimidate or coerce governments or societies in pursuit of goals that are political, religious or ideological.

*Cyberwar:* Refers to a more 'heavy' mode of new military conflict like destruction of the enemy's infrastructure through information technology.

*C4ISR:* Command, Control, Communications, Computing, Intelligence, Surveillance and Reconnaissance.

*Defacement:* The destruction of a web page on the Internet.

*Distributed Denial of Service attacks (DDoS):* DDoS attacks employ armies of 'zombie' machines (insecure server compromised by a hacker who places software on it that can launch an overwhelming number of requests, rendering the site inoperable).

*Domain Name Service attacks (DNS):* Domain name servers are the 'Yellow Pages' that computers consult in order to obtain the mapping between the name of a system and the numerical address of the system. If the DNS provides an incorrect numerical address for a website then the user's system will connect to the incorrect server. An attacker can disseminate false information this way and prevent access to the original site (Vatis,2001).

*E-government:* Government initiatives to provide online government services and civic information.

*Email petitions:* Petitions that contribute to electronic activism in their capacity for getting the word out of dates and times of organised protests, demonstrations and co-ordinated activities.

*Flaming:* To post an email message intended to insult and provoke.\*

*Gopher or archie servers:* Gopher presents a menuing interface to a tree or graph of links; the link can be to documents, runnable programmes or other gopher menus arbitrarily far across the net.\*

*Hacker:* Connotes a computer virtuoso who enjoys exploring the details of programmable systems and how to stretch their capabilities, one who programs enthusiastically, even obsessively.\*

*Hacktivism, online activism or electronic activism:* Takes two forms: When hackers attack virtually chosen political targets and when persons organise through the Internet or carry through email a political message.

*IVDA:* Individual Virtual Direct Action.



*ICT:* Information Communication Technologies

*Information warfare or cyberwarfare:* sustained terrorist information warfare strategies are the ongoing deliberate efforts of an organised political group against the military, industrial, civilian, and government economic information infrastructures or activities of a nation, region, organisation of states, population or corporate entity (Erbschloe).

*Internet Filtering:* Preventing viewers from viewing certain web content.

*IRC:* Internet Relay Chat.

*Malware:* Malicious code programmes.

*MVDA:* Mass Virtual Direct Action.

*Netwar:* Refers to information age conflict at the less military, low intensity, more social end of the spectrum conflict.

*Network-centric warfare:* platforms are the eyes, ears and fists of a broader entity.

*ISP:* Internet Service Provider.

*Ping saturation:* Denial of service attacks where a target computer is overwhelmed with ping requests.

*Proxy Server:* A server that sits between a client application, such as a web browser and a real server. It is used to improve performance or filter requests. In cyberconflict, it allows a user to access blocked sites, not through a system controlled by the government.

*Script kiddies:* They do mischief with scripts and programs written by others, often without understanding the exploit

*Spamming:* To mass email unrequested identical email messages, particularly advertising; to crash a program by overwhelming a fixed size buffer with excessively large input data.\*

*SPIN:* Segmented, polycentric, ideologically integrated network.

*Swarming:* Occurs actors spread over great distance, electronically converge a target from multiple directions, a tactic different from the traditional form of attack in waves, which delivers a knock out blow from a single direction on the Internet.

*UNIX:* Refers to the Unix operating system, an interactive timesharing system. Unix has become the most widely used multi-user general purpose operating system and since 1996 the variant Linux has been at the cutting edge of the open source movement.\*

*USENET:* From Users' Network: A Distributed bulletin board system supported mainly by Unix machines.\*

*Virtual Community or cybercommunity:* An online community with common beliefs who never meet each other that will move them to fight, believe or even love their cyebrcommunity.

*Virtual March:* When protesters bombard the switchboard of an organisation with calls and emails.

*Virtual Sit-In:* Activists download a page aiming to flood the server.

*Virus:* Most viruses are worms, which are enabled by 'buffer overflows'. Buffer overflow is an event in which more data is put into a buffer (computer holding area) than the buffer has been allocated.

Asterisks (\*) indicate that the definition is taken from *The online hacker Jargon*

*File 4.1.0*, last updated 27/10/03

## **Introduction**

The thrust of this analysis is to disclose the extent to which the internet has affected politics and political conflict in particular (cyberconflict) and provide a theoretical framework for explaining this phenomenon. The aim of the thesis is to first theoretically and then empirically locate and introduce the new issues confronting global politics today due to the impact of new communication technologies.

The structure of the thesis reflects this strategy. In the first chapter I feel my way into some of the main features of internet politics (social movements, power, participation, democracy, globalisation) in a form of a literature review, with the central argument that the political game remains traditional, despite of the use of a postmodern medium. Since the literature did not examine political conflicts manifest on the internet, I thought such study was urgently required to come to grips with the consequences of the use of this technology by political actors and groups. This leads to chapter 2, where in order to explain the empirical evidence of 'cyberconflict', I propose the integration of elements of social movement, conflict and media theories to a single analytical framework for cyberconflict. To understand cyberconflict we must examine the technical environment where this takes place (internet security, information warfare) and its sociopolitical implications. This I do in chapter 3.



Searching for a satisfactory description of empirical cases of cyberconflict led to the use of a classification between two types of cyberconflict: sociopolitical and ethnoreligious. In the following three chapters I examine cases of different types of this classification. Chapter 4 looks at the sociopolitical cyberconflicts: social movements, dissidents against governments and internet censorship in different countries. Chapter 5 examines examples of ethnoreligious cyberconflicts and the possibility of conflict resolution. I then turn to my last empirical chapter 6, where I discuss and analyse the internet's role in the organisation of anti-war protests during the Iraq 2003 conflict, its effect on media coverage and the impact of the war on the internet itself. In the conclusion of all the empirical chapters, I single out which of the variables mentioned in the integrated theoretical framework can be linked to the empirical examples outlined. In the concluding chapter 7, I summarise the most important arguments and findings this thesis brings forward.

In terms of methodology, the research is conducted on the following levels:

*Textual:* Review of internet political literature and main political concepts, social movement, conflict, media theory literatures and information warfare and internet security texts.

*Theoretical:* The use of the three theories is justified theoretically and the elements considered being crucial for cyberconflict analysis are integrated to a single theoretical framework.

*Empirical:* The study uses more than 300 articles and web sources (secondary sources) to locate examples of cyberconflict.

*Analytical:* Components of the proposed integrated theoretical framework are linked with the empirical evidence while examining these examples, attempting to prove the applicability of it to cyberconflict.

## **Chapter 1: How traditional concepts and issues fit into a global postmodern medium.**

Faces of Israelis and Saudis and Iraqis, detailed charts of military hardware, reports from over decorated generals, from people with strange accents and from points all over the world, a barrage of images and information, packaged in easy-to take portions, punctuated by commercial breaks where powerful fantasies flow by too quickly -the world has truly been faxed, cabled, express delivered.<sup>1</sup>

The field of my research is politics on the internet and more precisely how political conflict manifests itself on the internet. In the face of different approaches on internet politics, my aim is to analyse these approaches, indicate what the problems are and outline how my work fits into this background. The problem in politics this chapter will address is how new social movements use a postmodern medium like the internet to achieve traditional political goals, such as democracy, power and participation in an era of globalisation.

In political terms, the internet is viewed as a vehicle for educating individuals, stimulating citizen participation, measuring public opinion, easing citizen access to government officials, offering a public forum, simplifying voter registration

---

<sup>1</sup> Poster, M: (1995) *The Second Media Age*, Polity Press: Cambridge, p. 159

and even facilitating actual voting. It has been termed a powerful technology for grass roots democracy and one that by facilitating discussion and collective action by citizens, strengthens democracy. It also has been called potentially the most powerful tool for political organising in the past fifty years. The underlying purpose of this chapter is to demonstrate that while the demands of the groups using the internet remain traditional and modern in their characteristics, the medium itself is postmodern serving modernist ends.

It is important to understand what the central political aims of groups using communication technologies are, why and how they use them and to what effect. With this in mind, in this chapter we navigate through the literature, building a platform from which to embark on a study of cyberconflict and its meaning for new communication politics.



## 1.1 Political movements and their use of the internet

Social movement theory is particularly relevant to this research, because many of the groups using the internet have social movement characteristics, for example the Zapatistas movement in Mexico.<sup>2</sup> The internet is much cheaper than other broadcasting media, is not sufficiently censored yet to impede its use by diverse groups and has a potential worldwide audience, facilitating a successful new way for social movements to carry their message to a much greater audience. However, the issue is that what these groups struggle for, in the final analysis, are traditional modernist concepts like democracy, participation and above all power, which are going to be examined in that order in the next sections, in order to understand if these concepts remain traditional, when they are linked to a postmodern medium, such as the internet. Characteristically, Daniel Nugent asks of the Zapatista movement: 'How can the EZLN move beyond the politics of modernity when their vocabulary is so patently modernist and their practical organization so emphatically premodern?'<sup>3</sup> Taylor and Jordan in their work *Hacktivism* distinguish between two kinds of rights sought after by the Zapatistas:

---

<sup>2</sup> For more information see Ronfeldt, D, Arquilla J, Fuller, G.E, Fuller, M: (1998) *The Zapatista Social Netwar in Mexico*, Rand Corp: California. An exciting quote is the following : 'Meanwhile, the EZLN called on Mexican civil society - not other armed guerillas, but peaceful activists - to join with it in a nationwide struggle for social, economic, and political change, without necessarily taking up arms. The EZLN also called on international organizations (notably, the Red Cross) and civil actors (notably, human rights groups) to come to Chiapas to monitor the conflict. This was not at all a conventional way to mount the insurrection' (pp.2-3).

<sup>3</sup> Daniel Nugent (1995) in Ronfeldt, D, Arquilla J, Fuller, G.E, Fuller, M: (1998) *The Zapatista Social Netwar in Mexico*, Rand Corp: California

The primary demands of the Zapatistas are for health, welfare and citizenship rights... In this struggle, the Internet functions as a medium through which the demands for these rights and the struggles around these rights can be communicated. Information rights appear here as almost a second political order, serving the 'first order' rights to health, welfare and full citizenship.<sup>4</sup>

When basic interaction and networking is primarily conducted via the net, time and space no longer restrain individual engagement. In this respect, the density of a movement's targeted social group which has been portrayed as the major element in fabricating organised action has to be redefined. Politics outside governmental boundaries in non-governmental organisations (NGOs) or more broadly in social movements will also be restructured by shifts in information commodification. Most commonly discussed in this context is the Zapatista revolt in Mexico, where what initially looked like a guerrilla war quickly became a media war. Instead of fighting in the jungles, though there has been fighting and deaths, the Zapatistas used their weapons to create media events. On the day that the North American Free Trade Agreement (NAFTA) which was signed by Mexico, Canada and the USA came into effect as a free trade zone, the Zapatistas occupied an area of the Chiapas region in Mexico. When the army arrived, they withdrew to the rainforests. They successfully created such a media event that they were able to force the Mexican government into negotiation and avoid a full-

---

<sup>4</sup> Taylor, P.A and Jordan, T: (2004) *Hacktivism and Cyberwars: Rebels with a cause?*, Routledge: London, p. 97



scale war. They did this by full use of the new possibilities for information flow including the internet.<sup>5</sup>

Cyberspace offers a medium in which people can interact and coordinate their actions without relying on a face-to-face contact.<sup>6</sup> A thriving example of this is the anti-globalisation movement whose participants organise heavily through the net. Dissident political groups can now have a voice that is very difficult for governments to silence. Such groups have been able to mobilise support, in order to facilitate dialogue between such groups and their governments, such as happened for example between the Sendero Luminoso (Shining Path) and the Peruvian government.<sup>7</sup> Everard mentions that the lead-up to recent Indonesian elections and the subsequent overthrow of the Suharto regime saw the internet become an active player as Indonesians sought alternative sources of information, while the authorities tightened media controls. The left-wing People's Democratic Party went underground after they were blamed by Indonesian authorities for a riot in Jakarta in July 1996. They continued to respond to accusations in internet discussion lists. Activist groups are increasingly turning to the internet and other electronic media to provide information on their activities and on the activities of the opposite side. A similar thing happened in 1997 in Sri Lanka, when the government launched a national website to counter the Tamil Tigers, who have been fighting a long civil war to establish a homeland for Tamils in Sri Lanka.

---

<sup>5</sup> Jordan, T: (1999) *Cyberpower: The Culture and Politics of Cyberspace and the Internet*, Routledge: London, p.166.

<sup>6</sup> Tsagarousianou, R, Tambini, D and Bryan, C (eds.): (1998) *Cyberdemocracy: Technology, Cities and Civic Networks*, Routledge: London, p.8.

The Tamil Tigers had set up their own website giving their side of the dispute. Sri Lanka officials said their website will 'help in countering anti-Sri Lanka propaganda by enabling Internet surfers worldwide to have access through a single window to authentic news and information on Sri Lanka'.<sup>8</sup> In the Philippines in the late 1990s, media and political history was made by using SMS technology or texting in helping bring down former president Estrada.

Nevertheless, such political implications of the internet were not the first to be picked up by researchers. Early internet literature focused on issues of hacking, encryption and the use of the internet by extremist groups. It is nonetheless important to mention some of the main concerns expressed, if we are to understand the issues arising from the application of the internet in our every day lives.

Denning and Baugh commented on the international issue of encryption:

Law enforcement agencies have encountered encrypted email and files in investigations of pedophiles and child pornography, including the FBI's Innocent Images national child pornography investigation. In many cases the subjects were using Pretty Good Privacy to encrypt files and email...We were told of another

---

<sup>7</sup> Everard, J: (2000) *Virtual States*, Routledge: London, p.158

<sup>8</sup> Margolis, M and Resnick, D: (2000) *Politics As Usual*, Sage: London, p.20



case in which a terrorist group that was attacking business and state officials used encryption to conceal their messages.<sup>9</sup>

To this effect, Barrett brings a good point to our attention, when he asserts that the internet can support global chains of pyramid letters, anonymous hate mail, offensive graffiti and a range of other 'anti-social' activities:

Just as fraudulent traders are provided with the potential to operate from 'data havens', so too are political agitators and even terrorists afforded havens from which to criticise government policies - either our own or our allies' - from within the shelter of the UK, protected by anonymous ftp servers, by complicated cross-posting articles, or by the use of dial in access to some other country's machines. In early 1996 for example, plans of the British Army's establishment in Northern Ireland were published on the Internet.<sup>10</sup>

On the extremists' use of the internet, Rathmell argues that the most remarked upon users of Information and Communication Technologies (ICTs) have been right wing militias in the USA, Islamist opposition movements originating in the Middle East and single-issue pressure groups such as environmental activists or human rights campaigners.<sup>11</sup> However they may differ in aims, membership or ideology, all of these groups have been quick to exploit ICTs for propaganda and psychological operations. Many insurgents, from the provisional IRA through

---

<sup>9</sup> Denning and Baugh in Thomas, D and Loader, B (eds.): (2000) *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*, Routledge: London, p.108.

<sup>10</sup> Barrett, N: (1996) *The State of the Cybernation*, Kogan Page: London, p.203.

Mexico's Zapatistas to Lebanon's Hizbollah, have incorporated ICTs into their more traditional propaganda and fund-raising activities. They have websites as well as newspapers. But they do not appear to have supplemented their kinetic attacks, using bullets and bombs, with cyberattacks. Whine writes as follows: 'The German authorities express increasing concern about the Internet. They have noted the growth of far right home pages, from 30 in 1996 to 90 in 1997 and the manner in which football hooligans were mobilised during the 1998 football World Cup series by German Nazis via their websites'.<sup>12</sup>

Also in July 2002 right-wing extremists looking for converts appeared to be trying to subvert the anti-globalisation movement, using at least one intentionally confusing website and even showing up at major protests to recruit activists directly. In response to this move the Anti-Defamation League went on the offensive against a site of the 'Anti-Globalism Action Network' (g8activist.com), which could easily be accessed by mistake by those intending to visit the G8 Activist Network.<sup>13</sup> In December of the same year, the North Rhine-Westphalia state in Germany required internet providers to block two US-based neo-Nazi websites after a court ruled the measure did not violate the provider's rights. The providers were to appeal to a higher state court and threatened to leave the state for other German states that do not have limiting regulations.<sup>14</sup> A tough approach on net hate speech has also been taken by the Council of Europe, which has

---

<sup>11</sup> Rathmell in Thomas, D and Loader, B (eds.): (2000) *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*, Routledge: London, p.230.

<sup>12</sup> Whine in Thomas, D and Loader, B (eds.): (2000) *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*, Routledge: London, p.237.



passed a provision which updates the European Convention on Cybercrime, criminalising internet hate speech, including hyperlinks to pages that contain offensive content. In contrast with the Americans - the council cited a report finding that 2,500 out of 4,000 racist sites were created in the US - many European countries have existing laws outlawing internet racism.<sup>15</sup> European States have also set up the European Network and Information Security Agency set to begin in January 2004 and last until Dec 2008, with a budget of \$28.7 million. The agency would work on problems such as preventing network failures, computer crashes, viruses and unauthorised interception on communications, advising the EU institutions on information security matters.<sup>16</sup>

Extremist groups use the internet because it is cheap. For the price of a computer and a modem an extremist can become a player in national and world events. ICTs lower the threshold for participating in illegal acts and without state or other backing extremists will look for cost-effective instruments. Furthermore, ICTs act as a force multiplier, enhancing power and enabling extremists to punch above their weight. They can now have a reach and influence that was previously denied to them. Tragically, Helsinki experienced a transfer of activities on the net to real life late 2002, when a 17-year old boy in an internet chat room dealing with explosives was held for questioning in a deadly bombing at a suburban shopping

---

<sup>13</sup> Kettman, S: 'Make hate not globalization', wired, 13/7/02

<sup>14</sup> Associated Press: 'Frankfurt: Nein to neo-Nazi sites', 20/12/02

<sup>15</sup> Scheeres, J: 'Europeans outlaw Net hate speech', wired, 9/11/02

<sup>16</sup> Pruitt, S: 'EU approves creation of cybersecurity agency', IDG News service, London Bureau, 9/10/2003

mall. The teenager had contacts with a 19-year old, Peri Gerdt, suspected of making and planting the explosive device that killed him and six others.

To sum up, some political actors are denied access to traditional political means. Information and communication technologies (ICTs) provide new opportunities. The question is how do these new technological possibilities affect the political situation. With the emergence of this new technology, political actors have unlimited access to easier and cheaper means of political communication, such as the internet. Instead of using traditional means like election campaigns or public relations, the groups that use the internet are able to communicate messages to a wider audience than that reached by more traditional means of political communication. These new technological opportunities affect the political situation in various ways. Political communication becomes more mechanised, it is instant and cheaper and new groups previously excluded can take part in a political situation without feeling excluded through the new technology. The groups that use ICTs affect the political situation in that they put forward new rules of the game, the rules of new technology. As a result, traditional political means are less effective and need to adjust to these new technological possibilities. The use of ICTs and the internet in particular, provide endless opportunities to groups that are otherwise excluded from traditional political communication. This does not mean, however, that new social movements, like anti-globalisation, anti-capitalist or antiwar movements, when using the Internet to communicate political goals ask for anything that is not traditionally modern in



character like participation, democracy or power. The nature of the medium does not appear to affect the essentially modernist nature of the game. Lastly, what this first impression points to is that two types of actors use the internet for political purposes: sociopolitical movements and extremist or ethnoreligious groups like the ones mentioned above.

## 1.2 Internet politics: Democracy, participation, power

### *Democracy in internet politics*

In order to discuss the connection between democracy and the internet, it would be useful to include a conceptualisation of the term 'democracy', before we apply a political theory of democracy to our internet research. The internet brings forth new types of participation in government, thus challenging the traditional type of democracy, where new forms of power configurations can exist between communicating individuals. Arguably, information is the lifeblood of democracy. Keeping this in mind, can we speak of a new politics on the internet or is democracy a traditional term left unaltered by the postmodern realities of the new medium?

In the contemporary world democracy can only be fully sustained by ensuring the accountability of all related and interconnected power systems, from economics to politics. These systems involve agencies and organisations, which form an element of and yet often cut across the territorial boundaries of nation-states. This is how Held views it: 'The possibility of democracy must, accordingly, be linked to an expanding framework of democratic institutions and procedures - to what I have called the cosmopolitan model of democracy'.<sup>17</sup>

---

<sup>17</sup> Held, D: (1995) *Democracy and the Global Order*, Polity Press: Cambridge, p.267

Held makes three important points: First, the way processes of economic, political, legal, military and cultural interconnectedness are changing the nature, scope and capacity of the sovereign state from above, as its regulatory ability is challenged and reduced in some spheres; secondly, the way regional and global interconnectedness creates chains of interlocking political decisions and outcomes among states and their citizens, altering the nature and dynamics of national political systems themselves; and thirdly, the way local groups, movements and nationalisms are questioning the nation-state from below as a representative and accountable power system (see also the following discussion on social movement theory in 2.1). Democracy, as Held argues, has to come to terms with all three of these developments and their implications for national and international power centres.

In the same context, the hierarchical structure of the state system itself has been disrupted by the emergence of the global economy, the rapid expansion of transnational relations and communication, the economic growth of international organisations and regimes, and the development of transnational movements and actors - all of which challenge its efficacy. With the spread of the internet, there is scope for a newly international localism that is finding expression in 'virtual' communities, with some people going so far as to suggest that a new global cyberstate is forming.<sup>18</sup> There also signs that online communities will offer further

---

<sup>18</sup> See the concept of cybernation in Barrett, N: (1996) *The State of the Cybernation*, Kogan Page: London.



dimensions to personal identity within an already complex world. The problem with this, is that it is extremely doubtful that these changes will ultimately undermine the notion of sovereignty. According to Everard, people still live within a physical location and the idea of cybersovereignty falters, as it fails to think through the place of the body in cyberspace.<sup>19</sup> However, it can be argued that his view is rather limited considering more recent challenges facing states particularly undemocratic ones, which I discuss in section 4.2 and 4.3 below.

To continue with Held, the cosmopolitan model would seek the creation of an effective transnational legislative and executive, at regional and global levels, bound by and operating within the terms of the basic democratic law.<sup>20</sup> This would involve the creation of regional parliaments (for example, in Latin America and Africa) and the enhancement of the role of such bodies where they already exist (the European Parliament), so that their decisions become recognised in principle as legitimate independent sources of regional and international regulation. Accordingly, Held writes:

Those seeking to advance greater equity throughout the world's regions, peaceful dispute settlement and demilitarization, the protection of human rights and fundamental freedom, sustainability across generations, the mutual acknowledgement of cultures, the reciprocal recognition of political and religious

---

<sup>19</sup> Everard, J: (2000) *Virtual States*, Routledge: London, p.63

<sup>20</sup> Held, D: (1995) *Democracy and the Global Order*, Polity Press: Cambridge, p.272



identities, and political stability across political institutions are all laying down elements essential to a cosmopolitan democratic community.<sup>21</sup>

In conjunction, Held is right to argue that democracy has an appeal as the 'grand' or 'meta-political' narrative in the contemporary world, because it offers a legitimate way of framing and delimiting the competing 'narratives' of the good. This is particularly important, because it holds out the prospect of the constitution of the political good as the democratic good - the pursuit of the 'good life' defined under free and equal conditions of participation.

Commensurate with his argument, Held engages in what he calls 'the democratic thought experiment'. At its core, the democratic thought experiment is concerned to describe the obligations people would accept as necessary for the status to be met as equally free members of their political community. In his own words:

It is an enquiry which aims to abstract from existing power relations, in order to disclose the fundamental enabling condition for possible political participation and therefore for legitimate rule. It is thus, an analytical mechanism, which helps discriminate among forms of acceptance or compliance to political arrangements and outcomes.<sup>22</sup>

But, what is the role of citizens in Held's democracy? Citizens, he says, can enjoy liberty only if the power of the state is circumscribed by law; that is,

---

<sup>21</sup> *ibid.*, p.281

circumscribed by rules which specify limits on the scope of political activity - limits based on the rights of individuals to develop their own views and tastes to pursue their own ends and to fulfill their own talents and gifts. The stratification of autonomy produced by modern corporate capitalism goes beyond the immediate impact of economic inequalities on the capacities of citizens to participate as equals in their collective associations, for the very capacity of governments to act in ways that interest groups may legitimately desire is constrained.<sup>23</sup>

According to Held, democratic theory and practice are faced with a major challenge. The business corporation or multinational bank exercises a disproportionate 'structural influence' over the polity and, therefore over the nature of democratic outcomes. Political representatives would find it extremely difficult to carry out the wishes of an electorate committed to reducing the adverse effects on democracy and political equality of corporate capitalism. Democracy is embedded in a socio-economic system that grants a 'privileged position' to certain interests. For these reasons, individuals and interest groups cannot be treated as necessarily equal, and the state cannot be regarded as a neutral arbiter among all interests.<sup>24</sup>

A final point of interest highlighted by Held is that democracy is challenged by powerful sets of economic relations and organisations, which can - by virtue of

---

<sup>22</sup> *ibid.*, p.161

<sup>23</sup> *ibid.*, p.246

the bases of their operation - systematically distort democratic processes and outcomes. There is a case that if democracy is to prevail, the key groups and associations of the economy will have to be rearticulated with political institutions so that they become part of the democratic process - adopting within their very *modus operandi* a structure of rules, principles and practices compatible with democracy.<sup>25</sup>

When we test Held's hypothesis on our own research concern, namely the internet, we come up with two responses. The first one is that new media increase the scale and speed of information provision and give citizens more control over their information diet. Thereby, they better arm citizens with the information they need in order to participate.<sup>26</sup> In this respect, new media help reduce some of the inequalities in the capacities of citizens to participate that Held is referring to. As Tsagarousianou mentions for utopian visionaries, the promise of nearly unlimited information delivered to your monitor in mere seconds is the promise of a better democracy. The internet can help to make all of us more active and more knowledgeable about government, even if 'the state cannot be regarded as a neutral arbiter among all interests'.<sup>27</sup> The second response is the most common one among internet researchers, which states that the internet will not make a great difference or as Margolis and Resnick put it politics will continue as usual because 'in the tradition of American capitalism, the Information Highway is

---

<sup>24</sup> *ibid.*, p.247

<sup>25</sup> *ibid.*, p.251

<sup>26</sup> Tsagarousianou, R, Tambini, D and Bryan, C (eds.): (1998) *Cyberdemocracy: Technology, Cities and Civic Networks*, Routledge: London, p.6.



increasingly here to advertise and sell products and services, not to improve the democratic quality of American politics and civic life'.<sup>28</sup> Margolis and Resnick seem to disagree with potential claims about the power of the internet in relation to democracy. They intimately take the view that

what has occurred is the normalization of cyberspace. Cyberspace has not become the locus of a new politics that spills out of the computer screen and revitalises citizenship and democracy. If anything ordinary politics and commercial activity in all their complexity and vitality, have invaded and captured cyberspace. Virtual reality has grown to resemble the real world.<sup>29</sup>

They back this up by saying that political life on the internet has moved away from cyber-communities, in which civic life centers around free discussion and debate. It has entered an era of organised civil society and structured group pluralism with a relatively passive citizenry. Nevertheless, Margolis and Resnick realise that the Web is a wonderful vehicle for citizens who are already interested in politics. 'If they choose ordinary citizens can acquire a plethora of data and gain access to the public face of the democratic political process. It has functioned well as a tool for citizen awareness campaigns, although so far these have mostly concerned politics that affect the net'.<sup>30</sup>

---

<sup>27</sup> Held, D: (1995) *Democracy and the Global Order*, Polity Press: Cambridge

<sup>28</sup> Margolis, M and Resnick, D: (2000) *Politics As Usual*, Sage: London, p.73

<sup>29</sup> *ibid.*, p.2

<sup>30</sup> *ibid.*, p.22



What they also recognise is that to realise democratic control, it is necessary to restore the balance among branches of government. Computer-mediated communication, they believe, could be the vehicle for this, because among other things it can provide citizens with access to the same documentary information as bureaucrats. Nevertheless, such an account denies the effect of the internet and ICTs on the political process, which is empirically evident in countless ways in current communication practices.

Interestingly, the same authors see a way that the internet will help spread democracy; but not because more people will conduct more of their politics online. Rather, information being at the centre of new forms of economic growth will facilitate the spread of that wealth. Margolis and Resnick write:

Areas of the world lacking old-fashioned sources of wealth rooted in natural resources such as vast tracts of arable land or scarce minerals can now compete with nations more abundantly endowed. Because the information spread via the Internet will contribute to general world economic growth and because economic growth facilitates the rise of democratic government, the Internet will contribute to the spread of democracy.<sup>31</sup>

Respectively, it is very dubious to assert that for two reasons; first the authors do not provide evidence for their claim, namely that economic growth facilitates the rise of democratic government, which is problematic, especially if we look at rich

---

<sup>31</sup> *ibid.*, p.210

states in the Middle East. Second, there is no guarantee that this new economic wealth will not end up again in the already rich North.

However, one has to agree with Margolis and Resnick that one of the hardest things to predict is whether the internet will improve the quality of democracy by creating a more informed citizenry. On the one hand, the internet offers instant and almost cost free information, which could enable the ordinary citizen to be fully informed about all policy areas and follow government activity that was never possible in the past. On the other hand, one has to remain sceptical, since the availability of unlimited information might inspire those who are already politically active, but it does not mean that the internet itself will increase the attentive public. Unfortunately, those who are uninterested and remain uninvolved in politics will continue to be so, whether the internet exists or not. Also, As Gerodimos argues, '[t]he leveling of the playing field can liberate long-oppressed voices, but it can also create an alternative public sphere that suffers from a lack of transparency, accountability and regulation that resembles the deficit of the mass-mediated public sphere'.<sup>32</sup>

One element of Held's hypothesis, that democracy is challenged by powerful sets of economic relations and organisations which can - by virtue of the bases of their operation - systematically distort democratic processes and outcomes comes true, when we discuss the relationship between the internet and politics. The internet

---

<sup>32</sup> Gerodimos, R: 'Social movements and online civic engagement', 2<sup>nd</sup> International Conference Imaging Social Movements, 1-3 July 2004, Edge Hill College.

does now and will continue to discriminate economically. Internet use requires internet access, which costs money many people cannot pay. As Richard Davis's evidence suggests regarding internet use in the US, '[p]eople making over \$75,000 annually are far more likely to own a computer, have access to the Internet, and use the Internet to visit political sites than those who made under \$40,000. In contrast the average income nationally is approximately \$32,000'.<sup>33</sup>

Manuel Castells also provides us with evidence to support the notion that the Internet is not as democratic as one might think, offering an insight on the social, racial, gender, age and spatial inequality in internet access:

Worldwide, 30 per cent of Internet users had a university degree, and the proportion increased to 55 per cent in Russia, 67 per cent in Mexico and 90 per cent in China. In Latin America, 90 per cent of Internet users came from upper income groups. In China only 7 per cent of Internet users were women. Age was a major discriminating factor. The average age of Internet users in the US was 36 years, and in the UK and in China was below 30. In Russia, only 15 per cent of Internet users were older than 45. In the US households with income of \$75,000 and higher were 20 times more likely to have Internet access than those at the lowest level of income.<sup>34</sup>

A more recent EU report titled 'A sustainable eEurope: Can ICT create economic, social and environment value?' dated August 2003 found that 88 per cent of all

---

<sup>33</sup> Davis, R: (1999) *The Web of Politics*, Oxford University Press: Oxford, p.182



internet users account for only 15 per cent of the world's population in the industrialised world, while countries as digitally advanced as Finland, have more internet users than the whole of Latin America. There are also big differences within the developed world. In 2002, some 58 per cent of all Americans had internet access at home, compared to only 38 per cent in Europe. Within the EU the percentage varies between 60 per cent in the Netherlands and 10 per cent in Greece. The report also suggests that not enough research has been done to understand social problems caused by the digital divide.<sup>35</sup> Moreover, the future of cyberdemocracy is seen as deferred 'given the heavy handed involvement of untrammelled economic and commercial interests in deciding the fate of technologies putatively valuable from the point of view of extending opportunities for political involvement to a larger segment of US society'.<sup>36</sup>

In addition, Slevin in his work *The Internet and Society* has anticipated that the increasing influence of big business on the internet brings with it at least two fears for regulators and internet users:

- First, there is concern that if builders of network applications hold a monopoly, they may be in a position to determine license fees for the use of their products.
- Second, there is the worry that those who build applications and control the

---

<sup>34</sup> Castells, M: (2000) *The Rise of the Network Society*, vol.1 of *The Information Age: Economy, Society and Culture*, 2<sup>nd</sup> edn, Blackwell: Oxford, p.377

<sup>35</sup> <http://europa.eu.int/comm/enterprise/ict/policy/ict-sust/final-report.pdf>

<sup>36</sup> Loader, B (ed.): (1997) *The Governance of Cyberspace*, Routledge: London, p.113



interfaces may gain a considerable say over the content of the information communicated and accessed by way of the net.<sup>37</sup>

Yet, this fear of monopoly and the existent monopolies in communication be them on computer software or the more traditional media (for example Bill Gates or Rupert Murdoch) has not stopped the use of ICTs in remarkable ways. Network technologies are increasingly used in public and political debates and communications, thus promoting dialogue between opposing parties, one of the elements of true democracy. Frissen writes that several 'freenets' have been developed in the Netherlands. They are called 'Digital cities', use the internet and are organised by private actors supported by government. But the government is also using the internet to organise political debates. In his own words:

In 1995 we have been running an Internet discussion for the Netherlands' Ministry of Home Affairs regarding a new White Paper on information in public administration. One of the research questions in this project was whether the style and participation in a digital debate differed from ordinary political debates.<sup>38</sup>

Other crucial elements of a democratic polity are privacy and surveillance as scrutinised by Raab.<sup>39</sup> The claim that democracy and privacy reinforce each other means that the information-openness of democracy is not necessarily achieved at

---

<sup>37</sup> Slevin, J: (2000) *The Internet and Society*, Polity Press: Cambridge, p.39

<sup>38</sup> Frissen in Loader, B (ed.): (1997) *The Governance of Cyberspace*, Routledge: London, p.117

<sup>39</sup> Raab in Loader, B (ed.): (1997) *The Governance of Cyberspace*, Routledge: London, p.156.

the expense of privacy's information-restriction. The development of accountable democratic institutions and privacy-protecting processes cannot take place in separate compartments, for each is an important condition of the other. Intruding upon privacy, surveillance may impede democratic liberties, due to its 'chilling' effect on communication or expression. Surveillance thrives in authoritarian regimes that are not exposed to public debate and criticism. ICTs can promote communication, political expression and action amongst citizens who cannot meet in person, provided that they can trust the security of electronic media and their integrity against surveillance. It appears, however, that when participants with unorthodox opinions are being monitored by authorities, then the Information Superhighway's (ISH) potential as a reliable democratic tool is damaged. In this respect Raab claims that:

There is much debate, through these channels on the questions of free speech, censorship, pornography, the accessibility of officials and politicians through electronic mail, intellectual property rights, the legal position and liabilities of anonymous remailers, the ability to dispose of secure encryption, and the facilities afforded by secure ISH networks to drug-traffickers and money-launderers.<sup>40</sup>

The risk of new technologies such as the internet becoming rampant features of information exchange and communication produces the fear of push-button democracy becoming the norm in the twentieth-first century, not so much as a

---

<sup>40</sup> *ibid.*, p.166.



formal process of national referenda, but as a bastardized version of manufactured consent, generated by public relations experts and entrenched political machines.<sup>41</sup>

To continue, in their work *Cyberpolitics*, Hill and Hughes suggest that for any democracy, information is an essential resource. They point out that one of the major failings of democracy is that so few people take part in the democratic process. In 1996, less than one half of the eligible adult population voted in the US presidential elections, and far fewer are involved in such activities as campaigning, writing letters, or circulating petitions. Hill and Hughes examined both Usenet and chatrooms and came up with various conclusions. One of the important ones is that internet messages about less-democratic nations are far more likely to be anti-government than the messages about more-democratic governments: '[n]ot only is the relationship between country democracy and the probability that a message will be anti-government strong, but it is the only significant, consistent predictor of anti-government statements in the Usenet'.<sup>42</sup>

In the same line of argument, they examined the ideological balance in chat rooms and they found that right-wing threads not only dominate, but that these threads have more chatters and more messages. This might imply that right-wingers are more numerous, more active or both.<sup>43</sup> Or it might reflect the marginality of right-wingers, who feel unrepresented by parties and formal systems. Not surprisingly,

---

<sup>41</sup> Wilhelm, A (2000) *Democracy in the Digital Age*, Routledge: London, p.139.

<sup>42</sup> Hill, K and Hughes, J: (1998) *Cyberpolitics*, Rowman and Littlefield: Lanham, p.107



they concluded that chat rooms are a difficult format for thoughtful discussion, because of the short line space and the fast pace, which require people to make snap comments, not thoughtful ones. The level of information is low and there is a small amount of issue discussion. Most chat room conversations focus on the actions of people rather than the government and its role in society. Thus, Hill and Hughes counteract that the Usenet is a better format than chat rooms for political discussions. As they explain:

The Usenet is slow and more thoughtful and so has more potential for deliberation. We saw that Usenet threads tend to be more informative and they are more ideologically balanced. In general, we think electronic political discussion works better in a format as the Usenet, as opposed to a chat room style. It is not perfect, but we think it offers a better hope for deliberative democracy.<sup>44</sup>

One gets the same feeling when using similar more recent facilities like the Microsoft Network (MSN) or I Seek You (ICQ).

In *Cyberdemocracy* written by Tsagarousianou and colleagues, the writers examine several attempts by local authorities to provide access to their citizens electronically. As Tsagarousianou describes them, Amsterdam's Digital City, for example, combines a number of different communicative and civic functions, such as deliberation, public information, and some degree of support of grass root

---

<sup>43</sup> *ibid.*, p.129

groups. The IperBole project of the commune of Bologna supports citizens' deliberation, public information provision and to a lesser extent, supports grassroots groups. The Santa Monica Pen project enables deliberation and public information provision. The Manchester Information City initiative provides economic regeneration-related information dissemination as well as deliberation and civic information provision. In contrast, the official city of Berlin project is geared towards the provision of local authority and local area information, while Network Pericles in Athens has plebiscitary and deliberative aspects, and allows for limited information mainly.<sup>45</sup> These efforts by local governments connect very closely to Held's argument that regional and global interconnectedness can alter the nature and dynamics of national political systems, since local initiatives could be seen as a challenge to the national government.

I would mention one of the networks, namely, the Santa Monica' Public Electronic network (PEN), since it is one of the longest running and most innovative experiments in electronic democracy. The PEN system is an exceptionally valuable study, because Santa Monica was one of the first cities to offer its citizens access to an interactive public electronic network. Docter and Dutton have alluded to the problem:

Santa Monica's experience indicates that the Internet and the multimedia revolution will not short-circuit such major dilemmas of democratic participation

---

<sup>44</sup> *ibid.*, p.131

as public apathy. Most of the public in Santa Monica and other American cities are not very interested in either real or virtual participation. Nevertheless, technological change in the household and government, illustrated by burgeoning interest in the Internet, suggests that electronic participation is likely further to be developed by governments throughout the US.<sup>46</sup>

Moreover, as Tsagarousianou explains most, although not all, experiments in electronic democracy share a number of common characteristics. First, they are perceived by the social actors initiating or participating in them as means of reviving and invigorating democratic politics, which for a variety of reasons is perceived to have lost its appeal and dynamism. Second, they have been local or regional in their character, being related to more or less territorially bounded urban and suburban communities. Lastly, they have been based on broadly similar technological infrastructures.<sup>47</sup>

Graham Browning in his work *Electronic Democracy* is more concerned with the actual effects of the internet on political practice. He sets forth a very good example of the potential political power of the internet. Richard Hartman, a computer software engineer from Spokane, Washington, and his wife Mary helped bring about the surprise defeat of then Speaker of the House Thomas S. Foley through an anti-Foley political action committee they almost entirely

---

<sup>45</sup> Tsagarousianou, R in Tsagarousianou et.al: (1998) *Cyberdemocracy: Technology, Cities and Civic Networks*, Routledge: London, p.169

<sup>46</sup> *ibid.*, p.145

<sup>47</sup> *ibid.*, p.168



organised through the net.<sup>48</sup> Also, Browning mentions that online activists claim some of the credit for the election in January 1996 of Senator Ron Wyden, D-Ore, an enthusiastic supporter of free speech online. Wyden won his race by less than 18,000 votes, a measurable proportion of them supplied by voters attracted to Wyden's candidacy through his internet appeals, activists believe. Another example cited by Browning occurred in late September and early October 1994. This is how Browning (1996) describes it:

On September 29 of that year the House of Representatives passed a lobbying reform bill that many organisations feared would require them to reveal the names of their members and the amount of fees they paid lobbyists to represent them in Congress. After the vote, the Christian Coalition posted emergency alerts to the Internet and CompuServe, asking members to contact Congress immediately and register their opposition to the bill. In the 24-hour period before the lobbying reform bill reached the Senate on the following Friday, almost 250,000 people responded to those alerts. The bill died on the floor of the Senate.<sup>49</sup>

More recently, we had the phenomenon of 'blogs': short for a weblog, an online journal that can turn anyone with an internet connection into a mini-media outlet. Blogs are easy to create, cheap to set up, and commonplace on the web. They can draw thousands of readers per day and dozens of posted comments, similar to talk radio for the wired. An example of a famous weblog is Salam Pax from Baghdad

---

<sup>48</sup> Browning, G: (1996) *Electronic Democracy*, Wilton: London, p. 2

included later in the discussion, who influenced the media coverage during the March 2003 Iraq conflict. In relation to democratic politics, there is the example of Oliver Willis, 25, who has a political platform of his own despite the fact that he is not a rich man or a player in democratic politics. He ran a website called [oliverwillis.com](http://oliverwillis.com), where he posted an essay promoting Vermont Governor Howard Dean for democratic nominee, drawing comments from people he had never met. 'Blogs are the harbingers of a new, interactive culture that could potentially change how democracy works, turning voters into active participants rather than passive consumers, limiting the traditional media's role as a gate keeper, and giving the rank-and-file voter unparalleled influence'.<sup>50</sup>

Among the wired, there is a debate over whether blogs are a new form of discourse or simply an endless feedback loop, a self-enclosed circle of political junkies echoing and challenging each other. However, Willis and other bloggers say that their work has a way of spilling into the offline world, as blogs can often focus attention on issues the traditional media ignores. Due to the fact that official websites can be boring, blogs can lend an aura of authenticity to a campaign. During the presidential primaries of 2003-4, the Web was filled with unofficial blogs in support of Howard Dean, John Kerry, Richard Gephardt, Dennis Kucinich and President Bush. There was also a movement to draft retired Army General Wesley Clark for a presidential run, which drew much of its energy from

---

<sup>49</sup> *ibid.*, p. 3

<sup>50</sup> Weiss, J: ' "Blogs" shake the political discourse', *Globe Staff*, 23/7/03

blogs.<sup>51</sup> Nevertheless, the use of blogs is not seen as transforming the way presidential campaigns communicate, according to a report from Johns Hopkins University's CampaignsOnline.org project. The report found that while there has been much media attention concerning campaign blogs, only four of the nine Democratic candidates for president currently utilise blogs as part of their communication strategy.<sup>52</sup>

A stark example of e-democracy and internet politics is MoveOn.org, which played an influential role in the US 2003-4 primaries and in recent years has proven the ability to raise money - \$3.2 million in 2000 and \$4.1 million in 2002 - with a membership list of 1.4 million activists. The number of volunteers for MoveOn is ten times larger than any existing presidential candidate developed. In the future, a campaign's Internet strategy will become central to the campaign:

As the example of MoveOn is duplicated by other organizations from the national to the local level, the power and the impact of online organizing and campaigning will be greatly magnified. Any politician with sense enough to fill out qualifying papers will understand that the Internet must be central to their campaign and not an afterthought.<sup>53</sup>

Dean raised more than \$40 million through online donations. John Kerry in three months brought in almost \$50 million from 400,000 online donations. However,

---

<sup>51</sup> *ibid.*

<sup>52</sup> 'Howard Dean blogs, Gen. Clark and President Bush follow', AlwaysOn, 18/11/03

<sup>53</sup> 'The Moveon primary: what it means', politicsonline.com, 26/7/03



both Kerry and President Bush are eager to translate online support into actual votes.<sup>54</sup>

To sum up, there are two camps on the question of whether the internet enhances democracy. The optimist view is that the internet increases the scale and speed of information and gives more control over the information diet, so that the promise of unlimited information is the promise of a better democracy; projects like those cited here by local authorities to provide access to their citizens electronically can prove to be a tool for a better democracy and as examples of awareness campaigns have shown the internet can be a useful way to organise politically. On the other side of the coin, there are the arguments that those who are uninterested in politics and remain uninvolved will continue to be so, that the internet discriminates economically with social, gender, race, age and spatial inequality and that at the end the internet is dominated by economic interests and seems to be resembling more and more the real world. Both arguments have their merits and deserve detailed appraisal. It would be thus safer to assert that the internet might not yet be ready to take on the responsibility of a democratising tool; nevertheless its potential for helping to create a better democracy is undeniable. From the evidence presented so far, it does not seem that democracy is radically influenced much by the internet and it remains a traditional concept unaffected by the postmodern nature of the medium. The internet has provided improved access to the political system for outsiders and mechanisms for spontaneous expression

---

<sup>54</sup> Witt, L: 'Kerry net strategy now on voters', wired.com, 2/7/04.

of public attitudes, presenting a very powerful way of harnessing the political moment. Yet, even as they exploit the web, political professionals are somewhat mindful of its anarchic cultural heritage.

### *Participation in internet politics*

Another issue linked to my research is participation, because the groups that are availed with the internet use it to promote greater participation in their respective political agendas. Nevertheless, participation is not always linked to democracy. Carole Pateman<sup>55</sup> suggests that the collapse of the Weimar Republic, with its high rates of mass participation, into fascism, and the post-war establishment of totalitarian regimes based on mass participation, albeit participation backed by intimidation and coercion, underlay the tendency for 'participation' to become linked to the concept of totalitarianism rather than that of democracy.

Pateman refers to Dahl's view about the possible dangers inherent in an increase in participation on the part of the ordinary citizen. The lower socio-economic groups are the least politically active and it is also among this group that 'authoritarian' personalities are most frequently found. To the extent that a rise in political activity brought this group into the political arena, the consensus on norms might decline and hence polyarchy declines. Therefore, an increase in the

---

<sup>55</sup> Pateman, C: (1970) *Participation and Democratic Theory*, Cambridge University Press: Cambridge, p.2.

existing amount of participation could prove to be dangerous to the stability of the democratic system.

However, this analysis seems to amount to something akin to elitism and it is quite disturbing to think that lower socio-economic groups should be excluded from the democratic process because they lower the 'quality' of democracy. In relation to the internet, which can potentially involve mass participation in democratic politics, such an argument would be difficult to swallow.

Further, Pateman deems that certain conditions are necessary if the democratic system is to remain stable. The level of participation by the majority should not rise much above the minimum necessary to keep the democratic method (electoral machinery) working; that is, it should remain at about the level that exists at present in the Anglo-American democracies. The fact that non-democratic attitudes are relatively more common among the inactive means that any increase in participation by the apathetic would weaken the consensus on the norms of the democratic method, which is a further necessary condition. In her own words:

As we have seen, the formulators of the contemporary theory of democracy also regard participation exclusively as a protective device. In their view the 'democratic' nature of the system rests primarily on the form of the national 'institutional arrangements', specifically on the competition of leaders (potential



representatives) for votes, so that theorists who hold this view of the role of participation are first and foremost theorists of representative government.<sup>56</sup>

Again, keeping the level of participation to the minimum necessary to avoid weakening consensus, although valid as an argument, is a technical and cynical view of participatory politics and limits prospects of greater participation caused potentially by new ICTs.

Rousseau, Pateman writes, might be called the theorist par excellence of participation, and an understanding of the nature of the political system that he describes in the *Social Contract* is vital for the theory of participatory democracy. Rousseau's entire political theory hinges on the individual participation of each citizen in political decision making and in his theory participation is very much more than a protective adjunct to a set of institutional arrangements. It also has a psychological effect on the participants, ensuring that there is a continuing interrelationship between the working of institutions and the psychological qualities and attitudes of individuals interacting with them.

The analysis of the operation of Rousseau's participatory system makes two points clear: first, that 'participation' for Rousseau is participation in the making of decisions and second, that it is, as in theories of representative government, a way of protecting private interests and ensuring good government. Rousseau's

---

<sup>56</sup> *ibid.*, p.20

ideal system is designed to develop responsible, individual, social and political action through the effect of the participatory process. Rousseau also suggests that participation has an additional integrative function; it increases the feeling among individual citizens that they belong in their community. More important is the experience of participation in decision-making itself, and the complex totality of results to which it is seen to lead, both for the individual and for the whole political system; this experience attaches the individual to her/his society and is instrumental in developing it into a true community.

Moreover, Pateman believes that the theory of participatory democracy is built round the central assertion that individuals and their institutions cannot be considered in isolation from one another.<sup>57</sup> The existence of representative institutions at national level is not sufficient for democracy; for maximum participation by all people at that level, socialisation, or 'social training' for democracy must take place in other spheres in order that the necessary individual attitudes and psychological qualities can be developed. The major function of participation in the theory of participatory democracy is therefore an educative one, educative in the very widest sense, including both the psychological aspect and the gaining of practice in democratic skills and procedures. Pateman puts it this way:

No longer is democratic theory centered on the participation of 'the people', on the participation of the ordinary man or the prime virtue of a democratic political

system seen as the development of politically relevant and necessary qualities in the ordinary individual; in the contemporary theory of democracy it is the participation of the minority elite that is crucial and the non-participation of the apathetic, ordinary man lacking in the feeling of political efficacy, that is regarded as the main bulwark against instability.<sup>58</sup>

The final observation made by Pateman I want to include here is that when the problem of participation and its role in democratic theory is placed in a wider context than that provided by the contemporary theory of democracy, and the relevant empirical material is related to the theoretical issues, it becomes clear that neither the demands for more participation, nor the theory of participatory democracy itself, are based, as is so frequently claimed, on dangerous illusions or on an outmoded and unrealistic theoretical foundation.<sup>59</sup> Thus, Pateman suggests that we can still have a modern viable theory of democracy which retains the notion of participation at its heart.

Having said that, new technology, such as the internet can be harnessed to measure citizens' preferences in representative democracies, and may make it easier for citizens to respond, thus making political participation (access to information, deliberation, debate and voting) easier, and thereby resolving the perceived crisis of participation (citizen alienation, abstention and apathy) in

---

<sup>57</sup> *ibid.*, p.42

<sup>58</sup> *ibid.*, p.104

<sup>59</sup> *ibid.*, p.111



liberal democracies.<sup>60</sup> As earlier Tsagarousianou notes that since the early 1990s a number of European local authorities such as Amsterdam, Bologna, Manchester and civil society actors rather than central government have been engaged in experiments in electronic democracy, as have several cities in the UK and the U.S. The organisers of these initiatives frequently argued that by embracing information and communications technologies, they could resuscitate declining citizen participation and give new vigour to local politics.<sup>61</sup> Margolis and Resnick<sup>62</sup> also suggest that for optimists, political participation in cyberspace approximates an ideal type of communitarian democracy that emphasises mutuality. The time needed to become informed about any topic drops substantially when citizens can employ 'gopher' or 'archie' servers to locate and retrieve desired information on a vast variety of topics, including matters of public policy that comprise the formal business of government.

Nevertheless, there is another side to this story. Even if there has been a tremendous increase in the number of people now on the internet, there is no indication that their presence will inaugurate a new era in politics. The internet has become a mass medium, but the numbers tallied by those who estimate the growth of the internet have not been translated into comparable growth in political participation. Providing greater choice and opportunity only solves part of the problem of participation - for example, that related to reducing the cost of

---

<sup>60</sup> Tsagarousianou et.al: (1998) *Cyberdemocracy: Technology, Cities and Civic Networks*, Routledge: London, p.6

<sup>61</sup> *ibid.*, p.168

<sup>62</sup> Margolis and Resnick: (2000), *Politics As Usual*, p.100.

involvement - but it does not get to the heart of what motivates citizens to move from the state of disengagement to one of salutary involvement in civic life.<sup>63</sup> Wilhelm writes that while many communications researchers suggest that anonymity may liberate the individual and equalise participation in a forum where power is asymmetrically distributed, others argue that the individual's isolation coupled with invisible surveillance and hierarchical observation from the outside may lead to the veritable incarceration of the user.<sup>64</sup> Promoting a diversity of voices, while imperative, does not *eo ipso* guarantee deliberation, negotiation, and the contestation of viewpoints. Universal access is not sufficient, Wilhelm thinks, for realizing a discursive, democratic polity. Instead he argues that 'deliberation or critical-rational reflection is a necessary condition of salutary political conversation online, without which digital democracy may follow the lead of "mature" media and fail to meet expectations'.<sup>65</sup>

Another interesting point on the internet's potential for participation is made by Richard Davis.<sup>66</sup> He did a content analysis of three Usenet groups, an analysis of one week's worth of messages between June 14 and June 20, 1997. Davis, similarly to Hill and Hughes<sup>67</sup>, argues that Usenet 'possesses certain disadvantages as a forum for public discussion of political issues. Those include opinion reinforcement, flaming and under-representativeness'.<sup>68</sup> As Davis

---

<sup>63</sup> Margolis and Resnick: (2000), *Politics As Usual*, Oxford University Press: Oxford. p.207; Wilhelm, A: (2000) *Democracy in the Digital Age*, Routledge: London, p.87.

<sup>64</sup> Wilhelm, A: (2000) *Democracy in the Digital Age*, Routledge: London, p. 46

<sup>65</sup> *ibid.*, p.86

<sup>66</sup> Davis, R: (1999) *The Web of Politics*, Oxford University Press: Oxford.

<sup>67</sup> Hill, K and Hughes, J: (1998) *Cyberpolitics*, Rowman and Littlefield: Lanham.

<sup>68</sup> *ibid.*, p.161



suggests 'Usenet political discussion groups tends to favor the loudest and most aggressive individuals. Those who are less aggressive risk rigorous attack and humiliation'.<sup>69</sup> Also, over the past decade has been consistent support in the literature for the hypothesis that in the absence of social context cues the level of uninhibited verbal behaviour in CMC rises.<sup>70</sup>

Nevertheless, as a two-way mass communications medium that allows users to receive news and information, inasmuch as they participate in information, transmission and public discussion, the internet potentially diffuses power over information dissemination and public debate. The growth of the internet raises the prospect that the traditional groups who dominate American politics will become anachronistic, Davis argues, like organizational dinosaurs in the cyberspace age. In his own words:

They will be displaced by new organisations or by citizens who no longer need groups at all. They will become mediators in an era of unmediated communication. When citizens will be able to interact with elected representatives without the necessity of intermediary organisations, what then is the role of interest groups?<sup>71</sup>

---

<sup>69</sup> Davis, R: (1999) *The Web of Politics*, Oxford University Press: Oxford, p. 163

<sup>70</sup> Collins, M: 'Flaming: The relationship between social context cues and uninhibited verbal behavior in computer-mediated communication', Fall 1992, [www.emoderators.com/papers/flames.html](http://www.emoderators.com/papers/flames.html). See for example: Kiesler, S, Siegel, J and McGuire, T: (1984) 'Social psychological aspects of computer-mediated communication', *American Psychologist*, 39 (10): 1123-1134. Also, Smolensky, M.W, Carmondy, M.A and Halcomb, C.G: (1990) 'The influence of task type, group structure and extraversion on uninhibited speech in computer-mediated communication' *Computers in Human Behaviour*, 6: 261-272.



Furthermore, the internet is not a panacea for local apathy or loss of community nor is it the curse of atomisation. Rather, it is a tool that to the extent that it has effects at all, is most likely to maintain the status quo. Information at the local level will be more readily available, but again, whether average citizens will be inclined to utilise it is debatable. That is because Americans (or anybody else for that matter) will not be much different people, just because there are resources at their disposal to follow politics quite closely. Computer-assisted politics will not be radically different from today's politics. The argument here is that the internet is creating social fragmentation and an increase in both intolerance and incivility, as people end up seeing their fellow citizens as stupid or malicious. According to Davis, this is not healthy for democracy, because it encourages people to choose teams, rather than to think issues through.<sup>72</sup>

Nevertheless, the good news is that internet access is not limited to these hugely successful commercial gateways. The free-net phenomena, along with the explosion of homespun Bulletin Board (BBS) networks, ensure that access to information need not be 'filtered' by corporate or government interests. Free-nets, such as the Seattle Community Network, are a combination of electronic bulletin board and online service centred around a specific community. They generally operate on a nonprofit basis, gathering operating overheads through donations and community support. One item of interest to organisers, both social and otherwise, is that the National Public Telecomputing Network will help any community

---

<sup>71</sup> *ibid.*, p.63

<sup>72</sup> *ibid.*

center set up a free-net, and will provide assistance in maintaining the computers and databases essential for its use. Lack of technical expertise no longer need be a barrier to modest startups such as these. One cannot help feeling this when a day's email may contain messages from both local colleagues and from others in far-flung exotic places. The commonality of interest expressed in that interaction attests to the empowering nature of the medium.<sup>73</sup> Wellman and Gulia point out that '[t]he architecture of the Net facilitates weak and strong ties that cut across social milieus, be they interest groups, localities, organizations or nations, so that the cyberlinks between people become social links between groups that otherwise would be socially and physically dispersed'.<sup>74</sup> However, it is important to note that these virtual connective structures do not necessarily produce collective identity or ideological cleavage among the people involved and do not always create communities.

Borrowing Fisher and Kling's words, the inhabitants of these structures are a 'transclass grouping of constituencies and cultural identities'<sup>75</sup>, who recognise that 'there is a critical interaction between organizing efforts, national politics, and nationwide social movements'.<sup>76</sup> Building on these ideas, Fisher and Kling state that 'because community problems almost always originate beyond local

---

<sup>73</sup> Scott March: 'Community organizing on the Internet: Implications for social work practitioners', M.S.W

<sup>74</sup> Wellman and Gulia, 1995, p.15 as quoted in Scott March, M.S.W: 'Community organizing on the Internet: Implications for social work practitioners', <http://www.interweb.com/nsnnet/docs/march>

<sup>75</sup> Fisher and Kling, 1994, p.17 as quoted in Scott March, M.S.W: 'Community organizing on the Internet: Implications for social work practitioners', <http://www.interweb.com/nsnnet/docs/march>

<sup>76</sup> Fisher and Kling, p.223



borders, the ability to effect change depends to a great extent upon building coalitions, alliances, networks, and progressive political parties'.<sup>77</sup>

In synopsis, the evidence of the local authorities' initiative in European cities suggests that the internet has the potential to resolve the perceived crisis of participation in liberal democracies, however two points are important to note. First, that the growth of the internet has not translated into comparable growth in political participation and second, that universal access - if such a thing exists - is not sufficient for realising a discursive democratic polity.

Nevertheless, while this research was taking place, quite a lot seems to have changed. In stark contrast with these arguments and findings, I should include here evidence of the US primary elections, during which a lot of voter-action groups sprung up online, showing that the American public can be mobilised and show a strong online presence, although this does not necessarily translate into a 'real' voting presence. A series of democratic voter-action groups, starting with Howard Dean's supporters as well as John Kerry's, hoped to help their candidates win every possible vote to reach the White House. The Dean campaign, with Joe Trippi at the helm, shattered traditional top-down campaign models by allowing its supporters to act on their own. The campaign broke Democratic fund-raising records by collecting \$40 million from 280,000 individuals in 2003. Dean also mobilised 163,000 individuals to attend locally organised Meetups and drew

---

<sup>77</sup> *ibid.*, p.17



millions to the campaign's official and unofficial blogs. Simon Rosenberg, who as president of the New Democrat Network counts as a Washington insider, says politics has changed forever:

2003 was the first year of the Internet age of political communications, and the end of the broadcast era. From 1960 to 2003, political communications was dominated by the broadcast model where you spoke out and people consumed it as passive consumers. The Internet age is characterized by the medium, which is participatory, it is interactive, it is one-to-one.<sup>78</sup>

'To me, what this election is about is a test. A test of the questions of whether a spontaneously self-organizing group of activists on the left can outperform the hierarchically organized, centrally directed political organization on the right', said David Lytel of ReDefeatBush.com, a website run by The Committee to Re Deafeat the President. Driving Votes is another online effort that uses the internet to organise Democrats. This group uses its website as an information post where people nationwide can organise voter-registration road trips to various swing states. 'What's been interesting for me' says Lerner, 'is that there are a lot of people out there who want to do something bigger than they have done in the past. What is exciting to me about the Internet is just that it doesn't cost (much) money to make (our) website, and now lots of people are getting motivated, and I feel we will have a voice'. Lytel feels that while Republicans have integrated online and offline fundraising and voter-registration efforts, a great divide exists between

---

<sup>78</sup> Singel, R: 'Net politics down but not out', wired, 2/2/04

Democratic postal and electronic camps, with both sides feverishly protecting their turf. Another organiser, Khoe, explains that Run Against Bush has utilised the internet to sign up more than 2,000 members in 40 states. The group gets together people all over the country for literal anti-Bush running events called Jogs against Bush, or Jabs. Members check the website to find their local jabs, come together, and put on Run Against Bush T-shirts. Sites like these can mobilise the party's often lethargic members. 'Our typical member may be somebody who grumbles about the administration and about national security and fiscal policy, but they haven't felt comfortable, for whatever reason, doing something about it' said Khoe. And the other anti-Bush grass-roots groups are having similar experiences. Democrats were counting on the internet to help them build a base that would push Kerry over the top on election day. 'It appears that this sort of technique seems to be working well with a progressive mind-set or progressive people... because of the two way nature of true online grass-roots participation... The users are the ones who choose issues... It's a very back-and-forth, multiparticipant sort of thing', said ActBlue's Matt DeBergalis.<sup>79</sup>

A panel in May 2004 at the University of California at Berkeley Graduate School of Journalism concentrated on political activism in online communities. Their assessment was that the Web has been particularly effective in engaging politically apathetic people and motivating them to take politics back to the grassroots level. The Howard Dean campaign successfully attracted millions of

---

<sup>79</sup> quotes are extracted from Terdiman, D: 'Dems hold the high ground online', wired, 23/4/04



grassroots dollars because it worked counter to the traditional ways campaigns work, said Markos Moulitsas Zuniga, publisher of the Democratic activists blog Daily Kos<sup>80</sup>. Typically, consultants and political parties try to suppress voter turnout, but now activists are using the web specifically, in the form of activism networks and blogs, to fight back and reengage people, Moulitsas said. When Moulitsas launched his blog in early 2002, 'it was really difficult to be a progressive liberal. We were essentially nobodies. But people were taking us seriously. They reasoned that if they could build a large community without possessing any credentials, then they could possibly move that community to accomplish change'.<sup>81</sup> Joe Trippi, campaign manager for Howard Dean, contacted Moulitsas and his partner to become consultants. Moulitsas asserted that the campaign grew because people felt they were participating in a cause rather than following one. 'Blog audiences want to be part of the discussion. They don't want to be told what to do'. Perhaps that is why Moulitas doubts that the internet could get a candidate elected on its own. 'You still need the grass-roots activities. You still need the traditional media'.<sup>82</sup> This is also the opinion of Craig Newmark, of craigslist, who has commented that the challenge for blogs and social-networking sites, is to find a way to get the millions of people they attract to go beyond the echo chamber of the internet.<sup>83</sup>

---

<sup>80</sup> Zetter,K: 'Blogs counter political plottings', wired, 5/5/04

<sup>81</sup> *ibid.*

<sup>82</sup> *ibid.*

<sup>83</sup> *ibid.*



This section focused on issues of participation and the internet. The following section continues the discussion of what new political movements are looking for when using the internet by looking at the issue of power in internet politics.

### *Power in internet politics*

Power is an important element in internet politics, as in all realms of politics, since internet groups are interested in the accumulation of power. Apart from participation, the point to be highlighted is what they fight for. Particularly, my aim is to focus on the way opposing groups attempt to accumulate enough power to resolve a conflict in a way that suits them and to promote their own version of the truth. Despite this obvious connection between power and internet politics, the key issues can be complicated. More substantially, in this section I will try to apply a theory of power to my own internet research. The concept of power is a very traditional political concept, and it has been argued that it is what politics is about.

Steven Lukes in his work *Power: A Radical View*<sup>84</sup> identifies three views of power: the one-dimensional view, the two-dimensional view and the three-dimensional view. Firstly, in the one-dimensional view we find writers like Dahl, who in his early article, *The Concept of Power*, describes his intuitive idea of power as follows: A has power over B to the extent that s/he can get B to do something that B would not otherwise do. In short, as Polsby writes, in the

pluralist approach an attempt is made to study specific outcomes in order to determine who actually prevails in community decision-making. Thus, the pluralist methodology, Lukes contends, in Merelman's words 'studied actual behaviour, stressed operational definitions and turned up evidence. Most important, it seemed to produce reliable conclusions, which met the canons of science'.<sup>85</sup> Thus, Lukes concludes that this first one-dimensional view of power involves a focus on behaviour in the making of decisions over which there is an observable conflict of 'subjective' interests, observably expressed in policy preferences and revealed by political participation.<sup>86</sup> This focus on behaviour and decision-making on the part of the pluralists would not be entirely useful when applying a theory of power to internet politics. This is firstly, because power can have other, more complicated dimensions such as ideology, knowledge and social forces, and secondly, because the internet involves a much more networked form of power relationships, which the pluralist model is insufficient to explain.

The two-dimensional view of power is a critique of the pluralist view. In their critique, Bachrach and Baratz denoted that it is restrictive, and in virtue of that fact, gives a misleading and sanguine pluralist picture of American politics.<sup>87</sup> Power, they claim, has two faces. Their central point is this: to the extent that a person or group - consciously or unconsciously - creates or reinforces barriers to the public airing of policy conflicts, that person or group has power. A

---

<sup>84</sup> Lukes, S: (1970) *Power: A Radical View*, Macmillan: London.

<sup>85</sup> *ibid.*, p.13

<sup>86</sup> *ibid.*, p.25

<sup>87</sup> *ibid.*, p.16

satisfactory analysis of the two-dimensional power involves examining both decision-making and non-decision-making. A decision is a choice among alternative modes of action; a non-decision is a decision that results in suppression of a latent or manifest challenge to the values or interests of the decision-maker. As a result, non-decision-making is a means by which demands for change in the existing allocation of benefits and privileges in the community can be suffocated before they are even voiced. The two-dimensional view of power involves a qualified critique of the behavioural focus of the first view and it allows for consideration of the ways in which decisions are prevented from being taken on potential issues, over which there is an observable conflict of 'subjective' interests, seen as embodied in express policy preferences and sub-political grievances.

Lukes is criticising both views:

The trouble seems to be that both Bachrach and Baratz and the pluralists supposed that because power, as they conceptualise it, only shows up in cases of actual conflict, it follows that actual conflict is necessary to power. But this is to ignore the crucial point that the most effective and insidious use of power is to prevent such conflict from arising in the first place.<sup>88</sup>

So, Lukes offers a third view of power, the three-dimensional view, which involves a thoroughgoing critique of the behavioural focus of the first two views

---

<sup>88</sup> *ibid.*, p.23



as too individualistic and outlines the many ways in which potential issues are kept out of politics, whether through the operation of social forces and institutional practices or through individuals' decisions. Lukes defines the concept of power by saying that A exercises power over B, when A affects B in a manner contrary to B's interests. His suggestion is that the one-dimensional view of power presupposes a liberal conception of interests, the two-dimensional view a reformist conception and the three-dimensional view a radical conception.

Lukes criticises the one-dimensional view by saying that pluralists, by studying the making of important decisions within the community, were simply taking over and reproducing the bias of the system they were studying. The one-dimensional view of power cannot reveal the less visible ways in which a pluralist system may be biased in favour of certain groups and against others. The two-dimensional view goes some way to revealing this, but it confines itself to studying situations where the mobilisation of bias can be attributed to individuals' decisions that have the effect of preventing currently observable grievances, 'covert or overt', from becoming issues within the political process. This would not be a approach to internet conflict, which involves the use of the internet by opposing groups, because the two-dimensional view is restrictive, in the sense that it does not study power as exercised by collectivities. This suggests that Lukes's three-dimensional view of power is a better fit for our research concern, especially since it looks at collectivities:

How is one to identify the process or mechanism of an alleged exercise of power, on the three-dimensional view?...There are three features distinctive of the three-dimensional view, which pose peculiarly acute problems for the researcher. As I have argued such an exercise may in the first place involve inaction rather than observable action. In the second place it may be unconscious. And in the third place power may be exercised by collectivities, such as groups or institutions.<sup>89</sup>

Closely related to Lukes's radical view of power, although much more interestingly elaborated, is Foucault's conception of power and his concept of power/knowledge. These begin to achieve prominence in his work with the appearance of *Discipline and Punish* and *The History of Sexuality*. The twin term arises out of Foucault's analyses, as a result of his disciplinary theory, where surveillance enables the structures of domination to operate. To illustrate the notion of disciplinary power and surveillance, Foucault uses Bentham's Panopticon, a circular architectural structure in which cells are arranged around a central viewing tower in such a way as to ensure permanent surveillance, which ensures control of and discipline over the incarcerated bodies. In the two books mentioned above, systems of knowledge are defined as bound up with regimes of power and truth. Systems of power bring forth different types of knowledge. Foucault thinks that power and knowledge directly imply one another and that there is no power relation without the correlative constitution of a field of knowledge, nor a knowledge that does not presuppose and constitute at the same time power relations.

---

<sup>89</sup> *ibid.*, p.50



Consequently, recognised forms of knowledge always bring power and power in turn justifies the formation of specific kinds of knowledge. The subjects or objects to be known are all integral elements of power/knowledge strategies. Foucault saw these techniques of power undergoing a two-stage development. Initially, they were instituted as means of control or neutralisation of dangerous social elements and evolved into techniques of enhancing the utility and productivity of these subjected to them. The connection, he proposes, between power and knowledge is not just a particular institutional use of knowledge as means to domination. Foucault objects to the very idea of knowledge outside the network of power relations. He proposed these remarks about power and knowledge, first and foremost, to make sense of how the observation and classification of individuals and populations contributed to newly emerging strategies of domination and how their applications came to constitute knowledge.<sup>90</sup> In Poster's understanding of this process, the individual subject is interpellated by the super-panopticon through technologies of power, through the discourse of databases that have very little to do with modern conceptions of rational autonomy. The super-panopticon, as a perfect writing machine, constitutes subjects as decentred from their ideologically determined entity.<sup>91</sup>

Foucault is opposed to approaches to knowledge that privilege a 'sovereign subject' anterior to discourse. Discourse becomes meaningful not because of the

---

<sup>90</sup> Foucault, M: (1980) *Power/Knowledge*, Harvester Wheatsheaf: New York and London

<sup>91</sup> Poster, M: (1995) *The Second Media Age*, Polity Press: Cambridge., p.87



individual, but because of the discursive formation, providing subject-positions which the individual can occupy.<sup>92</sup> In this way Foucault argues that there cannot exist a subject prior to language. This is an illusion. Consequently, Foucault totally rejects of any notion of the subject. What he is interested in is to analyse the play of discontinuities in the history of discourses. He does not care about the meaning or the truth of a statement, but rather, is concerned with the rules of formation that determine the objects, concepts, operations and options of a particular discourse.<sup>93</sup> While Foucault does not recognise the system of dispersion as a tool to distinguish one discursive formation from another, he identifies four sets of rules of formation, such that if one or more is found in the analysis of dispersed statements, then we can identify a particular discursive formation. These are: the formation of objects, the formation of enunciative modalities, the formation of strategies and the formation of concepts.<sup>94</sup> Another principle he brings in is rarefaction, in order to explain why in a particular era everything that can be said is never said. This happens according to Foucault because of the reproduction of relations of social domination through the control of meaning. Discourses and meaning are the sites of social struggle.

In sum, Foucault's archaeological project is to examine statements by particular societies that make serious claims to truth and to describe the relation between statements and their historical transformation. One of the criticisms against his archaeological approach is that while he explains the construction of discrete

---

<sup>92</sup> McNay, L: (1994) *Foucault: A Critical Introduction*, Polity Press: Cambridge, p.68

<sup>93</sup> Torfing, J: (1999) *New Theories of Discourse: Laclau, Mouffe, Žižek*, Blackwell: Oxford, p.90

subject-positions within discourse, he offers no explanation of the social context in which these positions are embedded and which governs how they are filled, nor does he consider the issues of power that are inevitably vital when considering the social context of discourse.<sup>95</sup>

After being heavily criticised for treating discourses as autonomous systems of scientific statements whilst investigating madness, the clinic and scientific discourses in his *Archaeology of Knowledge*, Foucault took his revenge by turning philosophy on its head in his later genealogical accounts of power/knowledge, where discourses are related to non-discursive practices and processes, such as economic and political changes. Foucault now moves away from a mere description of the historical rules of discourse to investigate how social practices shape discourses and vice versa. His view of power is new. He sees it as not only a negative, but also a positive force (bio-power), where discipline aims not only to constrain those over whom it is exercised, but also to make use of their capacities.<sup>96</sup> In essence, what Foucault did was to articulate a vital aspect of social relations: discourses are products of power. Power relations and scientific discourses mutually constitute one another. However, Foucault does not abandon the archaeological perspective. It becomes an internal element of his genealogical approach with the two models brought together in what he calls problematisation. Nevertheless, as Howarth points out:

---

<sup>94</sup> McNay, L: (1994) *Foucault: A Critical Introduction*, Polity Press: Cambridge, p.67

<sup>95</sup> *ibid.*, p.84



We are thus confronted with four main difficulties in Foucault's conception of discourse. These are his failure to formalise satisfactorily his theory of discourse; his inadequate conceptualisation of power/resistance; his lack of concrete analyses of resistances to power; and his inability (or refusal) to examine the 'macro' strategies and outcomes of power/resistance struggles.<sup>97</sup>

Like Howarth, Simons comments that Foucault does not attempt to systematically break down the elements of power/knowledge. Rather, his accounts are a delicate entanglement of power and truth: 'Power/Knowledge is a knot that is not meant to be unraveled'.<sup>98</sup>

But let Foucault explain:

Nothing is fundamental. That is what is interesting in the analysis of society. That is why nothing irritates me as much as these inquiries - which are by definition metaphysical - on the foundations of power in a society or the self-institution of a society, etc. These are not fundamental phenomena. There are only reciprocal relations, and the perpetual gaps between intentions in relation to one another.<sup>99</sup>

The rise of the social and the atrophy of the political through the internet are making Foucault's writings increasingly relevant to this analysis. Perhaps we can

---

<sup>96</sup> Hindess (1999), p.113

<sup>97</sup> Howarth, D: (2000) *Discourse*, Open University Press: Buckingham and Philadelphia, p.84

<sup>98</sup> Simons, J: (1995) *Foucault and the Political*, Routledge: London and NY, p. 27

<sup>99</sup> as quoted in Moss, J (ed.): *The Later Foucault*, Sage: London, p.119



use Foucault's toolkit to confront our electronic world. As power has spread and broadly diffused, escaping the confines of states, it is everywhere, very much as Foucault thought. His disciplinary theory and his biopolitics seem to explain the internet as simply another form of social control through the control of information. Elimination of public space, reducing publics to masses of atomised social agents, connects to Foucault's conception of the institution of hierarchical communication in prisons.<sup>100</sup> Moreover, when we accept that power and knowledge are so tightly linked, then the internet could be viewed as a potential source of knowledge and information. It could be viewed as a powerful tool to those who are able to use it or more importantly to control it.

The reason I am interested in discourse theory is that in this research project different types of discourses are analysed (ethnoreligious, sociopolitical, media) and discourse analysis is part of the parameters used in my integrated theoretical framework, as deployed in section 2.4 below.

In response to Foucault's writings on discourse, Laclau and Mouffe wrote extensively on discourse theory. In contrast to Foucault who maintains a distinction between discursive and non-discursive practices, Laclau and Mouffe reject the distinction. They affirm that a) every object is constituted as an object of discourse, insofar as no object is given outside every discursive condition of emergence, and b) that any distinction between what are usually called the

---

<sup>100</sup> Foucault, M: (1979) *Discipline and Punish*, Prentice Hall: London, p.238

linguistic and behavioural aspects of social practice is either an incorrect distinction or ought to find its place as a differentiation within the social production of meaning, which is structured under the form of discursive totalities.<sup>101</sup>

Moreover, Laclau and Mouffe introduce four basic categories when they analyse identity: articulation, elements, moments and nodal points. Identity emerges through the articulation or rearticulation of signifying elements and articulation is 'any practice establishing a relation among elements such that their identity is modified as a result of the articulatory practice'.<sup>102</sup> Every discourse is constituted as an attempt to dominate the field of discursivity by expanding signifying chains which partially fix the meaning of the floating signifier. The privileged discursive points that partially fix meaning within signifying chains are called nodal points or as in Lacan, *points de capiton*. The nodal point creates and sustains the identity of a certain discourse by constructing a knot of definite meanings. Torfing explains that according to Žižek, this does not imply that it is simply the 'richest' word, the word in which is condensed all the richness of meaning of the field it 'quilts'.<sup>103</sup> The *point de capiton* is rather the word which, as a word, on the level of the signifier itself unifies a given field and constitutes its identity. Discourse is 'the structured totality resulting from this practice'; 'moments are the differential positions' that 'appear articulated within a discourse' when elements are those

---

<sup>101</sup> Laclau, E and Mouffe, C: (1985) *Hegemony and Social Strategy: Towards a Radical Democratic Politics*, Verso: London and New York, p.107



differences that are 'not discursively articulated' because of the 'floating' character they acquire in periods of social crisis and dislocation<sup>104</sup>. When Laclau and Mouffe consider the material character of discourse they argue that it cannot be found in the experience of a founding subject and that diverse subject-positions appear dispersed within a discursive formation. 'The practice of articulation, as fixation/dislocation of a system of differences, cannot consist of purely linguistic phenomena; but instead pierce the entire material density of the multifarious institutions, rituals and practices through which a discursive formation is structured'.<sup>105</sup>

Also, these two theorists present us with two useful concepts: equivalence and difference. Equivalence divides social space by condensing meaning around two antagonistic poles; on the contrary, difference weakens a sharp antagonistic polarity, in order to relegate that division to the margins of society. Another significant contribution of Laclau and Mouffe is to the concept of hegemony. After they analyse Gramsci's notion of hegemony, which asserts that political subjects are complex collective wills and that the collective will is a result of the politico-ideological articulation of dispersed and fragmented historical forces, and also other Marxist conceptions, they go on to argue that the two conditions of a

---

<sup>102</sup> Howarth, D, Norval, J and Stavrakakis, Y (eds): (2000) *Discourse Theory and Political Analysis: Identities, Hegemonies and Social Change*, Manchester University Press: Manchester and New York, p. 9

<sup>103</sup> Torfing, J: (1999) *New Theories of Discourse: Laclau, Mouffe, Žižek*, Blackwell: Oxford, p.98

<sup>104</sup> Howarth, D, Norval, J and Stavrakakis, Y (eds): (2000) *Discourse Theory and Political Analysis: Identities, Hegemonies and Social Change*, Manchester University Press: Manchester and New York, p.7

<sup>105</sup> Laclau, E and Mouffe, C: (1985) *Hegemony and Social Strategy: Towards a Radical Democratic Politics*, Verso: London and New York, p. 109



hegemonic articulation are the presence of antagonistic forces and the instability of the frontiers that separate them:

...in order to speak of hegemony, the articulatory moment is not sufficient. It is also necessary that the articulation should take place through a confrontation with antagonistic articulatory practices - in other words, that the hegemony should emerge in a field criss-crossed by antagonisms and therefore suppose phenomena of equivalence and frontier effects.<sup>106</sup>

To continue, Mouffe in her own work argues it is impossible to speak of the social agent as if we are dealing with a unified, homogeneous entity. Rather, the social agent is constituted by an ensemble of 'subject-positions' that can never be totally fixed in a closed system of differences, constructed by a diversity of discourses among which there is no necessary relation, but rather, a constant movement of overdetermination and displacement.<sup>107</sup> She also agrees with Derrida that the constitution of identity is always based on exclusionary practices and the establishment of a violent hierarchy between the resultant two poles. Lastly, in her most recent work, *The Democratic Paradox*, she follows Lacan in depicting discourse as inherently authoritarian, in the sense that only through a master-signifier can a consistent field of meaning emerge. This is how she puts it:

For Lacan, the status of the master signifier, the signifier of symbolic authority founded only in itself (in its own act of enunciation), is strictly transcendental:

---

<sup>106</sup> *ibid.*, p.135

the gesture that 'distorts' a symbolic field, that 'curves' its space by introducing a non-founded violence, is *stricto sensu* correlative of its very establishment. This means that if we were to subtract from a discursive field its distortion, the field could disintegrate, 'de-quilt'.<sup>108</sup>

Laclau and Mouffe offer a useful way of thinking about discourse and ideology, especially since it does not demand a strict mode of thinking by way of methodology, so you can do the research incorporating the thinking of other writers as well, without falling out of their own logic. If we accept the proposition that the social agent is constituted by an ensemble of 'subject-positions', it is far easier to understand the subject in virtual environments like the ones this thesis addresses.

Following the writers mentioned above, especially in politics and international relations, many writers have used discourse analysis in their work, with interesting results. The reason for this, in my opinion, has a lot to do with a point made by Freeden,<sup>109</sup> when he writes that the text as a pattern of words remains an objective constant, whereas all ideologies - because they are constructed from many texts - are in a continuous process of restatement. Bowman for instance argues, particularly in relation to the nation, that political identities are discursively constructed. He writes that a wide range of persons and collectivities can identify themselves as constituent parts of the nation without having their

---

<sup>107</sup> Mouffe, C: (2000) *The Democratic Paradox*, Verso: London and New York, p.77

<sup>108</sup> *ibid.*, p.137

readings and their allegiances to it challenged or denied by particular and exclusionary definitions. This unfixity can only be maintained, however, as long as the persistence of the nation is taken for granted; as soon as the nation is discursively posited as endangered, battle lines are drawn and processes of selective exclusion/inclusion are set in play.<sup>110</sup> This is particularly relevant to elements in the ethnoreligious cyberconflict component of my proposed theoretical framework.

For example, deploying Laclauian and Žižekian concepts, Renata Salecl uses discourse analysis and a theory of identity politics to account for the way Serbians create exclusionary identities for their enemies. Salecl writes that all images of the enemy are based on specific fantasies:

In Serbian mythology, the Albanians are understood as pure evil, the unimaginable: that which cannot be subjectivised - beings who cannot be made into people because they are so radically Other. The Serbs describe their conflict with the Albanians as a struggle of 'people with no-people'...The Croats are portrayed as the heirs of Goebbels, that is, as a brutal Ustashi butchers who torment the suffering Serbian nation - a nation whose fate is compared to that of Kurds.<sup>111</sup>

---

<sup>109</sup> Freeden, M: (1996) *Ideologies and Political Theory: A Conceptual Approach*, Clarendon Press: Oxford, p. 113

<sup>110</sup> Bowman in Laclau, E: (ed): ( 1994) *The Making of Political Identities*, Verso: London and New York, p. 144

<sup>111</sup> Salecl in Laclau, E: (ed): ( 1994) *The Making of Political Identities*, Verso: London and New York, p.212



David Campbell on his part urges us to abandon the realist discourse with respect to the Bosnian conflict and consider a range of political options offered by a deconstructive reading of the conflict.<sup>112</sup> Vivienne Jabri writing on discourses on violence argues that in recognising the constructive element of language, 'discourse analysis goes some way towards contributing to an understanding of conflict as an exclusionist discourse reifying a singular way of knowing. Discourses which reify ethnonationalist identity assume a uniformity in human experience which denies a pluralism of identities'.<sup>113</sup>

The way Jabri formulates her theory on discourses on violence is very important to my research, especially when combined with Campbell's actual analysis of conflicts and Stavrakakis's way of analysing ideologies. Like Roland Barthes, Michel Foucault conceives of textuality in terms of networks and links. In *Archaeology of Knowledge*, he points out that the frontiers of a book are never clear-cut, because the book 'is caught up in a system of references to other books, other texts, other sentences: it is a node within a network... [a] network of references'.<sup>114</sup>

The political significance of CMC (Computer-Mediated Communication) lies in its capacity to challenge the existing political hierarchy's monopoly on powerful communications media and perhaps thus revitalise citizen-based democracy. The

---

<sup>112</sup> Campbell, D (1998) *National Reconstruction: Violence, Identity and Justice in Bosnia*, University of Minnesota Press: Minneapolis, p.34

<sup>113</sup> Jabri, V: (1996) *Discourses on Violence: Conflict Analysis Reconsidered*, Manchester University Press: Manchester, p. 140

vision of a citizen-designed, citizen-controlled worldwide communications network is a version of technological utopianism that could be called the vision of the 'electronic agora'.<sup>115</sup> Jordan asserts that the politics of cyberspace is strung along the two axes of access to cyberspace and rights within cyberspace.<sup>116</sup> Access is a key area of cyberpolitical debate because demographics show that use of cyberspace (up to 1998) was largely confined to a small and privileged section of the offline population. Rights are a key area of cyberpolitics because the rights of avatars are unclear and subject to revision by offline interests. The politics of online rights has developed chiefly around the areas of censorship, privacy, intellectual property and encryption. To elaborate on the process, cyberspace can alter problems such as the broadening and democratisation of decision-making procedures by removing the constraint of physical presence. Discussions carried on through email or by asynchronous posting, as used on Usenet, open possible avenues for greater group participation. Cyberspace offers opportunities for breaking down hierarchies within institutions. The global nature of cyberspace is important here, as it only requires one country connected to the net to allow the publication of some information for that information to be let loose in cyberspace. Information restricted in an offline nation-state will then be available in cyberspace, subverting the national boundaries that have helped in the past to control access to information. Jordan puts it this way:

---

<sup>114</sup> Foucault, M: (1973) *The Order of Things*, Vintage: New York.

<sup>115</sup> Margolis, M and Resnick, D: (2000) *Politics As Usual*, Sage: Thousand Oaks, London and New York, p.1



Cyberspace appears as a place in which individuals can put aside many of the inequalities of offline life, simply because nobody knows if they are 'really' female, old or disabled.... Cyberspace appears to be a place that undermines the hierarchies of offline life, in which different hierarchies that come to exist depend on the quality of thought and writing - a place where even the destructive behavior that is peculiar to it, flaming, is still only words.<sup>117</sup>

Jordan also writes on the role of elites. Particular structures and pressures in cyberspace feed into the creation of technology according to values and its use or appearance as inert things. These pressures point towards growing control of cyberspace by elites who are defined by their technical expertise, i.e. their ability to alter the 'thingness' of technology that constructs online life. If cyberspace is crucial to areas of offline life, then those that control or manage these areas will understandably seek for some reassurance that cyberspace will continue to provide its services. Producers, consumers and others will all in different ways and through different representatives endeavor to ensure that the space they depend on is reliable and secured. To do this, governments will legislate about cyberspace, corporations will build and rebuild it to their design, politicians will apply it to electioneering and consumers will demand its support.

Another question to be asked is: Who uses or has the new power offered by the internet? The United States Commerce Department released a report titled

---

<sup>116</sup> Jordan, T: (1999) *Cyberpower: The Culture and Politics of Cyberspace and the Internet*, Routledge: London and New York.

<sup>117</sup> *ibid.*, p.87



‘Falling Through the Net II’<sup>118</sup> which was requested by then-Vice President Al Gore. It examined telephone and computer penetration rates to determine who is and who is not connected to the information infrastructure, in other words who has the power which internet knowledge can provide. The study concluded that the gap between the digital haves and the digital have-nots has been growing. There is a significant gap between key groups. Whites are more than twice as likely to own computers than African-Americans or Latinos. Among the least connected are the rural poor, rural and central city minorities, young households and single-parent female-headed households.<sup>119</sup>

Manuel Castells, in *The Rise of the Network Society*, stresses that internet-related firms are, and will increasingly be in the twenty-first century, at the heart of new information-technology industries. This is how he justifies it:

First, because of their potential dramatic influence on the way business is conducted. An often-cited projection by Forrester Research in 1998 put the extended value of electronic business transactions in 2003 at about \$1.3 trillion up from \$43 billion in 1998. But, secondly, the Internet industry has also become a major force on its own ground because of its exponential growth in revenue employment, and market capitalization value.<sup>120</sup>

---

<sup>118</sup> National Telecommunications and Information Administration, 1998

<sup>119</sup> Margolis, M and Resnick, D: (2000) *Politics As Usual*, Sage: Thousand Oaks, London and New York, p.144

<sup>120</sup> Castells, M: (2000) *The Rise of the Network Society*, vol.1 of the Information Age: Economy, Society and Culture, 2<sup>nd</sup> edn, Blackwell: Oxford, p. 149

As for the impact of the internet industries on the economy as a whole, Castells informs us that in the U.S, internet-related jobs increased from 1.6 million in the first quarter of 1998 to 2.3 million in the first quarter of 1999. E-commerce represented the fastest growing sector. According to Castells,

the speed of development of the new industry was without precedent: one-third of 3,400 companies surveyed in 1999 did not exist in 1996. The growth of revenue in Internet industries in 1999 was projected to account for \$200 billion- this in contrast to total growth in revenue in the US economy of about \$340 billion. By the turn of the century, the Internet economy, and the information technology industries, had become the core of the US economy - not only qualitatively but quantitatively.<sup>121</sup>

An example of the potential impact of the internet on the economy is when in November 1999, the city of Pittsburgh handed down the opportunity of electronic disintermediation by offering \$55 billion worth of municipal bond directly to institutional investors over the internet, thus bypassing Wall Street. As Castells believes, this was the first time municipal bonds were directly sold electronically and the entry of electronic trading into the \$13.7 trillion bond market is even likely to affect financial markets.<sup>122</sup> Nevertheless, it could be argued due to the collapse of e-companies and e-stock that this bubble is bound to burst (again).

---

<sup>121</sup> *ibid.*, p.151.

<sup>122</sup> *ibid.*, p.154.

To return to political issues, Jordan provides us with a definition of cyberpower.<sup>123</sup> Cyberpower, in his view, is the form of power that structures culture and politics in cyberspace and on the internet. It consists of three interrelated regions: the individual, the social and the imaginary. Cyberpower of the individual comprises avatars, virtual hierarchies and informational space and results in cyberpolitics. Power here appears to be exercised by individuals. Cyberpower of the social is structured by the technopower spiral and the informational space of flows and results in the virtual elite. Power, at this point, appears as forms of domination. Cyberpower of the imaginary consists of the utopia and dystopia that make up to the virtual imaginary. Power in this respect appears as the constituent of social order. All three regions are needed to map cyberpower in total and no region is dominant over any other.

Lyon, on the other hand, argues that the governance of the new social polarization and the new virtual culture is governance founded upon new matrices of power. State power seeps towards individuals - the new global citizens wired up to the Internet who, through the unintended consequences of their actions, are busily forming new patterns of sociality, new virtual communities and thus new bases for power.<sup>124</sup>

In the final analysis, internet politics, like any other politics, are closely related to power, because individuals or groups using the medium are inevitably involved in

---

<sup>123</sup> Jordan, T: (1999) *Cyberpower: The Culture and Politics of Cyberspace and the Internet*, Routledge: London and New York, p.208

<sup>124</sup> Loader, B (ed.): (1997) *The Governance of Cyberspace*, p.44



power relations. The problem is that not all people have the power of knowledge the internet can provide, since the medium as yet is mostly used by white, middle-class males, a trend that is starting to change slowly, as in our non-virtual social sphere. To explain, the internet offers opportunities for breaking down political hierarchies within institutions, while subverting the national boundaries that have helped in the past to control access to information. Social movements, in particular, might still be asking for traditional forms of political power; however, the new power they have because of the internet could be characterised as somewhat non-traditional, in the sense of giving them access to mass audiences they were previously denied.

### **1.3 The globalisation-internet connection.**

Another issue identified in my research is that of globalisation. The reason for this is that the internet can be seen as a global phenomenon, very much contemporaneous to globalisation, to the extent that, among its other effects, it has a globalising influence, allowing differing cultures the chance to co-exist. It is necessary, I think, to look briefly at the debate on globalisation, in order to place internet politics in their political environment, especially when the internet is seen by many as a tool of this process.

Processes of globalisation are challenging the bases of order in profound ways: First, by exacerbating inequalities both with and among states; and second, by eroding the capacity of traditional institutions to manage the new threats. Globalisation transforms the processes, the actors and capabilities, and the agenda of world politics, necessitating more effective international institutions of management. In more contemporary terms, institutions need to probe deeply into domestic politics, ensuring compliance with agreements on issues ranging from the environment to trade and arms control. The concept of globalisation describes dramatic changes in the transactions and interactions taking place among states, firms and peoples in the world. It describes both an increase in cross-border

transactions of goods and services and an increase in the flow of images, ideas, people and behaviour. Woods puts it this way:

Economistic views treat the process as technologically driven. Yet, globalization has also been driven by deregulation, privatization and political choices made by governments... In other words the impact of globalization has been strongly shaped by those with the power to make and enforce the rules of global economy.<sup>125</sup>

Globalisation is cementing old economic inequalities between 'haves' and 'have-nots' - not just in the sense of having technology or not, but also in the sense of having the capacity to make rules or not. Yet, at the same time, globalisation is creating a new set of requirements for regulation and enforcement which requires the cooperation of the so-called 'have-nots'.

Currently, there is a debate between globalists and sceptics in theoretical terms. Empirical examples of these two camps are found in the discussion of cyberpolitical dimensions in conflicts.<sup>126</sup> This debate involves fundamental considerations about the nature of world order - as it is and as it may be. Disagreements can range over at least three separate dimensions: First, the philosophical concern with conceptual and normative tools for analysing world order; second, the empirical-analytical concern with the problems of

---

<sup>125</sup> Woods in Held, D and McGrew, A: (2000) *The Global Transformation Reader*, Polity Press: Cambridge, p.389



understanding and explaining world order; and third, the strategic concern, which focuses on an assessment of the feasibility of moving from where we are to where we might like to be.<sup>127</sup>

Globalists seek to review the nature and meaning of the modern polity in its global setting. They reject the assumption that one can understand the nature and possibilities of political life by referring primarily to national structures and procedures. The transnational and global scale of contemporary economic and social problems presents, globalists contend, a unique challenge to the modern state. This challenge involves, in the first instance, the recognition of the way globalisation generates a serious 'political deficit' - a deficit which encompasses democracy, regulation and justice. Second, reexamining the changing context of the modern state entails recognising the way globalisation stimulates new political energies and forces, which are providing an impetus to the reconfiguration of political power. These include the numerous transnational movements, agencies and NGOs pursuing greater coordination and accountability in regional and global settings. Third, globalists affirm that a shift is and ought to be taking place between political and ethical frameworks based on the national political community and those based on a wider set of considerations.

---

<sup>126</sup> Introduction in Held, D and McGrew, A: (2000) *The Global Transformation Reader*, Polity Press: Cambridge.

<sup>127</sup> McGrew in Held, D and McGrew, A: (2000) *The Global Transformation Reader*, Polity Press: Cambridge, p.401

In stark contrast, sceptics hold that the modern theory of the state presupposes a community, which rightly governs itself. The modern theory of the sovereign democratic state, they contend, upholds the idea of a national community of fate - a community which properly governs itself and determines its own future. For the sceptics, particularly those who subscribe to the communitarian outlook, the values of the community take precedence over all universal requirements.

According to McGrew, globalisation presents modern democratic theory with a daunting task: how to reconcile the principle of rule by the people with a world in which power is exercised increasingly on a transnational or even global scale.<sup>128</sup> Today, McGrew believes, the fate of democratic communities across the globe is becoming ever more tightly interwoven by patterns of contemporary globalisation with the result that established territorial models of liberal democracy appear increasingly hollow. In his own words:

A new agenda for democratic theory is called for: one which breaks with conventional accounts of democracy in which the nation-state is conceived as the only proper incubator of democratic political life. Central to this new agenda is a critical enquiry into the necessity, desirability and possibility of 'global democracy' - that is of democracy beyond borders.<sup>129</sup>

Furthermore, Held argues that contemporary globalisation is transforming state power and the nature of political community, but any description of this as a

---

<sup>128</sup> *ibid.*, p.405

simple loss or diminution of national power distorts what has happened. For although globalisation is changing the relationship between states and markets, this is not straightforwardly at the expense of states. Held puts it this way:

States and public authorities initiated many of the fundamental changes - for example, the deregulation of capital in the 1980s and early 1990s. In other spheres of activity as well, states have become central in initiating new kinds of transnational collaboration, from the emergence of different forms of military alliances to the advancement of human rights regimes.<sup>130</sup>

Contemporary globalisation has contributed to the transformation of the nature and prospects of democratic political community in a number of distinctive ways<sup>131</sup>. First, the locus of effective political power is shared by diverse forces and agencies at national, regional and international levels. Second, the idea of a political community of fate - of a self-determining collectivity - can no longer be meaningfully located within the boundaries of a single nation-state alone, as it could more reasonably be when nation-states were being forged. Third, national sovereignty today, even in regions with intensive overlapping and divided political structures, has not been wholly undermined - far from it. Regarding the internet, it seems that a new form of nation has developed. It is what Barrett calls the 'cybernation'<sup>132</sup>. As the internet has been used by more and more people

---

<sup>129</sup> *ibid.*, p.405

<sup>130</sup> Held in Held, D and McGrew, A: (2000) *The Global Transformation Reader*, Polity Press: Cambridge, p.421

<sup>131</sup> *ibid.*, p.423

<sup>132</sup> Barrett, N: (1996) *The State of the Cybernation*, Kogan Page: London.



throughout the world, Barrett argues it has carved a unique cultural niche. The initial subculture of internet users evolved a set of acceptable behaviours, a common history and arguably a common identity of beliefs: free speech, protection of civil rights, impatience with naive questions from the newly initiated, etc. So, Barrett suggests that

a cybernation - a nation whose communication of commonly held beliefs and philosophies is effected by the Internet or similar mechanisms-already exists. This initial subculture has been added to and developed further as ever more people around the world find their way into 'cyberspace', creating an evolving and essentially self-organizing community.<sup>133</sup>

Another theme that usually comes up in discussions of globalisation, is that of world government. The classical argument for world government is that order among states is best established by the same means, whereby it is established among individual men within the state that is by a supreme authority, which perhaps too freely equates states to individuals. As Bull asserts:

It is often argued today for example that a world government could best achieve the goal of economic justice for all individual men, or the goal of sound management of the human environment. The argument against world government has been that, while it may achieve order, it is destructive of liberty or freedom: it infringes the liberties of states and nations and also checks the liberties of

---

<sup>133</sup> *ibid.*, p.15

individuals who if the world government is tyrannical, cannot seek political asylum under an alternative government.<sup>134</sup>

An argument entertained in the area of internet research, in relation to the issue of world government, is that with the spread of the internet, there is scope for a newly international localism; that is, finding expression in 'virtual' communities, with some people going so far as to suggest that a new global cyberstate is forming. There also signs that online communities will offer further dimensions to personal identity within an already complex world.

In the course of the ongoing discussion, one of the most prominent new tools of globalisation is the internet. The problem connected to the internet in terms of its globalisation potential is that of cultural homogenisation. Some countries on the receiving end of information are concerned that humanity is becoming homogenised, and that they will lose their cultural identity in the rush to become Anglo-Western. This is one of the main reasons cited by Singapore for enacting its draconian internet censorship legislation in 1996.<sup>135</sup> Malaysia, too, has noted this aspect of unfettered information flows and has expressed concern that images and lifestyles presented on the internet may offend, for example, Muslim sensibilities. Burma and Cambodia are not noted for their tolerance of opposition political groups. Their government have both expressed concern at the

---

<sup>134</sup> Bull in Held, D and McGrew, A: (2000) *The Global Transformation Reader*, Polity Press: Cambridge, p.445.

<sup>135</sup> *ibid.*, p.32

consequences of open and unfettered access to the internet, as all the while they come under increasing pressure to connect.

Another issue concerning internet and globalisation is that the internet for all its rhetoric of globalisation is conducted mostly in English. Those who want to access the internet must have a good knowledge of English, which presupposes a western-influenced education. Only the elites within developing countries can get that sort of education, which marginalises others, especially in rural areas. Moreover, few people in the South have access to the internet and not all speak the internet language English, and even post-colonially, information about the South is primarily written from information and research produced in the North. As Everard puts it, '[t]his can lead to erosion of cultural identity, national values and cultural integrity, through what Holderness describes as the homogenisation of humanity'.<sup>136</sup> More interestingly, while internet uptake is growing among those outside North America and Western Europe, internet-based communication within and between anti-capitalist movements continues to be dominated by English language users.<sup>137</sup>

The one area where cyberspace has undoubtedly brought political change is the emergence of a global system that restructures the power of the nation-state. Jordan explains: 'Finances flowing across national borders show little regard for

---

<sup>136</sup> *ibid.*, p.37

<sup>137</sup> Wright, S: 'Informing, communicating and ICTs in contemporary anti-capitalist movements' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p. 92



the interests of the nation-state they flow through. Information spreading instantly throughout cyberspace evades controls that are more easily put in place on nationally based, centralised broadcast media'.<sup>138</sup>

An example of this is when emails came out of Russia describing the attempted coup against Gorbachev, providing a commentary 'as it happened' that eroded state censorship. Again in Russia, more than a decade later, text messages broadcast on the internet were sent during the notorious Moscow theatre incident, while the audience was held hostage by Chechen autonomist rebels.

Another point that deserves attention is that of cultural imperialism on the net. In 'The Harvard Conference on Internet and Society' several people expressed their views on the subject.<sup>139</sup> An obvious one came from Anne-Marie Slaughter, a lawyer at Harvard School, who championed the idea that it is not cultural imperialism we should be worried about, but rather, the divide between those who are privileged and online, and the rest of the world. The second came from Izumi Aizu, an intercultural communications specialist in Japan, who maintained that the internet creates a global arena for 'seemingly minor culture... that the mass economy cannot pay attention to. In some developing countries people are now jumping into use the net, not only to absorb knowledge and information from the advanced countries, but to share their own with others'.<sup>140</sup>

---

<sup>138</sup> Jordan, T: (1999) *Cyberpower: The Culture and Politics of Cyberspace and the Internet*, Routledge: London and New York, p.162

<sup>139</sup> Slevin, J: (2000) *The Internet and Society*, Polity Press: Cambridge, pp. 208-210.

<sup>140</sup> *ibid.*, p.209

To sum up, the internet is one of the most prominent new tools of a globalised world. Despite the global rhetoric, there is a divide between those who are privileged and online and the rest of the world, with the appearance of the problems of cultural homogenisation and cultural imperialism, since internet traffic at the moment is mostly conducted in English. Moreover, information spreads instantly throughout cyberspace and so evades controls over it, even by the powerful states. The fact that the internet is part of the globalisation process could be used as a platform to argue that it does go beyond traditional politics of sovereignty and therefore is postmodern in nature.

#### **1.4 A postmodern medium?**

One reason for dwelling on the question of whether the internet is a postmodern medium is that the answer one gives is likely to determine one's assessment of the implications and effects of the internet on society, politics and culture. The central issues identified here concerning postmodernity and the internet are community, identity, discourse and structure. Let us examine these in turn. However, let me start with the lay out of the general approaches and issues on the subject first.

The use of ICTs, being an intellectual activity, has far-reaching implications for our notions of autonomy, sovereignty and self-determination. The individual in cyberspace is fragmented in databases and networks. As a result of this fragmentation, the individual as a meaningful entity becomes decentred and multiplied. Does this mean that we become postmodern?

The postmodern refers to a condition of disunity and the fragmentation of knowledge. Postmodernism involves an epistemological shift from the perceived wholeness of knowledge to a realisation that information is by its very nature fragmented. According to Chapman there are two views taken on the internet. The first is the transmission view, where the internet is viewed as simply a mechanism for the instantaneous distribution of information at the global level, and the second is the view of internet use as ritual, linked to terms such as sharing, participation, association, fellowship and the possession of common faith,



rendering the internet more than the transmission of signals and messages.<sup>141</sup> Or as Poster argues, modernity or the mode of production signifies patterned practices that elicit identities as autonomous and rational, whereas postmodernity or the mode of information indicates communication practices which constitute subjects as unstable, multiple and diffuse, where one gets a sense of fragmentation and decentred self, multiple and conflicting identities and a subverted order. The first view, essentially a modernist perspective, tends to reduce the internet to a hammer. 'In the grand narrative of modernity, the internet is an efficient tool of communication, advancing the goals of its users who are understood as preconstituted instrumental identities'.<sup>142</sup> In contrast, the second view takes account of the social dynamics of online culture, and cyberspace becomes the realm of pure possibility. Reason (the 'modern' Enlightenment catchphrase) becomes a space of possibility. Also, postmodernism is a viewpoint that emphasises the horizontal over the hierarchical, and the internet is a rhizomatic structure:

Cyberspace is a 'smooth space' whose potential for expansion is infinite. One rides a 'flux' and a 'flow' of information. One wanders. As a holding environment, cyberspace is rhizomatic (Deleuze and Guattari, 1987). It is like a subterranean stem that grows and spreads horizontally. In cyberspace thought is pushed to the level of the formal operational mind where the rules of thought are

---

<sup>141</sup> Chapman, R: 'Hyperlinks and HyperProtestantism: The Internet as a postmodern epistemological shift', Lincoln Trail College, Robinson, Illinois, undated

<sup>142</sup> Poster, M: 'Cyberdemocracy: Internet and the public sphere', University of California, Irvine, [www.humanities.uci.edu/mposter/writings/democ.html](http://www.humanities.uci.edu/mposter/writings/democ.html)

themselves transcended and where reason, as a consequence, becomes a space of possibility.<sup>143</sup>

This shift to a decentralised network of communication makes senders receivers, producers consumers, and rulers ruled, upsetting the logic of the first media age. This is why Poster is calling for a poststructuralist analysis of the modes of subject constitution.<sup>144</sup> Such an account would avoid the continued, limiting exclusive repetition of the logics of modernity, '[f]or the chief characteristics of subjecthood, the resistance of the new media to modernity lie in their complication of subjecthood, their denaturalizing the process of subject formation, their putting into question the interiority of the subject and its coherence'.<sup>145</sup>

Another characteristic of postmodernism is the simulation of reality. People lose touch with reality and replace it with symbols of reality. Due to the seeming weightlessness of the online environment, the reality of its production is hidden, negating its value and rendering its product an experience.<sup>146</sup> What exists in cyberspace, hyper-reality, image saturation, and simulacra, seem more powerful than the real and the cyborgian mixing of organic and inorganic, human and machine follows a postmodern logic:

---

<sup>143</sup> Emery, E: 'The postmodern desert: Solitude and community in cyberspace', Preconvention papers, The American Benedictine Academy, [www.osb.org/aba/aba2000/emery.html](http://www.osb.org/aba/aba2000/emery.html), p.4

<sup>144</sup> Poster, M: 'Cyberdemocracy: Internet and the public sphere', University of California, Irvine, [www.humanities.uci.edu/mposter/writings/democ.html](http://www.humanities.uci.edu/mposter/writings/democ.html)

<sup>145</sup> *ibid.*, p.41.

<sup>146</sup> Thiel, S: 'The online newspaper: A postmodern medium', *The Journal of Electronic Publishing*, University of Michigan Press, 4/01.



Just as we represent the hardware of human existence, so we express through these machines a collective consciousness – the software of human existence – a consciousness increasingly fragmented and eclectic – and we call that fundamentally postmodern embodiment, expressed on that representation of the postmodern body – The internet!<sup>147</sup>

### *Community in Cyberspace*

Prominent in Jordan's work is the idea that an imagined community exists in cyberspace. Anderson defined a nation as an imagined political community - and imagined as both inherently limited and sovereign.<sup>148</sup> It is imagined because it is impossible for all members of the community to meet; they must hypothesise their commonality. It is limited because there are always borders and beyond those borders there are other nations. It is sovereign because it creates its own rules within its borders. Finally, it is a community because regardless of actual inequalities between members of a nation, it is always conceived as a deep 'horizontal comradeship' in which all are equal as members of the nation. Though Anderson uses this definition to explore the nature of the nation state, something cyberspace helps to undermine, a similar community exists in cyberspace. Jordan comments:

---

<sup>147</sup> Poster, M: 'Cyberdemocracy: Internet and the public sphere', University of California, Irvine, [www.humanities.uci.edu/mposter/writings/democ.html](http://www.humanities.uci.edu/mposter/writings/democ.html).

<sup>148</sup> Anderson, B: (1991) *Imagined Communities*, 2<sup>nd</sup> edn, Verso: London, p.6.



There seems little doubt that alongside the virtual lives that individuals construct and the virtual societies technopower conditions, another layer of cyberpower exists on the fantasies and nightmares that collectively constitute the imagination of cyberspace. Here will be found the common beliefs of individuals who never meet each other that will move them to fight for their cybercommunity, believe in their cybercommunity and even love their cybercommunity.<sup>149</sup>

Similarly, Castells asks: 'So, in the end are virtual communities real communities?'<sup>150</sup> His answer is that virtual communities are communities but not physical ones, and they do not follow the same patterns of communication and interaction as physical communities do. For him, virtual communities are not 'unreal'; they just work in a different plane of reality. They are interpersonal social networks, most of them based on weak ties, highly diversified and specialised, still able to generate reciprocity and support by the dynamics of sustained interaction.

Slevin accepts that technologies such as the internet are opening up opportunities for new forms of communication, when he argues that the production and reproduction of social reality is becoming re-embedded in local communal life in ways which were largely unavailable in previous modern settings. He writes as follows:

---

<sup>149</sup> Jordan, T: (1999) *Cyberpower: The Culture and Politics of Cyberspace and the Internet*, Routledge: London and New York, p. 183.

<sup>150</sup> *ibid.*, p. 155

The possibilities of virtual reality are boosting to the extreme the dynamism of modern everyday life by heightening the process which Giddens describes as tearing 'space away from place by fostering relations between absent others'; 'the severing of time from space' he continues, 'provides a basis for their combination in relation to social activity...This phenomenon serves to open up manifold possibilities of change by breaking free from restraints of local habits and practices'.<sup>151</sup>

### *Identity in cyberspace*

In order to understand the impact of the internet on the individual, Slevin draws upon the work of Rheingold<sup>152</sup> who indicates that America has lost a needed sense of social commons and that, in the face of such loss, 'virtual communities' just happen to fulfil this need. In this fashion, internet users, Slevin argues, tend to appear as what Giddens describes as 'cultural dopes', not as actors who are highly knowledgeable 'discursively and facetly' about the institutions they produce and reproduce in and through their actions.<sup>153</sup> However, in *Between Facts*, Habermas had rejected much of the 'cultural dope' approach to media studies, arguing instead that citizens adopt strategies of interpretation against media messages.<sup>154</sup>

---

<sup>151</sup> Slevin, J: (2000) *The Internet and Society*, Polity Press: Cambridge, p.106.

<sup>152</sup> Reingold, H: (1994) *The Virtual Community: Surfing the Internet*, Minerva: London.

<sup>153</sup> Slevin, J: (2000) *The Internet and Society*, Polity Press: Cambridge, p.107.

<sup>154</sup> Salter, L: (2003): 'Democracy, social movements, and the Internet' in McCaughey, M and Ayers, M: *Cyberactivism: Online Activism in Theory and Practice*, Routledge: New York and London, p.125.

But what are the direct effects of the internet on individuals? Slevin comments that people who work at home or on the move, with no real place in the organisation which they can call their own, may feel alienated. They no longer have a fixed 'place' of work where they can develop shared experiences and a sense of belonging.<sup>155</sup>

To illustrate the point that the internet has a negative impact on the individual, Slevin refers to the HomeNet project. The families in the study came from eight diverse neighborhoods in Pittsburgh, Pennsylvania. According to the study, greater use of the internet was associated with subsequent declines in family communication. Greater use of the internet to communicate was also associated with declines in the size of both the local and the distant social circle. Individuals who made greater use of the internet also reported larger increases in loneliness. Remarkably, the researchers write that greater use of the internet was associated with increased depression and disengagement from real life.<sup>156</sup> Nonetheless, this writer is not sure of the validity of these findings, when brought under more empirical scrutiny.

Moreover, Everard's analysis focuses on identity issues when examining the internet. He cites Turkle who suggests that the use of multiple identities in cyberspace merely extends the range of selves available, thus making the individual in a sense more complete, and more comfortable to try out a range of

---

<sup>155</sup> Slevin, p.132.

<sup>156</sup> *ibid.*, p.167.



points of view. The point is that the modern notion of individuals being unitary is itself an illusion. The self of language and of symbolic order at large is always virtual - a simulation.<sup>157</sup> In addition, the internet allows individuals to expand beyond identities based on geographical territories, towards identities based more on the cultural terrain of cyberspace.

On the other hand, the issue of identity is not merely one of philosophical importance, but also as one of immense practical importance for the conduct of states - not to mention identifying the lines of flight from the status quo:

For example, the issue of the 'authentic' author is an aspect not only of intellectual property rights, but also of authentication for business transaction. Am I the purchaser that I am presenting myself as? Are you a genuine business to whom I can submit my credit card number? Will a third party intercept my credit card details? All these are questions of identity.<sup>158</sup>

### *Discourse in cyberspace*

At the core of the digital zone, moreover, is rapid access to the global, informational archive that simultaneously delights and overwhelms any user who turns to it only for empirical certainty, historical veracity, and subjective validation. In the zones of the internet and digital installation artwork, the graphic certitude of the factual is entwined in the figural play of the fictional, the privacy

---

<sup>157</sup> *ibid.*, p.125

<sup>158</sup> *ibid.*, p.159

of the personal erodes with the interactivity of the social, the patient quietude of reading is interlaced with the jumpy quickness of surfing, and the quasi-religious contemplation of textuality and high art becomes newly energised by the flashy multi-media quacking of art in the electrifying zone of the digital.<sup>159</sup>

In postmodernism we also find a suspicion and an ironic deconstruction of master narratives, and a trust and investment in micropolitics, identity and local political struggles. In information technology, writing/speech distinctions lose some of their meaning. The written word takes on a more immediate nature and begins to function as if it were speech. Writing thus achieves a 'transcendence' on the internet, as a third-order simulation of speech. This perspective helps to explain how power relations are constructed through discourse and how ideological work is done. This issue is addressed in Loader's *The Governance of Cyberspace*. In his own words:

It is precisely these postmodernist little narratives which may be characteristic of discourse in cyberspace. As Poster remarks 'the Internet seems to encourage the proliferation of stories, local narratives, without any totalising gestures and it places senders and addressees in symmetrical relations'. Moreover, these stories and the performance consolidate the "social bond" of the Internet community.<sup>160</sup>

Jordan also comments on the effects of cyberpunk culture on cyberspace:

---

<sup>159</sup> Murray, T: (2004) 'New media art and rhizomatic in-securities', Ctheory.net.

While it is clear that cyberpunk was a movement, its ideas have had a much broader effect than on just science fiction. Two ideas in particular were prefigured in cyberpunk science fiction that have had a lasting effect on cyberspace: the organisation of information as virtual spaces and the nature of virtual bodies...The first is the most significant, because it attempts to directly describe, picture, dissect and understand cyberspace.<sup>161</sup>

Cyberspace has been conceptualised as a net, a matrix, a metaverse and universally as a place constructed out of information. That is why it is not merely a medium easily controlled, but *another* place altogether: 'The performativity of an utterance...increases proportionally to the amount of information about its referent one has at one's disposal. Thus the growth of power, and its self-legitimisation, are now taking the route of data storage and accessibility, and the operativity of information'.<sup>162</sup>

Castells brings forward the actual form of language on the internet. He argues:

To some analysts CMC, and particularly email represents the revenge of the written medium, the return to the typographic mind and the recuperation of the constructed, rational discourse. For others, on the contrary, the informality,

---

<sup>160</sup> Loader, B (ed.): (1997) *The Governance of Cyberspace*, Routledge: London and New York, p. 8.

<sup>161</sup> Jordan, T: (1999) *Cyberpower: The Culture and Politics of Cyberspace and the Internet*, Routledge: London and New York, p. 25

<sup>162</sup> *ibid.*, p.37 quotes Lyotard J-F, *The Post-modern Condition: A Report on Knowledge*, University of Minnesota press: Minneapolis, 1984: 47



spontaneity, and anonymity of the medium stimulates what they call a new form of 'orality', expressed by an electronic text.<sup>163</sup>

When electronic communications are a factor in the theorist's understanding of the subject, language is understood as performative and rhetorical, and as an active figuring and positioning of the subject. With the spread of this regime of communications, the subject can only be understood as partially stable, as repeatedly reconfigured at different points of time and space, as non-self-identical and therefore as always partly Other.<sup>164</sup>

The internet is a loose, decentered network of mainframes and personal computers that sustains global connections among its users. Internet discourse is routinely off-topic, repetitive, inane or obscene. It is not too much to say that an ethic of anarchy, with disparate voices raised in electronic cacophony, often prevails.

Perhaps more so than any other contemporary theorist, Jean Baudrillard provides a provocative direction for 'navigating' this hyperreal terrain. Although he has not addressed worldwide networking and the internet specifically in his writing, his comments on telematics, along with more general critiques of modernity, provide an interesting means for exploring the internet. From a Baudrillardian perspective, this figuration of the internet as a kind of cybernetic terrain works to undermine

---

<sup>163</sup> *ibid.*, p.389

<sup>164</sup> Poster, M: (1995) *The Second Media Age*, Polity Press: Cambridge, p.59.

the symbolic distance between the metaphorical and the real.<sup>165</sup> Baudrillard's reading can be used to move internet studies beyond its modern closures. Replacing the one world with multiple possible worlds, the internet ultimately offers both the seductions and subductions of a postmodern world.

### *The postmodern argument*

When Nicholas Negroponte introduces us to his digital world, we find out that the impact of digital technology is great, and explore what being digital means and how our lives may be enhanced. Negroponte supports the view that even if nobody has a clear idea of who pays what on the internet, it appears to be free to most users. Even if this changes in the future and some rational economic model is laid on top of the internet, it may cost a penny or two to distribute a million bits to a million people. In Negroponte's view, computing no longer falls within the exclusive realm of military government and big business. It is being channelled directly into the hands of very creative individuals at all levels of society, thereby becoming the means for creative expression in both its use and development. In Negroponte's words:

The agent of change will be the Internet, both literally and as a model or metaphor. The Internet is interesting not only as a massive and pervasive global network, but also as an example of something that has evolved with no apparent

---

<sup>165</sup> Nunes, M: (1995) 'Baudrillard in cyberspace: Internet, virtuality, and postmodernity', *Style* 29, p.314.

designer in charge, keeping its shape very much like the formation of a flock of ducks. Nobody is the boss, and all the pieces are so far scaling admirably.<sup>166</sup>

For Baudrillard, the shift from the real to hyperreal occurs when we move from mere representation to simulation, a movement already existing in our virtual world. According to Baudrillard the screen represents an example of the 'satellisation of the real' by achieving the escape velocity of hyperreality: '[t]hat which was previously mentally projected, which was lived as a metaphor in the terrestrial habitat is from now on projected entirely without metaphor, into the absolute space of simulation'.<sup>167</sup>

Another characteristic of the internet, which gives it a postmodern character, is that it becomes a hyperreal vehicle for travelling across a simulated world. The image of 'cybertravel' offers a metaphorical world beyond a computer screen, a 'globe' of nomads that no longer stands for the world, because it has become the 'world'. The Microsoft question that pops on the screen 'Where do you want to go today?' creates the simulation of a form of power and the creation of a virtual world which destroys the conceptual possibility of distance. This is why Baudrillard writes that '[t]he Telecomputer Man experiences a very special kind of distance which can only be described as unbridgeable by the body...The screen is merely virtual and hence unbridgeable'.<sup>168</sup>

---

<sup>166</sup> Negroponte, N: (1995) *Being Digital*, Hodder and Stoughton: London, p.181

<sup>167</sup> Baudrillard, J: (1988) *The Ecstasy of Communication*, Semiotext: New York, p.16.



Moreover, the internet does not simply annihilate distance; it creates its own simulated world in place of the physical world of spatial distances. Once the internet moves closer to total connectivity, this metaphorical 'cyberspace' could become the hyperreal – more real than the real place it once simulated.<sup>169</sup> Baudrillard refers to this moment as the 'precession of simulacra', when the globe/model defines the world it once approximated.<sup>170</sup> Carrying this Baudrillardian reading to its further limits, one might conclude that what occurs is 'the end of space through cyberspace, the end of knowledge through information and the end of the imaginary through the hyperreal'.<sup>171</sup>

For millions of netters, cyberspace is a real place, more egalitarian than elitist and more decentered than hierarchical. Rheingold asks: '[h]ow are relationships and commitments as we know them even possible in a place where identities are fluid?'<sup>172</sup> We reduce and encode our identities as words on a screen, decode and unpack the identity of others. The fact that many people believe virtual communities to be real places in which they live real experiences, makes this blurring of the real and the unreal close to Baudrillard's postmodern moment of the hyperreal. The following abstract is telling:

---

<sup>168</sup> Baudrillard, J: (1993) *The Transparency of Evil*, Verso: New York, p.55

<sup>169</sup> Nunes, M: (1995) 'Baudrillard in cyberspace: Internet, virtuality, and postmodernity', *Style* 29, p.316.

<sup>170</sup> Baudrillard, J: (1983) *Simulations*, Semiotext: New York, p.2.

<sup>171</sup> Nunes, M: (1995) 'Baudrillard in cyberspace: Internet, virtuality, and postmodernity', *Style* 29, p.319

<sup>172</sup> Rheingold, H (1991) *Virtual Reality*, Secker and Warburg: London, p.61.

Cyberspace is not real! Hacking takes place on a screen. Words aren't physical, numbers...aren't physical...Computers simulate reality, such as computer games that simulate tank battles or dogfights or spaceships. Simulations are just make-believe, and the stuff in computers is not real. Consider this: If 'hacking' is supposed to be so serious and real-life and dangerous then how come nine-year-old kids have computers and modems? You wouldn't give a nine-year-old his own car, or his own rifle, or his own chainsaw - those things are 'real'.<sup>173</sup>

Finally, the promise of unlimited information and the threat of this information being controlled leads to the realisation that sophistication in technology produces more convincing simulations of information and more convincing strategies of deterrence. With the fascination of unlimited information what we are not realising is that in fact despite all this information we have nothing to learn:

The addiction we have for the media, the impossibility of doing without them... is not a result of a desire of culture, communication and information, but of this perversion of truth and falsehood, of this destruction of meaning in the operation of the medium. The desire for a show, the desire for simulation... is a spontaneous, total resistance to the ultimatum of historical and political reason.<sup>174</sup>

Nonetheless, it should be noted that Poster does not fail to criticise Baudrillard's work, which remains infused with a sense of the media as unidirectional, and

---

<sup>173</sup> Sterling, B: (1992) *The Hacking Crackdown: Law and Disorder on the Electronic Frontier*, Viking: London, p.84.

therefore does not 'anticipate the imminent appearance of bidirectional, decentralised media, such as the Internet, with its new opportunities for reconstructing the mechanisms of subject constitution'.<sup>175</sup> However, if we follow Baudrillard all the way, it seems as if the audiences comprise of helpless and gullible idiots who are incapable of interpreting or reinterpreting images of violence. Signs are made possible by the new technologies of the media in which signifiers flash past potential consumers. Once signifiers have been separated and abstracted in this way, floating free so to speak, in communicational space they can be attached to particular commodities by the arbitrary whim of advertisers. According to Baudrillard, individuals consume meanings rather than products, resulting in symbolic exchange.<sup>176</sup> As Poster argues:

Electronically mediated communication opens the prospect of understanding the subject as constituted in historically concrete configurations of discourse and practice.... [I]n turn such a prospect challenges all those discourses and practices that would restrict this process, would fix and stabilise identity, whether these be fascist ones which rely on essentialist theories of race, liberal ones which rely on reason, or socialist ones, which rely on labor.<sup>177</sup>

A poststructuralist approach to communication theory analyses the way electronically mediated communication (what Poster calls 'the mode of

---

<sup>174</sup> Poster, M: (1995): *The Second Media age*, Polity Press: Cambridge, p.16, quotes Baudrillard: (1988) *Selected Writings*, ed. Mark Poster, Polity Press: Cambridge; Stanford University Press: Stanford, p.55

<sup>175</sup> *ibid.*, p.19

<sup>176</sup> *ibid.*, p.107

<sup>177</sup> *ibid.*, p.77.



information') both challenges and reinforces systems of domination that are emerging in a postmodern society and culture: 'the figure of the self, fixed in time and place, capable of exercising cognitive control over surrounding objects may no longer be sustained... [E]lectronic communications systematically remove the fixed points, the grounds, the foundations that were essential to modern theory'.<sup>178</sup> Continuing from Derrida, Poster writes that both deconstruction and electronic writing understand the volatility of written language, its instability and uncertain authorship. Both see language as affecting a destabilisation of the subject, a dispersal of the individual, a fracturing of the illusion of unity and fixity of the self.<sup>179</sup>

Karim in 'Diasporas and their communication networks: Exploring the broader context of transnational narrowcasting' addresses the question of the postmodern, when he mentions Arjun Appadurai<sup>180</sup>, who sees the global cultural economy as characterised by fundamental disjunctures between what he identifies as five dimensions or 'scapes' of 'global cultural flow': ethnoscap (people), mediascapes (media content), technoscapes (technology), finanscapes (capital) and ideoscapes (ideologies).<sup>181</sup> The diasporic site becomes the cultural border between the country of origin and the country of residence - Homi Bhabha's

---

<sup>178</sup> *ibid.*, p.60.

<sup>179</sup> *ibid.*, p.72.

<sup>180</sup> Appadurai, A: (1996) *Modernity at Large: Cultural Dimensions of Globalization*, University of Minnesota: Minneapolis.

<sup>181</sup> Karim, H.K: 'Diasporas and their communication networks: Exploring the broader context of transnational narrowcasting' (Draft), School of Journalism and Communication, Carleton University, Ottawa.

'third space'.<sup>182</sup> Hall views this process as operating 'on the terrain of the global postmodern', which 'is an extremely contradictory space'.<sup>183</sup> These global networks are allowing for relatively easy connections for members of communities residing on various continents. In opposition to the broadcast model of communication, which apart from offering limited access to minority groups, is linear, hierarchical, and capital intensive, on-line media allow easier access and are non-linear, largely non-hierarchical, and relatively cheap.<sup>184</sup> As governments seek to prevent terrorism by more tightly sealing national borders, transnational movement is becoming problematic for potential emigrants from non-western states. Additionally, the loyalty of minority ethnic groups living in western countries is becoming suspect and their transnational connections and relationships are coming under scrutiny. The multiple and hybrid identities of diasporic members are under renewed pressure to conform to the mythical notion of a monolithic populace of the traditional nation-state.

The *homo politicus*, *le citoyen*, is no longer the dominant actor. Systems are becoming more and more intelligent and at a growing pace are better at several things. ICT, being an intellectual technology has far-reaching implications for our notions of autonomy, sovereignty and self-determination. Reality is the unintended result of decisions which are increasingly taken by machines, and the individual in cyberspace is fragmented in databases and networks. As a result of

---

<sup>182</sup> Bhabha, H: (1994) *The Location of Culture*, Routledge: New York.

<sup>183</sup> Hall, S: (1997) 'The Local and the Global' in A. McClintock et.al: *Dangerous Liaisons: Gender, Nation and Postcolonial Perspectives*, University of Minnesota: Minneapolis.

<sup>184</sup> Karim, cites Karim, Smeltzer and Loucheur, 1998



this fragmentation, the individual as a meaningful entity becomes decentred and multiplied. Thus we become postmodern.<sup>185</sup>

In pursuit of similar answers, albeit in a more philosophical mode, Deleuze and Guattari in their work *A Thousand Plateaus* provide us with a detailed analysis of the subject's multiplicities and dimensions.<sup>186</sup> They formulate the concept of the rhizome, which has the characteristics of connection and heterogeneity: any point of a network of rhizomes can be connected to anything else in the network, and must form such connections. This is very different from the tree or root, which plots a point and fixes an order. The linguistic tree on the Chomskian model still begins at a point S and proceeds by dichotomy. On the contrary, Deleuze and Guattari assert that not every trait in a rhizome is necessarily linked to a linguistic feature; semiotic chains of every nature are connected to very diverse modes of coding (biological, political, economic, etc.) that bring into play not only different regimes of signs but also states of things of differing status. There the subject is no longer a subject, but a rhizome, a Body without Organs. In other words, what these writers argue is that a rhizome ceaselessly establishes connections between semiotic chains and organisations of power.<sup>187</sup> Multiplicities cease to have any relation to the One as subject or object, natural or spiritual entity; rather, they are rhizomatic, they are flat, a plane of consistency of multiplicities, defined by the outside:

---

<sup>185</sup> Frissen in Loader, B: (1997) *The Governance of Cyberspace*, Routledge: London and New York, p. 125.

<sup>186</sup> Deleuze, G and Guattari, F: (1987) *A Thousand Plateaus*, Athlone Press: London

<sup>187</sup> *ibid.*, pp.6-7.



by the abstract line, the line of flight or deterritorialization according to which they change in nature and connect with other multiplicities. The line of flight marks: the reality of a finite number of dimensions that the multiplicity effectively fills; the impossibility of a supplementary dimension, unless the multiplicity is transformed by the line of flight; the possibility and necessity of flattening all of the multiplicities on a single plane of consistency or exteriority, regardless of their number of dimensions.<sup>188</sup>

Deleuze and Guattari use the example of a map to explain the rhizome. What distinguishes the map from the tracing is that it is entirely oriented towards an experimentation in contact with the real. It fosters connections between fields, the removal of blockages on bodies without organs, the maximum opening of bodies without organs onto a plane of consistency. It is itself a part of the rhizome: '[t]he map is open and connectable in all of its dimensions; it is detachable, reversible, susceptible to constant modification'.<sup>189</sup> This resembles the world of the internet, where we get connections between fields, bodies without organs, lines of flight and maps of planes of consistencies.

In contrast, arborescent systems are hierarchical systems with centres of significance and subjectification, controlled by central automata like organised memories. An element only receives information from a higher unit, and only receives a subjective affection along preestablished paths. Deleuze and Guattari

---

<sup>188</sup> *ibid.*, p.9

point to problems in information and computer science, when these sciences grant all power to a memory or central organ. The writers cite Pierre Rosenstiehl and Jean Petitot: 'accepting the primacy of hierarchical structures amounts to giving arborescent structures privileged status...In a hierarchical system an individual has only one neighbor, his or her hierarchical superior... The channels of transmission are preestablished: the arborescent system preexists the individual, who is integrated into it at an allotted place'.<sup>190</sup>

In contrast to these centred systems, the authors set forth acentred systems, finite networks of automata, in which communication runs from any neighbor to any other, channels do not preexist, and individuals are interchangeable, defined only by their state at a given moment; local operations are coordinated and the final, global result synchronised without a central agency.<sup>191</sup> That is also what happens when 'mass' movements or molecular flows are constantly escaping, inventing connections that jump from tree to tree and uproot them: a whole smoothing of space, which in turn reacts back upon striated space.<sup>192</sup> Or as Hardt and Negri put it, 'a world that knows no outside. It knows only an inside, a vital and ineluctable participation in the set of social structures, with no possibility of transcending them. This inside is the productive cooperation of mass intellectuality and affective networks, the productivity of postmodern biopolitics'.<sup>193</sup>

---

<sup>189</sup> *ibid.*, p.12

<sup>190</sup> Rosenstiehl, P and Petitot, J: 'Automate asocial et systemes acentres', *Communications*, no 22 (1974), pp.45-62 cited in Deleuze and Guattari, p.16.

<sup>191</sup> Deleuze and Guattari, p.17.

<sup>192</sup> *ibid.*, p.506.

<sup>193</sup> Hardt, M and Negri, A: (2000) *Empire*, Harvard University Press: Cambridge, MA and London, p. 413.

This again resembles the way new movements and cultures rely on new communication technologies and specifically the internet:

Little could this philosopher of the rhizome have foreseen the intensification of cross-global identity that has been catalyzed by digital culture. An aspect of Deleuze's notion of collective agency that bears noting, particularly in the context of current international politics, is its global positionality, one balanced always-between South and North, not to mention East and West, a positionality whose decisiveness to gesture no doubt varies depending on one's specific place on the global vector and the digital divide. Indeed the machinery of the digital divide now invades and erodes the beingness of always-between at almost every turn.<sup>194</sup>

### *Conclusion*

This chapter discussed how traditional concepts and issues fit into a global postmodern medium. It looked at early social movements and their use of the internet, addressed the question of whether the internet enhances democracy, analysed how issues of power and participation relate to the internet, examined the globalisation-internet connection and discussed the postmodern nature of the medium.

---

<sup>194</sup> Murray, T: (2004) 'New media art and rhizomatic in-securities', Ctheory.net.



The section on political movements on the internet provides examples of ethnoreligious and socopolitical cyberconflict, looking at early movements on the internet such as the Zapatistas in Mexico, nationalist opposition groups, right-wing extremist and Islamist opposition movements. The groups that use information communication technologies affect the political situation in that they put forward new rules of the game, the rules of new technology. Nevertheless, this does not mean that new social movements like the anti-globalisation, anti-capitalist and anti-war movements, when using the internet to communicate political goals, ask for anything that is not traditionally modern in character such as power, participation or democracy.

While questioning if the internet enhances democracy, I considered David Held's theory of democracy in relation to my own research concern: the internet. My conclusion is that there are two responses to the question about democracy. The optimist states that the internet, by increasing the scale and speed of information, promises unlimited information, which heralds the promise of a better democracy. Initiatives by local authorities in Europe are said to support this thesis. The pessimistic view is that those uninterested in politics will remain so and that the internet is dominated by economic interests, discriminating on grounds of social, gender, race, age and spatial inequality. Both views have limited applicability. Nevertheless, the internet has provided access to the political system for outsiders. This indicates that it enhances democracy now and can do so in the future.

Two other issues discussed in this chapter are participation and power. As far as participation is concerned, Pateman's theory suggests that we can still have a modern theory of democracy which retains the notion of participation at its heart. The problem of participation in relation to the internet emanates from the fact that providing greater choice and opportunity only solves part of the problem of participation and does not get to the heart of what motivates citizens to move from the state of disengagement to one of salutary involvement in civic life.<sup>195</sup> On the other hand, the architecture of the net facilitates weak and strong ties that cut across social milieus, so that the cyberlinks between people become social links between groups that otherwise would be socially and physically dispersed.<sup>196</sup> An example of participation hitting record numbers has been the Howard Dean web campaign for the U.S. primary elections. In other words, political participation can be enhanced by uses of the internet.

On the question of power in virtual politics, Lukes's radical view on power and the Foucauldian conception of power/knowledge and disciplinary power have relevance. A discussion of these theories led to a focus on discourse and an attempt to explain how discourse constructs power relations. Internet politics, like any other politics, are embedded in power relations. The internet offers opportunities for breaking down political hierarchies and subverting national boundaries. The new power experienced by social movements, because of the

---

<sup>195</sup> Margolis and Resnick, p.207; Wilhem, p. 87.

<sup>196</sup> Wellman and Gulia, p.15.



new medium, comes from this access to mass audiences previously denied, either through cost, time, physical or political restraints.

To continue, the consideration of globalisation and the internet led to the conclusion that there is a divide between those who are online and the rest of the world, with attendant problems of cultural homogenisation and cultural imperialism. Since the internet is part of the globalisation process, and patently goes beyond the traditional politics of sovereignty, this finding suggests it could be postmodern in nature.

This last point on the post-modern character of the internet is also taken up when addressing questions of identity and community, discourse and structure in cyberspace. An imagined community can be said to exist in cyberspace with common beliefs of individuals who never meet each other that will move them to fight for, believe in, and even love their cybercommunity. An element of the internet, which gives it a postmodern character, is that it becomes a hyperreal vehicle for travelling across a simulated world. Electronic communications systematically remove the fixed points, the grounds and the foundations that were essential to modern theory. Information technology thus has far-reaching implications for our notions of sovereignty, autonomy and self-determination. The individual in cyberspace is fragmented in databases and networks resulting in the 'self' becoming decentred and multiple. Thus, we become postmodern in the conduct of internet politics, while remaining modernist in our ambitions.



Finally, the problems this kind of literature creates for my research are various. In the first place, none of the literature addresses the phenomenon of cyberconflict (political conflict in computer mediated environments) in a direct way. Instead, it furnishes us with a more general understanding of cyberpower and cyberspace. My work will expand on this background in the existing literature by taking its concerns in a previously unexplored direction. It will not only examine the various groups using the internet in more depth, but also analyse the way in which opposing parties in a conflict use the internet, something missing from this literature. More broadly, the difficulty with this literature is that the internet is a rapidly-developing medium with the result that it is sometimes hard for the literature (and me!) to keep up with it.

There are various examples of this. One is that Negroponte is somewhat outdated when in 1995, he refers to the internet 'as a formation of a flock of ducks that nobody is the boss' since more recent evidence by Margolis and Resnick suggest there occurs a normalisation of cyberspace, which comes to more and more the real world.<sup>197</sup> To prove the point, in an interview in *Wired* magazine in 2002, Negroponte characterised our digital world as lilies in a pond.<sup>198</sup> A second example is Manuel Castells's use of economic data of the years 1998 and 1999, to state that the internet economy has become the core of the US economy with the Forrester estimation of \$1.3 trillion up in 2003 from \$43 billion in 1998, an

---

<sup>197</sup> Margolis, M and Resnick, D: (2000) *Politics As Usual*, Sage: Thousand Oaks, London and New York.

estimation that proved to be wildly optimistic. Keeping in mind that the most serious work on the internet was written in the last six years and that the medium has dramatically changed during these years, it is natural to expect that some of it might be outdated and that the more the internet grows and evolves, the better the literature develops. For instance, as the literature develops, we see a shift from the first years in which writers were concerned mainly with explaining more technical and more everyday life aspects of the medium, while in the past few years there is more of an emphasis on cultural issues, democracy, politics, identity and community, signifying that researchers are searching the subject more deeply and widely as internet use intensifies. Inevitably, therefore, internet politics has also developed in new and unexpected ways. This means that it is not feasible to examine the politics of cyberconflict using just one analytical approach.

The following chapter introduces the three theories deemed relevant when examining the phenomenon of cyberconflict and proposes an integrated theoretical framework. Social movement theory is analysed in order to advance our understanding of sociopolitical cyberconflicts, conflict theory is discussed in relation to ethnoreligious cyberconflicts and media theoretical perspectives are included to shed light on the media aspects of these conflicts.

---

<sup>198</sup> 'Being wireless', Wired magazine, issue 10.10, Oct.2002.

## Chapter 2: The Three Theories

### 2.1 Social Movement Theory.

This section looks firstly at the general themes of how the study of social movements evolved, how 'new' social movements are, if they are a shift to post-industrial society, and the middle-class orientation argument. Then more analytically, I use the classical resource mobilisation model of mobilising structures, framing processes and the political opportunity structure to analyse how these are affected by the use of the internet by new social movements.

The problem with social movement theories, as even a casual reader would immediately notice, is that most analyses make empirical generalisations rather than providing useful analytical concepts.<sup>199</sup> The result is that in the need of a theory to support their case studies, theorists pick and mix from their predecessors and come up with a theory of their own to explain their empirical findings. This means that an examination of thirty different social movements could easily lead to thirty different explanations of social movements. This is because theorists aim at getting a global explanation, despite the fact that the field of social movements is elusive and there are differences for instance between movements (as forms of

---

<sup>199</sup> Melucci, A: (1989) *Nomads of the Present: Social Movements and Individual Needs in Contemporary Society*, edited by John Keane and Paul Mier, Temple University Press: Philadelphia, p.23



mass opinion), protest organisations (as forms of social organisation) and protest events (as forms of action).<sup>200</sup>

Traditional approaches to collective action usually formulate several fundamental questions: Through which processes do actors construct collective action? How is the unity of the various elements of collective actions produced? Through which processes and relationships do individuals become involved in, or defect from, collective action?<sup>201</sup> Two forms of explanation recur. As in social theory in general, there is the agent/structure divide, so in social movement theory the explanation is usually based either on structural conditions and dysfunctions of the social system, or on the differences in values and the psychological differences between individuals.

This dualistic thinking is highly problematic. As far as collective action is concerned, it has been explained in terms of breakdown/solidarity models as pointed out by Tilly.<sup>202</sup> Breakdown theories view collective action as the result of economic crisis and social disintegration, while solidarity models see collective action as an expression of shared interests within a common structural location. The former reduces collective action to reaction and marginality, the latter fails to explain the transition from social conditions to collective action.<sup>203</sup> In a similar vein, the structure/motivation dualism is also problematic, as Webb points out,

---

<sup>200</sup> Tarrow, S: 'National politics and collective action', *Annual Review of Sociology*, vol. 14 (1988), pp.421-440.

<sup>201</sup> Melucci, p.20.

<sup>202</sup> Tilly, C: (1978) *From Mobilization to Revolution*, Addison-Wesley: Reading, MA.

because within this dualism, collective action is either a product of the logic of the system or a result of personal beliefs.<sup>204</sup>

The response to this problematic dualism was equally dual, meaning it was different in Europe than it was in the United States, with theorists formulating two different ways to deal with the 1970s social movements. In Europe, for example, Touraine<sup>205</sup> and Habermas<sup>206</sup> tried to move beyond the structure-agency dichotomy by emphasizing the need for a systemic approach that links new forms of social conflict to post-industrial capitalis, while other theorists emphasised the identity-oriented paradigm. In the United States theorists focused on resource mobilisation.<sup>207</sup> Their theory analysed how a movement is formed, how it persists through time, and how it relates to its environment.

To continue, the Weberian term 'closure' describes the processes by which groups come to be formed through strategies of inclusion and exclusion. The activity of social movements, though they also include processes of closure in this sense, typically represent the opposite side of this process: they are attempts by groups thus excluded to insert themselves into closed groups and into closed processes of negotiation between groups, and by so doing to gain access to new resources and opportunities. New social movements are typically either predominantly

---

<sup>203</sup> Melucci, p.21.

<sup>204</sup> Webb, K et.al: (1983) 'Etiology and outcomes of protest: new European perspectives', *American Behaviour Science*, 26:cpp.311-31.

<sup>205</sup> Touraine, A: (1985) 'An introduction to the study of social movements', *Soc.Res.* 52: pp.749-88.

<sup>206</sup> Habermas, 1976

<sup>207</sup> McCarthy and Zald, 1973, 1977, 1979, Gamson, 1975, Tilly, 1978.



movements of the educated middle class, especially the 'new middle class', or of the most educated/privileged section of generally less privileged groups. Scott makes a further point:

Social movements typically bring about change or attempt to bring it about not by challenging society as a whole, though they may appear to do so, but by opposing specific forms of social closure and exclusion. They do so by thematising issues excluded from normal societal and political decision-making, and by articulating the grievances of groups who are themselves excluded. These two aspects - the exclusion of issues and exclusion of groups - are not separate spheres of social movement activity.<sup>208</sup>

Furthermore, in his work *Ideology and the New Social Movements*, Alan Scott considers how social movement networks bind the individual to the movement by creating primary bonds in which interpersonal sanction and commitment can operate. The interpersonal character of these networks minimises problems of free-riding. More importantly, they create self-identification with the movement. Processes of reformation of the individual will be simultaneously formations of a collective will. Group identity, not merely individual identity, is formed by the movement at the level of its loose networks. By providing individuals with alternative lifestyles and identities, social movements break down barriers to collective action, challenge 'civil privatism' and substitute values of solidarity for instrumental rationality.

---

<sup>208</sup> *ibid.*, p.150



An analysis of social movements, Scott suggests, in terms of social closure and interest intermediation treats the integration of issues and groups into the polity as the criterion of social movement success. It thus implies that the continued existence of the movement is not an end in itself, because social movement activity can only be understood in the context of other forms of political expression, both institutionalised and non-institutionalised.

The study of social movements raises various issues. Firstly, there is the question: how *new* are the new social movements? 'The question is whether their meaning and place they occupy in the system of social relations can be considered to be the same'.<sup>209</sup> Also, Melucci claims that 'those who argue for the newness of social movements have simply mistaken an early phase of movement development for a new historical age of collective action'.<sup>210</sup> The same argument is made by Offe who argues that the values advocated and defended by the NSMs are not new but part and parcel of the dominant modern culture, which makes it difficult to think of movements as flowing either from 'pre-modern' or 'postmodern' subcultures.<sup>211</sup> The interesting question here would be: if the internet is influencing the formation of NSMs, does that qualify them as new types of movement? On the other hand, if NSMs are already established, they are just using the internet as a new way of doing the old thing. For example, the

---

<sup>209</sup> Melucci, p.105.

<sup>210</sup> Tarrow, S: 'Aiming at a moving target: Social science and the recent rebellion in Eastern Europe', *Political Science and Politics*, vol.24, no1 (Mar.1991), pp. 12-20.

Independent Media Center (IMC) movement has drawn on a legacy of organisational skills developed by earlier social movements. The IMC was able to surmount some of the barriers of similar earlier efforts by building on the experience of earlier networks, inviting many of the activists from the independent video, community radio, and open source movements to participate very early on in the planning, fund-raising, and gathering of production equipment. 'The four-hundred-strong crew also used all the old and new media from pens to laptops, and from inexpensive audio tape and cam-recorders to the latest in digital recording technologies'.<sup>212</sup> The IMC is now a collective of over 150 independent media outlets around the world, with hundreds of volunteer journalists offering grassroots noncorporate coverage. Their success is not mainly due to new communication technologies, but also stems from the fact that they carefully built a relationship with social movement activists rather than distancing themselves from political organising. A similar argument is made by Simon Tormey who writes that the internet did not create anti-capitalist activism; rather, anti-capitalist activities used the internet as a means of connecting to others.<sup>213</sup>

Another question to answer is: Are NSMs a product of a shift to a *post-industrial* economy? This is debatable, as 'cultural revolutionary activities of (NSMs) can be articulated with very different politico-ideological formations, social groups and

---

<sup>211</sup> Offe, C: (1985) 'New social movements: Challenging the boundaries of institutional politics', *Sociol. Res*, 52, p.848.

<sup>212</sup> Kidd, D: 'Indymedia.org.' in McCaughey, M and Ayers, M (eds.) (2003) *Cyberactivism: Online Activism in Theory and Practice*, Routledge: New York and London, p.61

<sup>213</sup> Tormey, S: (2004) *Anti-capitalism: A Beginner's Guide*, Oneworld: Oxford, p.159.



classes'.<sup>214</sup> The mere presence of NSMs in non-western nations provides evidence against both hypotheses of state intrusion (a change to a post-industrial economy) as well as the hypotheses of value changes discussed below (since the new "post-materialist" values are theorised as a product of the economic and physical security of a country's population which also is not characteristic of Latin American nations, for example).<sup>215</sup> What seems unique according to Richardo is their ideological (identity) characteristic that seems to break from the past.<sup>216</sup> Nevertheless, new social and political movements use the internet for protests against the post-industrial economy. The anti-World Bank protests used the internet mainly for internal and external communication, education and mobilisation, sharing activist resources and discussing logistical matters such as transportation and provisions at protest sites.<sup>217</sup> The anti-globalisation movement has made its voice heard at major demonstrations, for instance in Geneva (WTO, 5/98), Birmingham (G8, 5/98), Koln (G8, 6/99), Seattle (WTO, 11/99), Davos (WEF, 9/00), Washington (WB/IMF, 4/00), Melbourne (WEF, 9/00), Prague (WB/IMF, 9/00), Quebec (FTAA, 4/00), and Genoa (G7, 7/01).<sup>218</sup>

---

<sup>214</sup> Olofsson, G: (1988) 'After the working-class movement? An essay on what's "new" and what's "social" in the new social movements', *Acta*, 31:pp. 15-34.

<sup>215</sup> Richardo, N: (1997) 'New social movements: a critical review', *Annual Review of Sociology*, vol.23, pp. 411-430.

<sup>216</sup> *ibid.*, p.425

<sup>217</sup> Vegh, S: 'Classifying forms of online activism' in McCaughey, M and Ayers, M (eds.) (2003) *Cyberactivism: Online Activism in Theory and Practice*, Routledge: New York and London, p. 85.

<sup>218</sup> *ibid.*, p.88.



To continue, there is the new *middle-class* orientation of NSMs argument, which maintains that new social movements are an outgrowth of this new social class.<sup>219</sup> Eder writes that the struggle to overcome a fear of the non-realisation of universal moral concepts such as justice, peace or the good life is the reason for collective protest where 'the petit bourgeoisie fills a role which it has rehearsed throughout history: it plays the role of the guardian of the moral virtues of modernity, a role which has learned how to play since its birth'.<sup>220</sup> In addition, an explanation based on value-shift is given by Jenkins, who argues that the middle-class 'participation revolution' was rooted in the shift towards post-materialist values, emphasising self-fulfillment, supporting demands for direct participation and moral concern for the plight of others. 'When elites challenged these values by manipulative acts and outright rejection, the middle class rallied around the movements'.<sup>221</sup>

Such theories involve an exaggeration of the levels of dissent found in the new middle class.<sup>222</sup> Kriesi, looking at new social movements in Netherlands, found that the thesis of middle-class support for NSMs can be too narrow, because he found the working class to have an unexpectedly high support for these movements, and too broad, because only a part of the new middle class seems to

---

<sup>219</sup> Klandermans, B: (1994) 'Transient identities? Membership patterns in the Dutch peace movement' in Larana et.al: *New Social Movements: From Ideology to Identity*, Temple University Press: Philadelphia.

<sup>220</sup> Eder, K: (1985) 'The "new" social movements: moral crusades, political pressure groups or social movements?', *Soc.Res.*, 52, p.889

<sup>221</sup> Jenkins, J.C: (1983) 'Resource mobilization theory and the study of social movements', *Annual Review of Sociology*, vol.9, p.535.

<sup>222</sup> Brint, S: (1984) 'New class and cumulative trend explanations of the liberal attitudes of professionals', *American Journal of Sociology*, 90, pp.30-71.

support them.<sup>223</sup> The part of this new middle class that seems more likely to participate is the part which consists of social and cultural specialists. New middle-class radicals choose the welfare and creative professions, because these professions provide a kind of sanctuary, where they are able to escape direct implication in capitalist economic relations.<sup>224</sup> There is also a conflict inside this new middle class as explained by Kriesi in discussions of his findings in the Netherlands; there is 'an opposition of interests between on the one hand, the technocrats in private enterprises and public bureaucracies who try to manage their organisations, and on the other hand the specialists who try to defend their own and their client's relative autonomy against the intervention of the technostucture'.<sup>225</sup>

However, an emphasis on the new middle class is not entirely inappropriate. When looking specifically at who uses the internet, statistics point to the middle classes of industrialised nations. According to the United Nations, industrialised nations account for 15 percent of the world's 6 billion people, 88 percent of whom are internet users. Eighty per cent of the world's population has yet to make a phone call. More people use the internet in London than in all of Africa and there are more users in South Africa than in all African countries combined.<sup>226</sup>

---

<sup>223</sup> Kriesi, H: (1989) 'New social movements and the new class in Netherlands', *American Journal of Sociology*, vol.94, no5, p.1111.

<sup>224</sup> *ibid.*, quotes Parkin.

<sup>225</sup> *ibid.*, p.1078.

<sup>226</sup> Lebert, J: 'Wiring human rights activism' in McCaughey, M and Ayers, M (eds.) (2003) *Cyberactivism: Online Activism in Theory and Practice*, Routledge: New York and London, p.224.



Consequently, for the purposes of this thesis and since it seems difficult to adopt a single position on the issue, I intend to draw various arguments from writers belonging to different schools, although without claiming to have found a solution to the problem of theorising social movements or aiming at a global explanation.

Scott contends that an adequate theory of social movements would have to recognise the problematic and effortful nature of mobilisation and the consequent organisational constraints. This task has been tackled by theories of 'resource mobilisation'. At the same time, resource mobilisation theory (RMT) has generated a sophisticated analysis of the mechanics of collective action, of the barriers to it, and of the conditions under which it can operate. Nevertheless, while RMT does help us understand the organisational dilemma facing social movements, it is limited by its continued adherence to economic models of human agency, and says little about the content and context of social movements.

RMT, like other forms of political realism, sketches both the limits of political action and the largely instrumental and self-interested nature of that action. Resource mobilisation theorists have identified the following types of imperative placed upon organisations and movements by the limitations of collective action: (i) the necessity of providing divisible private benefits, as well as indivisible collective ones, places high organisational costs upon collective bodies; (ii) the search for resources such as external funding therefore becomes a major organisational preoccupation; (iii) at the same time, the organisation is restricted



in the demands and sacrifices it can realistically expect of participants in its costly and high-risk activities. Scott makes an additional point:

In stressing the continuity, rather than discontinuity, between social movements, parties and institutionalised forms of political action such as pressure groups and parties, RMT has developed a more plausible account of social movement development. That is to say, it is one which corresponds more closely to the typical development of social movements rather than counter-factually trying to explain the 'failure' of movements to retain their movement character.<sup>227</sup>

Resource mobilisation theory (RMT) has had a huge impact on social movement theories. It demonstrated that in order to orchestrate collective action, sophisticated organisational forms and modes of communication are needed. As summarised by Cohen, RMT theorists share the following assumptions: (1) social movements must be understood in terms of a conflict model of collective action; (2) there is no fundamental difference between institutional and non-institutional action; (3) both forms of action entail conflicts of interest built into institutionalised power relations; (4) collective action involves the rational pursuit of interests of groups; (5) goals and grievances are permanent products of power relations and cannot account for the formation of movements; (6) this depends instead on changes in resources, organisations, and opportunities for collective action; (7) success is evidenced by the recognition of the group as a political actor

---

<sup>227</sup> Scott, A: (1990) *Ideology and the New Social Movements*, Unwin Hyman: Boston, p.115

or by increased material benefits; and (8) mobilisation involves large-scale, special-purpose, bureaucratic, formal organisations.<sup>228</sup>

Critically assessing RMT, one could argue that it sets out a narrow and critically impoverished interpretation of human motivation, which reduces it to instrumental rationality. There are two more aspects of RMT which make it vulnerable to general sociological criticism: first, its decontextualised understanding of preferences, choices and actions; and second, the rigidity of the means/ends distinction it employs.

As Melucci and others argue, RMT-based theories do have problems:

Structural theories, based on system analysis, explain why but not how a movement is established and survives; they hypothesise potential conflict without accounting for concrete collective action. By contrast, resource mobilization models regard such action as mere data and fail to examine its meaning and orientation. In this instance the how but not the why of collective action is emphasised.<sup>229</sup>

In other words it looks as if resource mobilization could be defined independently from the nature of the goals and the social relations of the actor, as if all actors are finally led by a logic of economic rationality.<sup>230</sup>

---

<sup>228</sup> Cohen, J.L (1985) 'Strategy or identity: new theoretical paradigms and contemporary social movements', *Soc.Res.*52, p. 675.

<sup>229</sup> Melucci, p.21

<sup>230</sup> Touraine, A: (1985) 'An introduction to the study of social movements', *Soc.Res.*52, p.769.

For the purpose of this analysis, due to the the use of the internet as a resource by social movements, I will follow RMT in referring to three broad sets of factors in analysing the emergence and developments of social movements: (1) the structure of political opportunities and constraints confronting the movement; (2) the forms of organisation (informal as well as formal) available to activists; and (3) the collective processes of interpretation, attribution, and social construction that mediate between opportunity and action.<sup>231</sup> The focus will be on the mobilising structures (the network-style structure of movements using the internet, participation, recruitment, tactics, goals), framing processes (issues, strategy, identity, the effect of the internet on these processes) and the media (and the internet particularly) as a component of the political opportunity structure.

### *Mobilising structures*

The classical RMT model is used to understand, as McCarthy puts it:

how mobilising structural forms emerge and evolve; how they are chosen, combined, and adapted by social movement activists; and how they differently affect particular movements as well as movement cycle trajectories. The concepts

---

<sup>231</sup> McAdam, D, McCarthy, J and Zald, M (eds.): *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Structural Framings*, Cambridge University Press: Cambridge, p.2



of political opportunity and strategic framing are, I believe, particularly useful in illuminating these processes.<sup>232</sup>

Furthermore, according to Tarrow, people engage in contentious politics:

when patterns of political opportunities and constraints change and then, by strategically employing a repertoire of collective action, create new opportunities, which are used by others in widening cycles of contention. When their struggles revolve around broad cleavages in society, when they bring people together around inherited cultural symbols, and when they can build on or construct dense social networks and connective structures, then these episodes of contention result in sustained interactions with opponents – specifically, in social movements.<sup>233</sup>

In a very restrictive sense, a social movement consists of two kinds of components: (1) networks of groups and organisations prepared to mobilise for protest actions to promote (or resist) social change (which is the ultimate goal of social movements); and (2) individuals who attend protest activities or contribute resources without necessarily being attached to movement groups or organisations.

---

<sup>232</sup> McCarthy, J: 'Constraints and opportunities in adopting, adapting and inventing' in McAdam, D, McCarthy, J and Zald, M (eds.): *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Structural Framings*, Cambridge University Press: Cambridge, p.141

<sup>233</sup> Tarrow, S: (1998) *Power in Movement: Social Movements and Contentious Politics*, Cambridge University Press: Cambridge, p.19

One of the most important components of resource mobilisation theory is mobilisation. Mobilisation is the process of creating movement structures and preparing and carrying out protest actions which are visible movement 'products' addressed to actors and publics outside the movement.<sup>234</sup> It implies a process by which an actor augments its resources through gaining the support of other actors or a process by which those that have not taken an active part in politics are drawn into it.<sup>235</sup> As Robin Brown explains:

In evaluating the impact of mobilizations it is necessary to distinguish three levels of outcome. Firstly, the success or failure in gaining the support of potential supporters, secondly, success or failure in modifying the position of those that the mobilization is targeted against and thirdly, the impact on the prospects for future mobilizations.<sup>236</sup>

In terms of the mobilisational structure, NSMs are open, decentralised, nonhierarchical/ideal for internetted communication. Melucci characterises the new social movements as

---

<sup>234</sup> Rucht, D: 'The impact of national contexts on social movement structures: A cross-movement and cross-national comparison' in McAdam, D, McCarthy, J and Zald, M (eds.): *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Structural Framings*, Cambridge University Press: Cambridge, p. 186

<sup>235</sup> Brown, R: 'Mobilizing the Bias of Communication: Information Technology, Political Communications and Transnational Political Strategy', American Political Science Association Convention, Washington DC, 30 August- 3 September 2000, p.2

<sup>236</sup> Brown, R: 'Mobilizing the Bias of Communication: Information Technology, Political Communications and Transnational Political Strategy', American Political Science Association Convention, Washington DC, 30 August- 3 September 2000, p.5

segmented, polycephalic structures. The movement is composed by diverse, autonomous units that expend an important part of their resources on internal solidarity. A network of communication and exchange keeps the cells in contact with each other. Information, persons and models of behaviour circulate in the network, moving from one unit to another and thus promoting a certain homogeneity of the whole structure. Leadership is not concentrated but diffuse...<sup>237</sup>

We assume that the internet is used particularly by two kinds of movements' structures: (a) informal networks with a large geographical reach, and (b) big, powerful and more centralised social movement organisations. Moreover, the internet appears to play an especially crucial role in issue-focused, transnational campaigns.<sup>238</sup> Using again the Independent Media Center example, the IMC network is based on a non-hierarchical structure that relies on highly complex processes of networked consensus:

International meetings are held online. There are a wide array of listserv discussion groups that range from general discussions to finances to translation and technical issues. Meetings are conducted through highly complex processes

---

<sup>237</sup> Melucci, p.14.

<sup>238</sup> Van de Donk, W, Loader, B, Nixon, P, Rucht, D: (2004) *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p. 18



of decision-making, using a consensus model drawn from the direct action wing of the anti-globalisation movement.<sup>239</sup>

According to Tormey, the internet represents an activism based on networks of self-avowed minorities, rather than on classic models of political organisation. Those who wish to 'speak' can do so unmediated by the needs and interests of a perhaps distant leadership intent on sending the 'right' signals to the electorate, powerful states or global institutions. As Tormey puts it:

Networks can be *extended indefinitely* and in more than one or two dimensions. There is no 'membership' as such, just engagement. There is no brake, organisational, fiscal, or ideological on joining in - merely access to the network. Networks facilitate *temporary alliances, coalitions, agreements, events, interactions*. A network consists of chains of allegiance and intersection or what are sometimes called 'nodal points'; where there is convergence for the purpose of acting in support of some group or cause. (his italics)<sup>240</sup>

But is it unthinkable that political parties using ICTs to redesign themselves into a more 'social movement'-like type of organisation, or that social movements are using them to compete with political parties? ICTs might perhaps not profoundly change the very 'logic' of collective action, but they seem to change, in any case,

---

<sup>239</sup> Vegh, S: 'Classifying forms of online activism' in McCaughey, M and Ayers, M (eds.) (2003) *Cyberactivism: Online Activism in Theory and Practice*, Routledge: New York and London

<sup>240</sup> Tormey, S: (2004) *Anti-capitalism: A Beginner's Guide*, Oneworld: Oxford, p. 159.

the structure of political communication and mobilisation.<sup>241</sup> Political organisations that are older, larger, resource-rich, and strategically linked to party and government politics may rely on internet-based communications mostly to amplify and reduce the costs of pre-existing communication routines. On the other hand, newer, resource-poor organisations that tend to reject conventional politics may be defined in important ways by their internet presence.<sup>242</sup> ICTs can be effectively used to build and maintain powerful and centralised organisations, but empirical evidence also suggests that ICTs can be effective tools to establish and run decentralised networks that allow those who are technically linked to air their views, and, if needed, to mobilise a virtual or physical community of activists.<sup>243</sup>

Some websites are also products of spectacular alliances between NGOs, culture-jammers, small groups of activists, opinion leaders, or just ordinary citizens with the skills and credibility to succeed in the attention game on the world wide web. 'This could be called network politics – a process in which people, organisations, and groups are included not because of formal status, but because they have specific resources needed in the process'.<sup>244</sup> In addition, conventional print media produced by the transnational movements (TMs), e.g newsletters, newspapers, and magazines, appear to be of less importance than for the NSMs. Instead, the

---

<sup>241</sup> Van de Donk, W, Loader, B, Nixon, P, Rucht, D: (2004) *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p.5

<sup>242</sup> Bennett, W.L: (2004) 'Communicating global activism' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p. 125, cites Graber et. al. forthcoming

<sup>243</sup> Van de Donk, W, Loader, B, Nixon, P, Rucht, D: (2004) *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p. 9



use of electronic communication, in particular the internet, plays a crucial role for TMs and, to a growing extent, contemporary NSMs as well.<sup>245</sup>

Furthermore, the cycle of protests argument states that NSMs are simply recent manifestations of a cyclical pattern of social movements.<sup>246</sup> Some link the cycles to anti-modern or romantic-ideological reactions to the contradictory and alienating effects of modern societies, others to recurring waves of cultural criticism linked to changes in the cultural climate or to political and social events. Movements change in response to shifts in local or national political opportunities, available resources, the actions of counter-movements, changes in the strategy deployed by states, and public opinion.<sup>247</sup> Minkoff argues that 'trajectories of protest cycles are jointly determined by increases in the rates of protest and increases in the density of social movement organisation'.<sup>248</sup> It may be argued that the internet accelerates protest circles and generally makes it far easier to organise protest than used to be the case in the past.

Moreover, key issues to focus on when analysing mobilisation structures in NSMs are ideology, goals, tactics, participants, recruitment, entry, movement phase,

---

<sup>244</sup> Rosenkrands, J: (2004) 'Politicizing *Homo economicus*' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p.75.

<sup>245</sup> Rucht, D: (2004) 'The quadruple "A": Media strategies of protest movements since the 1960s' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p.50, cites Scott and Steer 2001

<sup>246</sup> Tarrow, S: (1983) 'Struggling to reform; social movements and policy change during cycles of protest', *West Soc. Pap*, no15, Ithaca, NY: Cornell University.

<sup>247</sup> Kriesi et al 1995, Tarrow 1994, Tilly 1995

<sup>248</sup> Minkoff, D: (1997) 'The sequencing of social movements', *American Sociological Review*, vol. 62, no5, p.780.



influence, self-label, distinguishing characteristics, key issues, and key organisations:

New social movements call into question the structures of representative democracies that limit citizen input and participation in governance, instead advocating direct democracy, self-help groups, and cooperative styles of social organisation. Taken together the values of NSMs center on autonomy and identity.<sup>249</sup>

Issues of participation and recruitment are very important and briefly three points should be taken into consideration as outlined by Snow, Zurcher and Olson<sup>250</sup>: the fewer and weaker the social ties to alternative networks, the greater the structural availability for movement participation; the greater the availability for participation, the greater the probability of accepting recruitment invitation; and, movements which are linked to other groups expand at a more rapid rate than more isolated and closed movements. This has been clearly observed with the anti-globalisation movement and the peace movement. The NSMs have taken to making good use of the greater participation offered on the internet, as well as the numerous links, cyberlinks or otherwise, translated into social links and ties. The NSMs use the internet to support external activity, they may work within the

---

<sup>249</sup> Offe, C: (1985) 'New social movements: Challenging the boundaries of institutional politics', *Soc. Res.*, 52, pp. 817-68.

<sup>250</sup> Snow, D, Zurcher, L and Olson, S.E: (1980) 'Social networks and social movements: A microstructural approach to differential recruitment', *American Sociological Review*, vol.45, no5, pp.790;794;797

internet to create a foundation for their activities, and they have attempted to influence policy affecting the internet.<sup>251</sup>

There is also a distinction between defensive/offensive *types* of movements. Contemporary movements combine features of both. They are defensive in that they 'defend spaces for the creations of new identities and solidarities' and offensive in that 'they involve conflict between social adversaries over the control of a social field'.<sup>252</sup> Here it could be argued that groups in ethnoreligious cyberconflicts are more of an offensive type of movements, in contrast to the more mixed (defensive and offensive) character of groups in sociopolitical cyberconflicts, as we will become evident in subsequent chapters.

In a very interesting theoretical synthesis, Touraine moves on to two analytical levels, looking at the structural and cultural dimensions of contemporary society and the conflictual processes of identity-formation of collective actors. He identifies these key elements: pursuit of collective interests, reconstruction of a social, cultural and political identity, changing the rules of the game, defense of a status or privileges, social control of the main cultural patterns, creation of a new order (revolution), national conflicts and neo-communitarianism.<sup>253</sup> Following Touraine, it could be argued here that groups in sociopolitical cyberconflicts pursue collective interests which relate to the reconstruction of a social, cultural

---

<sup>251</sup> Salter, L: 'Democracy, new social movements, and the Internet' in McCaughey, M and Ayers, M (eds.) (2003) *Cyberactivism: Online Activism in Theory and Practice*, Routledge: New York and London, p. 129.



and political identity. Evidence of this is found in the use of the internet by groups in the anti-globalisation and anti-war movements. By contrast, in ethnoreligious cyberconflicts, the element of national conflict is far more relevant.

As far as tactics (or modes of action-internal/external) are concerned, these include mobilising supporters, neutralising supporters and/or transforming mass and elite publics into sympathisers. Briefly, tactics are influenced internally by organisational competition and cooperation and externally by public opinion and the state. Since societies provide the infrastructure for movement industries, the development of tactics depends on the affluence, degree of access to institutional centers, preexisting networks and occupational growth of particular movements.<sup>254</sup> Also, important are movement participants' professional or communicative skills, which enable them to participate in the process of identity-building. Evidently, information transmitted by successful protest mobilisations becomes the key indicator of political opportunity for emerging movements and drives the development of broad-based protest cycles.<sup>255</sup> On the internet, social movement groups are able to communicate, to generate information and to distribute this information cheaply and effectively, allowing response and feedback:

---

<sup>252</sup> Cohen, J.L (1985) 'Strategy or identity: new theoretical paradigms and contemporary social movements', *Soc.Res.*52, p.689.

<sup>253</sup> Touraine, A: (1985) 'An introduction to the study of social movements', *Soc.Res.*,52, p.751.

<sup>254</sup> McCarthy, J and Zald, M: (1977) 'Resource mobilization and social movements: A partial theory', *The American Journal of Sociology*, vol.82, no6, p.1217.

<sup>255</sup> Tarrow, S: 'Aiming at a moving target: Social science and the recent rebellion in Eastern Europe', *Political Science and Politics*, vol.24, no1 (Mar.1991), p.59.



This is in large part because of [the internet's] structure as a decentred, textual communications system, the content of which has traditionally been provided by users. Again, such characteristics accord with the requisite features of NSMs: nonhierarchical, open protocols; open communication; and self-generating information and identities.<sup>256</sup>

It is equally important to note here, as Bennet does, that the effects on social movements are due not so much to the internet as to the network structures established through it: 'uses of the internet may have important effects on organisational structures, both inside member organisations and in terms of overall network stability and capacity'.<sup>257</sup> Studies have highlighted two functions of the net: first, it helps communication in terms of information dissemination, formal networking, and action coordination; second, it helps in building a collective identity among participants and potential participants of the movement.<sup>258</sup> This raises the broader question: have the new forms of communication changed the 'logic of collective action' or just the speed of protest diffusion?<sup>259</sup>

---

<sup>256</sup> Salter, L: 'Democracy, new social movements, and the Internet' in McCaughey, M and Ayers, M (eds.) (2003) *Cyberactivism: Online Activism in Theory and Practice*, Routledge: New York and London, p. 129.

<sup>257</sup> Bennett, W.L: (2004) 'Communicating global activism' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: (2004) *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p. 136

<sup>258</sup> Nip, J: (2004) The Queer Sisters and its electronic bulletin board in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p.233

<sup>259</sup> van Aelst, P and Walgrave, S: (2004) 'New media, new movements?' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p. 121

The internet delivers significant services to movements: information dissemination and information retrieval, recruitment, mobilisation, soliciting opinions, opinion polling, discussion, facilitating contacts between the organisation's members, service, networking, communication and coordination with other organisations.<sup>260</sup> As le Grignou and Patou argue, the internet is an important tool in terms of the diffusion of protest and the consistency of protest, in order to achieve a 'consensual mobilisation'.<sup>261</sup> Thus, the internet contributes to three different elements that establish movement formation: a shared definition of the problem as a basis for collective identity, actual mobilisation of participants, and the construction of a network of different organisations.<sup>262</sup> For example, during the 1999 anti-WTO campaign, while groups with local ties concentrated on mobilisation and direct action, more transnationally-based groups provided information and frames to feed the action.<sup>263</sup>

Mobilisation has been argued to be one of the crucial elements in the movements' organisation, incorporating the impact of technology on these movements. Brown emphasises its importance in this way: '[i]ndeed it may be more profitable to analyse the impact of information and communication technologies (ICTs) in terms of mobilisation rather than in the more sweeping terms offered by ideas

---

<sup>260</sup> le Grignou, B and Patou, C: (2004) 'ATTAC(k)ing expertise' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p.187

<sup>261</sup> *ibid.*, p. 171

<sup>262</sup> van Aelst, P and Walgrave, S: (2004) 'New media, new movements?' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p. 99

<sup>263</sup> *ibid.*, p. 101



such as cyberpolitik or netwar'.<sup>264</sup> Two key arguments support his conviction. These are the argument that mobilisation cuts across the distinction between material and ideational factors, and the argument that mobilisation keeps the technological issue firmly embedded in a social and political context.<sup>265</sup>

Not surprisingly for instance, websites are action mobilisers. According to Edwards' research on the Dutch women's movement online, first, the emphasis is on external information provision. The 'first generation' websites contain the basic (static) information about the organisation. Then, organisations expand their websites so as to include more information: background information on the problem area that they address, as well as dynamic information about their activities. Subsequently, organisations develop their ambitions further, and become more focused, using network technology for internal communication purposes. Next, organisations start to develop more advanced interactive functions of the internet in their communication with the environment.<sup>266</sup> However, as van Aelst and Walgrave argue, most sites offer the 'basics', such as feedback possibility or a newsletter, mostly via email. More sophisticated ways of interaction and debate such as forums or chatrooms are limited.<sup>267</sup> An illuminating aspect to their argument is that the concept of mobilisation should be extended

---

<sup>264</sup> Brown, R: 'Mobilizing the Bias of Communication: Information Technology, Political Communications and Transnational Political Strategy', American Political Science Association Convention, Washington DC, 30 August- 3 September 2000, p.2

<sup>265</sup> Brown, R: 'Information and the Power of Mobilization', International Studies Association Convention, New Orleans, March 2002, p.3, p.15

<sup>266</sup> Edwards, A: (2004) 'The Dutch women's movement online' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p.194



‘from (former) “unconventional” street actions such as demonstrations and sit-ins to new virtual actions varying from an online petition to pinning down the enemy’s server’.<sup>268</sup> Costanza-Chock, a community arts activist, has a similar opinion: ‘you have all these people collectively mobilizing, engaging in action together, telling their friends, discussing what’s happening, taking heart that they’re not alone in what they feel is a struggle against injustice. So you have the movement-building elements’.<sup>269</sup>

The conclusion is that the internet is reshaping the organisational infrastructure of the movements that use it at least in three ways: mobilisation of resources, maintaining relations with the environment and management of frames. However, as Edwards argues in relation to the Dutch women’s movement, ‘[t]he impact is most visible in the movement’s increased capacity for mobilizing resources. To a lesser extent, there are also effects in the management of frames...However, the interactive functions on the websites of organizations in the physical domain are still in their infancy’.<sup>270</sup> Next, we shall consider the effect of the internet on the framing process.

---

<sup>267</sup> van Aelst, P and Walgrave, S: (2004) ‘New media, new movements?’ in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p. 113

<sup>268</sup> *ibid.*, p. 114

<sup>269</sup> email interview 2001 in Taylor, P.A and Jordan, T: (2004) *Hacktivism and Cyberwars: Rebels with a cause?*, Routledge: London, p. 153

<sup>270</sup> Edwards, A: (2004) ‘The Dutch women’s movement online’ in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p. 200

*Framing process: Identity, issue, strategy.*

Frames are the specific metaphors, symbolic representations, and cognitive cues used to render or cast behaviour and events in an evaluative mode and to suggest alternative modes of action. Symbols, frames, and ideologies are created and changed in the process of contestation.<sup>271</sup>

The management of frames is a crucial element of collective action and mobilisation. '[B]uilding a movement around strong ties of collective identity, whether inherited or constructed, does much of the work that would normally fall to organization; but it cannot do the work of mobilization, which depends on framing identities so that they will lead to action, alliances, interaction'.<sup>272</sup>

Similarly, Doug McAdam argues that the concept of framing is an important and a necessary corrective to broader structural theories, which often depict social movements as the inevitable byproducts of expanding political opportunities (political process), emerging system-level contradictions or dislocations (some version of new social movement theory) or newly available resources (resource mobilisation).<sup>273</sup>

---

<sup>271</sup> Zald, M: 'Culture, ideology and strategic framing' in McAdam, D, McCarthy, J and Zald, M (eds.): *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Structural Framings*, Cambridge University Press: Cambridge, p. 262

<sup>272</sup> Tarrow, S: (1998) *Power in Movement: Social Movements and Contentious Politics*, Cambridge University Press: Cambridge, p.119

<sup>273</sup> McAdam, D: 'The framing function of movement tactics: Strategic dramaturgy in the American civil rights movement' in McAdam, D, McCarthy, J and Zald, M (eds.): *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Structural Framings*, Cambridge University Press: Cambridge, p.339



If we consider the concept of 'repertoires of collective action' introduced by Tarrow, action is shaped by and coordinated through the development of those models or scripts shared within a particular society at a particular historical juncture. As a resource, the presence of shared goals or models facilitates mobilisation.<sup>274</sup> This leads us to what the framing process involves: (1) the cultural tool kits available to would-be insurgents; (2) the strategic framing efforts of movement groups; (3) the frame contests between movement and other collective actors – principally the state, and countermovement groups; (4) the structure and role of the media in mediating such contests; and (5) the cultural impact of the movement in modifying the available toolkit.<sup>275</sup>

More specifically, through 'frame bridging', 'frame amplification' and 'frame extension', movements link existing cultural frames to a particular issue or problem, clarify and invigorate a frame that bears on a particular issue or problem, and expand the boundaries of a movement's primary framework to encompass broader interests or points of view. The most ambitious strategy is the fourth, 'frame transformation', framing device for movements that seek substantial social change.<sup>276</sup>

---

<sup>274</sup> Clemens, E: 'Organizational form as frame: Collective identity and political strategy in the American labor movement, 1880-1920', in McAdam, D, McCarthy, J and Zald, M (eds.): *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Structural Framings*, Cambridge University Press: Cambridge, p. 211

<sup>275</sup> McAdam, D, McCarthy, J and Zald, M (eds.): *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Structural Framings*, Cambridge University Press: Cambridge, p.19

<sup>276</sup> Tarrow, S: (1998) *Power in Movement: Social Movements and Contentious Politics*, Cambridge University Press: Cambridge p.110, cites Snow and Benford, 1992: 467-476



According to Zald, social movements draw on the cultural stock of how to protest and how to organise. Templates of organisation include skills and technology of communication (e.g writing newsletters, running meetings), of fund raising, of running an office, of recruiting members, and so on. Repertoires of contention include building barricades, organising marches, non-violent disruption, and the like. Templates of organisation may be drawn from the whole society, while repertoires of contention are available from the whole social movements sector.<sup>277</sup>

The dilemma concerning two of the three elements of framing (strategy, identity, issue) is the strategy or identity one, as identified by Cohen. In 'Strategy or Identity?', he cites Touraine's argument that the exclusive orientations to identity and to strategy are the opposite sides of the same coin, in that they both look at social conflicts in terms of the response to long term changes (modernisation) rather than in relational terms referring to the social structure. From such a standpoint, 'society' is stratified in terms of the actor's ability (power and privilege) to adapt to change successfully (elites), her or his success in securing protection from change (operatives) or her or his victimisation by change (marginalised masses).<sup>278</sup>

---

<sup>277</sup> Zald, M: 'Culture, ideology and strategic framing' in McAdam, D, McCarthy, J and Zald, M (eds.): *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Structural Framings*, Cambridge University Press: Cambridge, p. 267

<sup>278</sup> Cohen, J.L (1985) 'Strategy or identity: new theoretical paradigms and contemporary social movements', *Soc.Res.*52, p. 675, cites Touraine, 1982:223.

In terms of issues, NSMs engage with different types of issues like quality of life issues, redistributive issues, opposition to the present forms of social life, and issues that challenge modern state domination. The value-shift hypothesis states that NSMs stress issues of identity, participation and quality of life (referred to as 'post-materialist' concerns) rather than economic matters. This, however, may not necessarily be true, as the anti-globalisation and anti-capitalist movement have shown. The internet connection here is that the rise of technology could possibly have effects which alter the agendas adopted by social movements. One example is that maybe there is a link of the globality of computer networks with the globality of protest resulting in a fusion of disparate issues. As Kahn and Kellner argue:

Thus, while emergent mobile technology provides yet another impetus towards experimental identity construction and politics, such networking also links diverse communities such as labor, feminist, ecological, peace, and various anti-capitalist groups, providing the basis for a new politics for alliance and solidarity to overcome the limitations of postmodern identity politics.<sup>279</sup>

According to Whittier and Taylor, collective identity consists of three related processes: delineation of group boundaries, construction of an oppositional consciousness or interpretative frameworks for understanding the world in a

---

<sup>279</sup> Kahn, R and Kellner, D: 'New media and internet activism: from the "Battle of Seattle" to blogging', *New Media and Society*, 6 (1), Sage: London and Thousand Oaks.



political light, and politicisation of everyday life.<sup>280</sup> Another aspect of the process is formulating cognitive frameworks concerning the goals, means and environment of action, activating relationships among the actors, and making emotional investments which enable individuals to recognise themselves in each other.<sup>281</sup> Also, the category of collective interest requires prior analysis of 'what counts as collective advantage and how collective interests are recognised, interpreted, and able to command loyalty and commitment.'<sup>282</sup> Cohen argues that it is incumbent on the theorist to look into the processes by which collective actors create the identities and solidarities they defend.<sup>283</sup> This means that the logic of collective interaction entails something other than strategic or instrumental rationality. For instance, Pizzorno, who uses a pure identity model, argues that cost-benefit calculations cannot explain the collective action of new groups seeking identity, autonomy and recognition. An extended version of his claim would be to say that 'collective actors strive to create a group identity within a general social identity whose interpretation they contest.'<sup>284</sup> New social movements use sharp antinomies such as yes/no, them/us, victory and defeat, now or never, to build up their identities. This hardly allows for political exchange or gradualist tactics. Even more striking is that they do not rely for their self-identification on either the established political codes (left/right,

---

<sup>280</sup> Whittier, N and Taylor, V: (1992) 'Collective identity and lesbian feminist mobilization', pp. 104-29 in *Frontiers of Social Movement Theory*, edited by A.Morris and C.Mueller, Yale University Press: New Haven.

<sup>281</sup> Waterman, P: (2001) *Globalization, Social Movements and the New Internationalisms*, Continuum: London and New York, p. 35

<sup>282</sup> Cohen, J.L (1985) 'Strategy or identity: new theoretical paradigms and contemporary social movements', *Soc.Res*, 52, p. 685.

<sup>283</sup> *ibid.*, p.690.

<sup>284</sup> *ibid.*, p.694.



liberal/conservative, etc) nor on socio-economic codes (working class/middle class, poor/wealthy, rural/urban, etc.).<sup>285</sup>

An interesting study on collective identity by McKenna and Bargh<sup>286</sup> discusses the idea that Usenet groups provide a place for marginalised persons to communicate with others, thus increasing each person's self-esteem. Their theory hypothesises that group membership is incorporated into the self, so that the individual will feel her/himself to be a member of the group. As Myers<sup>287</sup> explains their conclusion is that virtual group identities are just as important to the self as face-to-face group participation, and that respondents felt and identified with the people within the Usenet group, '[t]o identify common themes, opportunities and potential drawbacks in the integration of ICTs into the communication repertoire of social movements'.<sup>288</sup>

Moreover, Touraine argues NSMs have an increasingly temporary and symbolic function, fighting for symbolic and cultural stakes and for a different meaning and orientation of social action.<sup>289</sup> This is especially true in collective actions taken in cyberspace where symbolic change is the key function. This is why the concept of

---

<sup>285</sup> Offe, C: (1985) 'New social movements: Challenging the boundaries of institutional politics', *Soc. Res.* 52, p.830.

<sup>286</sup> McKenna, K and Bargh, J: (1998): 'Coming out in the age of the Internet: Identity demarginalization through virtual group participation', *Journal of Personality and Social Psychology* 75, pp. 681-694.

<sup>287</sup> Myers, M: (2001) 'Collective identity.org: Collective identity in online and offline feminist activist groups', thesis submitted to the Faculty of Virginia polytechnic Institute and State University for the degree of Masters of Science in Sociology.

<sup>288</sup> Wright, S: (2004) 'Informing, communicating and ICTs in contemporary anti-capitalist movements' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York

<sup>289</sup> Touraine, pp. 798-800

movement itself becomes increasingly inadequate and one has to give attention to Touraine's preference to speak of movement networks or movement areas, as the network of groups and individuals sharing a conflictual culture and a collective identity. These networks allow multiple memberships, and personal involvement and effective solidarity are conditions for participation. This, however, is 'not a temporary phenomenon, but a morphological shift in the structure of collective action.'<sup>290</sup> Furthermore, the form of the movement itself is a message, a symbolic challenge to the dominant patterns. The structure of NSMs outlined previously by Melucci and Touraine is the basis for internal collective identity, but also for a symbolic confrontation with the system. 'It makes apparatuses to produce justifications, it pushes them to reveal their logic and the weakness of their reasons. It makes power visible'.<sup>291</sup>

Due to the fact that frames are transmitted and reframed by the mass media, and consequently the internet, it has been argued that 'the internet can function as a new medium to expose frames and problem definitions and as a space to create shared meaning and identities among the membership and the constituency'.<sup>292</sup> Pini, Brown and Previte, for instance note how new configurations in computer-mediated communication lead to new patterns and possibilities and foster new coalitions of ideas/identities/frames that challenge existing ones in the 'real'

---

<sup>290</sup> *ibid.*, p.800, cites Gerlach and Hine's work *People, Power and Change*, 1970

<sup>291</sup> *ibid.*, p.813.

<sup>292</sup> Edwards, A: (2004) 'The Dutch women's movement online' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p. 189



world.<sup>293</sup> I will now proceed to look at the triangle between framing, political opportunity structure, the media and particularly the internet.

*The political opportunity structure: The media - the internet*

Any attempt at examining this relationship should include a discussion of the issues of media sensitivity and event density.<sup>294</sup> The press is more likely to report protest events that are more violent, involve more people and persist longer. The key event characteristics they identify are size, violence and duration. These factors are collectively designated as event density. Moreover, researchers using the media as a main source of information have to rely largely on practitioners from another profession, such as reporters, editors and publishers, who make the decisions on which version of experience will ultimately be available for research purposes.<sup>295</sup> Normally the media provide information on the actors who disagree, but much less information on what they disagree about.<sup>296</sup>

Also, movements as it is commonly known have to walk the fine line between extreme forms of action, which alienate third parties but secure coverage, and

---

<sup>293</sup> Van de Donk, W, Loader, B, Nixon, P, Rucht, D: (2004) *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p. 24

<sup>294</sup> Snyder, D and Kelly, W: (1977) 'Conflict intensity, media sensitivity and the validity of newspaper data', *American Sociological Review*, vol.42, no.1, pp. 105-123

<sup>295</sup> Mueller, C: (1997) 'International press coverage of East German protest events', *American Sociological Review*, vol.62, no5, p.821.

<sup>296</sup> Klandermans, B and Goslinga, S: 'Media discourse, movement publicity, and the generation of collective action frames: Theoretical and empirical exercises in meaning construction' in McAdam, D, McCarthy, J and Zald, M (eds.): *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Structural Framings*, Cambridge University Press: Cambridge, p. 336



conventionality, which (even if potentially persuasive) is ignored by the media. In effect, radical reform groups must master the art of simultaneously playing to a variety of publics, threatening opponents, and pressuring the state, all the while appearing non-threatening and sympathetic to the media and other publics.<sup>297</sup> This has been a major concern for groups in sociopolitical cyberconflicts, where symbolic hacking, while drawing media attention, nevertheless deprives the other side of means of expression and invites counter-response. Social movements and mass media have several features in common: they are engaged in a struggle for attention; they want to maximise their outreach; they are confronted, though to different degrees, with competitors. Nevertheless, they not only follow a different functional logic, but also have a strikingly asymmetrical relationship when dealing with each other. This becomes clear when we consider the structural positions of the movements offering conflict, spectacle, surprise, threat, etc., on the one hand and the media (potentially) granting coverage, importance, sympathy, etc., on the other hand. In a nutshell, this asymmetry stems from the fact that most movements need the media, but the media seldom need the movements.<sup>298</sup>

Kielbowicz and Scherer indicate that the media are instrumental for social movements in at least three different ways: (1) media are important means of

---

<sup>297</sup> McAdam, D: 'The framing function of movement tactics: Strategic dramaturgy in the American civil rights movement' in McAdam, D, McCarthy, J and Zald, M (eds.): *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Structural Framings*, Cambridge University Press: Cambridge, p.344

<sup>298</sup> Rucht, D: (2004) 'The quadruple 'A': Media strategies of protest movements since the 1960s' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York.

reaching the general public, to acquire approval and to mobilise potential participants; (2) media can link movements with other political and social actors; and (3) media can provide psychological support for social movements.<sup>299</sup>

The media spotlight validates the movement as an important player. This suggests that the opening and closing of media access and attention is a crucial element in defining political opportunity for movements.<sup>300</sup> The media form a component of the political opportunity structure with both structural and dynamic elements. The media system's openness to social movements is itself an important element of political opportunity. On the one hand, the media play an important role in the construction of meaning and the reproduction of culture. On the other hand, the media are also a site or arena in which symbolic contests are carried out among competing sponsors of meaning, including movements.<sup>301</sup> The role of the media apparatus as a validator for the larger society about whose views need to be taken seriously makes it crucial target for movement efforts to open political space. The media system operates to favor extra-institutional actors in some ways and institutional actors in others.<sup>302</sup>

---

<sup>299</sup> cited in Klandermans, B and Goslinga, S: 'Media discourse, movement publicity, and the generation of collective action frames: Theoretical and empirical exercises in meaning construction' in McAdam, D, McCarthy, J and Zald, M (eds.): *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Structural Framings*, Cambridge University Press: Cambridge, p.319

<sup>300</sup> Gamson, W and Meyer, D: (1996) 'Framing political opportunity' in McAdam, D, McCarthy, J and Zald, M (eds.): *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Structural Framings*, Cambridge University Press: Cambridge, p.285

<sup>301</sup> *ibid.*, p.287

<sup>302</sup> McAdam, D, McCarthy, J and Zald, M (eds.): *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Structural Framings*, Cambridge University Press: Cambridge, p.289



In addition, Waterman uses the term communication internationalism to characterise the terrain in which contemporary movements operate.<sup>303</sup> He outlines four characteristics of communication internationalism: i. it operates in the field of ideas, information and images, revealing that which is globally concerned and new meanings for it, ii. it is particularly effective on the terrain of communication, media, and culture, iii. the basic relational principle is that of the network rather than the organisation, and iv. the movement needs to be primarily understood in communicational/cultural rather than political/organisational terms.

Interestingly, contemporary movements combine forms of action that impact upon different levels of the social system, pursue diverse goals and belong to different phases of development of a system or to different historical systems.<sup>304</sup> An example of this communication internationalism is what Howard Rheingold describes in his recent work *Smart Mobs: The Next Social Revolution* when he writes about 'smart mobs' (defined as 'people who are able to act in concert even if they don't know each other') reshaping the way societies organise and interact. His thesis is that the mobile internet provides far more than a version of the wired workstation. It is, he asserts, creating a quiet revolution. As Rheingold puts it, '[m]obile communications and pervasive computing technologies, together with social contracts that were never possible before, are already beginning to change the way people meet, mate, work, war, buy, sell, govern and create'.<sup>305</sup> Van de

---

<sup>303</sup> Waterman, P: (2001) *Globalization, Social Movements and the New Internationalisms*, Continuum: London and New York, p.215

<sup>304</sup> *ibid.*, p.43

<sup>305</sup> Glasner, J: 'Mobile junkies reshaping society?', *wired*, 9/10/02



Donk et.al are also supporting this view. They claim that '[t]he internet is not used as a mere supplement to traditional media, it also offers new, innovative opportunities for mobilising and organising individuals. The new technologies, however, do not determine these innovations. The internet provokes innovation, but this innovation has to be organised and disseminated'.<sup>306</sup>

The most interesting question is whether traditional media have been sidelined by the alternative media of the internet, a topic I shall return to in section 6.2. For example, ICTs could improve a movement's capacity to act in a coordinated and coherent way, to react more quickly to an external challenge, and to become less dependent on the established mass media in conveying their messages to a broader audience.<sup>307</sup> However, Rucht argues that the net has relativised, but has not replaced, the traditional means of both internal and external communication of the movements.<sup>308</sup>

In my view, the effect of the internet (as part of the political opportunity structure) on the framing process is in fact a striking one. In terms of framing, the groups that use the internet have been innovative in issues both of identity and strategy, and also in framing the issues themselves. As le Grignou and Patou argue, '[t]he internet makes visible the fragmented plurality of its action by listing together

---

<sup>306</sup> Van de Donk, W, Loader, B, Nixon, P, Rucht, D: (2004) *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p.6

<sup>307</sup> Van de Donk, W, Loader, B, Nixon, P, Rucht, D: (2004) *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p.11

<sup>308</sup> Rucht, D: 'The quadruple "A": (2004) 'Media strategies of protest movements since the 1960s' in *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p.53

subjects and causes... [I]t simultaneously makes homogenous and coherent a set of analyses, activities and movements which otherwise be scattered'.<sup>309</sup> The emergence of global justice movements that closely link a number of issues such as human rights, social rights, poverty and environmental issues has been greatly facilitated by the use of ICTs.

In identity terms, Nip for example found the participants on the Queer Sisters bulletin board developed a sense of solidarity with the Queer Sisters and shared a culture of opposition to the dominant order, but they fell short of harbouring a collective consciousness.<sup>310</sup> This could be explained perhaps by the difficulty in building collective trust in cyberspace. As Wright argues, 'ICTs have sometimes played a dramatic role in communicating rich, multiple impressions of particular events as they unfold, but they have been used less successfully in promoting a coherent, collective assessment of what these events mean within the overall process of social change.'<sup>311</sup>

At the final analysis, the internet could improve a movement's capacity to act in a coordinated and coherent way, to react more quickly to an external challenge, and to become less dependent on the established mass media in conveying its messages to a broader audience. The most extreme version of this argument is

---

<sup>309</sup> le Grignou, B and Patou, C: (2004) 'ATTAC(k)ing expertise' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p.172

<sup>310</sup> Nip, J: (2004) 'The Queer Sisters and its electronic bulletin board' in *Cyberprotest: New media, citizens and social movements*, Routledge: London and New York, p. 255



Diebert's who stresses that the role of the internet went beyond facilitating activism already in place; rather it helped create 'a new formation on the world political landscape'.<sup>312</sup>

Another significant factor in social movement theory is system uncertainty. Those who govern have not only to deal with institutional systems of representation, but also with new forms of action such as those used by social movements. The resulting conflicts cannot easily be adapted to the existing channels of participation and representation (e.g. transformed into political parties). In addition, social movements can test the limits of a system; they can 'violate the boundaries of a system, thereby pushing the system beyond the range of variations that it can tolerate without altering its structure'.<sup>313</sup> This system uncertainty is increased by the new tactics possible through the internet, which either directly use computers (such as hacking) or help social movements to organise, communicate and mobilise. The nature of the internet itself eliminates the boundaries of the state, challenging the certainty of state sovereignty and control.

Of course, social movements can be crushed by a totalitarian state. This issue is addressed in section 4.2, when talking about dissidents using the internet against such states. It is also relevant, for example, in connection to the peace and anti-

---

<sup>311</sup> Wright, S: (2004) 'Informing, communicating and ICTs in contemporary anti-capitalist movements' in *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p.90



globalisation movements, because 'social movements can easily become segmented, transform themselves into defense of minorities or search for identity, while public life becomes dominated by pro or anti state movements. That is what is happening today, especially in Germany and the US with peace movements'.<sup>314</sup>

This section looked at key elements of social movement theory, which can help us with our analysis of sociopolitical cyberconflicts. The subject of new social movements was approached differently by Europeans and Americans. Europeans emphasised the need for a systemic approach that links new forms of social conflict to post-industrial capitalism and the identity-oriented paradigm, while in the U.S. theorists focused on resource mobilisation theory. The key issues in social movement theory analysed here were: the 'newness' of NSMs, the NSMs as a product of a post-industrial economy, the alleged new middle-class orientation of NSMs, the mobilising structures (the network-style structure of movements using the internet, participation, recruitment, tactics, goals), framing processes (issues, strategy, identity, the effect of the internet on these processes) and the media (and the internet particularly) as a component of the political opportunity structure. This extensive discussion and analysis of central elements of social movement theory is going to prove useful when looking at new social movements and their use of the internet. The next section identifies elements of conflict theory, especially relevant to ethnoreligious cyberconflicts.

---

<sup>312</sup> Nip, J: (2004) 'The Queer Sisters and its electronic bulletin board' in *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p.233

<sup>313</sup> Waterman, P: (2001) *Globalization, Social Movements and the New Internationalisms*, p.29

<sup>314</sup> *ibid.*, p.780.

## 2.2 Conflict Theory.

The Other outrages our sense of the kind of nation ours should be in so far as s/he steals our enjoyment - to which we must add that this Other is always an Other in my interior, i.e. that my hatred of the Other is really the hatred of the part (the surplus) of my own enjoyment which I find unbearable and cannot acknowledge, and which therefore transpose ("project") into the Other via a fantasy of the "Other's enjoyment".<sup>315</sup>

Globalisation is often portrayed in broad terms of cultural and technological change: we share friends from different places, culture, food, and resources, and we show solidarity with faraway peoples. The problem is that not everybody has access to this opportunity-rich phenomenon. Actually, in certain instances, the idea of globalisation is an instance of rhetoric used by governments to justify their submission to financial markets. The same governments are challenged by these global flows of capital, technology, information and people. Also, people might find their identities threatened by such a process. At the same time globalisation itself can directly resuscitate local traditions and literally thrive on them.

---

<sup>315</sup> Eley and Suny 1996 quoted in Salecl, R: 'National Identity and Socialist Moral Majority', in G. Eley and R.G Suny (eds.), *Becoming National: A Reader*, Oxford University Press: Oxford, pp. 418-425.



In other words, the concept of globalisation is a conflation of two distinct phenomena: the corporate takeover of the world, and a process of fragmentation of national, ethnic and religious identity-communities, which is creating a more open social context. Whereas the former is to be resisted, the latter provides the basis for a transformative politics, if not a revolutionary macro-politics. The trick is not to try stopping deterritorialisation but rather, to use it as a resource. This has been the practice of global resistance movements, grassroots social movement organisations and social networks against governments and international institutions. As a result of the activity of such movements, neo-liberal governments and institutions face a counter-hegemonic account of globalisation, to which they have responded in a confused and often contradictory way. The challenge expresses itself as resistance and/or violent opposition against governments and against international institutions either in a sociopolitical or ethnoreligious context. This type of political activity is not sufficiently explained by new social movement theory. Instead, an approach that is capable of capturing the sources and nature of ethnoreligious conflict as well as its global context is needed. This part of the analysis will be framed by the works of Deleuze and Guattari, Khan, Chesters, Callinicos and Jabri, giving us another way of viewing the internet as a rhizome in the context of global conflict.

In relation to the ethnoreligious context we should mention here Campbell's definition of ontopology, which provides us with an explanation of complex conflicts like that in Bosnia. Ontopology, as Campbell explains, is the connection



of 'the ontological value of present-being to its situation, to the stable and presentable determination of a locality, the topos of territory, native soil, city body in general'. Campbell's analysis draws on how Derrida understands conflicts like that in Bosnia.<sup>316</sup>

In their work *A Thousand Plateaus*, Deleuze and Guattari argue that the information revolution is altering the nature of conflict by strengthening network forms of organisation over hierarchical forms. The network form of organisation could also be described as the rhizome.<sup>317</sup> They argue against a world where 'the tree is already the image of the world or the root the image of the world tree'.<sup>318</sup> All the various instances of desire, identity and belief are constructed as if they were elements within a single totality, 'arborescent' or 'striated' in Deleuze's terms, like the branches coming from the main trunk of a tree. One of the interesting aspects of their argument is that they prefer to explain the world with principles of connection, heterogeneity and multiplicity, where 'any point of a rhizome can be connected to anything other, and must be'.<sup>319</sup> In this vein, a rhizome establishes connections between semiotic chains, organisations of power and circumstances relevant to the arts, sciences and social struggles. In contrast to centred (even polycentric) systems with hierarchical modes of communication and pre-established paths, the rhizome is an acentred, nonhierarchical, non-

---

<sup>316</sup> Edkins et.al: (1999) *Sovereignty and Subjectivity*, Lynne Rienner: Boulder, p.27, cites Derrida, *Spectres of Marx*, 82

<sup>317</sup> Deleuze, G and Guattari, F (1987), *A Thousand Plateaus*, Athlone: London.

<sup>318</sup> Ibid., p.5.

<sup>319</sup> Ibid., p.7.

signifying system without a General and without an organising memory or central authority, defined solely by a circu.<sup>320</sup>

Based on this rhizomatic conceptualisation of the world, the internet is a typical rhizomatic structure and the groups using it are rhizomatic in character because they seem to have no leader, coming together for an event (for example anti-globalisation protests or hacking enemy websites) and dissolving again back to their own ceaselessly changing line of flight into the adventitious underground stems and aerial roots of the rhizome. Deleuze and Guattari might have been easily be speaking about the internet when they wrote:

To these centred systems the authors contrast acentred systems, finite networks of automata in which communication runs from any neighbour to any other, the stems or channels do not pre-exist, and all individuals are interchangeable, defined only by their state at a given moment - such that the local operations are co-ordinated and the final, global result synchronised without a central agency.<sup>321</sup>

The world system operates as an arborescent apparatus. However, such an apparatus is necessarily haunted by the possible emergence of 'lines of flight' which take its elements outside the framework it constitutes. The elements which escape the world system have a different structure – less arborescent than rhizomatic, emerging through underground networks connected horizontally and

---

<sup>320</sup> *ibid*, p.40.

<sup>321</sup> *ibid.*, p.17.

lacking a hierarchic centre. The system's resort to violence is an attempt to crush various rhizomatic and quasi-rhizomatic elements which tend to escape it.

It is no wonder that rhizomes are a source of threat to those whose commitments are structured around the positivist valuation of machines of control. Arguments like these were taken up by Arquilla and Ronfeldt to explore the future of conflict and network forms of social organisation. Particularly relevant to my research is the question of how the structure of the internet itself (a global network with no central authority) has offered another experience of governance (no governance), time and space (compression), ideology (freedom of information and access to it), identity (multiplicity) and fundamentally an opposition to surveillance and control, boundaries and apparatuses. In the final analysis, new information-age ideologies could easily be arguing for a transfer of virtual social and political structures to the offline world, reversing for once the existing process of online actors imitating real life in cyberspace. The internet is not a medium. It is 'another' place:

Global interpersonal communication is the greatest tool for world peace our species has ever known. We have the technology to achieve collective consciousness on a planetary scale. The potential of Electronic Revolution is awesome. Instead of electing an aristocracy whose choices are packaged by mass media marketing to govern us, we have the ability to transcend the physical



limitations of deceptive appearance and illuminate the truth of being through the digitized reflection of intelligence.<sup>322</sup>

The form of the internet is itself a message, a symbolic challenge to dominant patterns of hierarchical structures of governance. The wars in Iraq and Afghanistan largely follow the model of non- outlined in Baudrillard's analysis of the first Gulf War war and further extended by Ignatieff<sup>323</sup>. Rather than being collisions of two powers located symmetrically within a single discourse, they involve the feints and counterfeints of two sides separated by radical discursive difference. America and its allies were in both cases attempting to impose a discourse of control embodying a logic of deterrence. As General Wesley Clark said of the bombing of Yugoslavia, 'this was not, strictly speaking, a war'.<sup>324</sup>

Non-war happens within an almost virtual 'public sphere'. As Baudrillard argues, media images are now the continuation of war by other means. War, the most concentrated form of violence, has become cinematographic and televisual, just like the mechanically produced image.

The true belligerents are those who thrive on the ideology of the truth of this war, despite the fact that the war itself exerts its ravages on another level, through faking, through hyper reality, the simulacrum, through all these strategies of psychological deterrence that make play with facts and images, with the

---

<sup>322</sup> Taylor, P: (1999) *Hackers*, Routledge: London

<sup>323</sup> Ignatieff, M: (2000) *Virtual War: Kosovo and Beyond*, Chatto and Windus: London.

<sup>324</sup> *ibid.*, p.3

precession of the virtual over the real, virtual time over real time, and the inexorable confusion between the two.<sup>325</sup>

As Bloom argues, 'the mass public as a foreign policy variable will always react against policies that can be perceived to be a threat to national identity and to policies which protect or enhance national identity... national chauvinism is commercially successful'.<sup>326</sup> Another interesting point Bloom makes is that there is one tier of information possessed by the security services and decision-making elites; there is another tier in the public domain. The restriction on complete disclosure is precisely to avoid the possible triggering of the national identity dynamic which would take decision making out of the hands of the 'responsible' and informed few.<sup>327</sup>

Non-war often occurs in the form of ethnoreligious conflict, based on issues of ethnic, religious and national affiliation involving a strong sense of identity. Ethnic affiliation provides a sense of security in a divided society, reciprocal help, and protection against neglect of one's interests by strangers. Ethnic divisions reaffirm rather than undermine fixity and closure. As Horowitz puts it, '[i]n deeply divided societies ethnicity - in contrast to other lines of cleavage, such as class or occupation - appear permanent and all encompassing, predetermining

---

<sup>325</sup> Baudrillard, J: (1995) *The Gulf War Did Not Take Place*, Bloomington, Ind.: Indiana University Press, p.177

<sup>326</sup> Bloom, W: (1990) *Personal Identity, National Identity and International Relations*, Cambridge University Press: Cambridge, p.80.

<sup>327</sup> *ibid.*, p.88

who will be granted and denied access to power and resources'.<sup>328</sup> Ali Khan argues that there is an old and apparently primordial human inclination to maintain self-identity by continually creating an 'other'. Power systems become dependent on such identities and loyalties via patronage networks.<sup>329</sup>

The information revolution is likely to strengthen local and ethnic identities. In fact, territorial and ethnic communities may become even more cohesive and permanent. Communication resources in many nation-states are actually decentralised, creating local and provincial print media, radio and television. Pluralist and alternative viewpoints in national discourse are protected by allocating radio and television resources to ethnic, linguistic and cultural minorities. This resurgence of territorial and ethnic identities may weaken those nation-states that are built by joining disparate historic provinces, localities and ethnic populations.<sup>330</sup>

Khan's model is certainly relevant to politics in Iraq and Afghanistan, and is echoed in Vivienne Jabri's analysis of the ways in which discourses of inclusion and exclusion constitute individual identity in ways which lead to violent conflicts.

---

<sup>328</sup> Horowitz in Diamond and Plattner: (1994) *Nationalism, Ethnic Conflict and Democracy*, John Hopkins University Press: Baltimore and London, p.xviii.

<sup>329</sup> Khan, A: (1996) *The Extinction of Nation States: A World Without Borders*, Kluwer Law International: The Hague, p.128.

<sup>330</sup> *ibid.*, p.128



Since every search for identity includes differentiating oneself from what one is not, identity politics is always a politics of the creation of difference... What is shocking about these developments is not the inevitable dialectic of identity/difference that they display, but rather the atavistic belief that identities can be maintained and secured only by eliminating difference and otherness. The negotiation of identity/difference to use William Connolly's felicitous phrase is the political problem facing democracies on a global scale.<sup>331</sup>

Three phenomena challenge these traditional notions of sovereign bodies; corporate transnationalism/global economy, environmental unity, and the information revolution are in the process of transforming traditional notions of territorial communities tied to contiguous geographical areas. Information-driven communities require no geographical contiguity, threatening the core characteristic of the state structure.

Robin Brown, when considering the relevance of Schattschneider's work to the information society, argues that private matters become identified as public as the scope of conflict grows. Easier access to information, and the mobilisational possibilities that result, make it easier to expand the scope of conflict. As a result, the information society, by facilitating the diffusion of information on a global

---

<sup>331</sup> Jabri, V: (1996) *Discourses on Violence: Conflict Analysis Reconsidered*, Manchester University Press, p.3

basis, creates new possibilities for political strategy through the globalisation of conflict.<sup>332</sup> As Brown puts it:

Schattschneider's theory would suggest that groups that are disadvantaged at the current scope of politics would initially embrace the new technology. Dominant actors would seek to limit its impact but if this was not feasible they would have to adopt their own strategies to the new environment.<sup>333</sup>

In line with this argument, if some people want to expand the scope of conflict, then others want to reduce it. The ways to do this are multiple. 'The first is to ensure that people are unaware of potential issues or actual conflicts. The second strategy is to construct a political discourse that legitimates the involvement of some people but not others.'<sup>334</sup> An example of this can be found in political discourse during the 2003 Iraq war.

Furthermore, between the global resistance movements and the ethnoreligious movements, it is clear that very little of the periphery is subsumed into the world system in a stable and hegemonic way; there are, rather, flows of domination between 'rich and poor, hemispherically from N to S, regionally between peripheral and core nationally across class and ethnic boundaries'.<sup>335</sup> The 'line of flight' emerging from resistance movements could be best described as parallel

---

<sup>332</sup> Brown, R: 'The Contagiousness of Conflict: E.E. Schattschneider as a theorist of the information society', *Information, Communication and Society*, 5:2 2002, pp. 264-5

<sup>333</sup> *ibid.*, pp. 266-7

<sup>334</sup> *ibid.*, p.268

<sup>335</sup> Chesters, 'Shape shifting: Civil society, complexity and social movements', *Anarchist Studies*, 11, 1, pp.42-65

lines, a parallelogram of forces as Graeme Chesters argues: the whole of singularities against WTO, IMF, WB; People's Global Action, World Social Forum and suchlike have an ecology of action which indicates a web of horizontal social solidarities in which power might be devolved, or even dissolved. Anti-capitalist and other rhizomatic groups have constructed many new forms of political action, and also new forms of communication.

In theory that is. In practice what we get when we abstract the ethnoreligious movements or groups, we are left with antiwar groups, anti-capitalist/anti-globalisation movements, campaigns that focus on specific issues and grievances, and lifestyle-issue movements (the latter not quite relevant to our discussion, and as pointed by Callinicos<sup>336</sup>). These can be referred to as movements of a sociopolitical nature. In contrast to the closure of space, the violence and identity divide found in ethnoreligious discourses, these movements seem to rely more on networking and grassroots organising, much more than is the case with the hierarchical structures, states and their followers. Several metaphors have been used to describe a large number of groups being brought together under a common cause, groups that disperse as easily as they come together, a parallelogram of forces following a swarm logic like ants in an ant colony. It may be argued that because citizens do not believe in power through conventional politics, citizens are increasingly sympathetic to direct action.

---



Without the need for a leader and without a particular individual having a privileged insight, or being able to conceptualise the whole characteristics, there is an emphasis on participation, antipathy to hierarchy, a preference for consensus processes and/or directly democratic decision-making, an ethos of respect for differences and an assertion of unity in diversity. The project is less the capture of the state apparatus than the construction of an open and transnational public sphere, a rhizomatic extension of struggles operating through weak ties.<sup>337</sup>

Sometimes, ethnoreligious and sociopolitical conflicts overlap. Whatever the connection between the Palestinians' oppression and global capitalism in the shape of US imperialism, the system itself is not the centre of Palestinian consciousness when they fight the Israeli state. As Trotsky pointed out, sometimes the point of honour is not what one has in common with the movement, but in the particularity that distinguishes them from it.<sup>338</sup> Apart from the rhizo-terrorists such as al-Qaeda, anti-capitalist and other rhizomatic groups have constructed many new forms of political action, and also new forms of communication.

Furthermore, another part of conflict theory deals with conflict resolution. I think it would prove important for a later discussion in section 5.3 to deal here with some aspects of conflict resolution, such as mediation and negotiation.

---

<sup>336</sup> Callinicos: 'Regroupment, realignment and the revolutionary left', [www.swp.org.uk/INTER/regroupen.pdf](http://www.swp.org.uk/INTER/regroupen.pdf)

<sup>337</sup> Chesters, 'Shape shifting: Civil society, complexity and social movements', *Anarchist Studies*, 11, 1, pp.42-65

To begin with, Tidwell<sup>339</sup> refers to the work of Bush and Folger, *The Promise of Mediation*. The authors argue that there are four primary objectives found in mediation broadly-defined. The first is satisfaction theory, wherein mediation serves to satisfy human needs. The second is social justice, which emphasises the role of mediation in the formation of community. The third perspective is transformation, where mediation is the ability to transform both individuals and society as a whole. Transformation occurs when people alter their values and beliefs about themselves and others. Lastly, there is the oppression story, which views mediation as a tool for control and domination.

Another way of problematising negotiation is offered by what Rothstein calls the concept of interactive problem-solving.<sup>340</sup> According to him, negotiation should first of all treat the conflict as a problem shared by the parties. Second, negotiation explores ways of solving this problem, 'not by eliminating all conflict and potential conflict between the parties, but by addressing the underlying causes of the conflict and reversing the escalatory dynamics of conflict relationship'. His third step is that negotiation is an interactive process, capable of producing ideas to solve the problem which are responsive to the parties' fundamental concerns.

Furthermore, negotiation is very much affected by culture. Culture is brought into the negotiation process by individuals, groups and organisations. It conditions

---

<sup>338</sup> 'Trotsky: The new course', [www.marxists.org/archive/trotsky/1923-nc/index.htm](http://www.marxists.org/archive/trotsky/1923-nc/index.htm)

<sup>339</sup> Tidwell, A.C: (1998) *Conflict Resolved?*, Pinter: London and New York, p.156.



how they view the negotiation, the kind of game they perceive to be going on. As Berton and his colleagues argue, structural components of a negotiation are not culturally free.<sup>341</sup> External constraints, such as the legal framework and the organisational setting of a negotiation, are social constructs. The other main factors affecting negotiation include the number of parties involved, the number of issues at stake and the distribution of power between the parties. Also, beliefs express a set of values derived from the cultural background of the negotiator. In this way, cultural values directly affect the behaviour of actors involved. Tidwell has the same view when he argues that 'methods such as mediation or facilitation may not be appropriate within a given cultural context... [I]n cultures in which to speak directly about a conflict is regarded inappropriate, many Western methods would simply not work'.<sup>342</sup>

According to Cairns there is no single way to build a peaceful society after a war has ended. What both 'successful' and 'failed' peace processes show is that 'peace cannot be built simply on multi-party elections, after which most of the international community make a quick exit'.<sup>343</sup> What he recommends instead is reviving the community systems of mediation. This can sometimes be an effective means of resolving current conflicts. He uses the example of community leaders from both sides of Mali's conflict to make his point. They have formed so-called peace cells to resolve intercommunal disputes. This initiative has not replaced

---

<sup>340</sup> Rothstein, R.L: (1999) *After the Peace*, Lynne Rienner: Boulder, London, p. 193.

<sup>341</sup> Berton, P et.al: (1999) *International Negotiation*, St.Martin's Press: New York, pp. 21;26.

<sup>342</sup> Tidwell, A.C: (1998) *Conflict Resolved?*, Pinter: London and New York, p.6

<sup>343</sup> E: (1997) *A Safer Future*, Oxfam Publications: England, p.88.



traditional ways of dealing with conflicts, but it is built on them, including the web of alliances, which cross ethnic groups and families, known as 'cousinage'. Another positive case is Colombia with the growth of so-called 'communities of peace'. These are groups declaring neutrality in the fighting between military, paramilitary and guerrillas. The Antioqua Indigenous Organization, which Oxfam supports, combines practical help of food shelter and medicine with the use of the media to proclaim neutrality.

This section discussed the rhizomatic structure of new social movements and of the internet itself in the contexts of globalisation, issues of national identity, ontopology, ethnic affiliation and discourses of inclusion and exclusion. These issues are crucially linked to ethnoreligious cyberconflicts and the various ways the opposing parties in them develop and perform. I then looked at the structure of conflicts involving new social movements such as the anti-war and anti-capitalist movements, where there is an emphasis on participation, antipathy to hierarchy, and the project is less the capture of state apparatus and more the construction of an open and transnational public sphere. This discussion provided a context through which we can analyse new social movements and their use of the internet in sociopolitical cyberconflicts and a focus on national identity and discourse to help interpret ethnoreligious cyberconflicts. Lastly, I discussed some of the aspects of negotiation and mediation as part of conflict resolution techniques, which will prove useful in the discussion of attempts at conflict resolution on the

internet. The next section offers a discussion of media theory elements that would prove useful when looking at the internet as a medium.

## 2.3 Media Theory.

‘The Gulf War is over and the press lost’<sup>344</sup>

The total obliteration of war by information, propaganda, commentaries, with camera-men in the first tanks and war reporters dying heroic deaths, the mish-mash of enlightened manipulation of public opinion and oblivious activity: all this is another expression for the withering of experience, the vacuum between men and their fate, in which their real fate lies. It is as if the reified, hardened plaster cast of events takes place of events themselves. Men are reduced to walk-on parts in a monster documentary film which has no spectators, since the least of them has his bit to do on the screen.<sup>345</sup>

De Fleur Ball-Rokeach distinguishes between three different effects of the mass media on individuals, which are closely linked to the emergence and coverage of global conflicts. These are: cognitive effects (the creation and resolution of ambiguity, attitude formation, agenda-setting, expansion of people’s systems of beliefs, impact on values), affective effects (desensitisation, anxiety, morale and alienation) and behavioral effects (activation, deactivation).<sup>346</sup> Another particularly relevant issue is the dynamic of mass media construction of

---

<sup>344</sup> Barry Zorthian, Chief Pentagon Public Affairs spokesman, during the Vietnam war, to a National Press Club forum on March 19, 1991.

<sup>345</sup> p.55, Poster, M: (1995) quotes P.11 from Adorno, T: (1974) *Minima Moralia: Reflections from a Damaged Life*, trans. E.Jepcott, New Left Books: London.

<sup>346</sup> De Fleur, M and Ball-Roceach, S: (1982) *Theories of Mass-communication*, 4<sup>th</sup> edn, Longman: New York and London.



consensus, control, adaptation, conflict and change. These dimensions and their effects on conflict of either ethnoreligious or sociopolitical roots are the focus of this section.

One of the key issues is the way in which the media set an agenda. A useful approach looks at the actual language used by the media, especially appropriate for internet analysis because the most common feature of the internet is text. The questions that need to be asked, as outlined by Fairclough, are: how is the world (events, relationships) represented? What identities are set up between those involved in the story? What relationships are set up between those involved? What are, then, the particular representations of the world, particular constructions of social identities and particular constructions of social relations?<sup>347</sup> Among others, Fairclough provides an example of the analysis of discourses in texts when he examines press coverage of an air attack on Iraq by the USA, Britain and France on 13 January 1993, referring to five British newspapers. A brief glimpse of this analysis could prove useful as a guideline for my research:

The main headline and lead paragraph from the Sun show that formulations of the attack do not by any means draw only upon military discourse: Spank you And Good Night...and More than 100 allied jets ...gave tyrant Saddam Hussein a spanking. This is a metaphorical application of an authoritarian discourse of

---

<sup>347</sup> Fairclough, N: (1995) *Media Discourse*, Arnold: London and New York, p. 5.

family discipline which is a prominent element in the representations of the attack - Saddam as the naughty child punished by his exasperated parents.<sup>348</sup>

The Gulf War has inspired a lot of media research, being the ultimate television war,<sup>349</sup> and it will continue to do so in the future, because it was the first war extensively covered through the internet. Taylor poses key questions in relation to the control of information by military and political authorities: what arrangements were made for the release of information and why? How much censorship was taking place? How far back did the journalists stand from what was being told to them or were they merely drawn into the media management system? What alternative sources of information were available?<sup>350</sup> (This last question is especially interesting in relation to web coverage and blogging during the 2003 war in Iraq).

A good example of the media construction of social identities, and specifically the enemy identity, is the emphasis placed by Bush senior's administration on projecting the image of an enemy posing a serious military, economic and ideological threat to the New World Order. Saddam was represented as a formidable military power, ready to dominate the Middle East. Taylor puts it down very graphically: 'Kuwait had been "raped", Iraqi troops were "plundering" the tiny and helpless state and "butchering" its people...It was even claimed for

---

<sup>348</sup> *ibid.*, p.95

<sup>349</sup> Taylor, P (1992) *War and the Media Propaganda and Persuasion in the Gulf war*, Manchester University Press: Manchester, see also MacGregor 1997; Wolfsfeld, 1997

<sup>350</sup> *ibid.*, p.vii

domestic consumption, that this would be a war for the American way of life. Saddam must not be “appeased” as Hitler had been in Munich...’<sup>351</sup>

The fact that the CNN provided a public insight into the traditionally secretive world of diplomacy has altered the way modern warfare is projected onto the world’s television screens. What is more, it raises a lot of ambiguity over what truly happened in that war, that is, over the relationship between the ‘real’ war and the war as portrayed by the media.

One of the central questions is how censored or restricted journalists are while covering conflicts and how ‘unbiased’ they can be in constructing social reality, identities and relations. Knightley in his work on war correspondents from Crimea to Kosovo reveals how the role of the war correspondent as the heroic truth-seeker is in danger of becoming more that of a mythmaker. Again, the Gulf war conflict is taken as a turning point in the history of war correspondents. As Knightly argues, ‘[n]ot only was it a war in which the military succeeded in changing people’s perceptions of what battle was really like..., but one in which the way the war was communicated was as important as the conduct of the war itself.’<sup>352</sup>

War correspondents are just one part of a larger picture. As McGregor argues, the largely consistent findings show the news products to be, in one sense or another,

---

<sup>351</sup> *ibid.*, p.5



an artificial and very predictable symbolic construction of reality.<sup>353</sup> However, this conclusion is itself open to alternative interpretations, since homogeneity could result either from a hegemonic ideology or simply from the standardisation to be expected in mass production processes, or perhaps a combination of the two.<sup>354</sup> In the 'first living room war', the Vietnam War, despite the fact that the network news deserve credit for the eventual disillusionment with the war, at the same time they were also responsible for creating or at least reinforcing the illusion of American omnipotence in the first place.<sup>355</sup> An example of this was that American media delayed for two years the reporting of the My Lai massacre, not because of censorship, nor because the facts were not instantly available, but due to resistance to the story by the US media itself.<sup>356</sup> That was because the massacre occurred in 1967, when the storyline was focused on 'good news' about a war editors were persuaded the US was winning:

Other television reporters have detected significant media impact "only at moments of policy panic" or "where policymaking is weak or cynical". Although television assumed a high profile in accounts of policy influence, closer analysis revealed interdependence with other forms of news media.<sup>357</sup>

---

<sup>352</sup> Knightley, P: (2000) *The First Casualty: The War Correspondent as Hero and Myth-maker from Crimea to Kosovo*, Prion: London, p.500.

<sup>353</sup> McGregor, B: (1997) *Live, Direct and Biased? Making Television News in the Satellite Age*, Arnold: London and New York.

<sup>354</sup> *ibid.*, p.78, cites McQuail.

<sup>355</sup> Epstein quoted in Mercer, D, Mungham, G and Williams, K: (1987) *The Fog of War: The Media on the Battlefield*, Heinman: London, p.229.

<sup>356</sup> Mercer, D, Mungham, G and Williams, K: (1987) *The Fog of War: The Media on the Battlefield*, Heinman: London

<sup>357</sup> Koppel, T in 'Impact of television on US foreign policy', Congressional Hearing, 5

A much more recent 'construction of reality' by western media was in the Balkan conflicts, where civil wars were called 'ethnic cleansing' and painted with simple terms of 'goodies and baddies', portraying the situation as a conflict where the international community could do nothing. When Milosevic failed to 'stop the ethnic cleansing' of Albanians in Kosovo and the decision to bomb him into submission was taken, an impressive system of control and propaganda in both the US and Britain swung into action.<sup>358</sup> In the two main sections of interest, news of the fighting and justification for it, the Kosovo conflict was a case in point of propaganda-led warfare, because 'to sell a war in a democracy when you are not attacked, you have to demonise the leader or show that there are humanitarian reasons for going in'.<sup>359</sup> The extent to which the media were managed was high, as the words of Alastair Campbell, press officer and adviser to Blair betray: '[i]t was vital to try and hold the public's interest on our terms'.<sup>360</sup> The same Mr. Campbell was later accused in the media of spindoctoring, through what came to be known as the 'dodgy' dossier, a report which relied in part on a Ph.D. thesis on the web, justifying Britain's decision to go to war in Iraq in March 2003, leading to two inquiries that involved the Prime Minister himself.<sup>361</sup> Tony Blair has also won the top prize winning the 'Lifetime Menace' award for what the London-based Privacy International characterised as 'his active involvement in the government's attack on civil liberties', as he angered privacy groups with his

---

<sup>358</sup> Knightley, P: (2000) *The First Casualty: The War Correspondent as Hero and Myth-maker from Crimea to Kosovo*, Prion: London, p.502

<sup>359</sup> *ibid.*, p.502, Knightley quotes Robert Lichter, President for Media and Public affairs in Washington.

<sup>360</sup> *ibid.*, p.503, Knightley cites BBC2, October 16, 1999.

<sup>361</sup> Deans, J: 'Butler criticises 45-minute claim', *The Guardian*, 14/7/04



plans to force phone companies and internet service providers to retain users' data for 12 months as part of the state's stepped-up war on terrorism and crime.<sup>362</sup>

The implementation of policy decisions is often affected by the weight of media exposure. As Major General Lewis MacKenzie, commander of UNPROFOR in Sarajevo, commented:

Wherever the media goes, a lot of serious violations of human rights either move away or stop. The media was the only major weapon system I had. Whenever I went to negotiations with the warring parties, it was a tremendous weapon to be able to say: 'OK, if you don't want to do it the UN's way, I'll nail your butt on CNN in about 20 minutes'. That worked, nine times out of ten.<sup>363</sup>

Furthermore, there are three levels of media effect on policy: strategic (whether to intervene or not, withdraw, etc), tactical (innovations in the protection of Sarajevo that responded in part to media coverage), and presentational (they probably would not have happened apart from the media exposure that would accompany them). In addition, there are different degrees of media effect: primary (Somalia, Haiti, Rwanda), secondary (contributory effect, e.g. Iraq and Bosnia), and negligible.<sup>364</sup>

---

<sup>362</sup> Scheeres, J: 'Blair tagged as privacy threat', 25/3/03

<sup>363</sup> Quoted in New York Times, July 28, 1995, A4, cited in Minear, L, Scott, C and Weiss, T (1994): *The News Media, Civil War and Humanitarian Action*, Lynne Rienner: Boulder and London, p.59.



Moreover, as far as humanitarian intervention is concerned, the media had been criticised on several fronts. One complaint is that they pay too much attention to breaking events, while ignoring the historical and political context (reportage of the Rwandan crisis). Another is that the international media have focused on subjects of perceived interest to readers and viewers in developed countries, denigrating local institutions and overemphasising the importance of international and western initiatives.<sup>365</sup> More importantly, criticism often centres on the tendency of the media to perpetuate negative images and ethnocentric views, when those who suffer are often non-white and their 'rescuers' white, a portrayal which contributes to charges of racism in war coverage, or to media coverage as the 'pornography of suffering'.

In a media-intense environment, politicians and the public have become very unforgiving of even minor mistakes and transgressions. Events with minor operational effects, such as the killing of a Somali youth for stealing a soldier's sunglasses or the dramatic rescue of a downed F-16 pilot in Bosnia, often have disproportionately large effects on public opinion and therefore policy and outcomes. As a result, even the minutest aspect of military operations must now be planned with sensitivity to the public perception of the fight.<sup>366</sup>

---

<sup>364</sup> Minear, L, Scott, C and Weiss, T (1994): *The News Media, Civil War and Humanitarian Action*, Lynne Rienner: Boulder and London, p.71-72.

<sup>365</sup> *ibid.*, p.37

<sup>366</sup> Shapiro, J: (1999): 'Information and war: Is it a revolution?' in Khalizad, Z, White, J and Marshall, A: *Strategic Appraisal: The Changing Role of Information Warfare*, Rand: California, p.125.

Nationalism, constructed primarily (as Anderson shows) through traditional media such as newspapers and novels and also promoted by newer media such as TV, has the effect that the entire populace, not just the elite, identifies its interests with those of the government. Consequently, the government can mobilise the entire capacity of the society for a prolonged war, and even if the regular army is defeated, the people will continue to resist through irregular means. The inability of the government to control the information flow gives enemies a means to undermine this identity of interests. New techniques that allow the manipulation of video images and sound recordings and therefore allow the conduct of sophisticated psychological operations provide another resource for undermining the identity of interests between the government and the wider populace. Indeed, some believe that the real war in the information age will be for the hearts and minds of the populace or the fears and insecurities of the troops.<sup>367</sup>

But information technology is linked to the inventiveness, freedom, aspirations, and irrepressibility of the citizen. If anything, state power, in its traditional sense, can only retard this technology. The information revolution both liberates and requires liberation. As the U.S. experience shows, the freer the market, the greater the level of performance that information technology delivers.<sup>368</sup>

---

<sup>367</sup> Adams, 1996; Cooper, 1996; Nichiporuk and Builder, 1995 cited in Shapiro, J: (1999): 'Information and war: Is it a revolution?' in Khalizad, Z, White, J and Marshall, A: *Strategic Appraisal: The Changing Role of Information Warfare*, Rand: California: p.126

<sup>368</sup> Gombert, D (2001): 'Right makes might: Freedom and power in the information age', p.50 in Libicki, M and Shapiro, J: *Strategic Appraisal: The Changing Role of Information Warfare*, Rand: California.



An extreme example of the possibilities and impact of the individual in virtual political reality was during the Chechen hostage crisis in the Moscow theatre in October 2002, when one of the hostages, Rankov, contacted his friend, Olga Brukovsky, on a cell phone while the standoff was in progress. She took down his words and published them online at LiveJournal.com, a website that is popular amongst Russians, initiating a flurry of responses especially when Russian security police raided the theatre in a controversial rescue attempt, killing 117 hostages. Anton Nossik, one of the founders of LiveJournal's Russian community and chief editor of Lenta.Ru, the country's leading online news service, said at the time that the site had become an especially important source of information for people living in remote locations, such as Siberia and the Far East, where news agencies seldom send reporters. While Russian authorities attempted to control the flow of information (one television station was temporarily shut down, along with the website for the radio station Echo of Moscow), LiveJournal served as 'a good mirror of public opinion' according to Roman Leibov, a professor of Russian literature at Tartu University.<sup>369</sup>

In relation to the LiveJournal experience, the Europeans after having watched a number of heavily-hyped US internet publications struggle have chosen more modest and long-term business plans. For example, Transitions Online, based in Prague, after it ran out of money as a print publication, sought refuge on the internet. The publication, which charges its subscribers a small fee but still raises

---

<sup>369</sup>Kettman, S: 'Europe's spin on web reporting', wired, 18/7/2001



90 per cent of its budgets through grants, has a network of local correspondents in more than two dozen Central and Eastern European countries and has won a NetMedia award in 2001 for outstanding contribution to online journalism in Europe. The vast majority of their correspondents had never met until a conference was organised.<sup>370</sup>

The online records of activity are commonly falsified either by direct modification of the records themselves or by replacement of the monitoring software that produces these records. While there are analogies to these activities in the physical world, the ease, rate, and invisibility of these activities on the internet especially complicates the analysis task. Direct support for dissidents or embryonic democratic institutions is increasingly available both from the governments and non-governmental organisations of the democratic core. The penetrability of even self-isolated societies is growing, especially when sophisticated transnational 'civil society' groups make it their business to network with the oppressed.

Advanced technological systems will not only help shape the environment of future conflict but will also magnify the importance of the psychological battle to conflict outcomes. Leaders of the several former Yugoslav republics used television, radio, and print media to promote ethnic hatred and mobilise their publics to take up arms to advance or defend communal political and territorial

---

<sup>370</sup> *ibid.*

interests. Indeed, some observers believe the media became the 'main instruments in stirring up and managing' the conflict in the former Yugoslavia. Similarly, broadcasts from the government-controlled Rwanda Radio did much to foster the 1994 genocide in Rwanda by deliberately fomenting ethnic hatred among the Hutus and inciting the mass killings of Tutsis. After the Hutu government had been routed by Tutsi forces, a mobile radio still under the control of former Hutu government officials precipitated the massive flight of Hutu refugees into Tanzania and Zaïre by assuring them that they faced 'certain slaughter' if they fell under Tutsi control<sup>371</sup>. Hostile radio broadcasts also helped to undermine the U.S. and UN intervention in Somalia. To counter U.S. and UN attempts to marginalise him politically, Aideed successfully used his radio station in Mogadishu to rally support for his continued leadership and to foment anti-U.S. and anti-UN sentiment among his countrymen.<sup>372</sup>

The U.S. and other news media will become an increasingly ubiquitous presence on the future battlefield. The media will have an independent capability to gain access to future conflict arenas and to provide real-time visual and audio coverage of battlefield events. Thus, the media will be able to report promptly the human costs of U.S. combat involvement to both U.S. domestic and international audiences. Evidently, embedded journalists with the troops during the 2003 Iraq conflict is a step in that direction. As the U.S. experience in Vietnam and Somalia demonstrated, media news coverage and commentary will help shape U.S.

---

<sup>371</sup> Adelman, H and Suhrke, A: (1996) *Early Warning and Conflict management : Genocide in Rwanda*, p. 38.



domestic perceptions about whether a U.S. military involvement is effective or not and, most importantly, whether it merits continued public support.<sup>373</sup>

Advanced technological information systems will allow state and substate actors, including news services, non-governmental organisations, and even individual citizens, to make voice, video, and written information instantly available to audiences located in the remotest areas of the globe. 'ICTs have sometimes played a dramatic role in communicating rich, multiple impressions of particular events as they unfold..., but they have been used less successfully in promoting a coherent, collective assessment of what these events mean within the overall process of social change'.<sup>374</sup>

The idea of this thesis is to try and look at media and conflict together and focus on their interaction, followed up by more analysis on ethnoreligious conflict as a phenomenon and how it is affected by the presence of the media. With the internet ranking as the top information source, outpacing TV, newspapers and radio - as found by a UCLA study - media theory should relate, analyse and discuss the new medium in a more rigorous manner.

---

<sup>372</sup> Hirsch and Oakley, 1995, pp.116-117.

<sup>373</sup> Hosmer, S: (1999) 'The information revolution and psychological effects' in Khalizad, Z, White, J and Marshall, A: *Strategic Appraisal: The Changing Role of Information Warfare*, Rand: California.

<sup>374</sup> Wright, S: 'Informing, communicating and ICTs in contemporary anti-capitalist movements' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p.90



A theoretical model that attempts to discuss media and conflict together is Gadi Wolfsfeld's political contest model.<sup>375</sup> The thrust of this model is that the best way to understand the role of the news media in politics is to view the competition over the news media as part of a larger and more significant contest among political antagonists for political control. Wolfsfeld's model rests on five major arguments. First, that the political process is more likely to have an influence on the news media than the news media on the political process. Second, the authorities' level of control over the political environment is one of the key variables that determine the role of the news media in political conflicts. Political conflicts are characterised by moves and counter-moves, as each antagonist tries to initiate and control political events, to dominate political discourse about the conflict, and to mobilise as many supporters as possible to their side. Those who have success in these areas also enjoy a good deal of success in the news media. Third, the role of the news media in political conflicts varies over time and across different circumstances. It varies along with such factors as the political context of the conflict, the resources, skills and political power of the players involved, the relationship between the press and each antagonist, the state of public opinion, the ability of the journalists to gain access to the conflict events, and last by what is happening in the field. The fourth argument is that those who hope to understand variations in the role of the news media must look on the competition among antagonists along two dimensions, one structural and the other cultural. The structural dimension looks at the extent

---

<sup>375</sup> Wolfsfeld, G: (1997) *Media and Political Conflict*, Cambridge University Press: Cambridge, p.3-5.

of mutual dependence between the antagonists and each news medium to explain the power of each side in the transaction, while the cultural dimension focuses on the construction of media frames of conflict events. Wolfsfeld's fifth argument is that while authorities have tremendous advantages over challengers in the quantity and quality of media coverage they receive, many challengers can overcome these obstacles and use the news media as a tool for political influence.

More analytically, according to Wolfsfeld the ability of an antagonist to control the political environment can be understood in terms of three variables: the ability to initiate and control events, the ability to regulate the flow of information, and the ability to mobilise elite support.<sup>376</sup> The first factor relies on the fact that governments are in a much better position to coordinate their press relations when they can anticipate the events that will be covered. When, on the other hand, the powerful are forced to react to events, it suggests that others are setting and framing the media's agenda. The second variable is the ability to regulate the flow of information. Governments, both democratic and non-democratic, often find compelling reasons to employ censorship during political conflicts and this increases the value of official sources of information by eliminating competition. The ability of the powerful to regulate the flow of information to the press is also affected by the nature of the logistical and geographical environment. Powerful governments prefer to operate under conditions in which they can isolate the areas of actual conflict and regulate the entry and exit of journalists. While the physical circumstances of certain locales facilitate government control, other locations are



more porous and offer easier access for reporters, thereby increasing the level of journalistic independence. The third variable that decides the powerful's level of control over the information environment is the ability to mobilise elite support:

When the various factions within a government are promoting different frames about a conflict, it is more difficult to control the informational environment because journalists can choose among a variety of sources. When on the other hand, the official frame is the only frame available among elites, journalists will have little choice but to adopt the frame.<sup>377</sup>

The construction of media frames is another important issue in Wolfsfeld's work. He claims there are three major elements that contribute to the construction of media frames of conflict: the nature of the information and events that are being processed, the need to create a good news story, and the need to create a story that resonates politically within a particular culture:

The news media have a large variety of frames waiting on the shelf for those activists who are skilled enough to construct an effective package and lucky enough to be promoting them at a time when the authorities are vulnerable to attack. In these cases the news media can play a critical role by legitimating oppositional frames that increase the status, resources, and power of challengers.<sup>378</sup>

---

<sup>376</sup> *ibid.*, pp.25-28

<sup>377</sup> *ibid.*, p.29



The 1991 Gulf conflict represents an excellent example of a case in which the news media enthusiastically adopted the authorities' law and order frame and virtually ignored the injustice and defiance frame being promoted by the challenger. The Allied forces enjoyed a multitude of advantages in the structural field that allowed them to control a great deal of the media discourse about the war. Saddam Hussein was defined early by the news media as the aggressor and the international consensus around the law and order frame made it extremely difficult for Iraq to promote its particular version of the injustice and defiance frame.<sup>379</sup>

This section looked at various elements of media theory such as: media discourse and construction of social identity and relations citing the First Gulf War; the construction of reality by western media in the Balkan conflicts; the relationship between the media and humanitarian intervention; and the effect of the internet on conflict (the LiveJournal experience). The next section combines elements of the theories analysed so far, deriving an analytical framework for cyberconflict.

---

<sup>378</sup> *ibid.*, p.55

<sup>379</sup> *ibid.*, p.192

## **2.4 Deriving an integrated framework for cyberconflict**

This part is bringing together the three theories - social movement, conflict and media theories - into an integrated model for analysing cyberconflict in its ethnoreligious and sociopolitical dimensions. Firstly, I provide a justification of why these theories are necessary for any explanation of cyberconflict. Secondly, I lay out a proposed model for such an analysis drawing on these theories, and finally, I call for a reversal of the two modalities of cyberconflict, from hierarchical to rhizomatic and (almost) vice versa.

### *Reasoning*

The central argument of this thesis is that there are two types of political conflict on the internet (cyberconflict): ethnoreligious and sociopolitical. In order to analyse 'real' political conflicts, political scientists have devised 'Conflict Theory' and 'International Conflict Analysis'. The problem of just using conflict theory is that it cannot fully account for two important parameters of cyberconflict: its sociopolitical dimension (social movements or dissidents using the internet against antagonistic institutions) and the fact that conflict is taking place within or with the help of a medium (the internet). Again, in order to understand how social movements are engaging in cyberconflicts and are affected by the use of IT technology, it would be logical to use the theoretical tools already

there from the new social movement theorists. The problem with this approach is that it leaves out a more thorough examination of the media context (in this case cyberspace) in which sociopolitical cyberconflicts are taking place. Again, if one decides to just use media theory to analyse cyberconflict, many questions of what conflict in these different dimensions means for the ethnoreligious and sociopolitical groups engaging in them are going to remain unanswered. Lastly, an attempt to integrate social movement and media theories, while leaving conflict theory out, will miss explanations of ethnoreligious conflict. The reason for this is that social movement theory, as far as I discussed it and analysed it above, does not seem to engage with conflict in ethnic and religious terms. In other words, any attempt to analyse an ethnoreligious conflict (such as the Israeli-Palestinian conflict) using social movement theory just seems implausible.

The political environment of the internet is analysed here not in terms of the internet as a mass medium in the traditional sense (i.e. what would be an internet news bureau's or the online version of an already established medium's influence on the political outcome of a conflict), but rather as a significant new resource used by the opposing parties in a conflict. This presents us with a major theoretical challenge, because there is no theoretical model to date that can provide us with the conceptual tools to analyse the use of the internet by the actual parties in the conflict (endogenously) and not just theorise about the way in which the media influence - or not - the political outcome of a conflict (exogenously). The reason for this, as we saw in the section 1.4 above, is that the



internet is not a traditional medium, for access to which groups, institutions, or states compete. It may be used by anyone, at any time, from most places on the planet. Furthermore, despite the fact that actors using the internet might still seek traditional political goals like power, participation or democracy, the postmodern nature of the medium makes a more complex theoretical approach necessary. Explaining cyberconflict in a single framework, for instance a media studies approach, a conflict theory approach or even a social movement approach such as resource mobilisation theory (RMT) would provide us with a one-dimensional and inadequate discussion. My interest lies in examining this phenomenon under as many 'theoretical lights' as possible and at the same time refraining from being blinded by the radiance of the novelty of the medium itself.

### *Theoretical Framework*

Searching for a satisfactory theoretical framework, I have come up with the following parameters to be looked at while analysing cyberconflicts.

1. Environment of Conflict and Conflict Mapping (real and virtual). The world system generates an arborescent apparatus, which is haunted by lines of flight, emerging through underground networks connected horizontally and lacking a hierarchical centre (Deleuze and Guattari). The structure of the internet is ideal for network groups (since it is a global network with no central authority) and has offered another experience of governance (no governance),

time and space (compression), ideology (freedom of information and access to it), identity (multiplicity) and fundamentally an opposition to surveillance and control, boundaries and apparatuses. However, in ethnoreligious cyberconflicts, where the groups' systems of belief and organisation aspire to hierarchical apparatuses (nation, religion, identification with parties and leaders), this network form is not always evident. This is why there is a dual modality of cyberconflict: one rhizomatic and one hierarchical.

2. Sociopolitical Cyberconflicts: The impact of ICTs on: a. Mobilising structures (network style of movements using the internet, participation, recruitment, tactics, goals), b. Framing Processes (issues, strategy, identity, the effect of the internet on these processes), c. Political opportunity structure (the internet as a component of this structure), d. hacktivism.
3. Ethnoreligious Cyberconflicts: a. Ethnic/religious affiliation, chauvinism, national identity, b. Discourses of inclusion and exclusion, c. Information warfare, the use of the internet as a weapon, propaganda and mobilisational resource d. Conflict resolution, which depends on the legal and organisational framework, the number of parties and issues, the distribution of power, and the content of values and beliefs.
4. The internet as a medium: a. Analysing discourses (representations of the world, constructions of social identities and social relations), b. Control of

information, level of censorship, alternative sources, c. Wolsfeld: Political contest model among antagonists: the ability to initiate and control events, dominate political discourse, mobilise supporters, d. Media effects on policy (strategic, tactical, representational).

*Calling for a Reversal: From hierarchical to rhizomatic and (almost) vice versa.*

Dual Modality: If ethnoreligious cyberconflicts are mapped as representing/defending loyalties of hierarchical apparatuses and sociopolitical cyberconflicts are empowering network forms of organisation, then as a result:

Actors in ethnoreligious CC need to operate in a more *network* fashion, if they are fighting network forms of terrorism or resistance. Actors in sociopolitical CC need to operate in a more *organised* fashion, if they are to constructively engage with the present global political system or parts of that system. Conflict resolution will be possible, only when hierarchical apparatuses become more networked and rhizomatic groups become more conscious of the rest of their hosting network.<sup>380</sup>

---

<sup>380</sup> A further observation that can be made here is that ethnoreligious dimensions to cyberconflict environments are going to prove crucial to future 'high' information warfare, targeting national and international infrastructures. Sociopolitical dimensions in both real and virtual environments are equally relevant to future 'low' societal end of the spectrum warfare, targeting real international bodies and movements and their virtual representatives. Unfortunately my 'footnote' observation at this early stage cannot be supported by empirical evidence.



*Sociopolitical Cyberconflicts and the argument for greater organisational efficiency:*

The majority of groups engaging in sociopolitical cyberconflicts, as we see in section 4.1 where I discuss the anti-globalisation/anti-capitalist movement and in section 6.1 where I look at the anti-war movement, can be placed under the category of transnational social movements (TMs). Movements are changing from fairly coherent national organisations into transnational networks, with highly fragmented and specialised nodes composed of organisations and less organised mobilisations, all of which are linked through new technologies of communication.<sup>381</sup>

Tarrow defines TMs as 'sustained interactions with opponents - national or nonnational - by connected networks of challengers organised across national boundaries'.<sup>382</sup> In these movements we find what is called 'cross-border diffusion': the communication of movement ideas, forms of organisation, or challenges to similar targets from one centre of contention to another.<sup>383</sup> Tarrow's preoccupation with transnational movements highlights the difficulties of aggregating people with different demands and in different locations in concerted campaigns of collective action. This involves 'mounting collective challenges, drawing on social networks, common purposes, and cultural frameworks, building

---

<sup>381</sup> Tarrow, S: (1998) *Power in Movement: Social Movements and Contentious Politics*, Cambridge University Press: Cambridge, p.178, cites Garner 1994: 431

solidarity through connective structures and collective identities to sustain collective action'.<sup>384</sup> The dangers resulting from such an attempt are, first, the search for transnational common denominators that will resonate at some level with many cultures and tradition, and second, following a variety of issues that take root in particular places, which can produce ideological divergence within the same transnational network, as activists adapt the network to their cultures.<sup>385</sup>

These dangers are indeed present for transnational movements. My concern is here to demonstrate the need to strengthen the organisational structures and informal weak connective structures these non-hierarchical movements normally have. Without sufficient organisation - whether formal or informal - political opportunities are not likely to be seized. An emerging international pattern of social movement organisation seems to be appearing: a combination of small professional leaderships; large but passive mass support; and impersonal network-like structures.<sup>386</sup>

One of the explanations of why new social movements are decentralised or rhizomatic is that strong executive power structures in a given political system tend to induce a fundamental critique of bureaucratic and hierarchical political forms, which is then reflected in the movements' emphasis on informal and

---

<sup>382</sup> *ibid.*, p. 84

<sup>383</sup> *ibid.*, p.86

<sup>384</sup> *ibid.*, p.4

<sup>385</sup> *ibid.*, p. 191

<sup>386</sup> *ibid.*, p. 133



decentralised structures.<sup>387</sup> Explaining this, however, does not imply that the following can be ignored: 'SMOs [social movement organisations] with formalized and professionalized structures tend to have easier access to public authorities, because government bureaucracies prefer to deal with organizations with working procedures similar to their own'.<sup>388</sup>

As it happens, Bennet argues that new waves of movements with their variform and shifting organisations, their tendency to produce rapid and rapidly-liquidated coalitions, their focus on short- and medium-term issues rather than fully-fledged ideologies do not produce standing activist commitments or deeply held loyalties.<sup>389</sup> Although I find this largely convincing, let me just state a reservation about Bennet's argument. Rapid coalitions can also have a positive impact on the flexibility and mobility of these movements, if we consider the example of the anti-globalisation movement. Such coalitions have greater discretionary resources, enjoy easier access to the media, have cheaper and faster geographic mobility and cultural interaction, and can call upon the collaboration of different types of movement-like organisations for rapidly organised issue campaigns.<sup>390</sup>

---

<sup>387</sup> Rucht, D: 'The impact of national contexts on social movement structures: A cross-movement and cross-national comparison' in McAdam, D, McCarthy, J and Zald, M (eds.): *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Structural Framings*, Cambridge University Press: Cambridge, p. 192

<sup>388</sup> Kriesi, H: 'The organizational structure of new social movements in a political context' in McAdam, D, McCarthy, J and Zald, M (eds.): *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Structural Framings*, Cambridge University Press: Cambridge, p. 158

<sup>389</sup> Bennett, W.L: (2004) 'Communicating global activism' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p. 128, citing Tarrow, 1999: 30.



Brown following Tarrow has expressed the hierarchical/network dilemma in similar terms.<sup>391</sup> His argument is that networks

with decentralized decision-making have the advantage of being better able to deal with local conditions than centralized and hierarchical organizations. However, networks may find it difficult to develop cultures or perspectives and while their superiority to hierarchies is asserted the advantage of hierarchy is that it allows concentration of resources behind a common purpose quickly and easily.<sup>392</sup>

Following this reasoning, I think that here, the most illuminating perspective is provided by Tarrow, who explains that the problem for movement organisers is to create organisational models that are sufficiently robust to structure sustained relations with opponents, but are flexible enough to permit the informal connections that link people and networks to one another to aggregate and coordinate contention. The most effective forms of organisation are based on partly autonomous and contextually-rooted local units linked by connective structures, and coordinated by formal organisations.<sup>393</sup> Tarrow develops the argument further:

---

<sup>390</sup> Tarrow, S: (1998) *Power in Movement: Social Movements and Contentious Politics*, Cambridge University Press: Cambridge p.207

<sup>391</sup> Brown, R: 'Conceptualizing the Impact of Communication Technologies on World Politics: Space, Time, and Mobilization', International Studies Association Conference, Washington DC 17-21 February 1999, p.9 cites Tarrow, 1998, ch.8

<sup>392</sup> Brown, R: 'Mobilizing the Bias of Communication: Information Technology, Political Communications and Transnational Political Strategy', American Political Science Association Convention, Washington DC, 30 August- 3 September 2000, p.11

<sup>393</sup> Tarrow, S: (1998) *Power in Movement: Social Movements and Contentious Politics*, Cambridge University Press: Cambridge, p. 124

The dilemma of hierarchical movement organizations is that, when they permanently internalize their base, they lose their capacity for disruption, but when they move in the opposite direction, they lack the infrastructure to maintain a sustained interaction with allies, authorities, and supporters. This suggests a delicate balance between formal organization and autonomy – one that can only be bridged by strong, informal, and nonhierarchical connective structures.<sup>394</sup>

One may then plausibly argue for stronger organisation with strong informal and nonhierarchical connective structures which, although remaining autonomous, would be coordinated by formal organisations. This might solve some of the problems stated above.

It is equally important to stress the impact of new communication technologies on these movements, because in several instances the internet has been responsible for the rapid cross-border diffusion of movement ideas and organisation of protest and even the globality of protest itself:

The growth of broad networks despite (or because of) relatively weak social identity and ideology ties, the transformation of both individual member organizations and the growth of patterns of whole networks, and the capacity to communicate messages from desktops to television screens. The same qualities

---

<sup>394</sup> Tarrow, S: (1998) *Power in Movement: Social Movements and Contentious Politics*, Cambridge University Press: Cambridge, p. 137



that make these communication-based politics durable also make them vulnerable to problems of control, decision making and collective identity.<sup>395</sup>

This is the reason why stronger organisation is of paramount importance. In order for communication revolution to change the political opportunity structure and challenge the scope of political life, 'rather than assuming that the impact of technology makes organisation irrelevant, this suggests that the fragmentation of media spheres will actually make organization more important as a way of triggering political action'.<sup>396</sup>

As Van Aelst and Walgrave have argued, although the availability of new communication technologies makes traditional organisations somewhat dispensable for mobilisation purposes, a certain institutionalisation remains necessary in order to exert a more lasting political influence.<sup>397</sup> But if the network is the prevalent organisational form surfacing from the integration of the internet, the movement's goals can be achieved only when combined strategies of traditional and new media usage are implemented.<sup>398</sup> The reason for this is that 'while networked communication may help sustain the campaigns that organize global activism, these leaderless networks may undermine the thematic coherence

---

<sup>395</sup> Bennett, W.L: (2004) 'Communicating global activism' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p. 144

<sup>396</sup> Brown, R: 'The Contagiousness of Conflict: E.E Schattschneider as a theorist of the information society', *Information, Communication and Society*, 5:2 2002, p.271

<sup>397</sup> Edwards, A: (2004) 'The Dutch women's movement online' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p.200

<sup>398</sup> Van de Donk, W, Loader, B, Nixon, P, Rucht, D: (2004) *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p. 161



of the ideas that are communicated through them'.<sup>399</sup> Moreover, communication in diverse networks is ideologically thin and 'as anyone who has caught the internet virus can attest, virtual activism may serve as a substitute – and not as a spur – to activism in the real world'.<sup>400</sup>

Before concluding that the world is entering an unprecedented age of global movements, we will 'need to follow some of the recent campaigns that have been assisted by electronic communication to find out whether it increases the movement's power or merely changes how it frames its message'.<sup>401</sup> Three kinds of long-term and indirect effects of movements are important: their effect on the political socialisation of the people and groups who have participated in them; the effects of their struggles on political institutions and practices; and their contribution to changes in political structure.<sup>402</sup> The central question raised by new waves of social protest is whether they are creating a transnational movement culture that threatens the structure and sovereignty of the national state.<sup>403</sup>

---

<sup>399</sup> Bennett, W.L: (2004) 'Communicating global activism' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p. 134

<sup>400</sup> Tarrow, S: (1998) *Power in Movement: Social Movements and Contentious Politics*, Cambridge University Press: Cambridge p. 193

<sup>401</sup> *ibid.*, p.194

<sup>402</sup> *ibid.*, p.164

<sup>403</sup> *ibid.*

*Ethnoreligious Cyberconflicts and the argument for moving towards network forms of organisation*

This idea has been fundamental in Arquilla and Ronfeldt's works on conflict in the information age. They basically argue that hierarchies have a difficult time fighting networks (e.g. Colombia, Algeria, the Zapatistas). It takes networks to fight networks and whoever masters the network form first and with the most success will gain major advantages.<sup>404</sup> What Arquilla and Ronfeldt argue is that terrorists will continue moving from hierarchical to information-age network designs and that within groups 'great man leaderships will give way to flatter decentralised systems. This way more effort will go into building arrays of transnationally internetted groups than into building state-alone groups'.<sup>405</sup> As a result, power seems to be migrating to nonstate actors, who are able to organise into 'sprawling multi-organizational networks', which are more flexible and responsive than hierarchies in reacting to outside developments and are better than hierarchies at using information to improve decision-making.<sup>406</sup>

This vision emphasises adapting to a major consequence of the information revolution – the rise of network forms of organisation. Especially after 9/11 it has become essential for states to become more flexible, in order to be able to face network-style organisations. Arquilla and Ronfeldt's thesis is that the challenge is

---

<sup>404</sup> Arquilla, J and Ronfeldt, D: (2001) (eds.) *Networks and Netwars: The Future of Terror, Crime and Militancy*, Rand: California, p.55

<sup>405</sup> Lesser et.al, p. 41

<sup>406</sup> *ibid.*, p.45

to develop *hybrids* in which “all channel” networks are fitted to flattened hierarchies. The major benefits may accrue in the areas of interagency and interservice cooperation. Since militaries must retain hierarchical command structures at their core, their hybrids should retain - yet flatten - the residual hierarchy, while allowing dispersed maneuver “nodes” to have direct, all channel contact with each other, and with the higher command.<sup>407</sup>

The information revolution is favoring and strengthening networked organisational designs, often at the expense of hierarchies. States need to wake up to this fact and realise that networks can be fought effectively only by flexible network-style responses. For now I will rest this argument, but I shall come back to it in section 3.1, where I discuss information warfare more substantially.

---

<sup>407</sup> Arquilla, J and Ronfeldt, D: (1997) ‘Looking Ahead: Preparing for Information-Age Conflict’ in Arquilla, J and Ronfeldt, D (eds.) *In Athena’s Camp: Preparing for Conflict in the Information Age*, Rand: California, p.440



### **Chapter 3: The environment of Cyberconflict**

By the turn of the century a new kind of conflict, named 'cyberconflict' to mean conflict in computer-mediated environments (cyberspace), had emerged and become prevalent. This thesis seeks to introduce the key terms and themes of cyberconflict and argue that two different types of conflict occur: one between ethnic or religious groups fighting over in cyberspace, as they do in real life, and second, conflicts between a social movement and its antagonistic institution (hacktivism). This chapter unfolds the environment of cyberconflict by analysing the terms involved and engaging with the current debates in information warfare and security. More specifically, it includes analyses on hackers, information warfare, cyberterrorism, internet security analysis and cyberconflict's sociopolitical implications.

The political use of the internet has created a new lexicon, spawning terms like 'cyberwar', 'cyberattack' and 'netwar'. The term 'cyberconflict' (CC) - the generic reference to a certain form of politics on the internet - is now in regular use, but it has not yet been sufficiently clarified. This is because there are problems in defining and categorising the wide variety of events occurring in cyberspace that fall under this conceptual umbrella. Here, the term cyberconflict is used to refer to conflicts of the real world spilling over to cyberspace. Typical of cyberattacks is the use by opposing parties of either Information Technology as

such or IT as a weapon - for example worms<sup>408</sup>, Distributed Denial of service attacks (DDoS)<sup>409</sup>, Domain Name Service attacks (DNS)<sup>410</sup>, or unauthorised intrusions<sup>411</sup> - to attack the other side. The argument of this thesis is that cyberconflict includes two different categories of cyberpolitical action. These categories are sometimes blurred, but need to be distinguished in order to understand internet politics.

One of these theoretical lights is Gadi Wolfsfeld's political contest model. As discussed above, his work *Media and Political Conflict* (1997) looks at the role of the media in political conflicts by building what he calls the political contest model. According to Wolfsfeld, the best way to understand the role of the news media in political conflict is 'to view the competition over the news media as part of a larger and more significant contest among political antagonists for political

---

<sup>408</sup> Most contemporary viruses are worms, enabled by 'buffer overflows'. Buffer overflow is an event in which more data is put into a buffer (computer holding area) than the buffer has been allocated. In recent years they have become very popular with new worms such as Code Red, Code Red II, which allows it to gain control of the infected machine and the Nimda worm. (Vatis, M: 'Cyber Attacks During The War on Terrorism: A Predictive Analysis', Sep., 22, 2001, Institute for Technology Studies, Dartmouth College). Some researchers have predicted the emergence of new worms (Warhol worms, flash worms), spreading in seconds, leaving no time for system administrators to react. (Weaver, N: 'Warhol Worms: The potential for very fast internet plagues', University of California Berkley, Aug.15, 2001)

<sup>409</sup> DDos attacks employ armies of 'zombie' machines (insecure server compromised by a hacker who places software on it that can launch an overwhelming number of requests, rendering the site inoperable). As demonstrated in the Kosovo conflict, military websites and communications systems are especially likely to receive DDos variants (Vatis,2001)

<sup>410</sup> Domain name servers are the 'Yellow Pages' that computers consult in order to obtain the mapping between the name of a system and the numerical address of the system. If the DNS provides an incorrect numerical address for a website then the user's system will connect to the incorrect server. An attacker can disseminate false information this way and prevent access to the original site (Vatis,2001).

<sup>411</sup> A series of intrusions known as Moonlight Maze, which are believed to have originated in Russia were firstly detected in March 1998 and hundreds of unclassified networks used by the Pentagon, NASA and the Department of energy, may have been compromised.



control'.<sup>412</sup> However, the true relevance of his work to cyberconflict can be seen in his discussion of the three variables that constitute the ability of the antagonist to control the political environment, which in turn increase the ability of an antagonist to dominate public discourse about a particular issue.<sup>413</sup> These are the ability to initiate and control; the ability to regulate the flow of information; and the ability to mobilise support. The problem with this is that Wolfsfeld is talking about 'real' political conflicts, where the news media outside the conflict (exogenously) respond to events. However, we are interested in how the parties in a 'cyberconflict' (either socio-political or ethnoreligious - and this is where Wolfsfeld's variables prove helpful in order to understand the differences) use a medium directly (endogenously) without third parties (traditional news media) to influence the political outcome of a conflict.

### *Netwarriors: Terrorists or Social Activists?*

It is not surprising that the internet has been used vigorously by social activists and campaigners all over the world. The internet quickly puts information into the hands of organisers, allows rapid replication of a successful effort, allows users to select their level of activity and helps publicise the campaign. It is therefore an organising tool *par excellence*, because the more traditional telephone trees or fax machines are too slow and the physical distances are too difficult and too

---

<sup>412</sup> Wolfsfeld, p.3.

<sup>413</sup> *ibid.*, p.25.



expensive to cover.<sup>414</sup> However, the internet is not only used by social activists. An examination of historical precedents indicates that major political and military conflicts are increasingly accompanied by a significant amount of online aggressive activity. Ongoing conflicts also show that cyberattacks are escalating in volume, sophistication and coordination.<sup>415</sup> Parties in cyberconflicts have been described as terrorists or social activists depending on the discursive mood of their critics. This is why it is important to examine the politics of this phenomenon and understand its implications for future conflicts.

---

<sup>414</sup> Danitz, T and Strobel, W: (2001) 'Cyberactivists use the Internet to promote democracy in Burma', in J. Arquilla and D. Ronfeldt (eds), *Networks and Netwars: The Future of Terror, Crime and Militancy*, Rand: California, p.162

<sup>415</sup> Vatis, M: (2001) 'Cyberattacks during the war on terrorism: A predictive analysis', Institute for Security Technology Studies, Dartmouth College: Dartmouth.

### 3.1 Information Warfare

#### *Hackers*

It is vital to include an analysis of the hacking phenomenon and a discussion of where it fits in the political environment of cyberconflict. Essentially those involved in ethnoreligious or sociopolitical environments of cyberconflict are hackers - excepting of course social movement actors using the internet as a mobilisational resource. I will briefly focus on Paul Taylor's<sup>416</sup> influential work *Hackers*, which provides excellent interviews and discussion on hackers, computer scientists, and computer security practitioners.

In contrast to my analysis of computer-mediated conflict between opposing sides of a 'real world' conflict, Taylor concentrates upon the conflict between the computer security industry and the computer underground (hackers). The computer cognoscenti are split into two camps: the 'doves' who are prepared to cooperate with the computer underground, arguing that hackers represent an important stock of technical knowledge that society should not prematurely isolate itself from by adopting a 'punish first, ask questions later' approach, and the 'hawks', who advocate that the computer underground should be punished in

---

<sup>416</sup> Taylor, P: (1999) *Hackers: Crime in the Digital Sublime*, Routledge: London.

the courts.<sup>417</sup> Similarly, a definition of a 'hacker' varies, according to the discursive mood of the speaker:

...to the lay person the phrase is likely to conjure up sensationalised images of malicious computer geeks in darkened rooms obsessively typing away; meanwhile to the computer aficionado, the phrase is more likely to be associated with its dramatic fictionalisation in the movies and the postmodern literary genre of cyberpunk; to the computer programmer the term may refer to some of the earliest and most imaginative people involved in programming; and finally, within the computer security industry, the term *hacker* is likely to present a cue for opprobrium to be directed at 'electronic vandals'.<sup>418</sup>

The word 'hacker', coined at MIT in the 1960s, connoted a computer virtuoso, who according to the *New Hacker's Dictionary* 'enjoys exploring the details of programmable systems and how to stretch their capabilities; one who programs enthusiastically, even obsessively'. The meaning has evolved from the highly skilled, but playful activity of academic computer programmers searching for the most elegant programming solution to being increasingly associated with its present day connotation of illicit computer intrusion.<sup>419</sup> Today's generation-x anarchist hackers share with their artisan and activist hacker predecessors a distrust of authority, a libertarian attitude and a tendency to position themselves

---

<sup>417</sup> *ibid.*, p.xi

<sup>418</sup> *ibid.*, pxii

<sup>419</sup> *ibid.*, pp.13-14



outside bourgeois society's norms and values.<sup>420</sup> The main characteristics of a hack according to Taylor are: a. simplicity (the act has to be simple, but impressive), b. mastery (the act involves sophisticated technical knowledge), c. illicitness (the act is against the rules).<sup>421</sup> Thus, a hacker is defined not just by what he does but how he does it. The motivations for hacking are: feelings of addiction, the urge of curiosity, boredom with the educational system, enjoyment of a feeling of power, peer recognition, and political motivations. The computer industry is accused of over-emphasizing the vandal-oriented motivations and pathological aspects of hacking.<sup>422</sup> So how does hacking feel?

...the adrenaline rush I get when I'm trying to evade authority, the thrill I get from having written a program that does something that was supposed to be impossible to do, and the ability to have social relations with other hackers is all very addictive...For a long time, I was extremely shy around others, and I am able to let my thoughts run free when I am alone with my computer and a modem hooked up to it...If I were ever in a position where I knew my computer activity was over with the rest of my life I would suffer withdrawal.<sup>423</sup>

Part of it was a sense of power. You were running an informal network of about 250 computers and no-one else outside your close circle of friends knew about it. The final goal was total world domination, to have everything under control. It was the ultimate game on the ultimate scale. You got a thrill out of knowing how

---

<sup>420</sup> *ibid.*, p.24 Taylor cites Hannemyr 1997:2

<sup>421</sup> *ibid.*, p.15

<sup>422</sup> *ibid.*, p.46

<sup>423</sup> *ibid.*, p.48, Maelstrom, email interview

much power you had. It was possibly hitting back at society. There was a sort of political anarchism involved. The main thrill was beating the system.<sup>424</sup>

In *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*, Thomas writes that what is talked about in terms of hackers is the manner in which hackers themselves exist in a shadow space of secrecy, possessing near-mystical powers that allow control of technology that itself is beyond discourse. The hackers themselves are coded in such a way that they literally become the secret that needs to be broken. Fundamentally, one can watch a hacker's actions, even monitor them online, but this means nothing until they can be attached to a real body and therefore become prosecutable. The reason for looking at hackers is that individuals and groups engaged in sociopolitical and ethnoreligious cyberconflicts are part of the hacking culture in a particularly politicised way.

Nowadays, hackers fight for clearer political goals than their forebears, especially campaigning for information freedom. Many hackers believe that electronic communications are unsafe, with governments legally tapping data lines, copying electronic mail and with suspicion of hacking often enough to get search warrants or to confiscate equipment. Accordingly, Goggans, another hacker Taylor interviewed, argues:

---

<sup>424</sup> *ibid.*, p.56, Taylor cites Bowcott and Hamilton (1990:42)

I know all too well how simple it is to view and alter consumer credit, to transfer funds, to monitor telephone conversations etc... I can monitor data on any network in existence, I can root privileges on ANY Sun Microsystems UNIX. If I, a 22 year-old, non-degreed, self-taught, can do these things, what can a professionally taught profit motivated individual do? THERE IS NO PRIVACY... People need to know the truth about the vulnerabilities of the computers they have entrusted their lives to.<sup>425</sup>

However, as Taylor and Jordan argue, '[h]ackers' over-identification with technical means over political ends and their parasitical relationship to various technological systems means that although they are at the heart of the exercise of power, they remain in an ultimately powerless dependent relationship'.<sup>426</sup>

Further, the computer underground is anarchic, a confederation of phreakers/hackers and virus writers from all over the world whose common interests transcend culture or language. 'They change IDs, aliases, sites, their methods and gang membership as rapidly as the authorities track them. Stamping out hacking is like trying to pin down mercury'.<sup>427</sup>

Hacking can potentially perform a variety of benevolent services to the security industry: it has been responsible for many of the most progressive developments in software development, it reflects the ways in which the development of high

---

<sup>425</sup> *ibid.*, p.70, Goggans email interview

<sup>426</sup> Taylor, P.A and Jordan, T: (2004) *Hactivism and Cyberwars: Rebels with a cause?*, Routledge: London, p.162



technology has outpaced orthodox forms of institutional education, it is an important form of watchdog counter-response to the use of surveillance technology and data gathering by the state and to the increasingly monolithic communications power of giant corporations, and finally as guerilla know-how, it is essential to the task of maintaining fronts of cultural resistance and stocks of oppositional knowledge as a hedge against a techno-fascist future.<sup>428</sup> Also, the hacker presence constantly pushes forward the limits of computer security and thus contributes to a general climate of improved security consciousness, without which 'the nation would be nakedly awaiting serious attack from thieves and foreign agents'.<sup>429</sup>

On the other side of the coin, the business sector is reluctant to report computer crime for two reasons. Firstly, for fear of adverse publicity, public embarrassment or loss of good will. Secondly, for fear of the loss of investor or public confidence and the resulting economic consequences. Official statistics on hacking incidents tend to be unreliable, firstly because the organisations affected may be totally oblivious to security breaches that have occurred, leading to possible under-reporting, and secondly because there is a tendency for both computer security figures and hackers to hyperbolise the situation, leading perhaps to over-reporting. At the same time, serious security incidents are whitewashed, because otherwise the management would be accused of negligence.<sup>430</sup>

---

<sup>427</sup> *ibid.*, p.28, Taylor cites Clough and Mungo (1992:18)

<sup>428</sup> *ibid.*, p.43 Taylor cites Ross (1991: 82)

<sup>429</sup> *ibid.*, p.97, Maelstrom, email interview

<sup>430</sup> *ibid.*, pp.67-68

One of Taylor's main arguments is that a knowledge gap exists between the computer security industry and the computer underground. Due to the fact that computer security is lacking in any theoretical grounding, the only true way to test security is to actually attempt to breach a system. There is a scarcity of theoretical knowledge surrounding computer security with various calls for more hands-on experience of security to supplement more formal theory. 'The knowledge gap is thus rooted in the difference between theoretical concepts and guidelines to security and the "nitty gritty" of real world computing situations where security weaknesses flourish in the interstices of continually expanding and evolving computer systems'.<sup>431</sup> Hackers are sometimes used to do the testing. The problem, however, is that hackers may have potentially useful knowledge, but such knowledge often does not sit comfortably with the academic and commercial world's preference for ethically unproblematic and rigorously researched knowledge. Often, hackers are labelled as deviant despite the fact that the hacker community shares some of the same characteristics as its computer security industry counterpart.

These are tough time for hackers. Federal agencies now have broad new powers to spy on them, thanks to provisions in the anti-terrorist USA PATRIOT Act. The House of Representatives in the United States passed a law that could send hackers to prison for life, and on top of that, former hackers have difficulty

---

<sup>431</sup> *ibid.*, p.79



finding a job, because there are enough people with the same level of skills around.

### *Information warfare and cyberterrorism*

The most common of the views on information warfare and the future of conflict, whose best-known exponents are Heidi and Alvin Toffler<sup>432</sup>, extrapolates from the idea that territory, population, and natural resources are becoming less important relative to human capital and the possession of information. Taking this process to its logical conclusion, these theorists see information soon becoming the key source of wealth and power, equivalent to steel, coal, and oil in the industrial age or fertile land in the agricultural age. This change will eventually amount to a social revolution whose scope is equivalent to only two previous such transformations: the agricultural and industrial revolutions.<sup>433</sup> Just as the transition from agriculture to industry was correlated with the industrialisation of warfare, so too counterparts aver that people war as they work.<sup>434</sup> The transition will be from industry to information-based services and this will correlate with the 'informatting' of warfare. War waged in cyberspace might be bloodless and even clean, a possibility that has led one high-ranking military officer to see information technology as 'America's gift to warfare.'<sup>435</sup> Sun Ji is an icon in this pantheon, with his observation that the 'acme of skill' consists in winning without

---

<sup>432</sup> Toffler, A: (1980) *The Third Wave*, Morrow: New York.

<sup>433</sup> Shapiro, J: (1999): 'Information and war: Is it a revolution?' in Khalizad, Z, White, J and Marshall, A: *Strategic Appraisal: The Changing Role of Information Warfare*, Rand: California p.117



fighting. Advanced technological systems will not only help shape the environment of future conflict but will also magnify the importance of the psychological battle to the conflict outcome.

One definition of cyberterrorism is ‘computer-based attacks intended to intimidate or coerce governments or societies in pursuit of goals that are political, religious or ideological’.<sup>436</sup> So, who can be a cyberterrorist? The answer is anyone, David and Sakurai argue, citing a CERT/CC April 2002 report, which states the level of automation in attack tools continues to increase. Automated attacks commonly involve four phases: (1) Scanning for potential victims, (2) Compromising vulnerable systems, (3) Propagating the attack, (4) Coordinated management of attack tools.<sup>437</sup>

Indeed, the problem for American defence experts is that they don’t know who the enemy is:

Whether they are disgruntled Americans, Hamas terrorists or pariah dictators as Saddam, the attackers could wage cyber warfare undetected on any laptop computer from the Sinai desert to Singapore. Just as exasperating for the government would be deciding how to deploy its military. ‘If you don’t know who your enemy is, how can you retaliate?’ said one expert. This makes cyber

---

<sup>434</sup> Owens, 1995.

<sup>435</sup> *ibid.*

<sup>436</sup> Denning, D: (2001) ‘Is cyberterrorism next?’ [www.ssrc.org/sep11/essays/denning/html](http://www.ssrc.org/sep11/essays/denning/html)

<sup>437</sup> David, M.W and Sakurai. K: ‘Combating cyberterrorism: Improving analysis and accountability’, *Journal of Information Warfare* (2003) 2, 2: 15-26

warfare the great equaliser, a cheap and effective weapon for any third world rogue state or small terrorist organisation wanting to wage war against a super-power and win. All they might need is a few million dollars to hire a handful of 'cyber mercenaries' capable of penetrating supposedly secure systems.<sup>438</sup>

Michael Vatis, director of the institute for Security Technology Studies in Dartmouth reported the following on September 26<sup>th</sup> 2001 before a US House Subcommittee:

- (1) the likelihood of cyberattacks against the US and allied information infrastructure is high;
- (2) such attacks could come from terrorists and/or their nation-state sponsors, but are more likely to come from sympathisers of terrorists or of nation states targeted by US military operations;
- (3) such attacks will almost certainly target the websites of government agencies and private companies in the US and allied countries, but could also attack more high-value targets such as networks that control critical infrastructures;
- (4) such attacks could utilize destructive worms and viruses, Distributed Denial of Service exploits, and intrusions to disrupt targeted networks;
- (5) such cyber exploits could be combined into a potent mix to cause widespread disruption, and also combined with physical terrorist attacks to maximize the destructive potential of both sets of terrorist tools.<sup>439</sup>

---

<sup>438</sup> Sunday Times 17 May 1998, p.26

<sup>439</sup> David, M.W and Sakurai. K: 'Combating cyberterrorism: Improving analysis and accountability', *Journal of Information Warfare* (2003) 2, 2, pp.15-26



The concept most commonly used to connect IT and the military is information warfare. What is meant is that the object of conflict is no longer territory or resources, but information. The object of information warfare is the control over information as a source of wealth and power.<sup>440</sup> The U.S. Air Force has described it as encompassing 'any action to deny, exploit, corrupt or destroy the enemy's information and its functions, protecting ourselves against those actions and exploiting our own military information functions'.<sup>441</sup> The battlespace of information warfare is cyberspace - an ethereal place which does not fit neatly into the land, sea air space metaphors, where conflicting parties strive for information superiority and dominance. According to Shapiro, 'information dominance means that your side has the ability to collect, communicate, and protect information without disruption, while the other side does not'.<sup>442</sup> Taking out all information-transfer media would bring down a country's stock market, banking system, air traffic control, emergency dispatches and more. In November 2003, the US Homeland Security Department's first simulation of a terrorist attack on computer, banking and utility systems exposed problems with the ways victimised industries communicated vital information during the crisis. It simulated physical and computer attacks on banks, power companies and the oil and gas industry. Electronic communications may have been used by the Sept.11 terrorists and are certainly used by some of those accused of related terrorism offences, such as alleged 911 accomplice Moussaoui, who requested that

---

<sup>440</sup> Shapiro, J: (1999): 'Information and war: Is it a revolution?' in Khalizad, Z, White, J and Marshall, A: *Strategic Appraisal: The Changing Role of Information Warfare*, Rand: California, p.119 cites Toffler and Toffler (1993) Dearth and Williams (1996) and Schwartau (1994).

<sup>441</sup> Larsen, J, Director, Institute for National Security Studies.



prosecutors turn over their records of messages sent and received through his email account, claiming his email could help him establish his alibi.<sup>443</sup>

Remarkably, terrorists are being bred and trained to be technologically savvy and to attack, disrupt, damage and perhaps even destroy technology infrastructures and computer-based economic activities. They are the biggest threat to the information infrastructure and the new digital economy.<sup>444</sup> Cyberterrorists could act in the name of one religion or another and support or be supported by one or more outlaw nations. They will attack anything that is vulnerable and will focus their attacks on headline-grabbing efforts to make civilian populations fearful and to embarrass government officials and organisations. Erbschloe has offered the following conclusions as far as terrorists' use of information warfare is concerned:

Because of the international nature of information warfare, existing political structures are not prepared to immediately investigate the source of attacks and to appropriately respond to and counter information warfare scenarios. It is not likely that all governments will equally participate or cooperate in the investigation or information warfare attacks or that they will work together to halt attacks... Information warfare attacks can effectively impact the economics

---

<sup>442</sup> Shapiro, p.130

<sup>443</sup> Delio, M: 'Did FBI bungle email evidence?', wired.com, 30/8/02

<sup>444</sup> Erbschloe, M: (2001) *Information Warfare: How to Survive Cyber Attacks*, McGraw-Hill: Berkely, California, p.37

of a nation or region without destroying infrastructures or disabling military capabilities.<sup>445</sup>

According to Erbschloe sustained terrorist information warfare strategies are the ongoing deliberate efforts of an organised political group against the military, industrial, civilian, and government economic information infrastructures or activities of a nation, region, organisation of states, population or corporate entity.

In purely information-warfare terms, there are five dynamics that favor the outlaw attacker in comparison to the defender.<sup>446</sup> Firstly, a fundamental dynamic of information warfare is that defenders must always succeed in protecting systems, whereas if attackers do not succeed, they can try again or move to another target. A second dynamic is the growth of computer networks and the increase of internet connectivity. A conversation with a director of computer security at a large telecommunications firm reveals the magnitude of the problem. When asked, 'Are all of the computers in your company secure?' the answer was: 'They will be when I find out where they all are'.<sup>447</sup> A third dynamic is that the attackers have access to all of the same technology the defender has as well as all of the technical information about systems, including weaknesses in hardware and software. Relating to that is that the attackers can use the internet and become members of the same clubs, chat rooms, bulletin boards and email lists that defenders use to get information about products and to talk with their peers.

---

<sup>445</sup> *ibid.*, p.95

<sup>446</sup> *ibid.*, pp. 174-5

Lastly, attackers not only can work from almost anywhere in the world, but they can easily outnumber defenders. Also, hackers and computer bandits take as much pride in their abilities and accomplishments as do the people trying to stop them. Similar levels of pride have been noted for terrorists, especially those who have a religious basis for their actions. Ultimately, as Erbschloe argues, religious or politically motivated terrorists usually gain little in the way of financial compensation, but are often revered in their community and can die as heroes in their country.<sup>448</sup>

In such an arena, several questions emerge. First, is a strategic information attack tantamount to a physical attack? Second, can a military advantage in information technology guarantee success within low-intensity conflict, against low-tech asymmetrical strategies?<sup>449</sup> Third, is there a transition from platform-centric warfare (wherein networks exist to enhance platform performance) to network-centric warfare (wherein platforms are the eyes, ears and fists of a broader entity)?<sup>450</sup> Although it is too early to answer, there are some early indications. As far as Shapiro is concerned, there will be a definite change in battle dynamics: 'commanders would no longer be encouraged to use intuition or take risks because "dominant battle space knowledge" would render such attributes unnecessary or even dangerous. A radically different military and a very different

---

<sup>447</sup> *ibid.*, p.174

<sup>448</sup> *ibid.*, p.259

<sup>449</sup> Gombert., p.61

<sup>450</sup> Libicki, M and Shapiro, J: (2001) *Strategic Appraisal: The Changing Role of Information Warfare*, Rand: California.



style of fighting would certainly result'.<sup>451</sup> Also, command, control, communications, computing, intelligence, surveillance, and reconnaissance (C4ISR) will control the outcome of the conflict.<sup>452</sup>

At the systemic level, information warfare is the organisation of information to provide warfighters with what has been termed 'dominant battlespace knowledge', an important component of which is the American Department of Defense's nascent 'system of systems.' Insofar as the ability to kill what can be seen makes seeing (locating, identifying, and tracking) the key to war, seeing is increasingly best done by networking sensors and human observers to create a shared ground truth that forms the basis of command, control, and operations.

One of the most influential centres analysing information warfare is the Rand Corporation. Starting with their work *Countering the New Terrorism*, Lesser, Hoffman, Arquilla, Ronfeldt, Zanini and Jenkins introduced the concept of cyberterrorism and, in subsequent publications analysed below, gave a thorough analysis of the issues involved.

Terrorism according to these authors has always been about information:

... from the fact that trainees for suicide bombings are kept from listening to international media, through the ways that terrorists seek to create disasters that

---

<sup>451</sup> Shapiro, J: (1999): 'Information and war: Is it a revolution?' in Khalizad, Z, White, J and Marshall, A: *Strategic Appraisal: The Changing Role of Information Warfare*, Rand: California,

will consume the front pages, to the related debates about countermeasures that would limit freedom of the press, increase public surveillance and intelligence gathering, and heighten security over information and communication systems.<sup>453</sup>

According to a report released on May 1999 by the Rand Corporation, which was the result of a year-long project sponsored by the Airforce's Deputy Chief of Staff for Air and Space Operations, there will be a new form of terrorism known as 'netwar':

The rise of networks is likely to reshape terrorism in the Information Age and lead to the adoption of netwar - a kind of Information Age conflict that will be waged principally by nonstate actors. There is a new generation of radicals and activists who are just beginning to create Information Age ideologies. New kinds of actors, such as anarchistic leagues of computer- hacking 'cyboteurs' may also partake of netwar.<sup>454</sup>

The same report advised that the U.S Air Force should slow its modernisation plans and rethink its connections to the internet if it wants to fight off a revolutionary, as yet undeveloped form of cyberterrorism. The rise of networks is likely to reshape terrorism in the Information Age and lead to the adoption of

---

p.146

<sup>452</sup> Gombert, p.59

<sup>453</sup> Lesser, I, Hoffman, B, Arquilla, J, Ronfeldt, D, Zanini, M, Jenkins, B.M: (1999) *Countering the New Terrorism*, Rand: California, p.72

<sup>454</sup> Verton, D: 'New cyberterror threatens AF', Federal Computer Week, 3/5/99

netwar - a kind of Information Age conflict that will be waged principally by non-state actors.<sup>455</sup>

The Rand report also predicts that cyberterrorists will use new tactics such as 'swarming', which occurs when members of a terrorist group, spread over great distances, electronically converge on a target from multiple directions, a tactic different from the traditional form of attacking in waves, which delivers a knockout blow from a single direction on the internet.<sup>456</sup>

However, it would be useful to stress that terrorists might be more interested to keep the internet up and running than to disrupt or destroy its components. One has to agree with Arquilla and Ronfeldt that network-based conflict will become a major phenomenon of the future and this can be clearly demonstrated with al-Qaeda long before the September 11<sup>th</sup> attack, with reports of bin Laden having advanced information systems designed by Egyptian computer scientists.<sup>457</sup> As Arquilla and Ronfeldt argue:

These protagonists are likely to consist of dispersed small groups who communicate, co-ordinate and conduct their campaigns in an internetted manner, without a precise central command... To give a string of examples, netwar is

---

<sup>455</sup> D. Verton, 'New cyberterror threatens AF', Federal Computer Week, 3/5/99

<sup>456</sup> For more information see Arquilla, J and Ronfeldt, D: (2000) *Swarming and the Future of Conflict*, Rand: California.

<sup>457</sup> Arquilla and Ronfeldt, (2001) *Networks and Netwars*, Rand: California. The authors cite: 'Arab Afghans said to launch world-wide terrorist war', Paris al-Watan al-Arabi, December 1, 1995, pp22-24/ Afghanistan, Saudi Arabia: 'Editor's journey to meet Bin Laden described', London al-Quds al-Arabi, 1997, pp.4 -8



about the Middle East's Hamas more than the Palestine Liberation Organisation (PLO), Mexico's Zapatistas more than Cuba's Fidelistas, and the American Christian patriot movement more than the Ku Klux Klan.<sup>458</sup>

Arquilla and Ronfeldt argue that power seems to be migrating to nonstate actors, who are able to organise into 'sprawling multi-organizational networks', which are more flexible and responsive than hierarchies in reacting to outside developments, and appear to be better than hierarchies at using information to improve decision-making.<sup>459</sup> Essentially, what these writer argue is that conflicts will evolve around 'knowledge' and the use of 'soft power'. This would come about with the help of information-age ideologies, in which identities and loyalties shift from the nation-state to the transnational level of global civil society.

When Lesser et al. talk about networks, they describe three types: a. the chain network where actors move along a chain of separated contacts, and where end-to-end communication travels through the intermediate nodes; b. the star, hub or wheel network, where a set of a actors is tied to a central node or actor, and must go through that node to coordinate; and c. the all-channel network, as in a collaborative network of small, militant groups where every group is connected to every other.<sup>460</sup> It is important to note that netwar is not simply a function of the

---

<sup>458</sup> *ibid.*, p.45.

<sup>459</sup> Lesser, I, Hoffman, B, Arquilla, J, Ronfeldt, D, Zanini, M, Jenkins, B.M: (1999) *Countering the New Terrorism*, Rand: California

<sup>460</sup> *ibid.*, p.49

internet; it does not take place only in cyberspace or the infosphere. As Lesser et. al argue:

Some key *battles* may occur there, but a *war's* overall conduct and outcome will normally depend mostly on what happens in the real world. Even in information-age conflicts, what happens in the real world is generally more important than what happens in the virtual worlds of cyberspace or the infosphere. Netwar is not Internet war.<sup>461</sup>

For example, Hamas uses internet chat rooms and emails in the United States to coordinate their activities across Gaza, the West Bank, and Lebanon, making it difficult for Israeli security officials to trace their messages and decode their contents.<sup>462</sup> In a 1998 US News and World Report there was evidence of 12 of the 30 groups on the US State Department's list of terrorist organisations on the Web. More recently, it seems that virtually every terrorist organisation is on the internet.<sup>463</sup> For instance, the presence of Middle Eastern terrorist organisations on the internet is suspected in the case of the Islamic Gateway, a World Wide Website that contains information on a number of Islamic activist organisations based in the United Kingdom. British Islamic activists use the World Wide Web to broadcast their news and attract funding; they are also turning to the internet as an organisational and communication tool. While the vast majority of Islamic

---

<sup>461</sup> *ibid.*, p.53

<sup>462</sup> Denning, D: 'Activism, hacktivism and cyberterrorism: The Internet as a tool for influencing foreign policy' in Arquilla and Ronfeldt, 2001, the author cites 'Israel: US Hamas activists use the Internet to send attack threats', *Tel Aviv IDF Radio*, FBIS-TOT-97-001-L, 0500 GMT Oct.13, 1996.



activist groups represented in the Islamic Gateway are legitimate, one group - the Global Jihad Fund - makes no secret of its militant goals.<sup>464</sup>

Moreover, an internet site claiming to represent al-Qaeda said that the network decided to launch suicide attacks against Israel with the goal being the destruction of the Jewish state. US government officials believe that the site indeed speaks for al-Qaeda, and intelligence officers had been monitoring it for some time. Bruce Hoffman, a terrorism expert with the Rand Corporation research group, commented that al-Qaeda's new attacks on Israel stem from terrorists looking for work, with al-Qaeda desperate to appear relevant, to be a player in Middle Eastern politics.<sup>465</sup> Also, Rep. Lamar Smith (R-Texas) warned in closed-door briefings for members of Congress that there is a 50 per cent chance that the next time al-Qaeda terrorists strike the United States, their attack will include a cyberattack. Smith said that officials from federal law enforcement and intelligence-gathering agencies disclosed that al-Qaeda operatives have been exploring US websites and probing the electronic infrastructure of American companies in search of ways to disable power and water supplies, disrupt phone services and damage other parts of the critical infrastructure.<sup>466</sup> In more subtle terms, Azzam Publications, based in London and named after Sheikh Abdullah Azzam, a mentor of Osama bin Laden, has a site dedicated to Jihad around the world. It is alleged that the site, which sold Jihad-related material from books to videos, was raising funds for the

---

<sup>463</sup> Denning, D: 'Activism, hacktivism and cyberterrorism: The Internet as a tool for influencing foreign policy' in Arquilla and Ronfeldt 2001, p. 252.

<sup>464</sup> Lesser et. al p. 66

<sup>465</sup> Mintz, J: 'Al Qaeda website points at new terrorist target Israel', Washington Post



Taliban in Afghanistan and for allied guerrillas fighting the Russians in Chechnya.<sup>467</sup>

Also, US forces hunting down al-Qaeda and Taliban fighters strung fiber-optic cables through the treetops and installed satellite uplinks, providing thousands of American troops with a crucial link to home: the internet. The technology of course stands in stark contrast to the spartan surroundings, as few people in Afghanistan have phones and fewer still have ever seen the internet.<sup>468</sup>

Jerry Everard, in his work *Virtual States*, argues that a developed nation engaged in open conflict with a small, less-wired nation could find its own economic system targeted, with its banking system, its stock exchanges, its telecommunications and power grid systems, and its logistical support networks being systematically targeted from any point on earth. 'Such activities could result in swaying the hearts and minds of the domestic polity of the developed west toward the conclusion that big states may find the cost of small wars far greater than they bargained for'.<sup>469</sup>

Advanced technological information systems will allow state and substate actors, including news services, non-governmental organisations, and even individual citizens, to make voice, video, and written information instantly available to

---

<sup>466</sup> Matthews, W: 'Al-Qaeda cyber alarm sounded', 25/7/02

<sup>467</sup> 'Terrorists using the net to raise funds reach public', Miami Herald 3/4/01

<sup>468</sup> 'US forces using the Net to contact home', USA today, 5/7/02

audiences located in the remotest areas of the globe. This touches on another important factor: information classification. Up until now, information data in the US was put into separate partitions, where only a few people had access to it.

What is needed for effective governance, however, is that authorities need to make information available 'by job' to whoever needs it - regardless of their security clearance. 'We have to change the way we classify information. The old system may have worked against the Soviet Union. But today, the federal government needs to make information available to law enforcement, and the security staff guarding the power plant', Jim Caverly, who heads the Homeland Security's Department's Information Analysis and Infrastructure Protection division, has commented.<sup>470</sup>

Steven Aftergood, who heads the Federation of American Scientists' Project on Government Secrecy, has also pointed out that 'any attempt to control the flow of information impedes the whole. It's the difference between a top down command structure and a network'.<sup>471</sup> Military and intelligence officials are trying to move away from their old hierarchies and toward a structure in which every soldier, every drone and every general is connected by computer networks. As Jordan Crandall writes:

---

<sup>469</sup> Everard, J: (2000) *The Internet, Democracy and Democratization*, Frank Cass: London and Portland, p. 115

<sup>470</sup> Schachtman, N: 'Spies attack White House secrecy', wired, 16/10/03

<sup>471</sup> *ibid.*

Computerization has brought massive changes in the development and coordination of databases, the speed and quality of communication with intelligence and tactical agencies, operations and combat teams. New technologies of tracking, identification, and networking have increased this infrastructure into a massive machinery of proactive supervision and tactical knowledge. Originally conceived for the defense and intelligence industries, these technologies have, after the cold war, rapidly spread into the law enforcement and private sectors.<sup>472</sup>

Furthermore, due to the fact that netwar defies and cuts across standard boundaries and jurisdictions, governments have difficulty assigning responsibility to a single agency (military, police or intelligence) to respond. This poses a challenge to the state, because traditionally, ideals of sovereignty and authority are 'linked to a bureaucratic rationality in which issues and problems can be neatly divided, and specific offices can be charged with taking care of specific problems. In netwar, things are rarely so clear'.<sup>473</sup>

Mulveron contemplates various scenarios in *The People's Liberation Army in the Information Age*, assessing the capabilities of the US and China in a possible confrontation. He writes that there are important differences between Chinese and American Information Warfare (IW) literatures. People's Liberation Army (PLA) writers look at IW in strictly military terms, while Western authors accept the dichotomy between information warfare waged between states or militaries

---

<sup>472</sup> Crandall, J: 'Anything that moves: Armed vision', [http://ctheory.net/text\\_file?pick=115](http://ctheory.net/text_file?pick=115)



(cyberwar) and information warfare waged between substate actors and states (netwar). Both US and Chinese authors are guilty of over-using Sun Ji, especially the notion of 'winning the battle without fighting'. Chinese theorists are also forced to discuss from an inferior technologically standpoint, in opposition to an advanced foe.<sup>474</sup> Nevertheless Mulveron believes that IW presents the Chinese with a potentially potent, if circumscribed, asymmetrical weapon. 'Defined carefully, it could give the PLA a longer-range power projection capability against US forces that its conventional forces cannot currently hope to match... to attack its information systems, especially those related to command and control and transportation'.<sup>475</sup>

The reason for this is that launching a cyberattack is fairly inexpensive. One knowledgeable hacker with a computer can wreak havoc on an automated pipeline. A cell of 'cyber-space guerrillas' armed with few thousand dollars' worth of hardware could disable a nation's power grid. Several hackers together can dramatically increase the capabilities of a terrorist group.<sup>476</sup> More guerrilla groups will be attracted to cyberwarfare, because they can spread propaganda, recruit sympathisers and collect data. The possibilities are endless: military espionage, control and disruption of information flow, destruction, distortion and fabrication of data, electronic bombs and psychological operations could be potential tactics.

---

<sup>473</sup> *ibid.*, p.54

<sup>474</sup> Mulveron, J and Yang, R: (1999) *The People's Liberation Army in the Information Age*, Rand: California, p.182

<sup>475</sup> *ibid.*, p.175

On the other hand, Winn Schwartau, author of *Pearl Harbor Dot Com*, argues against those who believe that information warfare is just a hype, that cyberattacks can cause terror and that the fundamental flaw in the sceptics' argument is their assumption that because things haven't gone wrong before, they will never go wrong. It relies on a flawed fortress mentality, which has never worked as a defense.<sup>477</sup> An example he gives of viable electronic terrorism is waging an IW attack against a series of US domestic air carriers where the attackers do not use a conventional bomb but rather, an electromagnetic bomb, which sufficiently interferes with the avionics of the plane to cause it to crash.<sup>478</sup>

As early as 1995, the Pentagon's assistant director for strategic planning made clear that the problem is real enough:

... as the information age matures, a truly revolutionary form of warfare will emerge. Information warfare will be fought in a different environment, with adversaries grappling in cyberspace. As every potential adversary achieves access to multiple information systems, warfare will be conducted virtually at the speed of light over global distances. Domination of cyberspace may render the need to employ conventional forces and firepower less likely.<sup>479</sup>

---

<sup>476</sup> Jane's International Police issues: 'Information warfare: the coming threat', 2 Dec 1998

<sup>477</sup> Shachtman, N: 'Terrorists on the Net? Who cares?', wired, 20/12/02

<sup>478</sup> Venke, B: 'Information warrior', wired, 4/8/1996

<sup>479</sup> J. Guisnel (1997), *Cyberwars*, Plenum Trade: New York and London.



Consequently, there must be some perceived threat, as the US government has devoted dozens of committees to deal with information warfare. The most important ones are the National Information Protection Center (NIPC), consisting of FBI agents and military and national security components, the Critical Infrastructure Coordination Group and the US Commerce Department's Critical Infrastructure Assurance Office (CIAO). The latter include business and private-sector specialists.<sup>480</sup> The special force is the Air Force Information Warfare Center (AFIWC) at Kelly Air Force Base in San Antonio, which monitors activity in the nation's defense networks and in case of attack goes on the offensive. However, in January 2003, the US government issued a revised Cybersecurity plan reducing by nearly half its initiatives to tighten security for vital computer networks, placing more emphasis on the New Homeland Security Department and eliminating the plan to consult regularly with privacy experts. The plan was to launch some tests against civilian US agencies and improve the safety of automated systems that operate the nation's water, chemical and electrical networks, while also reserving the right to wage cyberwarfare if the nation is attacked.<sup>481</sup> 'When a nation, a terrorist group, or other adversary attacks the United States through cyberspace, the US response need not be limited to criminal prosecution', the plan said. Also, the US government asked internet users and businesses to practice 'safe computing online' and promised to bolster its own cyber-defenses.<sup>482</sup>

---

<sup>480</sup> Pence, S: 'How today's playgrounds become tomorrow's battlefields...or will it?', wired.

<sup>481</sup> 'Revised cybersecurity plan issued', Associated Press, 7/7/02



However, this National Strategy to Secure Cyberspace imposes few new requirements on the private businesses that control 85 per cent of the global computer network. 'Instead the Bush administration sees its role largely as a cheerleader, encouraging businesses to keep their networks secure and supporting publicity campaigns to encourage greater individual use of anti-virus software, firewalls and other security tools'.<sup>483</sup> The Department of Homeland Security is expected to lead a response when cyberattacks occur, set up programs to develop a more tech-savvy work force and encourage business sectors like banking and utilities to bolster security standards on their own.

The full extent of the US cyber-arsenal is among the most tightly held national security secrets, even more guarded than nuclear capabilities. Because of secrecy concerns, many of the programmes remain known only to strictly compartmented groups, a situation that in the past has inhibited the drafting of general policy and specific rules of engagement. As Maj. Gen. James David Bryan, who heads the Joint Task Force on Computer Network Operations explains, his group has three main missions: to experiment with cyber-weapons in order to better understand their effects; to normalise the use of such weapons, treating them 'not as a separate entity', but as an integral part of the US arsenal; and to train a professional cadre of military cyberwarriors.<sup>484</sup>

---

<sup>482</sup> *ibid.*

<sup>483</sup> 'US plans for online defense', Reuters, 19/2/03

<sup>484</sup> Graham, B: 'Bush orders guidelines for cyberwarfare', Washington Post, 7/2/03

Furthermore, McCaffrey, a highly decorated combat veteran, told attendees at the American Society for Industrial Security (ASIS) annual conference that the government's ability to protect the country is 'only as good as the technology that backs it up'.<sup>485</sup> The government's current snooping system, known as Carnivore, makes it too easy to enable the reading of all emails with only a warrant. As a result, indiscriminate access makes it difficult for local law-enforcement agencies to find useful evidence in a sea of data. Kelly Kuchta, a cybersecurity expert who is chair of ASIS's information technology security council, sees private security firms as being more willing to work with law enforcement agencies since Sept. 11, 2001, sharing information about cyberattacks with the FBI as part of InfraGuard, a cooperative program between the public and private sectors.<sup>486</sup> The Bush administration has toughened anti-hacking laws since Sept. 11 and increasingly lobbied governments to cooperate in international computer-crime investigations. The United States and Britain were among 26 nations that last year signed the Council of Europe Convention on Cybercrime, an international treaty that provides for hacker extraditions even among countries without other formal extradition agreements.

Such zeal on behalf of national governments could be explained, if we consider the economic, military and socio-political aspects of cyberconflict. The protection of commercial information infrastructure is a national security concern, which cannot be disregarded easily. According to a study conducted by the FBI, nearly

---

<sup>485</sup> *ibid.*

<sup>486</sup> Gartner, J: 'Terror Czar: The war is digital', *wired*, 11/9/02

90 per cent of US businesses and government agencies suffered hacker attacks in 2002, only a third of companies that suffered attacks reported the intrusions to law enforcement, and around 78 per cent of companies surveyed also said that employees had abused their internet access privileges by downloading pornography or private software.<sup>487</sup>

The burden is therefore on the government to demonstrate that the protection of commercial information infrastructure is a national security concern that cannot be discharged any other way. Convincing a population wary of government intervention of the need for such intrusive government action may require a crisis such as Sept.11.

---

<sup>487</sup> Newbytes: 'American companies fail to report intrusions', [www.nua.com](http://www.nua.com)



### 3.2 Internet Security Analysis: Incidents and Responses

#### *Incidents and Responses*

An examination of historical precedents indicates that major political and military conflicts are increasingly accompanied by significant cyberattack activity. Ongoing conflicts also show that the cyberattacks are escalating in volume, sophistication and coordination.<sup>488</sup>

It would be useful here to include some cases of internet security breaches. As early as March and April 1994 Air Force computer security experts discovered that their classified network at the Rome (New York) Laboratories had been attacked. Attackers gained complete access to all Rome networks, copying sensitive (though not classified) information, and while they could have brought the network down, they chose not to.<sup>489</sup> Through the Rome Lab they accessed other classified sites like the South Korean Atomic Research Institute. The hackers were discovered as codenamed 'Kuji' and 'Datastream Cowboy'. Datastream was identified through an informant after he bragged and left his phone number with him. He turned out to be a sixteen-year-old using nothing more than a 486sx PC.<sup>490</sup> In 1994, they were arrested in England, and turned out

---

<sup>488</sup> Vatis, M: 'Cyberattacks during the war on terrorism: A predictive analysis', Institute for Security technology Studies, Dartmouth College.

<sup>489</sup> Shapiro, J: (2001) 'Information and war: Is it a revolution?', p.132 in Libicki, M and Shapiro, J: *Strategic Appraisal: The Changing Role of Information Warfare*, Rand: California

<sup>490</sup> Selden, Z: 'Information security: The implications of cyberwar for national security', *Business Executives for National Security Report*, Nov 1996, [www.bens.org.pubs](http://www.bens.org.pubs)

to have planted eavesdropping software that allowed them to monitor emails and other sensitive information.<sup>491</sup>

In one long-running operation, the subject of a U.S. spy investigation dubbed 'Storm Cloud' and 'Moonlight Maze', hackers traced back to Russia were found to have been quietly downloading millions of pages of sensitive data, including one colonel's email inbox. Most recently in April 2001, government computer operators watched as reams of electronic documents flowed from Defense Department computers, among others. Remarkably, Gary McKinnon, a British hacker indicted for hacking into scores of US military computers, installed copies of a commercial remote access utility called RemotelyAnywhere on Navy and other military systems he hacked. For nearly a year, McKinnon was able to control a vast network of defense computers without detection, authorities said. Using a personal computer connected to an ISP in England, McKinnon downloaded a trial copy of RemotelyAnywhere in March 2001 from a server maintained by Binary Research, the Milwaukee-based distributor of RemotelyAnywhere. To obtain a special code to unlock the demonstration software, McKinnon also provided his girlfriend's email address. McKinnon was indicted in federal courts in Virginia and New Jersey on eight counts of computer crimes. McKinnon was facing on each count a maximum sentence of 10 years in prison and a \$250,000 fine. Investigators characterised the hacker as 'a conspiracy

---

<sup>491</sup> 'Indictment due against hacker', Associated Press, 12/11/02



theorist' who 'seemed to think that the government was controlling all sorts of things'.<sup>492</sup>

A more publicised incident was the Slammer worm, also known as Sapphire, which spread in 10 minutes in the last weekend of January 2003, quickly crippling many computer systems around the world offline. It targeted Microsoft's SQL Sever 2000 as well as applications created with the Microsoft SQL Server 2000 Desktop Engine. Microsoft had released a patch for Slammer in July 2002, but security experts said a successful installation required users to manually edit system files, a compilation that resulted in some patches being installed incorrectly, if they were installed at all. The worm inflicted 247,000 computers worldwide, while the code is exceedingly condensed and does not include references to hacker aliases or locations. It used a transmission method that made it especially easy for its author to throw off investigators by falsifying his digital trail.

Many top experts believe the programming for the internet worm was based on software code published on the Web months before by a respected British computer researcher, David Litchfield, and later modified by a virus author within the Chinese hacker community known as Lion. Litchfield said he originally published the blueprints for computer administrators to understand how hackers might use the program to attack their systems.<sup>493</sup> Another issue cropping up with

---

<sup>492</sup> McWilliams, B: 'Dot-mil hacker's download mistake', wired 15/11/02



the Slammer worm was that the internet security firm Symantec withheld information about the worm for hours after spotting it, sharing the information only with select customers, leaving the rest of the global community to cope with the impact of Slammer. South Korean telephone systems administrator Lee Ji-Ho, whose country's entire communications system collapsed for roughly 24 hours because of Slammer, said: '[m]y country was hurt hard by this Slammer. We could have been prepared and maybe avoided had we known ahead'.<sup>494</sup> Code Red and Nimda spread around the world in a matter of hours, but Slammer took under three minutes to affect thousands of machines, and was able to compromise nearly all vulnerable systems in about half an hour. Another computer virus found in the wild in October 2003, called Mimail.C, was capable of turning infected personal computers into 'spamming' machines.<sup>495</sup>

As far as viruses are concerned, about 1,000 viruses are created every month by virus writers who increasingly intend to target new operating systems. Jan Rhuska, the chief executive of Sophos, the world's fourth largest anti-virus provider, has commented that the number of viruses created would continue to climb in the coming years and said of the virus writers, believed to be computer-obsessed males between the ages of 14 to 34 years, that 'have chronic lack of girlfriends, are usually socially inadequate and are drawn compulsively to write self-replicating codes'.<sup>496</sup> In January 2003, Welsh virus writer and Web designer

---

<sup>493</sup> 'Few clues in worm whodunnit', Associated Press

<sup>494</sup> Delio, M: 'What Symantec knew but didn't say', wired

<sup>495</sup> 'New virus dresses up as email', Reuters, 31/10/03

<sup>496</sup> 'Not just your average loser', Reuters, 18/3/03

Simon Vallor, 22, was sentenced to two years in jail for spreading three mass-mailing computer viruses that infected more than 27,000 computers in 42 countries. Some of the viruses like Klez, a mass mailing worm that originated in November 2001, just refuse to go away.<sup>497</sup> Members of the computing industry and law enforcement, when testifying before the technology subcommittee of the House Committee on Government reform in the US, proposed solutions for these kinds of attack such as better standards for producing software, computing ethics education directed at children, increased funding and training for computer forensics to catch hackers and virus writers, and protocols for information sharing that would aid in capturing perpetrators across borders.<sup>498</sup>

The year 2003 has been deemed the worst in computer-virus history by security experts, despite the fact that worm and virus writers displayed no significant technological progress in the code of their new creations. That year computer worms managed to shut down ATMs, slow airline and train travel by affecting reservation and signaling systems, clog emergency phone services, and crash networks controlling critical systems at hospitals and at least one nuclear plant. ‘The scary thing is that the Blaster and Slammer worms were not intended to take down critical systems. The worms were just programmed to propagate. Imagine what could have happened if they had carried a malicious payload’, said Mikko Hypponen, director of anti-virus research for F-Secure.<sup>499</sup>

---

<sup>497</sup> *ibid.*

<sup>498</sup> Zetter, K: ‘Just say no to viruses and worms’, *wired*, 11/11/03



The most troubling development in 2003 was that spammers and virus writers have evidently decided to partner, resulting in a demon love-child virus-worm that both infects computers and spews spam. Slammer, released in January 2003, has been described by many as the biggest attack against the internet ever. Spreading over network connections, Slammer searched for victims so aggressively that it caused an enormous amount of network traffic, dramatically slowing network response times across the internet.

Following Slammer the next big virus was Blaster (aka MS Blast), detected in August, which wormed into computers through a hole in the Windows operating system. Millions of Windows 2000 and Windows XP users were alerted to the presence of Blaster in their computers when they saw an error message informing them their machine would be restarting in 60 seconds. Just a week after that, Sobig.F was released, quickly becoming the worst worm ever, sending over 300 million infected messages around the world, according to anti-virus experts. 'It is likely that there is a virus-writer group behind Sobig. They used the worm to infect a huge number of computers and then sold various spammer groups lists of proxy servers, which would be open for spreading spam. It was clearly a business operation', commented Hypponen, a security expert with F-Secure. Experts expect that this type of commercial activity will increase, and say that viruses will quickly become the spammers' tool of choice in their never-ending efforts to force junk mail into people's inboxes.<sup>500</sup>

---

<sup>499</sup> Delio, M: 'The Internet is a very sick place', wired, 23/12/04

<sup>500</sup> *ibid.*



The same pattern was noticeable in January 2004 with the MyDoom virus, whose social engineering specifically targeted the corporate world. 'Malicious hackers have been selling the use of compromised computers to spammers for some time now - it's good money for them. Compromised home-user machines are already in widespread use by spammers and MyDoom-infected machines will only add to that pressure on inboxes' said Jose Nazario, security analyst for Arbor Networks.<sup>501</sup> Additionally, German police have arrested an 18-year-old suspected of creating the Sasser computer worm, which surfaced in May 2004 wreaking havoc on personal computers. 'Hopefully this arrest will limit their activities. If we can start catching these guys it will certainly put more pressure on existing virus writers' said Hyponnen.<sup>502</sup> Also, due to the fact that pieces of code found in a recent version of the Netsky worm made references to Sasser, Graham Cluely, consultant at Sophos, said the police may have cracked the Netsky gang with the arrest. The economic toll of Sasser may never be known, but it has claimed some big scalps, including Germany's Deutsche Post, Britain's coastguard stations and investment bank Goldman Sachs.<sup>503</sup>

The economic threat in cyberspace manifested itself when a Mafia-led syndicate used banking and telecommunications insiders to break into an Italian bank's computer network, diverting the equivalent of \$115 million in European Union aid to Mafia-controlled bank accounts overseas before Italian authorities detected

---

<sup>501</sup> Delio, M: 'Worm slowing, but still dangerous', wired, 28/1/04

<sup>502</sup> Delio, M: 'The Internet is a very sick place', wired, 23/12/04

the activity.<sup>504</sup> Additionally in June 2003, a huge internet piracy ring was shut down in an Italian financial police operation that resulted in the arrest of 181 people and the recovery of pirated software worth about \$139.5 million. The piracy network used email and illegal websites to market itself and distributed goods via mail order.<sup>505</sup> Moreover, one of the most impressive cyberattacks occurred in October 2002, when nine of the thirteen computer servers that manage global internet traffic were crippled. The attack lasted for an hour, but it was described as the most sophisticated, large-scale assault against these crucial computers in the history of the internet.<sup>506</sup>

Despite the fact that there have been several serious incidents of cyberattack, doubts have been raised as to the real or exaggerated nature of cyberwar. Several experts think that information warfare will likely go much further than nuisance attacks by hacktivists. In a rather humorous mood the Crypt Newsletter wrote that '[t]he wonderful thing about secret cyberwar is that it can be anything anyone wants it to be. In secret cyberwar, it is not really necessary that anyone be an actual reliable witness to it or that effects of it even be presented or seen'.<sup>507</sup> The point made is that there are instances where cyberwar stories are reported in the media, but not experienced by anyone else. The criticism the Crypt Newsletter made late in 1998 in *Issues in Science and Technology* magazine was that one has to be skeptical of the warnings of information warfare, because those alarms often

---

<sup>503</sup> 'Sasser worm suspect confesses', Reuters, 8/5/04

<sup>504</sup> [www.cia.gov](http://www.cia.gov)

<sup>505</sup> Sturgeon, W: 'Italian police shut down piracy ring', CNET News.com, 16/6/03

<sup>506</sup> Wired news report: 'DoS attack maims web servers', 23/10/02

<sup>507</sup> Crypt Newsletter at [Sun.soci.niu.edu/~crypt](http://Sun.soci.niu.edu/~crypt)



come from the very people who are to benefit from government spending to combat the threat. An example they give to reinforce this argument is that the primary author of a January 1997 Defense Science Board report on information warfare, which recommended an immediate \$580 million investment (and \$15 billion over five years) in private sector R&D for hardware and software to implement computer security, was Duane Andrews, executive vice president of SAIC, a computer security vendor and supplier of information warfare consulting services.<sup>508</sup>

Another instance of absurd claims was criticised by the Crypt when the *Economist* reported a Pentagon estimate that the Taiwanese spread two viruses, known as the Bloody 6/4 and Michelangelo, damaging 360,000 computers in China at a cost of \$120 million. The Crypt Newsletter wrote that, contrary to such claims, neither virus is spread on the internet or by networked computer connections and that both have been essentially distinct on western computers. Therefore, there is controversy as to whether media reporting is accurate, since it takes a modicum of technical expertise to report on such incidents and second as to whether there is vested interest in exaggerating cyberwar reports to receive funding – for instance the FBI receives special funding for such projects outside normal budgets.<sup>509</sup>

Another example was the ‘Fluffy Bunny’, which for a six-month period starting in mid 2001 penetrated the networks of several top internet firms, including Exodus,

---

<sup>508</sup> *ibid.*

<sup>509</sup> Crypt newsletter



VA Software and Akamai. The hackers also vandalised websites operated by leading security outfits including the SANS institute.<sup>510</sup> However, despite the thousands of hackable holes found in email, websites, files and operating systems, few of the hacks in 2002 turned out to have any real impact on most computer users. The Klez virus infected some machines and the Linux Slapper worm made more work for system administrators for while. Sweeny, an internet security expert commented in December 2002 that '[t]he average user wouldn't know a hack if it walked up and hit them. And many of the so-called security holes require a very specific event to occur and the odds are very slim that it will occur'.<sup>511</sup> This is an opinion also shared by Jim Lewis, a 16-year veteran of the State and Commerce Departments, who compiled an analysis for the Centre for Strategic and International Studies. 'A hacker or a large group of hackers would need to find vulnerabilities in multiple systems to significantly disrupt the power supply and even then, an attack might only disrupt service for a few hours'.<sup>512</sup>

### *Internet Security Analysis*

There are two components in computer security: virus protection (lack of trust in outside sources) and authentication (verifying that a person is known to you). But the first notion of 'common sense' is far less effective in securing computers. We expect our machines to do what they are told, but such expectations leave them

---

<sup>510</sup> McWilliams, B: 'Fluffy Bunny no longer energized', wired, 29/7/02

<sup>511</sup> Delio, M: 'So many holes, so few hacks', wired, 30/12/02

<sup>512</sup> Shachtman, M: 'Terrorists on the Net? Who Cares?', wired, 20/12/02

prey to low-level, but insidious, information-warfare attacks.<sup>513</sup> In Britain, three-quarters of all companies have been hit by hackers. Each attack costs 120,000 pounds on average.

By contrast, the question of 'what forms of attack' is somewhat more approachable than the 'who' questions. It is tempting to see intrusions in terms of a pyramid that goes from transient vulnerability probing and defacing of websites at the base to large scale efforts to undermine the critical missions of an organisation or the critical functions of a nation at the top - and to suggest that there is an inverse relationship between frequency and significance, with many trivial incidents and comparatively few of the more serious incidents. This lack of congruence between limited intent and far-reaching consequences stems from the capacity of worms and viruses for infinite replication and multiplication.

---

<sup>513</sup> Libicki, M and Shapiro, J: (2001) *Strategic Appraisal: The Changing Role of Information Warfare*, Rand: California, p.441.

Consider the 'I love you' virus for example, which caused an estimated \$6.7 billion in damages in the first 5 days. It was caused by a single individual with poor support and little preparation. As Shimeall et.al argue, the lesson was very clear: 'the development of national and global information systems has out paced appropriate safeguards and security measures. This provides new targets and new opportunities for criminal organisations, terrorist groups and hostile nations'.<sup>514</sup>

One further barrier here may be the structure of the intelligence community itself, which for constitutional reasons has been partitioned into domestic and foreign intelligence. While this distinction is critical in the physical world, it vanishes rapidly in the cyber-world. The intelligence community has been left with the uncomfortable choice of violating important barriers, an unacceptable option, or yielding the cyber world to transnational threats, likewise an unacceptable option.<sup>515</sup>

In Shimeall et al.'s internet security analysis, six problems are prominent: 1. the lack of borders, which is different from the more familiar domains of intelligence; 2. the identification of intruders, which is critical to the assessment of the challenge and the nature of the response; 3. the forms of attack which either fall far short of what was intended, or far exceed what the perpetrator initially envisaged; 4. The question of how intrusions take place, which is the most technical aspect of the problem and the easiest to answer; 5. the legal issue of who

---

<sup>514</sup> Shimeall, T, Dunlevy, C, Williams, P: *Intelligence Analysis for Internet security: Ideas, Barriers and Possibilities*, Certo Analysis Center, Carnegie Mellon University May 2001, p.2



gets notified when analysts attribute an intrusion to a foreign individual; 6. the structure of the intelligence community itself, which for constitutional reasons has been partitioned into domestic and foreign intelligence.<sup>516</sup>

Another problem in internet security analysis is that of disclosing computer intrusions publicly. US cybersecurity director Richard Clark, in November 2002, and virtually all software companies insisted that software vendors should have a chance to fix problems before security researchers disclose them publicly.<sup>517</sup> Researchers have criticised Symantec for encouraging people to create and release malicious code. 'Given that Symantec also sells security and antivirus software, I think there is a terrible conflict of interest here.'<sup>518</sup> Moreover, security experts caution IT managers not to publicise security holes simply to embarrass vendors into action, because within hours, black-hat hackers would know the vulnerability and use it. One test case is NASA where more than 24 percent of attempted hack attacks penetrated the system in the third quarter of 2000, but by the end of 2001, after scanning and fixing system flaws, only a fraction of 1 percent of attacks were successful.

More specifically, methods of intrusion are the online equivalent of military tactics, and just as in the military world there has historically been a dialectic between defense and offense, similarly on the internet, there is a dialectic between

---

<sup>515</sup> *ibid.*, p.10

<sup>516</sup> *ibid.*, pp. 5-10

<sup>517</sup> Delio, M: 'How much hack info is too much?', *wired.com*, 19/11/02

<sup>518</sup> *ibid.*

protection and intrusion. Intruders manipulate the sources of intrusion and the online records of activity. The sources of intrusion are manipulated either by staging intrusions through a series of already-intruded and corrupted hosts, or by falsifying source information from the network traffic. Online records on the other hand are falsified either by directly modifying the records themselves or by replacing the monitoring software that produces these records.<sup>519</sup> The following are of paramount importance: details of the victim's infrastructure, the nature of the intrusion, identity clues left by the intruder, network traffic flow, and intrusion tools left as traffic artifacts on the victim hosts.

The latest in internet security is that angry computer users fed up with attacks from internet hackers are hacking back. They are buying counterstrike software to turn the tables on the hackers. The new software could spawn a generation of vigilante net users prepared to take the law into their own hands to protect their hard drives.<sup>520</sup> In other words, the users of the internet are not easily controlled or subverted. As Foucault has suggested, every exercise of power whether it is by a government or a cyberwarrior will create a resistance somewhere, even among the 'public'.

---

<sup>519</sup> Shimeall et al, p.8

<sup>520</sup> Harding, D: 'Vigilantes fight back by hacking the hackers', Metro, 10/6/04

### 3.3 Sociopolitical Implications

To continue, Gombert believes that competitiveness in information technology depends on economic and political freedom and on integration into the core. By integration into the core he means the core of power in western democratic states. According to this view integration to the core creates shared stakes that eclipse, or at least qualify, power politics and point toward a democratic commonwealth of interests and values.<sup>521</sup> The idea behind this is that the constantly-changing nature of this technology favours open economic systems:

The main economic uses to which information technology is put - distributing information, decentralising functions and decision-making, creating horizontal links, improving producer-consumer contact, sharpening external awareness and adaptability - correspond with strong market forces. Even if the supply of information technology becomes less dependent on economic freedom over time, the demand will not. Therefore, we should expect capitalist systems to retain their advantage through the information age.<sup>522</sup>

What this amounts to is that other powers that want to get into the game where open market democracies dominate will have to 'open up to the pressures for

---

<sup>521</sup> Gombert, D (2001): 'Right makes might: Freedom and power in the information age', p.50 in Libicki, M and Shapiro, J: *Strategic Appraisal: The Changing Role of Information Warfare*, Rand: California.

<sup>522</sup> *ibid.*, p.54



reform and freedom that create modern knowledge-based power'.<sup>523</sup> According to Gombert there are three reasons why this is the case. First, competitiveness in information technology depends on economic and political freedom and on integration into the core. Second, military power and other forms of national power depend on broad-based competitiveness in the creation and use of information technology. Third, integration into the core creates shared stakes that eclipse, or at least qualify, power politics and which point towards a democratic commonwealth of interests and values.<sup>524</sup> Interestingly, Gombert argues:

Direct support for dissidents or embryonic democratic institutions is increasingly available both from the governments and nongovernmental organizations of the democratic core, thanks to (what else?) information technology. The penetrability of even self-isolated societies is growing, especially when sophisticated transnational "civil society" groups make it their business to network with the oppressed.

Most information products and services work well only when embedded in a society whose skills and infrastructure are undergoing a larger information revolution. These technologies are increasingly interdependent, especially as computer networking expands; individual items of hardware are of limited utility. What good are desktop computers without networks and a steady diet of software upgrades? Information technology is constantly being modified, enhanced, and overtaken by better ideas, leaving importing states to engage in an expensive and

---

<sup>523</sup> *ibid.*, p.61

never-ending game of catch-up technologies which have been conducive to state power, even to coercive state power.

On the socio-political aspect of cyberconflict, the lack of central control, cheap remote access from anywhere and interconnectivity promise to render cyberspace an unprecedented power-enhancer against repressive regimes and societies. This is one of the reasons that the US has devoted so many committees to monitoring the web and defending electronic frontiers. In a report entitled 'Strategic Assessment: the Internet', dating back to July 1995, Charles Swett, assistant for Strategic Assessment, office of the Assistant Secretary of Defense for Special Operations and low intensity conflict, writes:

Current information about conflicts placed on the Internet in real time by on-the-scene observers and alternative news sources will be voraciously devoured by the world audience and will have an immediate and tangible impact on the course of events. Video footage of military operations will be captured by inexpensive, hand-held digital video cameras operated by local individuals, transformed unedited into data files, and then uploaded into the global information flow, reaching millions of people in a matter of minutes. Public opinion and calls for action (or calls to terminate actions) may be formed before national leaders have a chance to develop positions or to react to developments.<sup>525</sup>

---

<sup>524</sup> *ibid.*, p.50

<sup>525</sup> Swett, C: 'Strategic assessment: The Internet', July 1995, web paper

This is more or less what happened with the anti-globalisation movement, with the anti-war movement and in various other conflicts. Indicative example are the photos of naked prisoners at Abu Ghraib, as well as the video of Nick Berg's murder by fundamentalists in Iraq shown globally through the internet. Three other important points Swett makes which are relevant here are, firstly, that if protest groups opposing oppressive regimes persuade trade unions or organisations from richer countries to equip them with the necessary facilities, they can reach a world wide audience, a situation that any government would find difficult to control. Swett's claim is supported by the efforts of several dissidents, as the Zapatista, East Timorese, Tunisian, Chinese, Iraqi, African and Indian social movements have demonstrated. Secondly, such a threat would be very difficult to counter, because personal contact of people living under oppressive regimes with the free world would 'open' their eyes to the distorted propaganda of the regime and discredit their government.<sup>526</sup> Third, the internet has the potential to significantly influence the course of a conflict. In Swett's words:

Thus the Internet can indirectly play an important role in the way the world deals with a conflict, without having substantial physical presence within the conflict. The Internet can play an important positive role during future international crises and conflicts. In the chaotic conditions usually present in such situations, normal government and commercial reporting channels are often unreliable or

---

<sup>526</sup> *ibid.*



unavailable, and the Internet might be one of the few means of communication present.<sup>527</sup>

To continue, the largest and most active international political groups using the internet appear to be the San Francisco-based Institute for Global Communications (IGC) and the Association for Progressive Communications (APC). Therefore, a review of the IGC can provide a good perspective on the breadth of DoD (US Department of Defense)-relevant information available on the internet. According to a text file placed on the IGC's publicly-accessible internet site:

IGC provides computer networking tools for international communication and information exchange. IGC is the U.S. member of the Association for Progressive Communication (APC), a coalition of computer networks providing services to over 25,000 activists and organizations in more than 130 countries. The IGC networks - PeaceNet, EcoNet, ConflictNet and LaborNet - together with APC partner networks, comprise the world's only computer communications system dedicated solely to environmental preservation, peace, and human rights. New technologies are helping these worldwide communities cooperate more effectively and efficiently... Send and receive private messages to and from more than 18,000 international peace, environmental and conflict resolution users on our affiliated networks or to millions of users on virtually any other network...<sup>528</sup>

---

<sup>527</sup> *ibid.*

The Association for Progressive Communication (APC) provides low-cost computer communication services and information sharing tools to individuals and NGOs working on social issues. So, in a way we find 'solidarity in cyberspace'<sup>529</sup>, where a new 'electronic fabric of struggle' is being constructed, helping to unite activist movements around the world.<sup>530</sup> However, as Arquilla and Ronfeldt<sup>531</sup> argue, there is concern about the internet being used for crying wolf and for manipulation by people with hidden agendas. The concern is that government actors may post misinformation and disinformation on the internet in order to provoke an overreaction that embarrasses the activists. The internet is a potent tool for inflammatory rumor, as well as 'black' and 'grey' propaganda, in that actual affiliation of the provider of information can be masked easily and any news materials that are put on the Web can be transformed so as to make faked events appear true.<sup>532</sup>

Further, in recent conflicts the internet has been cited by both parties as playing a key role. As early as 1989, during the heyday of the pro-democracy movement in China, Chinese students used the internet to exchange information, and news was faxed to China to inform people who were unable to obtain information because of the censorship imposed by the Chinese government. In October 1989, after the Tiananmen massacre, students organised a rally in Washington through email,

---

<sup>528</sup> *ibid.*

<sup>529</sup> Mansbach, R (2000): *The Global Puzzle*, 3<sup>rd</sup> ed., Boston: Houghton Mifflin

<sup>530</sup> quote from Cleaver 1995 found in Arquilla and Ronfeldt, 1999

<sup>531</sup> Ronfeldt, D, Arquilla, J, Fuller, G.E and Fuller, M: *The Zapatista "Social Netwar" in Mexico*, Rand 1998, p.71

<sup>532</sup> Hosmer, S: 'The Information revolution and psychological effects' in Khalilzad, Z, White, J.P, Marshall, W (1999): *The Changing Role of Information Warfare*, Rand: California

with 40,000 people across the country participating. Also, they successfully lobbied Congress, using email as the major communications medium to pass the Chinese Students Protection Act of 1992, which protected them from being forced to go back to China and face prosecution.<sup>533</sup>

Also, new global conflicts have involved cross-fertilisation and combination of energies generated at a local, grassroots level. As Cleaver points out,

local conflicts between citizen groups and governments have expanded into global efforts in response to two things: first, to a spreading uniformity of policies and international agreements among governments to implement world-wide sets of rules and second, to the resultant perception of common interests in challenging not only those rules but any set of uniform mandates unrelated to local situations.<sup>534</sup>

An example mentioned by Cleaver is when OECD opened to dialogue after failing to pass the Multilateral Agreement on Investment, which aimed at a global set of rights for corporate investors. This temporary defeat has been credited to the use of the internet in organising a campaign against MAI in countries around the world.<sup>535</sup> This pressure caused the OECD to halt negotiations for six months in April 1998, and France pulled out of the negotiations, undermining them.

---

<sup>533</sup> Wang, F: 'Subscribing to democracy through the Internet', *JAH*, p.16. The author cites Li, T: 'Computer mediated communications and the Chinese students in the US', *The Information Society*, 1990, pp.125-137

<sup>534</sup> Cleaver, H: 'Computer linked social movements and the global threat to capitalism', [www.antenna.nl/~waterman/cleaver2.html](http://www.antenna.nl/~waterman/cleaver2.html).

<sup>535</sup> *ibid.*, p.7



Nevertheless, there have been criticisms of activists using the internet. The first criticism is that on certain occasions, the target is badly chosen because they are not properly connected to the group their actions are supposedly supporting. Second, the use of hacking tactics denies the opponent of freedom of speech and provides a precedent for activists to be attacked in the same way. Third, there is the problem of gaining legitimacy through providing evidence that the action involved a fair amount of people and not just a small number of hackers.<sup>536</sup> Moreover, there is information about all kinds of political struggle out there in cyberspace, which have not yet been connected, because the availability of information does not guarantee that the necessary connection will be made to generate action. Worse, the very amount of information and the number of groups using it will make this situation deteriorate.

However, unlike newspapers, radio and television media where feedback is slow, the internet enables quick interaction, and email lists with ongoing flows of discussion form an alternative community of debate, outside traditional policymaking institutions.<sup>537</sup> Moreover, the groups involved have characteristics which reflect the democratic character of the medium. Users of the internet are colour-, class- and gender-blind and, in contrast to face-to-face interaction where

---

<sup>536</sup> *ibid.*, p.17

<sup>537</sup> *ibid.*, p.16

the status of the speaker is primary, attention is focused on what is said, not who is saying it.<sup>538</sup>

Even though the internet's potential for mobilising world opinion is likely to be diluted by the increasingly large number of issue-oriented groups contending for attention in cyberspace, it will still remain a potent instrument for rallying like-minded people to support or oppose particular actions and causes.<sup>539</sup> Unfortunately, news materials that are put on the web can be masked easily and any visual 'news' materials can be transformed as to make faked events appear true. Moreover, new problems constantly arise, such as spamming, which has been tormenting users for some time now. British lawmakers plan to use a new tactic to stop the torrent of junk email spam that floods in from overseas, extraditing the mass-mailers and bringing them to trial in the United Kingdom. While the initial policy would be used to target spammers, it could be expanded to include suspects in other cybercrime offences such as virus-writing and hacking.<sup>540</sup>

### *Conclusion*

This chapter has examined the environment of cyberconflict by defining the terms involved and the approach to be taken, looking at cyberterrorism, information

---

<sup>538</sup> Wang cites Kraut (1991)

<sup>539</sup> Hosmer cites Mburjo (1997)

<sup>540</sup> 'UK plans to extradite spammers', Reuters, 30/10/03

warfare, internet security analysis and the sociopolitical implications of cyberconflict. The central argument of the thesis is that two types of cyberconflict occur: firstly, between ethnic or religious groups fighting in cyberspace as they do in real life, and secondly, between a social movement and its antagonistic institution (hacktivism). This distinction is needed because we can use social movement theory to explain sociopolitical cyberconflicts and conflict theory to understand ethnoreligious cyberconflict, under the more general umbrella of media theory, as we discuss a new medium.

These issues were addressed by analysing the internet not in terms of a mass medium in the traditional sense, i.e. its influence on the political outcome of a conflict, but rather as a resource used by the opposing parties in a conflict. In this context I discuss Wolfsfeld's political contest model, Deleuze and Guattari's rhizomatic politics and Arquilla and Ronfeldt's argument that the information revolution is altering the nature of conflict by strengthening network forms of organisation over hierarchical forms.

Following these theoretical insights, I provided an analysis of the hacking phenomenon. The motivations for hacking as explained by Taylor are feelings of addiction, the urge of curiosity, boredom with the educational system, peer recognition and political action. Hacking can potentially perform a variety of benevolent services to the security industry, for instance as a watchdog counter-



response to the use of surveillance technology and data gathering by the state, contributing to a general climate of improved security consciousness.

The section on information warfare draws attention to the idea that territory, population and natural resources are becoming less important relative to human capital and the possession of information. Moreover, intelligence officials are trying to move away from their old hierarchies and towards a structure in which every soldier, every drone and every general is connected by computer networks. This is because power seems to be migrating to non-state actors, which are more flexible and responsive than hierarchies at using information to improve decision-making.

Despite this trend, doubts have been raised as to the real or exaggerated nature of cyberwar. There is controversy as to whether media reporting on cyberattacks is accurate and as to whether there is a vested interest in exaggerating cyberwar reports to receive funding. Nevertheless, the U.S. government has created dozens of committees to deal with information warfare. Notably, the full extent of the U.S. cyberarsenal is among the most tightly held national security secrets, even more guarded than nuclear capabilities. Moreover, the Bush administration has toughened anti-hacker laws since September the 11<sup>th</sup> and increasingly lobbies governments to cooperate in international computer crime investigations.

The section on internet security analysis looks at incidents like the Slammer, Blaster and MyDoom viruses which made the year 2003 the worst in computer-virus history, reaching the conclusion that the development of national and global information systems has outpaced appropriate safeguards and security measures. This provides new targets and new opportunities for criminal organisations, terrorist groups and hostile nations. Another problem in internet security analysis is that of disclosing computer intrusions publicly.

On the sociopolitical implications of cyberconflict, which ultimately justify its study, I found that if protest groups opposing oppressive regimes persuade supporters in richer countries to equip them with the necessary facilities, they can reach a worldwide audience, a situation any government would find difficult to control. Also, in international crises and conflicts where normal government and commercial reporting are unreliable, the internet might be one of the few means of communication present. An example of alternative reporting is the internet's effect on the 2003 Iraq conflict, discussed in section 6.2. On the downside, there is information about all kinds of political struggle out there in cyberspace, which have not yet been connected, because the availability of information does not guarantee that the necessary connection will be made to generate action.

In the following chapter I use elements of social movement theory to look at sociopolitical cyberconflicts, where social movements use the internet against

antagonistic institutions and also address the issue of dissidents using the internet to oppose their respective governments.



## **Chapter 4: Sociopolitical Cyberconflicts**

This chapter looks at sociopolitical cyberconflicts, providing an explanation of the forms and types of this kind of conflict and discussing instances of it, such as the anti-globalisation movement. It also includes an extensive examination of Chinese cyberdissidents and the Chinese government's cyberstrategies, as well as a brief look at internet censorship and dissidents internationally. The main argument of the chapter is that groups involved in sociopolitical cyberconflicts use the internet as an organisational and mobilisational resource attempting to reframe issues and take advantage of the openings of the political opportunity structures offered by new communication technologies. Lastly, I explicitly link the examples with my proposed integrated theoretical framework.

### **4.1 Sociopolitical Cyberconflicts**

Sociopolitical cyberconflicts can be placed into two broad groups, either those which are primarily concerned with global issues such as the environment, issues in relation to which the level of negotiation with governments is open for debate, and those involving groups who are much less inclined to negotiate with governments, being as they are concerned with issues such as their own liberation from the control of the state.<sup>541</sup> One aspect of the problem seems to be that with the explosion of the size of the internet, protests and political activism have

entered a new realm. Political activism on the internet has generated a wide range of activity such as using email and websites to organise, web defacements and denial-of-service attacks, described above. These politically motivated attacks are called hacktivism. Stanton McCandlish, program director of the Electronic Frontier Foundation describes it as follows: '[a] kind of electronic civil disobedience in which activists take direct action by breaking into or protesting with government or corporate computer systems. It's a kind of low-level information warfare, and it is on the rise'.<sup>542</sup> The main purpose of these activists is to influence or challenge public or enemy opinion and battle for media access and coverage. In many respects, then, the archetypal netwar design corresponds to what earlier analysts called a 'segmented, polycentric, ideologically integrated network' (SPIN):

By segmentary I mean that it is cellular, composed of many different groups...  
By polycentric I mean that it has many different leaders or centers of direction...  
By networked I mean that the segments and the leaders are integrated into reticulated systems or networks through various structural, personal, and ideological ties. Networks are usually unbounded and expanding... This acronym [SPIN] helps us picture this organization as a fluid, dynamic, expanding one, spinning out into mainstream society.<sup>543</sup>

---

<sup>541</sup> Arquilla, J and Ronfeldt, D: (eds) (2001) *Networks and Netwars: The Future of Terror, Crime and Militancy*, California: Rand, p. 15.

<sup>542</sup> Phrack Magazine, vol8, no54, Dec 1998

<sup>543</sup> This SPIN concept, a precursor of the netwar concept, was proposed by Luther Gerlach and Virginia Hine in the 1960s to depict U.S. social movements. It anticipates many points about network forms of organization that are now coming into focus in the analysis not only of social movements but also some terrorist, criminal, ethno-nationalist, and fundamentalist organisations.<sup>543</sup> See Luther P. Gerlach, 'Protest Movements and the Construction of Risk', in B.



The quality of networks contrasts sharply with the tendency to forge social and political order through mutual identifications with leaders, ideologies and memberships in conventional social and political groups. Gerlach applied the SPIN model to contemporary global protest networks. First, he replaced the idea of polycephalous organisation with polycentric order, indicating that, like earlier SPIN movements, global activist networks have many centres or hubs, but unlike their predecessors, these hubs are less likely to be defined around prominent leaders. In addition, he noted that the primary basis of movement integration and growth has shifted from ideology to more personal and fluid forms of association.<sup>544</sup>

Sociopolitical cyberconflict could be seen as taking two forms, one being when proper hackers attack virtually-chosen political targets, the other being when persons organise through the internet to protest, or carry through email a political message. One of the first examples of hacktivism conducted by hackers was back in 1999 when the 24-member Legions of the Underground called for an information warfare campaign against China and Iraq against human rights violations in those countries.<sup>545</sup> However, hackers around the world condemned the initiative by issuing a statement signed by well-known names in the computer

---

B.Johnson and V. T. Covello (eds.), *The Social and Cultural Construction of Risk*, D. Reidel Publishing Co., Boston, Massachusetts, 1987, p. 115, based on Luther P. Gerlach and Virginia Hine: (1970) *People, Power, Change: Movements of Social Transformation*, The Bobbs-Merrill Co: New York.

<sup>544</sup> Bennett, W.L.: (2004) 'Communicating global activism' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York, p. 126



underground such as 2600, the Chaos Computer Club, L0pht, Heavy Industries, Phrack, Toxyn, Cult of the Dead Cow, !Hispahack, Pulhas and several Dutch hackers. The joint statement said: 'Legions of the Underground will do little to alter existing conditions and much to endanger the rights of hackers around the world. Declaring "war" against the country is the most irresponsible thing a hacker group could do. This has nothing to do with hacktivism or hacker ethics and is nothing a hacker could be proud of'.<sup>546</sup>

One kind of online activism is the distribution of email petitions, where each person adds his or her name to a list of names that will then be forwarded to friends and acquaintances. The original email petition then splits into several lists. The result is that if the originator of the petition tries to count the number of people who signed the original list, he or she would have to sift through potentially thousands of duplicate signatures. Also the opportunity for forgery looms large. For these reasons, politicians treat them as dubious. On the other hand, petitions posted on a website show the signer actively logging onto the site and allow the reader more time to engage with the issue. Web-based petitions are utilised more in the activist world, but email petitions contribute to electronic activism in their capacity for getting the word out of dates and times of organised protests, demonstrations and coordinated activities.<sup>547</sup>

---

<sup>545</sup> Glave, G: 'Crackers call off war', wired, 8/1/99

<sup>546</sup> *ibid.*

<sup>547</sup> Lebowitz, R: 'Can Internet technology still revolutionize activism?', Digital Freedom Network

Cronauer has looked at how the use of electronic mailing lists contributed or hindered mobilisation of list subscribers, by examining messages sent through two electronic mailing lists. Specifically, at how groups form their goals and activities; how individuals respond to these online framing efforts; how structural features of electronic mailing lists shape online messages; and how the context such lists are used affect online interactions.<sup>548</sup> Cronauer's two electronic mailing lists, in the course of several months were used to organise opposition and create alternatives to the globalisation agenda pursued and represented through an APEC summit in Canada and both a European Union and a G7/G8 summit in Germany. In both cases local groups formed specifically to protest the respective meetings to exist only temporarily. The mailing lists were, however also used by other groups, including those the newly formed groups came out of, thereby allowing for long-term involvement. She identifies the following aspects of online mobilisation: outreach, networking, increase of visibility, opinion formation, and strategic planning. Even more importantly, she found that electronic mailing lists impact social activist groups in various ways:

they may result in different (be that additional or alternative) means of communication and hence in different ways to communicate; inhibit individuals from becoming mobilised that otherwise may have become mobilised; or prompt

---

<sup>548</sup> Cronauer, K: 'Activism and the Internet: Uses of electronic mailing lists by social activists', University of British Columbia, based on research conducted during the Social Research Council's Program on Information technology, International Cooperation and Global Security in the summer 2001 at the University of Berkeley California, web accessed 11/04



individuals to become mobilised that otherwise may not have become mobilised.<sup>549</sup>

An example of an organised protest through the internet on a small scale occurred in Madrid in November 2002, when the cyberpunks, who gather at the site Ciberpunk, discovered that Gallardon, president of the Community of Madrid, had proposed a law that would classify Madrid's cybercafes as casinos. If the law had passed, minors would not have been allowed in cybercafes, from which roughly 20 per cent of Spain's young internet users connect to the internet. In October, the country passed a law requiring all internet users to register with the government. But Gallardon announced he would not support the law, an action reported in Spanish newspapers as a win for cyberpunks, who credit their victory to the internet and getting non-net users involved. 'The Internet is still a strange land to our politicians, who are not used to facing such an immediate reaction' said activist David de Ugarte.<sup>550</sup>

Tim Jordan writes that social activists or hacktivists have found two uses for the internet, Mass Virtual Direct Action (MVDA) and Individual Virtual Direct Action (IVDA).<sup>551</sup> According to Jordan, MVDA involves the simultaneous use by many people of the internet to create electronic civil disobedience. An example of Mass Virtual Direct Action on the internet is the one organised by the Electronic Disturbance Theatre (EDT). To demonstrate solidarity with the Zapatistas, an

---

<sup>549</sup> *ibid.*



estimated 10,000 people from all over the world participated in the sit-in on September 9, 1998 against the sides of President Zedillo, the Pentagon and the Frankfurt stock exchange, delivering 600,000 hits per minute to each. There are two characteristics of this type of hacktivism. First, hacktions are not aimed at halting a target permanently, but have symbolic dimensions. Second, MVDA activists rarely try to hide their identities, seeking public debate and discussion. IVDA differentiates from MVDA in that it could be taken by an individual and does not depend on a mass protest. The actions taken are either semiotic attacks (i.e. defacements), computer intrusion or attacks on network security.

According to more recent analysis from Jordan and Taylor, hacktivism breaks down into two broader streams of actions:

1. Mass virtual direct actions, which use cyberspatial technologies of limited potential in order to re-embody virtual actions.
2. Digitally correct actions, which defend and extend the peculiar powers cyberspace creates.<sup>552</sup>

As Taylor and Jordan explain, mass action hacktivism is the kind of action most closely associated with the anti-globalisation movement. Here we find the most direct attempts to 'turn' traditional forms of radical protest, such as street demonstrations, into forms of cyberspatial protest. Digitally correct hacktivism,

---

<sup>550</sup> Delio, M: 'Cyber-rights activists log a win', wired.com, 26/11/02

<sup>551</sup> Jordan, (2001), *Mapping Hacktivism*, p.8

consists of online direct actions that are influenced perhaps more by the history and technical concerns of hacking than by the more directly political concerns of anti-globalisation protests.<sup>553</sup> Mass electronic disobedience creates the complex situation in which an embodied presence at a terminal uses direct action to become an abstract virtual presence, which in turn joins with other abstractions to jam up a virtual site. Legitimation comes from the embodied presence, action from the virtual presence.<sup>554</sup>

An example of mass action hacktivism would be the Seattle anti-World Trade Organisation protests at the end of November 1999, which were the first to take full advantage of the alternative media network via the internet. Protestors used cellphones, direct transmissions from independent media feeding directly onto the internet, personal computers with wireless modems broadcasting live video, and a variety of other network communications. As Naomi Klein pointed out in the *New York Times*, this is a movement

born of the anarchic pathways of the Internet... the most internationally minded, globally linked movement the world has ever seen... When protesters shout about the evils of globalization, most are not calling for a return to narrow nationalism, but for the borders of globalization to be expanded, for trade to be linked to democratic reform, higher wages, labor rights and environmental

---

<sup>552</sup> Taylor, P.A and Jordan, T: (2004) *Hacktivism and Cyberwars: Rebels with a cause?*, Routledge: London, p.116

<sup>553</sup> *ibid.*, p.68

<sup>554</sup> *ibid.*, p.170

protection. This is what sets the young protesters in Seattle apart from their 60s predecessors.<sup>555</sup>

During the anti-WTO protests, hacktivists managed to acquire the URL [www.gatt.org](http://www.gatt.org), using the GATT address for a parody WTO site, looking identical to the original WTO one, but included a text criticising WTO trade policies. Another famous hacktion was an MVDA by the Electrohippies, which included a virtual sit-in with a downloadable web page aiming to flood the WTO server. The Electrohippies claim that 400,000 hits in this MVDA had slowed down the WTO and at times completely halted it.<sup>556</sup> The Electrohippies developed what they called a client-side DDOS, whose central feature was that each client or end computer had to choose to initiate the attack on its own, thereby depending on many people to initiate a mass action.<sup>557</sup> Electrohippies Collective 2000 stated that '[w]e have to treat cyberspace as if it were another part of society. Therefore, we must find mechanisms for lobbying and protest in cyberspace to complement those normally used in real life'.<sup>558</sup>

The anti-WTO protesters were able to initiate a newsworthy event, putting the other side on the defensive. Using the internet, they could send stories directly from the street for the whole world to see, rendering the flow of information uncontrollable. Thirdly, they were able to mobilise support by promoting an

---

<sup>555</sup> Kneen, K: 'Battle in Seattle', Rams Horn Article, [www.interweb-tech.com/nsmnet](http://www.interweb-tech.com/nsmnet), accessed 3/10/02

<sup>556</sup> Jordan, 2001, p.8

<sup>557</sup> Taylor, P.A and Jordan, T: (2004) *Hactivism and Cyberwars: Rebels with a cause?*, Routledge: London, p. 77



alternative frame for the event. More recently, in September 2003, during the WTO meeting in Cancun, activists used a peer-to-peer video-sharing service called v2v to transmit broadcast-quality video of the protests to television stations and other activists. They also set up wireless networks at the protest welcome centre in a nearby town, streaming recordings of interviews and speeches over the internet for rebroadcast on participating radio stations. Two tactics were not used in Cancun: the use of Distributed Denial of Service attacks to shut down the WTO site and the 'flash mob' concept, a way of mobilising large groups of people by sending out a single message to awaiting participants. With just 10 per cent of Mexico's population online, it evidently wouldn't work.<sup>559</sup>

There is a debate between hacktivists concerning Denial of Service attacks and web defacements. On the one hand, there are activists who claim that such actions run contrary to other people's right to freedom of speech, and on the other, there are those who view these actions as the only way to get the public's attention. In any case, the fact is that web defacements cannot be dismissed as electronic graffiti and Denial of Service attacks as nuisances, because there is concern by online companies that it could affect share prices, reduce earnings and cause damage to reputation and customer confidence. Indeed, this is the reason why there should be more analysis on the reasoning underpinning hacktivism and its political rationale.

---

<sup>558</sup> *ibid.*, p. 78

<sup>559</sup> Arasavala, A: 'Today's tech-dependent activists', 28/8/03

Real hacktivism is not supposed to be about taking down servers and websites and grafitting webpages. Hacktivism as defined by the Cult of the Dead Cow, the group of hackers and artists who coined the phrase, was intended to refer to the development and use of technology to foster human rights and the open exchange of information.<sup>560</sup> Professor Ronald Deibert from the University of Toronto's Citizen Lab, which sponsors and develops technology used by activists said real hacktivism is fast becoming understood and accepted by mainstream human rights activists and is now being supported by large foundations like the Soros foundation, Markle Foundation and Ford Foundation, which funds groups such as Privatererra, eRiders and Indymedia, which use technology to defend civil rights.<sup>561</sup> Additionally, a network of radical internet service providers has sprung up, including Riseup, Mutualaid, resist.ca, Interactivist, OAT, and others. Radical geeks brought together by antiglobalisation protests and the Indymedia network have developed their own international network of mutual aid, support, skills sharing, free software and solidarity.<sup>562</sup>

A very explicit example of the schism in the hacktivist community between those that support hack attacks and those who believe it to be an infringement of free speech is what happened during the Republican National Convention (August 30<sup>th</sup> through to September 2<sup>nd</sup> 2004). Protest organisers used web sites and printed

---

<sup>560</sup> Delio, M: 'Hacktivism and how it got there', wired.com, 14/7/04

<sup>561</sup> Delio, M: 'Hacktivism and how it got there', wired.com, 14/7/04

<sup>562</sup> Munson, C: 'Seattle Weekly trashes anti-globalization movement', [www.couterpunch.org](http://www.couterpunch.org), 30/11/04



fliers to direct thousands of supporters to rallies and marches. But police also were surfing the web and collecting those same fliers in order to mobilise their own sizable forces. In many cases, police arrived at protest sites well before the demonstrators, pre-empting marches and rallies before they coalesced, using the protesters' own lines of communication to keep most of them well away from Madison Square Garden, the convention site.<sup>563</sup> The Times reported that during the weeklong protests, the police were monitoring websites. Authorities at the highest level of government seem to be paying attention. Just as the week of protests was kicking off, the Justice department announced it had opened a criminal investigation into the New York City Indymedia centre for posting names of Republican delegates.<sup>564</sup>

In addition to the various groups using SMS text messaging to send out action alerts, warnings, news and announcements, the New York Independent Media Center (IMC) set up an automated information line that activists could call 24 hours a day to hear breaking news from Indymedia and to listen to a live streaming broadcast from the A-noise radio collective, which was broadcasting live reports from the streets. The SMS messages alerted activists of routes that remained open to travel to protests when police blocked off large sections of the city. It alerted Indymedia journalists of where cameras were needed to document protests, legal observers of real-time rights violations and activist medic teams of

---

<sup>563</sup> Zucchino, D: 'Internet helps corral protesters', Chicago Tribune, 4/9/04

<sup>564</sup> Scahill, J: 'Indymedia and the text message jihad', [www.counterpunch.org](http://www.counterpunch.org), 9/9/04.



where people were in need of medical attention.<sup>565</sup> In contrast to previous protests Indymedia was not only available to people at home but went mobile. Evan Henshlaw-Path, the Indymedia tech activist who developed the info-line concept has commented:

Our task is to help facilitate horizontal communication and information distribution to all activists in the streets. The police want to keep the protests under control and stay a step ahead of the protesters. So, all of this communications infrastructure helps on a tactical level. We've appropriated technology as an essential tool for radical social change.<sup>566</sup>

Nevertheless the internet was not only used as a resource but also as a weapon, as hacktivists launched a campaign of electronic disobedience to coincide with the demonstrations against the Republican National Convention.<sup>567</sup> They targeted major credit card corporations, disrupting various right-wing fascist groups, and performed an electronic sit-in against Republican websites. Credit card numbers stolen from major news corporations were used by anti-RNC hacktivists to make \$2600 in donations to various humanitarian and civil rights organisations. A right-wing fascist organisation known as ProtestWarrior was also hacked and defaced a week before the convention began: 'By infiltrating and crashing legal, peaceful assemblies, the ProtestWarriors are fighting against the democratic process while

---

<sup>565</sup> *ibid.*

<sup>566</sup> Scahill, J: 'Indymedia and the text message jihad', [www.couterpunch.org](http://www.couterpunch.org), 9/9/04

<sup>567</sup> For examples of protest and hacktivist resources look at [infoshop.org](http://infoshop.org), [crimethnic.com](http://crimethnic.com), [broadleft.org](http://broadleft.org), [thehacktivist.com](http://thehacktivist.com), [electronicdisturbancetheatre.org](http://electronicdisturbancetheatre.org), [hackthissite.org](http://hackthissite.org), [2600.com](http://2600.com),

claiming to uphold the core values of this country'.<sup>568</sup> The cell/home phone numbers, names, addresses, and passwords of the site's lead organisers along with the email addresses of all ProtestWarrior members were posted to the site and emailed out to every member.<sup>569</sup>

The Internet Liberation Front hacked and defaced six Republican websites. These hackers do not believe hacktivism to be a violent tactic. By using direct action techniques such as website defacements and financial disruption, 'hacktivists' believe they are putting pressure and on politicians to make progressive and revolutionary changes:<sup>570</sup>

The will of the people was not expressed in these elections. Imperialist war, tax cuts for the rich, and ecological destruction are not in the interest of working people or the stability of our global society. The Bush administration are rich lying thieves, these inaugurations are a joke, and the whole system is corrupt.

Speaking of protests, on the down side, the epic qualities of the best demonstrations, both in terms of size and drama, are lost in cyberspace. While mass action hacktivism clearly involves symbolic actions, and it can draw large numbers of people together to protest, some of the qualities of a symbolic

---

hbx.us, fromthewilderness.com, and an example of a counterconvention site [www.counterconvention.org](http://www.counterconvention.org).

<sup>568</sup> Indymedia: 'Hacktivism: A week of electronic disruption during the Republican National Convention', [www.indymedia.org](http://www.indymedia.org), 5/9/04

<sup>569</sup> *ibid.*

<sup>570</sup> 'E-activists hack republicans', forwarded from the [e-resistance@yahoogroups.com](mailto:e-resistance@yahoogroups.com), release 18/1/05

demonstration are lost.<sup>571</sup> However, as stated earlier, ‘online protests have the advantage of being able to pass a great amount of information, in forms that mean people can take a little and explore a lot. In non-virtual spaces it is difficult to hand over more than a leaflet, even if volumes could be devoted on the particular cause’.<sup>572</sup> As Taylor and Jordan argue, in the overarching context of virtual times, and born both from hacking and from the anti-globalisation movement of the twenty-first century, hacktivism is perhaps the first widespread social and political movement of the new millennium.<sup>573</sup>

## 4.2 Chinese Dissidents

The stronger the state, the weaker its encouragement of institutional participation and the greater the incentive to confrontation and violence when collective action does break out.<sup>574</sup>

The argument from state strength runs like this: centralised states attract collective actors to the summit of the political system, whereas decentralised states provide a multitude of targets at the base.<sup>575</sup> Gary Marx distinguished repressive actions

---

<sup>571</sup> Taylor, P.A and Jordan, T: (2004) *Hacktivism and Cyberwars: Rebels with a cause?*, Routledge: London, p. 80

<sup>572</sup> *ibid.*, p.80

<sup>573</sup> *ibid.*, p.43

<sup>574</sup> Tarrow, S: ‘States and opportunities: The political structuring of social movements’ in McAdam, D, McCarthy, J and Zald, M (eds.): *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Structural Framings*, Cambridge University Press: Cambridge, p. 46

<sup>575</sup> Tarrow, S: (1998) *Power in Movement: Social Movements and Contentious Politics*, Cambridge University Press: Cambridge, p.81



into different categories according to their specific aims: the creation of an unfavorable public image, disinformation, restricting a movement's resources and limiting its facilities, derecruitment of activists, destroying leaders, fuelling internal conflicts, encouraging conflicts between groups, and sabotaging particular actions.<sup>576</sup>

Direct support for dissidents or embryonic democratic institutions is increasingly available both from the governments and non-governmental organisations of the democratic core. The penetrability of even self-isolated societies is growing, especially when sophisticated transnational 'civil society' groups make it their business to network with the oppressed. Laclau and Mouffe offer a useful way of thinking about discourse and ideology, especially since it does not restrict methodological enquiry, nor necessarily following their own logic. Discourse is 'the structured totality resulting from... practice', when elements are those differences that are 'not discursively articulated' because of the floating character they acquire in periods of social crisis and dislocation.<sup>577</sup>

In a RAND report on the political use of the internet, Chase and Mulveron describe and analyse Chinese dissidents' use of the internet and the Chinese

---

<sup>576</sup> Della Porta, D: 'Social Movements and the state: Thoughts on the policing of protest' in McAdam, D, McCarthy, J and Zald, M (eds.): *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Structural Framings*, Cambridge University Press: Cambridge, p. 65

<sup>577</sup> Howarth, D, Norval, J and Stavrakakis, Y (eds): (2000) *Discourse Theory and Political Analysis: Identities, Hegemonies and Social Change*, Manchester University Press: Manchester and NY, p.7.

government's counter-strategies.<sup>578</sup> The dissidents have used email spamming, set up proxy servers to access blocked sites, set up sophisticated websites, used email lists, bulletin board sites, file trading and e-magazines and a particular group even organised a mass demonstration and a press conference through the internet. Nevertheless, there have been arguments that China will not change, politically until the Chinese people demand change. The internet may help citizens of the People's Republic break free of centuries of kowtowing to imperial rule, but it is not going to cause that rupture by itself.<sup>579</sup>

This report is important for our understanding of how the internet could be used to achieve political aims, because both the dissidents and the Chinese leadership itself have not only realised the political potential of the internet, but as the RAND report indicates, are already engaging in an online battle over the internet, which touches reality as well.

The question the two authors address is whether the internet provides dissidents with new tools that they can use to break through the barriers of censorship and ultimately undermine the power of non-democratic regimes or whether it is more likely that those authoritarian governments will use the internet as another instrument to repress dissent, silence their critics, and strengthen their own power.<sup>580</sup> The main dissident groups examined in the report are the Falungong

---

<sup>578</sup> Chase, M and Mulveron, J: (2002) *You've Got Dissent! Chinese Dissident Use of the Internet and Beijing's Counter-strategies*, Rand: California.

<sup>579</sup> Leonard, A: 'Will the Net save China?', Salon.com, 21/3/02

<sup>580</sup> Chase and Mulveron, p. xi



religious sect, the Chinese Democratic Party (CDP) and the Tibetan community-in-exile.

The Falungong is a religious sect banned in China, whose membership is estimated to be in the millions. It combines meditation with certain quasi-spiritual beliefs.<sup>581</sup> On July 20 1999, hundreds of key members were arrested in the middle of the night, and the next day the sect was banned for allegedly spreading 'superstitious, evil thinking.' In October 1999, Falungong held a clandestine conference in Beijing to tell the world about police beatings of detained members. This conference was attended by foreign journalists, and was again organised through the internet.<sup>582</sup>

Because the sect is banned in China, email is vital for communication and information dissemination. The sect's leader Li Hongzhi, now living in the U.S., has set up email lists to connect followers in the U.S. and China. After his retreat from 'public' life, all his new writings are disseminated through email lists via Minghui Net. Email lists gained even more importance after the Falungong bulletin boards and chatrooms were attacked by the state.<sup>583</sup> The official Chinese news agency, Xinhua, stated in February 19<sup>th</sup> 2004 that a court in western Chongqing had found three men and two women guilty of 'vilifying the

---

<sup>581</sup> In August 2002 the world's leading psychiatric association decided to look into reports that China is silencing political dissidents by confining them to mental wards, where some including members of the Falungong sect are drugged or undergo electric shocks. The group said that among those are nearly 500 members of the Falungong. Thousands of its followers have reportedly been arrested and sent to labor camps. (Greimel, H: 'Psychiatry group hopes to probe Chinese mental wards for dissidents', Aug., 26<sup>th</sup> 2002, Associated Press online)

<sup>582</sup> Chase and Mulveron, p.10



government's image through spreading fabricated stories on persecution of cult practitioners' and had given them prison terms of 5 to 14 years. Reporters Without Borders has called for the release of 22 Falungong members imprisoned for publishing news on the internet about the spiritual movement. 'The crackdown on members of this spiritual movement is completely unjustified. The five Internet users were convicted for posting online what is already very well-known to human rights organisations, that members of Falungong are systematically tortured in prison,' commented Julien Pain, who researches internet speech issues for the group.<sup>584</sup>

The Chinese Democratic Party announced its existence on June 24, 1998. Their formation was timed to coincide with Clinton's visit to China. However, as US-Chinese relations deteriorated, Beijing decided on a crackdown against the CDP and in late December 1998, the CDP's most prominent members, Wang Youcai, Xu Wenli and Qin Yongmin, were sentenced to long prison terms on charges of endangering state security. At least two dozen more CDP members have since been imprisoned, and many others are being held in detention. Despite the crackdown, a number of CDP members remain active on the mainland. The CDP has also developed an organisation-in-exile in the United States.<sup>585</sup> Several CDP members assert that the use of email and the internet was critical to the formation of the party and allowed its membership to expand from about 12 activists in one region to more than 200 in provinces and municipalities throughout China in only

---

<sup>583</sup> *ibid*, p.17

<sup>584</sup> 'Net dissidents jailed in China', *wired.com*, 24/2/04

four months.<sup>586</sup> The Chinese Democratic Party is an example of a sociopolitical group seeking participation, power and democracy using information technology techniques to voice those demands, in a country where power and political participation is only kept for the communist party and where dissidents are arrested and democracy is non-existent.

The third dissident group examined is the Tibetan government-in-exile and its supporters, and more than a dozen associated NGOs. Two-way email communication is an important channel for Falungong members, Tibetan exiles, and various NGOs and human rights advocacy groups to pressure U.S government officials. Nevertheless, one official Chase and Mulveron interviewed opined that because of the vast quantity of email received on a daily basis, the messages have largely lost their effect.<sup>587</sup>

This extract is from an article that represents some of the strong views appearing on Chinese dissident websites: 'Can you establish your own political party? Can you set up a free labor union? Can you freely publish your political ideas? Organise groups? Demonstrate? As long as you don't have those few things, you don't have anything.'<sup>588</sup>

---

<sup>585</sup> Chase and Mulveron, pp.12-13

<sup>586</sup> *ibid*, p.15, the authors cite Farley, M: 'Hacktivists besiege China', Los Angeles Times, January 4, 1999 and Becker J: 'Review of dissidents, human rights issues', South China Morning Post, January 12, 1999.

<sup>587</sup> *ibid*, p.18 interviews with U.S government executive and legislative officials, May-June 2000

<sup>588</sup> 'True democracy, fake democracy or no democracy' by Backgo, posted on the China Popular Marxist Liberal Left wing ideology website.

Other technologies used by dissidents are bulletin board sites and chat rooms. The number of postings to the forums has tended to peak around the time of important events. This is how the authors describe it:

For example our observations indicate that traffic on these sites increased around the time of the diplomatic standoff that ensued after the April 2001 collision of a US reconnaissance aircraft and a Chinese fighter aircraft. In addition, in 2000, the number of postings on such sites surged around the times of the Taiwanese presidential election, Chen Shui-bian's inauguration, the permanent normal trade relations (PNTR) vote in the US congress, and the anniversary of the June 4, 1989, Tiananmen Square crackdown.<sup>589</sup>

Several dissident groups maintain their own BBS. The CDP established more than a dozen Chinese language BBS in May 2000. The Tibetan exile community also makes extensive use of BBS and chat rooms.<sup>590</sup>

In some cases, postings have led to arrests. One example is Fu Lijun, 37, an assistant professor at Xinxiang Medical College in Henan, who was arrested in October 1999 for posting an article in a chat room detailing how Falungong could cure illness.<sup>591</sup> Several other Chinese cyberdissidents are undergoing protracted legal battles over their online writings. A court has rejected appeals on behalf of 4 other people who were each given multi-year prison sentences for expressing

---

<sup>589</sup> Chase and Mulveron, p.21

<sup>590</sup> *ibid*, p.22



themselves in cyberspace. Another online protestor, He Depu, was sentenced to 8 years in prison for his activities in connection with the banned Chinese Democratic Party and for posting supposedly subversive writings on the internet.

The harsh treatment of online dissidents has prompted protests from human rights groups. Robert Menard, the secretary-general of Reporters Sans Frontiers, expressed 'regret that the Chinese authorities have turned a deaf ear to the growing number of voices speaking out in China and abroad against their policy of cracking down on cyberdissidents'.<sup>592</sup> In November 2003, about 500 intellectuals in China and overseas signed a petition urging Beijing to free internet essayist Du Daobin, who was detained for allegedly 'subverting the state administration'.<sup>593</sup> According to Amnesty International's records, by January 2004, 54 people had been detained or imprisoned for expressing their opinions and downloading information from the internet, a 60 per cent increase on the November 2002 figures.<sup>594</sup>

Chase and Mulveron offer us plenty of information on how Chinese students have used the internet extensively in the past five years:<sup>595</sup> during the 1996 Diaoyu Islands dispute; in the aftermath of the accidental bombing of the Chinese Embassy in Belgrade in May 1999; following the murder in late May 2000 of Qiu

---

<sup>591</sup> *ibid*, p.22 the authors cite 'Doctor jailed for promoting Falungong on Internet' <http://www.june4.org/news/database/jan2000/doctorjaled.html>

<sup>592</sup> 'New wave of Chinese net dissident arrests', Information Society News, 18/11/03.

<sup>593</sup> Wo-Lamp Lam, W: 'China pressured over Net dissident', CNN.com, 9/11/03.

<sup>594</sup> 'China: Controls tighten as Internet activism grows', Amnesty International Press Release, 28/1/04.

<sup>595</sup> Chase and Mulveron, p.23

Qingfeng, a Beijing university student; after the April 2001 collision of a US EP-3 surveillance plane and a Chinese F-8 fighter; and following the September 11 terrorist attacks on the United States. During the summer of 1996, renewed friction related to the longstanding dispute between China and Japan over the Diaoyu Islands prompted an outpouring of nationalistic sentiment and unauthorised public protests in China. The students used internet bulletin boards, chat rooms and email to disseminate information not carried in official media and to organise protests. Chinese leaders, worried that nationalistic outbursts could harm Sino-Japanese relations and even be directed against the regime for failing to be more assertive, temporarily shut down internet bulletin board sites at several universities in Beijing and 'advised' the organiser of the protest campaign to leave the capital for 'vacation' in the remote Gansu Province.<sup>596</sup> As for officials in Beijing, BBS offer potential political advantages:

First, there is some evidence to indicate that government officials use popular sites such as the Strong Country forum to gauge opinion on a broad range of domestic and foreign-policy issues. Although the ultimate effects of the Internet remain to be seen there already been significant developments. Indeed in a forthcoming study of the Internet and the development of civil society In China, Guobin Yang argues that through the use of means such as chat rooms and

---

<sup>596</sup> *ibid*, p.23 the authors cite Chen Chiu 'University students transmit messages on defending the Diaoyu islands through the Internet, and the authorities are shocked at this and order the strengthening of control', Sing Tao Jih Pao, Sept 17, 1996, in FBIS, Sept 18, 1996



bulletin board sites, Chinese Internet users “are engaged in the discursive construction of an online public sphere”.<sup>597</sup>

Amnesty International has reported similarly:

Nevertheless, Internet Activism appears to be growing in China as fast as the controls are tightened. Over the last year, there have been signs of Internet users acting increasingly in solidarity with one another, in particular by expressing support for each other online. Such expressions of solidarity have proved dangerous as a growing number of people have been detained on the basis of such postings.<sup>598</sup>

Furthermore, there is a new way dissidents use to communicate their views: email spamming. While to most users spamming is a nuisance, it can enable groups to transmit uncensored information to an unprecedented number of people within China, and to provide recipients with ‘plausible deniability’. The publishers of two Chinese-language electronic magazines, Tunnel (Suidao) and VIP Reference (Da Cankao), have mounted the best-publicised and most sophisticated efforts. Tunnel, the first Chinese e-magazine, is published weekly and is reportedly compiled and edited largely within China, then sent to Silicon Valley, and finally mass-emailed back to the PRC from anonymous, US-based email accounts, such

---

<sup>597</sup> *ibid*, p.27 the authors cite Guobin Young, ‘The impact of the Internet on civil society in China: A preliminary assessment’, p.24

<sup>598</sup> ‘China: Controls tighten as Internet activism grows’, Amnesty International Press Release, 28/1/04



as nobody@usa.net.<sup>599</sup> The editors opine that computers and the internet can be used to 'disintegrate the two pillars of an autocratic society: monopoly and suppression'.<sup>600</sup> The VIP Reference magazine contains articles from Hong Kong, Taiwan and western news sources that are not available to the public in China. The magazine declines to reveal how many mainland subscribers it has, but is reportedly sent to between 250,000 and 300,000 Chinese email addresses. The editors frequently change website addresses and use different email addresses every day to prevent Chinese security services from blocking distribution of their electronic publications. 'We are computer experts, and above all we like the concept of free speech. We are destined to destroy the Chinese system of censorship over the Internet. We believe that the Chinese people, like any other people in the world, deserve the rights of knowledge and free expression', said the Chinese editor of VIP reference.<sup>601</sup>

Moreover, users in China have translated Freenet, which allows people to exchange files over the internet through a shared network, like Kazaa and Gnutella, to Mandarin Chinese and have adapted it for distribution on a single floppy-disk. The reasoning behind this is to use it to share documents the government has been trying to censor, relating to the Tienanmen Square massacre and Falungong.<sup>602</sup> File-sharing networks, using the same technology that gives American music and movie companies fits, can help dissidents communicate.

---

<sup>599</sup> Chase and Mulveron, p.29

<sup>600</sup> *ibid*, p.30, the authors cite Suidao, June 3 1997.

<sup>601</sup> Farley, M: 'Dissidents hack holes in China's new wall', Los Angeles Times, [www.gis.net/~cht/dissidents.html](http://www.gis.net/~cht/dissidents.html).

Since networks like Gnutella and Kazaa have no central source, they are harder to turn off than centralised websites, chatrooms and BBS.<sup>603</sup> Also, numerous efforts are under way in the west to help Chinese web users get around China's censorship of the internet. In 2001, Bill Xia, who left China for the U.S. in the 1990s, and some other U.S.-based volunteers started Dynamic Internet technology. This allows a user inside China to access the internet, not through a system controlled by the government, but through a proxy server. Another idea is to present the Chinese authorities with so many proxy addresses that they would never be able to block them all. The US-based group, [peacefire.org](http://peacefire.org), has adopted this approach.<sup>604</sup>

Often, the use of proxy servers becomes a controversy in itself. For example, Symantec has labelled a program that enables Chinese surfers to view blocked websites as a Trojan horse. Users of Norton Anti-Virus cannot access Freegate, a popular program which circumvents government blocks. Freegate lets users view sites banned by the Chinese government by taking advantage of a range of proxy servers assigned to changeable internet addresses.<sup>605</sup>

Nevertheless, dissidents, Falungong adherents, and Tibetan exiles utilise websites for communication and motivation. The overseas branch of the CDP, Frank Liu, Falungong, and the Tibetan exile community maintain particularly interesting and

---

<sup>602</sup> Jardin, X: 'P2P App's aim: Defend free speech', 29/10/02

<sup>603</sup> 'China dissidents thwarted on net', Associated Press, 27/8/02

<sup>604</sup> 'Bypassing China's net firewall', BBC news, 3/11/04



informative websites. The CDP web page includes links to organisational information, important CDP documents, a publicity department, an invitation to join the CDP, and a variety of BBS forums. It includes a list of members of the CDP's national committee, with links to biographies of the most prominent members.<sup>606</sup> Frank Siqing Liu, director and lone employee of the Hong Kong Information Center for Human Rights and Democracy, maintains a web page that features daily bulletins on arrests of dissidents and practitioners of Falungong, information on workers demonstrations and links updates from a variety of international sources such as the BBC and Radio Free Asia. Liu's website was hacked and the site was replaced with a message that said, 'this site sold to [www.islam.org](http://www.islam.org).'<sup>607</sup>

The Falungong site ([www.falundafa.org](http://www.falundafa.org)), which is bilingual, frequently updated, and well organised, contains messages from the cult's founder Li Hongzhi, links to 26 Falungong sites, a calendar of conferences and events, and audio downloads that enable practitioners to listen to Master Li's lectures from anywhere in the world. Also, Falungong has used text messages to send out thousands of messages, totally undetected. Meanwhile, the Tibetan community-in-exile and its supporting NGOs maintain a sophisticated and informative set of websites around

---

<sup>605</sup> IndyMedia: 'Symantec helps China crush freedom of information', [newswire.indymedia.org](http://newswire.indymedia.org), 14/9/04

<sup>606</sup> Chase and Mulveron, pp.32-33

<sup>607</sup> *ibid*, p.33



the world. The main advocacy sites can be divided between those of officials, supporters and radicals.<sup>608</sup>

These efforts towards political participation by Chinese dissidents mirror both the unprecedented opportunities offered by the internet and communication technologies in general, and the actual pressing need to use them as an alternative information source and coordination network, providing information citizens need to participate in political life and fight for a more open and democratic system.

According to Chase and Mulveron there are five key future trends in dissident use of the internet:

First, in the short term, the Internet will require some human rights NGOs and advocacy groups to change their traditional focus on reporting arrests. Second, it will permit small groups and individuals with limited resources to exert much greater influence than would otherwise be possible. Third, it appears likely that overseas dissidents, and perhaps even mainland dissidents, will engage in more email spamming campaigns in the near future. Fourth, dissidents may increasingly turn to emerging “peer-to-peer” technology to exchange information. Finally, dissidents and other unauthorised organisations will try to find new ways to exploit the Internet’s motivational and organisational potential.<sup>609</sup>

---

<sup>608</sup> *ibid*, pp.33-34, for more details on the categorization of the Tibetan dissidents see also p.35

<sup>609</sup> *ibid*, p.40

In contrast to Chase and Mulveron's findings, administrative assistant Wang Yi, like many of her friends, is aware of the political nuances that can 'scupper' her surfing, but isn't too concerned about the situation.

The truth is most young people are just not that interested (in politics). I want to know how to improve my chances of a good job, others want to chat and find a boyfriend, and many just want to escape from hard studies by playing games like Counter-Strike. Personally, I know no one interested in cyber dissidents. It's just not part of our lives.<sup>610</sup>

This view is also supported by Bobson Wong, an independent researcher based in New York, who says that the majority of Chinese web users are not looking to be cyberdissidents. 'These are not people itching to read CNN. There have been surveys done of internet users in China, and surveys reveal that most internet users in China trust the government'.<sup>611</sup>

Despite the political use of the internet by dissidents, the Chinese government has been able to deal with it effectively using both low-tech and high-tech solutions. Installing advanced telecommunications infrastructure to facilitate reform has complicated internal security for the Chinese government. As Nina Hachigian puts it, the challenge for the regime is to 'prevent this commercial goldmine from becoming political quicksand'.<sup>612</sup> President Jiang Zemin specifically threatened

---

<sup>610</sup> Mackenzie, H: 'Chinese work around net blocking', wired, 26/6/03

<sup>611</sup> 'Bypassing China's net firewall', BBC News, 3/11/04

<sup>612</sup> Chase and Mulveron, p.46, the authors cite Hachigian, N: 'China's cyberstrategy'

computer programmers, along with artists and writers, with stiff jail terms if they 'endanger state security'.<sup>613</sup>

The low-tech solutions employed by the Chinese authorities include the use of informers and surveillance, arrests of internet dissidents, the promulgation of regulations, and, in some cases, the physical shutdown of network resources.<sup>614</sup>

The government also has the ability to search for key words and block sensitive email messages. Several hundreds of thousands of web pages, such as those devoted to Taiwan, the Falungong and foreign news, are blocked by the government. Chinese censors employ filtering technology to block and intercept emails to and from the country's close to 80 million internet users. This is how Paul Mooney of the Herald Tribune describes it:

Beijing has become skilled at hunting down proxy servers that allow users to maneuver around firewalls... Nor are Internet cafés safe havens any longer for exploring the Internet. Cafés in some provinces are experimenting with swipe cards linked to customers' national ID cards. One café manager showed me a back room where a police-linked computer, connected to four spy cameras, monitored users.<sup>615</sup>

---

<sup>613</sup> Farley, M: 'Dissidents hack holes in China's new wall', Los Angeles Times.

<sup>614</sup> Chase and Mulveron, p.49

<sup>615</sup> Mooney, P: 'China's big mamas vs. online dissidents', International Herald Tribune, 23/4/04.



Reporters Without Borders also reported that messages critical of the Chinese government either never appear or are purged from popular chat rooms, while Chinese law enforcement agencies track down and even jail the authors of the messages. The most filtered topics are human rights, Taiwanese independence, pornography, oral sex, SARS, the BBC and the Falungong movement.

A list obtained by the China Internet Project in Berkeley found that over 1,000 words, including 'dictatorship', 'truth', and 'riot police' are automatically banned in China's online forums.<sup>616</sup>

The strategy of the security apparatus is to create a climate that promotes self-censorship and self-deterrence. This is exemplified by the comments of a public security official: 'People are used to being wary, and the general sense that you are under surveillance acts as a disincentive. The key to controlling the net in China is in managing people, and this is a process that begins the moment you purchase a modem'.<sup>617</sup> No one knows exactly how big China's internet police force is, although estimates run as high as 40,000.<sup>618</sup>

Low-tech solutions include shutting down internet cafes, an approach used especially after the Lanjisu fire, but already present. For example, the Ministry of Public Security authorities in Baoding City, Hebei Province, issued new regulations for 100 internet cafes in the city. The regulations announced a 'point

---

<sup>616</sup> New Scientist: 'The "blog" revolution sweeps across China', Special Report from New Scientist Print Edition, [www.newscientist.com](http://www.newscientist.com), 24/11/04

<sup>617</sup> Chase and Mulveron, p. xiii

<sup>618</sup> Mooney, P: 'China's big mamas vs. online dissidents', International Herald Tribune, 23/4/04

system', whereby a café 'allowing a customer to browse "reactionary" information will be deducted 10 points'. If a café loses 30 points within a single year, its license will be suspended for one year.<sup>619</sup>

Following the fire at Lanjisu internet café in Beijing in June 2002 which killed 25 people, the Public Security Ministry closed down 2,400 internet cafes in Beijing, ostensibly for safety reasons. The government ordered all internet cafes to augment their filtering software within weeks and to keep records of all users for a 90-day period. The software prevents access to 500,000 foreign websites, while those attempting to access these banned sites are automatically reported to the Public Security Bureau. Internet police in cities such as Xi'an and Chongqing can reportedly trace the activities of the users without their knowledge and monitor their online activities by various technical means.<sup>620</sup> In March 2002, the authorities introduced a voluntary pledge, entitled, *A Public Pledge on Self-Discipline for the China Internet Industry*, to reinforce existing regulations controlling the use of the internet in China. Over 3000 Chinese internet business users have signed the pledge, including the US-based search engine Yahoo!. In protest against the measures taken by authorities to control freedom of expression, information and association on the internet, a group of 18 dissidents and

---

<sup>619</sup> Chase and Mulveron, p.60 the authors cite 'Eight reactionary activists from Jilin who were imprisoned before call for reversing the verdict on the June 4<sup>th</sup> incident and for government compensation', Hong Kong Information Center for Human Rights and Democracy, June 3, 2000 in FBIS

<sup>620</sup> 'People's Republic of China: State control of the Internet in China', Amnesty International, 26/11/02.



intellectuals published a *Declaration of Citizens' Rights for the Internet* on July 29 2002.<sup>621</sup>

The net police closed almost half of the country's 200,000 internet cafes and installed surveillance software in the rest. In Liaoning province, where 40% of the people who go online do so in internet cafes, software was installed in 7000 cafes to track down web users' online movements and keep records of their names, addresses and ID numbers.<sup>622</sup>

As the Head of Human Rights in China Xiao Qiang explains:

There are new subjects and topics being banned by the government and [internet] users need to come up with new key words or phrases for these topics. While the overall censorship is still effective, the Net has already created a bottom-up force and is constantly negotiating this new space with the old style, top-down censorship and propaganda regime. The transformative effect of the internet has already set China on an irreversible course towards greater openness and public participation in social and political life'.<sup>623</sup>

Government inspectors have checked up on 1.8m cafes since the campaign began, seeking out those letting kids play violent games or access subversive foreign

---

<sup>621</sup> *ibid.*

<sup>622</sup> New Scientist: 'The "blog" revolution sweeps across China', Special Report from New Scientist Print Edition, [www.newscientist.com](http://www.newscientist.com), 24/11/04

<sup>623</sup> Greenberg, A: 'China: Web users get their ten cents worth despite the censors', South China Morning Post, 5/10/05



sites. In addition to the 1,600 cafes closed permanently, 18,000 have been shut down for 'rectification'. The government said that since the summer (2004) 445 people have been arrested and 1,125 web sites have been shut down.<sup>624</sup> Beijing does not actually label sites as 'blocked'. Instead, when a user clicks on a blocked site, the page will begin to down load, slowly, and the user is redirected either to an error message or back to a Chinese search engine.<sup>625</sup>

In one prominent example, email, mobile phone text messaging, and world news coverage that made it to China in part via the internet are widely credited with forcing the central government to go public with the facts and scope of the 2002-3 SARS epidemic.

In addition to traditional methods of control, the Chinese authorities have also made use of high-tech countermeasures, such as blocking websites and email, government-sponsored hacking, monitoring and filtering of email and online propaganda, denial, deception, and misinformation.<sup>626</sup>

Nevertheless, the most effective line of defence in China's internet security strategy is the use of bureaucratic regulations to shape the market environment and the incentives of key participants in ways favorable to the state's interests. Since 1995, the Chinese government has promulgated a blizzard of rules governing nearly every aspect of the internet market. In particular, the 1997

---

<sup>624</sup> Sherriff, L: 'China shuts 1,600 cybercafes', [www.theregister.co.uk](http://www.theregister.co.uk) 1/11/04

<sup>625</sup> McLaughlin, K: 'Internet prods Asia to open up', [www.csmonitor.com](http://www.csmonitor.com), 9/9/04

Public Security Bureau regulation entitled 'Computer Information Network and Internet Security, Protection and Management Regulations' places most of the onus for monitoring, reporting, and preventing anti-regime use of the internet on domestic providers.<sup>627</sup> As a result, ISPs have implemented certain self-censoring policies to avoid trouble with the authorities. According to a January 24, 2000 Reuters story, ISP employees monitor chatrooms and bulletin boards, ferreting out risky political commentary, foul language, and unwanted advertisements. The most recent regulations on the use of the internet were promulgated by the Ministry of Information Industry in January 2002. These regulations require ISPs to maintain detailed records about their users, install software to record email messages sent and received by their users, and send copies of any emails that violate PRC law to the appropriate Chinese governments departments.<sup>628</sup>

Also, authorities at various times have blocked politically 'sensitive' websites, including those of dissident groups and major foreign news organisations such as the Voice of America, the Washington Post, the New York Times, and the BBC. In September 2002, they even banned the search engine Google. Google is hugely popular among China's internet users because of its wide-ranging capacity. A search in English for former President Jiang Zemin's name turns up links to 156,000 websites mentioning him as opposed to a search on Sina.com, which turns up 1,600 mentions of Jiang. The Chinese-language service of Yahoo turns up just 24, largely because Yahoo has offices in Beijing and follows the

---

<sup>626</sup> *ibid*, p.61

<sup>627</sup> *ibid.*, p.57



censorship restrictions. Also, in the case of Google, even if a site is made unavailable by a government or an ISP, Google makes the site available through the cache of pages it photographs as it crawls the web. The fact that numerous news sites especially are blocked by the Chinese authorities indicates that they are not prepared to let access to information - a basic ingredient for citizen participation and democracy - be a democratising force in the People's Republic of China. The dissident groups fighting against censorship and for democracy in China are prosecuted by the state, spied upon, arrested and then given jail sentences of up to 15 years in prison.

Matters became worse for Chinese surfers just before November 2002 Communist Party Congress. State media quoted Jiang in August as telling propaganda officials to create a 'sound atmosphere' for the meeting. Michael Robinson, chief technical officer of Beijing-based Clarity Data Systems, was quoted as saying at the time: '[t]his is a serious escalation. They are not acting as administrators. They are acting as hackers. They are impersonating authority they don't actually have'.<sup>629</sup> The move appeared to have been ordered by public security authorities and implemented locally via internet servers run by the country's fixed phone giant China Telecom. Nevertheless, the battle for Google between Chinese authorities and the country's millions of internet users ended in defeat for the web censors. The censors allowed access to be restored after a complete block on the

---

<sup>628</sup> *ibid.*, p.61

<sup>629</sup> Bodeen, C: 'Search engine Google blocked in China', Associated Press, 3/9/02



site for almost ten days. However, they also put on filters that would refuse searches for President Jiang and other politically sensitive queries.<sup>630</sup>

Blocking certain sites in China is easily done for internet service providers as flipping a light switch. As much as 80 per cent of the country's internet traffic flows through ChinaNet, a subsidiary of China Telecom. 'On balance, we believe that having a service which links that work and omits a fractional number is better than having a service that is not available at all. It was a difficult trade-off for us to make, but the one we felt ultimately serves the best interests of our users located in China', Google said in its blog. The organisation Reporters Without Borders has accused Google of pandering to Chinese interests and filtering its Chinese language site.<sup>631</sup> Bill Xia, Dynamic Internet Technology, a research firm striving to defeat online censorship, suspects that Google is cooperating with the Chinese government's censorship efforts to smooth the way for expansion plans that could help them boost future profits.<sup>632</sup> Although China no longer blocks Google in its entirety, a Chinese user of Google can potentially have a much different experience than one from another country due to China's content filtering practices. Chinese Internet users' access to Google is filtered for specific keywords, and this filtering disrupts Google searches as well as access to the Google cache. The isolation and filtering of the text string 'search?q=cache' suggest that the Chinese state knows how access to Google's cache can be used as

---

<sup>630</sup> Gittings, J: 'Sense and censorship', 17/9/02

<sup>631</sup> Singer, M: 'China's Google block sparks media group's protest', [www.internetnews.com](http://www.internetnews.com), 30/11/04

<sup>632</sup> Associated Press: 'Google bows to Chinese censorship', [www.wired.com](http://www.wired.com), 25/9/04

an ad hoc form of censorship circumvention and has taken steps to limit its accordingly. The fact that other search engines' cache functions are not filtered suggests that China has deliberately targeted Google for filtering.<sup>633</sup>

Most of the government's attempts to prevent the viewing of banned websites use multiple layers of filtering, ranging from the ISP to the network carrier to the non-technical aspects of web surfing in China (e.g. registration with the police, observation by internet café workers). In addition, blocks on websites are often temporarily removed when high-level foreign delegations visit China. During the October 2001 Asia Pacific Economic Cooperation (APEC) meeting in Shanghai, for instance, Beijing permitted access to several websites that are normally blocked, including those of the Washington Post and CNN. This was presumably intended to avoid embarrassing international media reports which would burnish China's image, in order to make a good impression on visiting world leaders. As soon as President Bush and other world leaders left Shanghai however, the websites were once again blocked.<sup>634</sup>

Despite these types of efforts to block sensitive sites, however, the China News Digest (CND) is at the forefront of the promotion of one of the most potent weapons used in fighting website blocking: proxy servers. A proxy server sits between a client application, such as a web browser, and a real server, and, as well as evading blocking, proxy servers are also used to improve performance and

---

<sup>633</sup> OpenNet Initiative: 'Google search and cache filtering behind China's great firewall', [www.opennetinitiative.net](http://www.opennetinitiative.net), 30/8/04



filter requests. The CND website contains a guide to using proxy servers to circumvent firewalls and internet censorship, as well as a call for volunteers to provide CND with additional proxy services. However, Chinese authorities have redoubled their efforts to block access to popular proxy servers.<sup>635</sup> For the moment at least, Beijing has the upper hand in the website blocking battle. Chase and Mulveron cite one activist who recently visited the mainland: '[t]he authorities have become much better at finding and blocking proxies in China; I was there for eight days and experienced eight days of Internet black out'.<sup>636</sup>

Zittrain and Elderman, who did an empirical analysis of internet filtering in China, tracked 19,032 websites that were inaccessible from China on multiple occasions, but while remaining accessible from the United States. The authors concluded (1) that the Chinese government maintains an active interest in preventing users from viewing certain web content; (2) that it has managed to configure overlapping nationwide systems to effectively - if at times irregularly - block such content from users who do not regularly seek to circumvent such blocking; and (3) that such blocking systems are becoming more refined even as they are probably more labour and technology intensive to maintain than cruder predecessors.<sup>637</sup>

---

<sup>634</sup> Chase and Mulveron, p.64

<sup>635</sup> *ibid*, pp.66-67

<sup>636</sup> *ibid*, pp. 69-70, interview Chinese activist, March 2002

<sup>637</sup> Zittrain, J and Elderman, B: 'Empirical analysis of Internet filtering in China', Berkman Center for Internet and Society, Harvard Law School, last updated 20/3/03



Furthermore, Chase and Mulveron argue that there is some evidence to suggest that the Chinese government or elements within it have engaged in hacking of dissident and anti-regime computer systems outside of China. Because of the difficulty in establishing official culpability for hacking attacks without additional evidence, governments can claim a reasonable measure of plausible deniability in these cases. This is how the authors describe it:

The Chinese origin hacking attacks that occurred against Taiwan in August 1999 and against Japan in February 2000 are examples of incidents in which government culpability, either limited or complete, is difficult to determine solely on the basis of the intrusion data. Stronger evidence exists to support the conclusion that the Chinese government or elements within it were responsible for one or more of the China-origin network attacks against computer systems in the United States, Australia, Canada, and the United Kingdom.<sup>638</sup>

In October 2003, it was revealed that a Beijing-based internet company was implicated in creating a program specifically designed to spy on computers of pro-Tibet dissidents. The attempt to spy has been done through sending innocuous-looking messages, purportedly from officials of the Tibetan Government-in-Exile (TGIE) and members of Tibet Support Groups (TSG), with subject matters listing current developments, including a recently held Fourth International Tibet Support Group Conference in Prague. Once attachments to such emails were opened, they planted a Trojan horse on the computer, which

---

<sup>638</sup> Chase and Mulveron, p.71

made its content accessible to the Internet Group in China. These emails came from a Chinese IP and contained attachments of a Trojan horse that can potentially do anything.

This was not the first time that organisations in China have tried to penetrate into the network system of TGIE. Jigme Tsering of the Dharamsala-based Tibetan Computer Resource Centre (TCRC) has revealed that there have been repeated attempts in the past to infect TGIE computers with viruses in order to obtain information. In an interview to the UK internet news site *The Register* in September 2002, Tsering warned that Tibet supporters were being targeted by an unnamed virus which was designed to fool the unwary by posing as an email from the Dalai Lama's office.<sup>639</sup> It is no secret that in addition to forcing ISPs and internet cafes to use filtering software, government minders hand-delete individual messages from discussion boards and change the domain-server records of forbidden sites so visitors are routed to authorised pages.

Another incident indicates how the Chinese government deals with dissidents' use of the internet. Human Rights Watch reported that in May 1998, the Ministry of Labor and Social Security installed monitoring devices at the facilities of ISPs that can track individual email accounts.<sup>640</sup> In January 2000, Liu Ming, the younger sister of student leader Liu Gang, wrote an indictment against the

---

<sup>639</sup> 'Chinese internet group found spying on Tibetan government computers', [www.savetibet.org](http://www.savetibet.org), 28/10/03

<sup>640</sup> Chase and Mulveron, p.82 The authors cite US Department of State, 'China country report on human rights practices'.



Changchun City Public Bureau, which was then disseminated abroad via the internet by Leng Wanbao, a noted dissident in Changchun City, Jilin province. Leng was picked up and interrogated for three hours by the police, who knew about the activity immediately.<sup>641</sup> Chinese authorities have also detained Du Daobin, a civil servant, whose essays are banned by Beijing on the internet, on charges of subversion. Du who works for the municipal medical reform office, signed an online petition calling for the release of fellow cyberdissident Liu Di, a female psychology student from Beijing Normal University who was detained in the capital in November 2002.<sup>642</sup>

In November 2003, a court turned down the appeals of four internet dissidents who were sentenced to up to 10 years in jail for posting their political views. They were arrested in March 2001 after they set up the 'New Youth Association', an academic study group that discussed China's growing social problems.<sup>643</sup> Similarly Li Zhi, a 32-year old local official from Dazhou has been charged with conspiracy to subvert state power, according to the Human Rights in China (HRIC) group. Li frequently expressed his views on online bulletin boards and in chatrooms, and he has also been accused of communicating with overseas dissidents. Liu Qing, the president of HRIC has commented that '[m]onitoring email and internet chat rooms is an unacceptable invasion of privacy, and a

---

<sup>641</sup> *ibid*, p.82, the authors cite 'Report on PRC controlling dissidents' email', Hong Kong Information Centre for Human Rights and Democratic Movement in China, Jan 19, 2000 in FBIS, Jan 19, 2000

<sup>642</sup> 'China locks up Net dissident', Reuters, 31/10/03

<sup>643</sup> 'Cyber activists lose court appeal', South China Morning Post, 11/11/03



reprehensible method of gathering evidence for prosecution of a political crime'.<sup>644</sup>

### The Chinese forums

use a system of filters that enable them to sort the messages to two categories: those containing banned words and the rest. Messages in the first category are systematically blocked... Site Web Masters are supposed to check these blocked messages to establish whether they really need to be censored. But in fact, it is very rare for a message that has been filtered out to be manually restored to the forum.<sup>645</sup>

Some analysts argue that, at least in the short to medium term, the spread of the internet will tend to benefit authoritarian regimes at the expense of dissidents and pro-democracy activists.<sup>646</sup> As Kalathil and Boas observe, for example, China and other authoritarian states have responded effectively to the dissident challenge by implementing a combination of reactive measures, including blocking websites and jailing activists, and proactive policies, such as distributing propaganda online and proffering e-government services.<sup>647</sup> China's proactive efforts to use the internet to bolster regime power, however, have thus far produced only limited results. For example, although Beijing has actively promoted a 'government

---

<sup>644</sup> 'China online dissident charged', BBC news, 24/9/03

<sup>645</sup> Ching, F: 'The Internet dissidents', Globe and Mail, 22/5/03

<sup>646</sup> Chase and Mulveron, p.87

<sup>647</sup> *ibid*, p87, the authors cite S. Kalathil and Boas, T, 'The Internet and state control in authoritarian regimes: China, Cuba, and the counterrevolution', Carnegie Endowment working papers, no 21, July 2001, pp 1;10;15;18

online' plan, a recent survey of e-government initiatives around the world found that China ranked eighty third out of 196 countries.<sup>648</sup>

While Beijing has done a remarkable job of finding effective counterstrategies to potential negative effects of the information revolution, the scale of China's information-technology modernisation would suggest that time is eventually on the side of the regime's opponents.<sup>649</sup> Nina Hachigian predicts that 'control over information will slowly shift from the state to networked citizens', leading to potentially 'seismic' changes.

Interestingly, this is how Chase and Mulveron put it:

The government will not lose the upper hand soon though, because the government's strategy is also aided by the current economic environment in China, which encourages the commercialisation of the Internet, not its politicisation. Thus the Internet, despite the rhetoric of its most enthusiastic supporters, will probably not bring "revolutionary" political change to China, but instead will be a key pillar of China's slower, evolutionary path toward increased pluralization and possibly even nascent democratisation.<sup>650</sup>

The fact that the internet is so hard to control has also given it a role in making other media more open. According to Liu Qing, a prominent dissident who left

---

<sup>648</sup> *ibid*, p.88, the authors cite World Markets Research Centre and Brown University, 'Global e-government survey', Sept. 2001

<sup>649</sup> *ibid*, p.89, the authors cite Hachigian, N, 'China's cyberstrategy'.

China after his release from jail in 1992, and who is now chairman of the US-based Human-Rights in China, '[n]o matter how sophisticated its technology there is no way the government can fully control the internet. That's why in China these days you can see all kinds of organisations and activities springing up, moving the country towards real change'.<sup>651</sup> The latest news of China's censoring techniques is that China is expanding its censorship controls to cover text messages sent using mobile phones.<sup>652</sup>

By the end of October 2004, China had more than 45 large blog-hosting services. Any tech-savvy user can download and install blogging software themselves, bypassing the controls. Blogs play an important role in republishing information as quickly as it is banned from official websites. For example when China's most influential bulletin board Yitahutu (the site had more than 300,000 registered users and 700 discussion forums), was closed down by the net police. After the closure, all the major university bulletins were instructed to delete any discussion of the event. Even the name was censored from Chinese search engines. But the net police found it harder to purge discussion, because bloggers found euphemisms for the event despite key word filtering.<sup>653</sup>

Bloggers in China have had email messages telling them to register or face sanctions. And, according to Reporters without borders, one blogger who

---

<sup>650</sup>ibid, p.90

<sup>651</sup> Luard, T: 'Chinese activists evade web controls', BBCnews Online, 30/1/04

<sup>652</sup> Lim, L: 'China to censor text messages', wired, 2/7/04.



contacted the Shanghai police to register was told there was no point in registering as independent blogs would not be granted permission to continue.<sup>654</sup> By January 2003, China had about 2000 bloggers when, without warning, the Chinese government blocked all access to blogspot.com, the server that hosts all blogs registered on blogger.com. The net police do not make the reasons for such actions public, but Chinese bloggers point out that DynaWeb, an anti-censorship service run by overseas Chinese, had been using a blog on blogspot.com to publish proxy addresses that allowed users to get around the Great Firewall. The authorities' blanket blockade affected all China's bloggers, leaving them suddenly unable to reach their journals.<sup>655</sup>

A study from the Harvard Law School found that the Chinese government has become increasingly sophisticated at controlling the internet, taking a multilayered approach that contributes to precision in blocking political dissent by blocking just specific references to Tibetan independence without blocking all references to Tibet. John Palfrey, one of the researchers of the study sees China as the most successful country in the world to manage to filter the internet despite the fast changes in technology. The testing determined that though some dissidents complain that email newsletters sent in bulk are sometimes blocked, individual messages tend not to get filtered. This is because individual internet

---

<sup>653</sup> New Scientist: 'The 'blog' revolution sweeps across China', Special Report from New Scientist Print Edition, [www.newscientist.com](http://www.newscientist.com), 24/11/04

<sup>654</sup> The Enquirer, 'China forces websites, bloggers to register', 7/6/05, [www.theinquirer.net](http://www.theinquirer.net).

<sup>655</sup> New Scientist: 'The 'blog' revolution sweeps across China', Special Report from New Scientist Print Edition, [www.newscientist.com](http://www.newscientist.com), 24/11/04

service providers, cybercafé owners and discussion forum moderators deploy additional blocking under threat of penalties by the state apparatus.<sup>656</sup>

The Chinese case is closely related to my research and the five research parameters - democracy, participation, power, globalisation and social movements - because these movements are globalised, involve groups that seek participation and power (Falungong), or in some cases, participation, democracy and power (CDP and Tibetan exile community). The information restricted in the Chinese state offline is available in cyberspace, subverting the national boundaries that have in the past helped the Chinese government to control access to information. Despite the fact that the Chinese authorities have been competent in internet filtering and arresting cyberdissidents, ultimately the total control of information spreading through the internet is impossible. This is why cyberdissidents will in the future have more opportunity to voice their viewpoints and coordinate their activities through the net, demanding more participation, more power and definitely more democracy from the Chinese state.

---

<sup>656</sup> Associated Press: 'China's filters strong, subtle', wired.com, 14/4/05

### 4.3 Internet censorship internationally

In its 2004 report 'Internet Under Surveillance', the RSF gave positive grades only to Japan and Taiwan for internet freedom. The US was considering allocating \$100 million to thwart internet censorship by authoritarian regimes with the introduction of a bill that would establish an Office of Global Internet Freedom to foster development of censorship-busting technology for users in countries including China and Saudi Arabia. The bill would allocate \$50 million each for 2003 and 2004. The Bill says: 'With nearly 10 per cent of the world's population now online and more gaining access each day, the internet stands to become the most powerful engine for democratization and the free exchange of ideas ever invented'.<sup>657</sup> The bill cites a catalogue of censorship techniques: surveillance of email and message boards, blocking content based on keywords, blocking individuals from visiting proscribed websites, blacklisting users, and wholesale denial of internet access. An attempt to overcome this is with Six/Four, developed by the Hacktivismo Group, was planned as a full-scale peer-to-peer platform for all internet activities.

Ironically, in June 2002 with the restructuring of the US government, Attorney General John Ashcroft scrapped the guidelines that govern the FBI's conduct, allowing the bureau to monitor websites, public gatherings and religious

---

<sup>657</sup> Wagner, M: 'Fighting net censorship abroad', wired.com, 3/10/02



institutions that are not under criminal investigation. Ashcroft also said that the government would photograph and fingerprint up to 100,000 foreigners entering the country from Arab and Muslim countries. Marc Rotenberg, director of the Electronic Privacy Information Center, commented: 'I think we've reached the point in the debate where we need to ask larger questions about where this administration is taking the US government. Someone needs to apply the breaks or the United States will become a "police state" '.<sup>658</sup> The Congress approved a bill in November 2003 that expands the reach of the Patriot act, shifting the balance of power away from the legislature and the courts, while expanding the power of the FBI to subpoena business documents and transactions without first seeking approval from a judge. Under the PATRIOT Act, the FBI can acquire bank records and internet or phone logs simply by issuing itself a so-called national security letter saying the records are relevant to an investigation into terrorism. The target institution is issued an order and kept from revealing the subpoena's existence to anyone, including the subject of the investigation.<sup>659</sup> A new law officially called the Domestic Security Enhancement Act of 2003, called PATRIOT II by privacy advocates, calls for the creation of a terrorist DNA database, eases laws pertaining to search, seizure and admissible evidence, and would allow the attorney general to revoke the citizenship of any resident who provides 'material support' to terrorist groups.<sup>660</sup> Similar concerns are raised in an EU report released by the European Commission which argues that after the Sept.11 terrorist attacks in the US, 'many governments enhanced their

---

<sup>658</sup> Manjoo, F: 'Do dots connect to police state?', wired, 7/6/02

<sup>659</sup> Singel, R: 'Congress expands FBI spying power', wired, 24/11/03

surveillance powers, but at the risk of affecting privacy'. Phillipe Busquin, the European Union's commissioner for research has stated that 'citizens are not prepared to let privacy be one of the casualties in the war on terrorism'.<sup>661</sup>

An example of the use of state powers against privacy would be when in September 2002 the University of California had to reconsider their decision that would have forced a student activist group to remove from its website a link to a guerilla group accused of being a terrorist organisation. The campus activist group, known as Burn, provided a link which directed visitors to the official site of the Revolutionary Armed Forces of Colombia (FARC), one of the 34 groups on the US government's list of foreign terrorist organisations. Gary Ratcliff, UCSD University Centers director sent the initial cease-and-desist letter to the Che Café Collective, the university group that sponsors Burn, which cites a section of the USA PATRIOT Act that deems it unlawful for any U.S. citizen to provide 'material support or resources' to foreign terrorist organisations. Civil rights groups have heavily criticised the PATRIOT Act, claiming it violates constitutional rights.<sup>662</sup> A UCSD student and member of the Collective who says her name is Allie Katz noted that Burn would not take down the link if the university decided to stand by its initial demand. 'We see this as a free-speech issue,' she said. 'Merely having a link doesn't constitute material support'. Ratcliff responded that '[t]he academic computing department has found that some outside groups have Unix accounts on the Burn server. We're not sure if

---

<sup>660</sup> Delio, M: 'Do privacy fears allow terrorism?', wired, 3/4/03

<sup>661</sup> Wenzel, E: 'More privacy protections needed', Associated Press, 18/11/03



FARC does, but that's why we'd like to talk further with the students'.<sup>663</sup> In April, UCSD officials had succeeded in having the Groundwork Collective, Burn's previous sponsor, remove a link to the PKK. If the university stands by its initial demand and succeeds in having the FARC link removed by way of the PATRIOT Act, the decision could set a precedent for other public institutions looking to eradicate controversial links and sites. Another story relating to academia in the US is the website [www.campus-watch.org](http://www.campus-watch.org), set up by Middle East Forum, a think-tank set up 'to monitor the attitudes of American professors and universities toward Islamic fundamentalism'. What gave the site instant notoriety was its posting of extensive dossiers on eight dubious professors. The students were invited to 'inform' on any other of their teachers who should join the 'treacherous octet!'<sup>664</sup>

Moreover, in contrast with China, which targets political freedom, Saudi Arabia, clamps down on personal freedom, being more concerned about personal morality than political subversion. According to a Harvard Law School study in the Saudi Arabian case, the Saudi government is keeping its subjects from viewing sites about drugs, women and rock-and-roll. The Saudi case is more typical than China's, although a few regimes like China exist, notably Vietnam and the United Arab Emirates which actually attempt to filter their entire national internet traffic wholesale.<sup>665</sup> Ben Edelman, one of the analysts behind the report on Saudi Arabia, has commented: '[i]f you are trying to get into the club of rich, industrialised

---

<sup>662</sup> *ibid.*

<sup>663</sup> Asaravala, A: 'College questioning site's link', Associated Press, 28/9/02

<sup>664</sup> Sutherland, J: 'Campus watch', wired, 7/10/02

<sup>665</sup> Shachtman, N: 'Why countries make sites unseen', wired, 18/7/02



countries, filtering is not something you want to be seen as doing. But you need to be wealthy enough to afford a filtering system. So it's not happening in Africa, for example. There's no money for it'.<sup>666</sup> For the study, Jonathan Zittrain and Ben Edelman tested 64,000 websites, with the full collaboration of the Saudi government. Most other countries are not willing when asked. The Saudis are open about their censorship of the web. If a site is blacklisted, the user is directed to a web page that informs him or her that access is denied, in contrast with China where a surfer simply gets an error message.<sup>667</sup>

Radical Islamic websites are not the only contribution of Islamic faith on the web, as more moderate groups struggle to break the monopoly of the state in setting the political and social agenda. These sites aim particularly to attract younger Muslims by offering a modern interpretation of Islam disseminated by modern or perhaps postmodern technology. Examples of sites include the Cairo-based Islamonline website ([www.islamonline.net](http://www.islamonline.net)), set up by Egyptian Islamist intellectuals with a twenty-four hour news service providing a wealth of information with the objective 'to work for the good of humanity and to support principles of freedom, justice, democracy and human rights'.<sup>668</sup> Also, the Al Shaab newspaper, the mouthpiece of the Islamist-oriented Labor Party, went online after being banned, with the editor publishing fierce criticism of the regime. This resulted in censorship from the state and the site was hacked many

---

<sup>666</sup> Manjoo, F: 'Do dots connect to police State?', wired, 7/6/02

<sup>667</sup> 'Net use is catching on in Saudi Arabia', BBCnews, 31/7/02

<sup>668</sup> Abdel-Latif, O: 'Cyber-struggle: Islamist websites versus the Egyptian state', Carnegie Endowment for International Peace, *Arab Reform Bulletin*, December 2004.

times. Another newspaper of the Muslim Brotherhood, shut down from the Egyptian government, went online ([www.ikhwanonline.com](http://www.ikhwanonline.com)) connecting to audiences home and abroad, and fielding 54 candidates as independents.<sup>669</sup>

Text messaging is also a more recent part of Arab dissent during the past 15 years. Saudi exiles and Islamic activists waged an underground war of faxed pamphlets during the early and mid-1990s. Satellite television channels transformed the images and ideas available to Arab viewers during the same period. More recently, CDs, DVDs and the World Wide Web have dominated underground political publishing in the Gulf.

As Coll writes:

The technology also helps democratic organizers who are often overmatched by the Gulf's authoritarian governments. In a region where formal political parties are banned but loose political societies are often tolerated, text messaging allows organisers to build unofficial membership lists, spread news about detained activists, encourage voter turnout, schedule meetings and rallies, and develop new issue campaigns – all while avoiding government-censored newspapers, television station and websites.<sup>670</sup>

---

<sup>669</sup> *ibid.*

<sup>670</sup> Coll, S: 'In the Gulf, dissidence goes digital: Text messaging is new tool of political underground', Washington Post Foreign Service, 29/3/05

He mentions the example of Kuwaiti women organising protests for voting rights said they had been more effective during their 2005 campaign than during their last serious effort five years ago because text messaging had allowed them to call younger protesters out of schools and into the streets.<sup>671</sup>

And things can get really dangerous for cyberdissidents in these countries. Massoud Hamid, a 29 year-old Syrian journalism student was sentenced to three years in prison for posting photographs on a website. The photos showed a peaceful Kurdish demonstration outside UNICEF's Damascus headquarters. Hamid has already spent 14 months in prison.<sup>672</sup>

In a world wide trend of repressive governments cracking down on internet journalists and dissidents, Tunisia's crackdown on cyber-dissidents took an ominous turn with the arrest and detention of journalist Zouhair Yahyaoui, founder and editor of the online news site TUNeZINE. Better known under the pseudonym Ettounsi ("The Tunisian"), Yahyaoui was charged under clause 2 of Article 306b of the Tunisian criminal code for 'knowingly putting out false news' and also for 'stealing' internet connection time at a local cyber café where he was working. Yahyaoui set up the site in July 2001 to put out news about the fight for democracy and freedom in Tunisia.<sup>673</sup> He published opposition material online and was one of the first people to circulate a letter from his uncle, Judge Mokhtar Yahyaoui, to President Ben Ali, criticizing the country's legal system. Between

---

<sup>671</sup> *ibid.*

<sup>672</sup> Kiss, J: 'Student jailed for web pics', [www.journalism.co.uk](http://www.journalism.co.uk), 14/10/04



May 26 and 28 2002, TUNeZINE organised an online forum on a recent government referendum and the state of the opposition, which drew a large number of participants. The TUNeZINE website, which is hosted in France, has been censored by the Tunisian authorities from the outset, but each week a list of 'proxy' addresses has been available so Tunisians could get around the blockage and access the site. Reporters Without Borders denounced as 'scandalous' Yahyaoui's jailing for two years and four months. His lawyer, who visited him in prison, said he had been slapped and hit on the head while being interrogated. He was undressed and tortured three times by being made to hang by his arms with his feet barely touching the ground. After the last session of this, he revealed the password to his site, which enabled the authorities to block public access to it.<sup>674</sup>

Iran also leads in crackdowns on internet journalists and dissidents according to a report from *The Guardian*.<sup>675</sup> The report specifically cites the arrest of journalist Sole Sa'di following an article he had written online criticising supreme leader Ayatollah Ali Khamenei and the arrest of Mohamed Mohsen Sazegra, the manager of news site alliran.net, as signs that the clerics who run the society will not put up with the relative freedoms that flourish on the internet. Moreover, a number of internet service providers have been shut down, leading to the resignation of the head of the national association of Iranian ISPs in protest.<sup>676</sup>

---

<sup>673</sup> McGrath, D: 'Tunisian Net dissident jailed', Associated Press, 13/7/02

<sup>674</sup> *ibid.*

<sup>675</sup> 'Iran cracks down on internet journalists', Europemedia.net, 10/3/03

<sup>676</sup> 'Iran cracks down on internet journalists', Europemedia.net, 10/3/03

Blogging has served as an outlet for dissent. According to Hossein Derakhshan, a 28 year-old blogger, '[u]ntil there is a free press in Iran again weblogs will flourish. In the last few years about 90 per cent (pro-democracy) newspapers in Iran have been shut down. So people have turned to the Internet to get news.'<sup>677</sup> But the relative tolerance of blogging may be coming to an end, since journalist Sina Motallebi was arrested in Tehran for blogging. According to the Islamic News Agency he has been charged with 'undermining national security through cultural activities' through the content of his blog, as well as in his other writings and the interviews he gave to foreign media outlets.<sup>678</sup> His arrest brought fear to other bloggers, as people have stopped blogging or have censored their blogs by removing any posts that might offend.

Nevertheless, the socio-cultural importance of blogging is substantial. 'The blogs show that [Iranians] are carrying new values and promoting new lifestyles. Older generations try to hide their personal feelings and opinions from others. Individuality, self-expression and tolerance are new values which are quite obvious through a quick study of the content of Persian web logs', Derakhshan said.<sup>679</sup> Similarly REDCAT, a theatre in Los Angeles, has been screening a series of films from Iran's hidden cinema. Underground film-making means that as more filmmakers hit the streets with digital camcoders in their backpacks, the Iranian government may have a hard time tracking them down:

---

<sup>677</sup> Delio, M: 'Blogs opening Iranian society?', wired, 28/3/03

<sup>678</sup> *ibid.*



With the advent of digital modes of recording, a lot of things we thought we knew about repressive regimes and modes of censorship of cinema are not true anymore. With a pocket digital camera you can record professional images, and you can have an editing system at home, so you don't need a permit. And you can walk outside of the country and present these images in the world.<sup>680</sup>

Iran's hardline clerics publicly 'disqualified' more than 2500 reform candidates for Parliament, but could not shut down either the 30 major political websites which are accessible in Iran or the 20,000 Iranian blog sites. The fundamentalists' landslide victory in Iran's Summer 2004 elections might have disheartened western observers, but these alternate channel of communications show signs that the internet has become the most successful way to work around oppression.<sup>681</sup>

Hundreds of Iranian online journals have been protesting against media censorship by renaming their websites after pro-reformist newspapers and websites that have been banned or shut down by authorities. It is thought that the number of Iranian blogs is now between 10,000 and 15,000. Some recent reports have suggested that Iranian authorities are considering the creation of a national intranet –an internet service just for Iran- in an attempt to separate from the world wide web.<sup>682</sup>

---

<sup>679</sup> *ibid.*

<sup>680</sup> Berenice Reynaud quoted in Silverman, J: 'Iran's most wanted: Filmmakers', *wired*, 6/2/04

<sup>681</sup> Thomas, L: 'Electronic resistance: Young Iranians go digital in their quest for freedom', fwd from Smygo list

<sup>682</sup> BBCnews: 'Iran's bloggers in censorship protest', [www.bbc.co.uk](http://www.bbc.co.uk), 22/9/04



Iran has a thriving community of around 46,000 bloggers, but the government has persisted in persecuting people connected with the pro-democracy writing.<sup>683</sup> An imprisoned Iranian blogger Mojtaba Saminejad, arrested in November 2004, after writing about the arrests of three fellow bloggers. He was released on payment of £30,000, but was rearrested for relaunching his blog. In May he went on hunger strike. While in prison his blog was hijacked by hackers connected to the Hezbollah group. The international group Committee to Protect Bloggers organised a day of protest for the blogger and offer campaign banners and advice on writing letters to the Iranian government.

In Iraq, The blog Iraqthemodel.blogspot.com, and reportedly 60 others are bringing to light events and public opinion in Iraq that are not commonly being aired in the conventional media in the United States and elsewhere.<sup>684</sup> While American bloggers have challenged the veracity of major media reports, their Iraqi counterparts are creating a true, free press, online, in their homeland, for the first time in that country's modern history, using internet technology. The blogs are getting 3,000 to 6,000 visits per day – up to 200,000 visitors per month. Another blogger Zeyad, of the HealingIraq.blogspot.com, did reporting on the demonstrations against terrorism last December, which went unreported by the international and local media. Sam, a blogger who runs Hammorabi, reported on his site that Dutch troops who are participating in the coalition have received

---

<sup>683</sup> Kiss, J: 'Bloggers rally to support voice of dissent in Iran', [www.journalism.co.uk](http://www.journalism.co.uk), 18/3/05

many threats to kill them, up to the top level. Some of these threats came as telephone calls to their private phones or as messages inside their mobile phones or to their emails.

Moreover, at least pre-war, the internet was too expensive for Iraqis, with academics and government officials allowed to open email accounts on a monthly fee of \$25 dollars a month, in an nation where a university professor is lucky to earn \$120 a month. Censorship was also present. For example if one typed 'Israel', one got 'Your access has been denied'. A reporter for *Wired* turned the tables when he hacked into Saddam Hussein's email account through his 'send mail to' link on the official Iraq website.<sup>685</sup>

In Afghanistan, where the internet is too expensive for the public to use anyway, viewing is censored by running Net Nanny, a program that allows administrators to block sites, chats and newsgroups, as well as monitor online activity. Despite these measures, motivated users will always find ways around technical mechanisms intended to control their web browsing. Technologies aimed at controlling internet content tend to fail in two different ways. 'Not only are they unable to reliably block access to the forbidden fruit, but they also tend to

---

<sup>684</sup> Koprowski, G: 'The Web: Iraqi blogs building free speech', United Press International, [www.upi.com](http://www.upi.com), 6/10/04

<sup>685</sup> 'Blocked browsing: Iraq censors web surfing for few with Internet access', ABC news, undated



inappropriately block innocent materials, often of social, health, political or other major importance'.<sup>686</sup>

In Pakistan, the military government, as a matter of policy, blocks websites. For instance, they have curtailed access to a Washington-based news website *The South Asia Tribune*, which was launched in 2002 by journalist Shaheen Sehbai. It was blocked by the Pakistan Internet Exchange (PIE), a subsidiary of the Pakistan Telecommunication Company which provides internet bandwidth in Pakistan. The PIE since the beginning of 2003 is denying access to objectionable websites, and also banning internet telephony and voice/chat websites. But technology surpasses such bans, as internet users in Pakistan are logging-on *en masse* to proxy servers, thousands of which are available on the world wide web.<sup>687</sup>

North Korea, in keeping with the country's isolationist, agrarian agenda, has simply rendered internet access illegal. Computers are rare and internet access is almost non-existent, yet North Korea is suspected to have a military academy specialising in electronic warfare, turning out 100 cybersoldiers every year for nearly two decades.<sup>688</sup> Graduates of the elite program at Mirim College are skilled in everything from writing computer viruses to penetrating network defenses and programming weapon guidance systems. In May 2003, South Korea's Defense Security Command raised the issue at a cybersecurity seminar. In fact, the North Korean government would be grossly negligent if it failed to beef up its

---

<sup>686</sup> Weinstein, L: 'Filters, laws won't clean up Net', wired, 16/12/02

<sup>687</sup> Mustafa, W: 'Pakistan's netizens outsmart censors', wired, 4/6/03



information warfare capability, because South Korea, one of the most wired nations in the world, makes no secret that preparing for war is a top military priority.<sup>689</sup>

South Korea, the world leader in broadband access, with more than half the population online, is not above net censorship. In July, two students have been arrested for posting material online that mocked political candidates and others for promoting communism via the web. The government blocked a reported 18,000 web pages last year according to Reporters Without Borders.

Another example of conflict between dissidents and the government occurred in Ukraine, when Ukraine's successor to the KGB, known as the SBU, wanted to take over the top-level domain name. Dmitry Kohmanyuk, a network systems administrator who officially has control of the domain name and runs it with a group of volunteers in the US, said at the time that he would give it up, but only if the new system was based on the internet principle of non-discrimination, and was open to everybody. The reason he did not trust the SBU was because in 2000 Georgiy Gongadze, the founder of a feisty political site Ukrainian Truth, was found murdered outside Kiev.<sup>690</sup>

Also, Burmese dissidents are operating more and more from neighbouring countries such as India, where they use the net to campaign against the military

---

<sup>688</sup> McWilliams, B: 'North Korea's school for hackers', wired, 2/6/03

<sup>689</sup> McWilliams, B: 'North Korea's school for hackers', wired, 2/6/03

government. Aung Naing, editor of the Dhaka, Bangladesh-based Network Media Group has commented that 'online independent news groups have become the window for the international community to peer inside this opaque country'. Burmese dissidents complain that their email systems are always coming under virus attacks.<sup>691</sup>

In South Africa in July 2002, internet professionals accused the government of trying to hijack the world wide web and petitioned President Mbeki not to sign a new bill that would allow the government to take control of the registration and administration of internet domains (website names, addresses and space), and give it free access to information stored on the web.<sup>692</sup> Also, in Zimbabwe, the country's only independent newspaper was relaunched online despite being banned by the government. Production stopped when armed police raided the newspaper's office in Harare. Staff were ordered from the premises and computer equipment was confiscated. Just days after arrest warrants were issued for 45 *Daily News* journalists, Ngunjiri Nderitu, web editor of the newspaper, hoped that the internet would allow them to reach their readership in Zimbabwe. *Daily News* staff moved to Johannesburg to avoid government action, and their website remained active throughout the difficulties.<sup>693</sup>

---

<sup>690</sup> Barton, J: 'Ukraine's domain in dot-dispute', wired, 22/6/01

<sup>691</sup> 'Groups campaign online against Burmese dictators', USA Today, undated

<sup>692</sup> Wagner, M: 'Fighting net censorship abroad', wired.com, 3/10/02

<sup>693</sup> 'Zimbabwe's Daily News battles on-online', dotjournalism, 18/11/03



Another example is Cuba, where, despite the strict censorship of the net (the Cuban government has banned the sale of computers to the public), the government launched a website in September 2002 to refute US charges that it sponsors terrorism and to seek support in the United States for the release of five Cubans imprisoned there for spying. Cuba is still on Washington's blacklist along with Iran, Iraq, Libya, North Korea, Syria and Sudan, for providing a haven for Basque separatist group ETA and supporting Colombian guerillas. The site [www.antiterroristas.cu](http://www.antiterroristas.cu) published an interview with Noam Chomsky, who criticised his country for using the term 'terrorism' only for acts of violence against the United States.

Vietnam is another interesting case in point, where the government spies on internet café customers to prevent them from accessing documents it considers politically and morally objectionable. Vietnamese people living abroad, as well as dissidents inside the country, use the internet to circulate documents critical of the government. There have been cases where people were arrested for posting on the web, such as Pham Hong Son, who was arrested for translating and circulating on the net an article about democracy from a US state department internet site. Internet service providers in Vietnam are responsible for filtering websites, but internet café owners are required to monitor customers as well. The Prime Minister also issued a directive prohibiting all citizens, except top Communist party and government officials, from watching international satellite TV.<sup>694</sup>

---

<sup>694</sup> 'Vietnam to monitor "reactionary" web use', wired, 26/6/02



A report titled *Internet Under Surveillance* by Reporters without Borders in June 2004 summarised the censorship tactics of authoritarian regimes. These are: blocking sites, targeted filtering, modified mirrors (authorities in Uzbekistan change the content deemed unfavourable), prohibiting web-based emailing and owning ISPs, forcing cybercafes users to show IDs, and banning access and equipment.<sup>695</sup>

### *Conclusion*

This chapter examined empirical examples of sociopolitical cyberconflict and dissidents' use of the internet against authoritarian governments. In particular, it looked at the anti-globalisation movement and Chinese dissidents' use of the net, as well as the Chinese government's counterstrategies. The remainder of the chapter included examples of dissidents fighting online against other authoritarian regimes. This showed how widespread both censorship activities by states and attempts to circumvent these controls have become.

The integrated theoretical framework, proposed in section 2.4, urges us to focus on the following parameters when looking at sociopolitical cyberconflicts:

2. The sociopolitical impact of ICTs on:

a. Mobilising structures (network style of movements using the internet, participation, recruitment, tactics, goals), b. Framing Processes (issues, strategy, identity, the effect of the internet on these processes), c. Political opportunity structure (the internet as a component of this structure), d. Hacktivism.

Each of the examples laid out in this chapter can be explicitly linked with these components of the model. The network forms of these groups, like the structure of the internet itself, can be explained as rhizomatic, netwar, or SPIN. Global activist networks have many centres or hubs, but unlike their predecessors, those hubs are less likely to be defined around prominent leaders. Movement integration has shifted from ideological integration towards more personal and fluids forms of association based on weak ties and informal connective structures. This leads to a rhizomatic style of politics which fully realises the organisational and mobilisational potential of internet network structures (see 2a).

The successful protest against an internet regulation in Spain demonstrated the speed of diffusion of protest and the effect of the internet as an informational, mobilisational and organisational tactic (see 2a). The virtual sit-in to demonstrate solidarity with the Zapatistas reflects an impact of the internet on the framing process, using symbolic interplay in cyberspace (see 2b). In the Seattle protests, alternative media were used as part of new communication technologies affecting protest and lobbying in cyberspace and the capture of windows of political

---

<sup>695</sup> Scheeres, J: 'Progress report for net censors', wired, 22/6/04

opportunities (see 2c, 2d). The anti-globalisation movement (Indymedia, anticorporate hacktivism, etc.) are also given fuller attention in section 2.1 above.

Chinese dissidents have used email spamming, proxy servers to access blocked sites, sophisticated websites, email lists, bulletin board sites, file-trading and e-magazines to express their dissent online. Dissident use of the internet exhibits characteristics that are typical of NSM activity. Links between issues raised in this chapter and the proposed theoretical framework include: issues of media sensitivity and event density, a political opportunity structure opened by the internet to allow cyberdissidents to reach international public opinion (online dissent, activism and arrest is extensively reported by foreign media - see 2c), the structure of the online dissident movement (it seems to have no central leadership and looks network-type in character, for example the internet was crucial for recruitment for the CDP party - see 2a), the use of technologically-enhanced tactics, opening up alternative information and coordination networks (see 2b), collective identity (cyberdissidents increasingly show solidarity towards each other - see 2b), and the problematic relationship with the state (there is a crackdown on dissidents by the state). Those using the internet against their governments seek power, participation and democracy, making demands that governments are not only unwilling to provide, but more importantly, which prompt counterstrategies to crack down on these cyberdissidents (see 4d in next component, internet as a medium: medium effects on policy). The internet is therefore a battleground for these opposing interests and it remains to be seen



whether it will develop into a powerful engine for democratisation, or will fall under the pressure and regulation of authoritarian regimes.

#### 4 The internet as a medium:

a. Analysing discourses (representations of the world, constructions of social identities and social relations), b. Control of information, level of censorship, alternative sources, c. Wolsfeld: Political contest model among antagonists: the ability to initiate and control events, dominate political discourse, mobilise supporters, d. Media effects on policy (strategic, tactical, representational).

The anti-WTO protesters were able to initiate a newsworthy event, putting the other side to the defensive. Using the internet they could send stories directly from the street for the whole world to see, rendering the information uncontrollable. Thirdly, they were able to mobilise support by promoting an alternative frame for the event (see 4c).

Dissidents against governments were able to use a variety of internet-based techniques (email lists, email spamming, BBS, peer-to-peer and e-magazines) to spread alternative frames for events and a possible alternative online democratic public sphere (see 4b: alternative sources). A discourse analysis (see 4a) of BBS messages, for instance those asking: ‘‘Can you establish your own political party? Can you set up a free labor union? Can you freely publish your political ideas?

Organise groups? Demonstrate? As long as you don't have those few things, you don't have anything'<sup>696</sup>, shows the determination of dissidents to question the monopoly of the state, the censorship and the repressive structure of Chinese politics, whilst creating an alternative public sphere.

An example of dissidents' use of the internet is spamming e-magazines to an unprecedented number of people within China, a method which provides recipients with 'plausible deniability'. The VIP Reference magazine is reportedly sent to between 250,000 and 300,000 Chinese email addresses. Also, file-trading networks like Kazaa and Gnutella can help dissidents communicate, since they have no central source and would be harder to turn off (see 4b). China has responded effectively to the dissident challenge by implementing a combination of reactive measures, including blocking websites and jailing activists and proactive policies, such as distributing propaganda online and proffering e-government services (see 2d). Also, in the other countries mentioned it is crucial to analyse the effect of government control and censorship (see 4b).

If we take Cronauer's argument on the long term effects and the interlinkage of groups using emailing lists, the effects of networking, recruiting and the development of strategies, then the mobilisation structure is affected greatly by online efforts (2a, 2b, 2c). Hacktivism and its dilemmas are expressed vividly during the RNC protests (2d). Hacktivist attempts at entering the mainstream

---

<sup>696</sup> 'True democracy, fake democracy or no democracy' by Backgo, posted on the China Popular Marxist Liberal Left wing ideology website.



through funding by big foundations and using the internet as a resource on the one hand, and on the other, different fractions within the hacktivist movement insisting on using the internet as a weapon for financial disruption and virtual attacks demonstrations a dilemma that deserves attention in any future discussion or analysis of future sociopolitical cyberconflicts. In terms of the media component (4) the new technological elements of 24 hour coverage, mobile reporting and organizing in protests demonstrate the notion that citizen journalism or open source journalism has entered mainstream. (An undeniable fact if we consider the example of the 7/7 terrorist blasts in London, where 1,000 photos and 20 pieces of amateur video were sent into the BBC news website alone, and even featured in newspaper front pages.<sup>697</sup>) This has potentially media effects on policy (4d), as the immediate coverage can have all sorts of negative and positive effects on the coverage and outcome of the outcome of conflicts.

In relation to China and internet censorship issues (4b) it is obvious that most governments get negative points for the freedom of their citizen's access to the network. Bypassing censorship and using techniques to get banned information or to transmit forbidden information affects media coverage in all these countries and this again can affect policy. Interestingly, the key words or the themes banned in most authoritarian regimes if analysed discursively (4a) point to either desired banned topics and ideologies, such as democracy, participation, revolution, reform etc, or very negative ones, such as massacre, or historical events of

---

<sup>697</sup> Twist, J: 'Mobiles capture blast aftermath', BBCnews, [www.bbc.co.uk](http://www.bbc.co.uk), 8/7/05



oppression, repression and conflict. Online efforts, such as pro-democracy, activist or anti-government websites point to the fact that people believe in the power of the medium enough to organize and run thousands of these sites and in many cases they are able to initiate and control events, mobilize and recruit others for their cause (4c), as in the case of sites in the Islamic world, in China, in Latin America, activist sites for anti-globalisation and single-issue protests and mobilizations both on national and international levels.

This framework for looking at sociopolitical cyberconflict includes the most basic aspects of the phenomenon and it is not suggested as definitive. It is offered as an analytical tool for future students of political conflict on the internet and as a way of opening space for discussion. The next chapter looks at a different type of cyberconflict, focusing on ethnoreligious conflicts, using conflict theory as the theoretical standpoint.

## **Chapter 5: Ethnoreligious Cyberconflict**

This chapter looks at ethnoreligious cyberconflicts, that is, real-world conflicts with ethnoreligious characteristics which spill over into cyberspace, such as the Kosovo conflict, the Israeli-Palestinian conflict, the Kashmir dispute, the Sino-American incident and Al-Qaida on the web. It also includes an assessment of ethnic conflicts and a discussion of whether the internet could be used as a tool of conflict resolution, using examples of particular efforts in the Israeli-Palestinian conflict. The main argument concerning this type of conflict is that the groups involved use the internet not as a resource with which to reframe the issues, but rather as a weapon, like throwing stones. Lastly, the chapter ends by linking these examples of ethnoreligious cyberconflict with the proposed integrated theoretical framework.

### **5.1 Ethnoreligious Cyberconflicts**

#### **KOSOVO**

On the October 20, 1998, the Kosovo Information Centre (KIC), which supports the party of the ethnic Albanian leader, Dr. Ibrahim Rugova, reported that hackers claiming to be members of the Serbian terrorist organisation Crna Ruka (Black Hand) hacked its webpage. The hackers left an image of the Serbian nationalist

symbol and wrote in Serbian and English: '[w]elcome to the Web page of the biggest liars and killers... Brother Albanians, this coat of arms will be in your flag as long as you exist'.<sup>698</sup> After the pages were restored, the hackers came back with a message saying who they were and posting the slogan 'Long Live Serbia'. The same cyber-unit also attacked other Albanian sites and the largest Croatian daily English newspapers. Croatian hackers retaliated by crashing pages of the Serbian National University Library.

Later, in April 2000, more than fifty websites were taken over by Serb hackers. The visitors to high-profile websites such as those of Adidas and Manchester United were surprised to see the image of a double-headed eagle, with the slogan 'Kosovo is Serbia'. Also hacked were the Albanian site Kosovapress and the Albanian newspaper *Koha Ditore*, as well as the Serbian Ministry of Information and Bosnian, Croatian and Yugoslav sites. The Serbian Ministry of Information said that sites of Yugoslav providers, political parties and firms were attacked in a synchronised manner.<sup>699</sup>

The technical director of WebDNS, a domain monitoring company, also commented that the attack was part of a sustained campaign. The way he explained it was that the hackers replaced the contact details in Network Solutions, under which most of the sites were registered, by transferring the contact addresses to a Yugoslav site and then to an Albanian one. They probably

---

<sup>698</sup> 'War of words on the Internet', BBC on line, 25/10/98



tricked Network Solutions by sending an email requesting a change of address and pretending to be from the companies that were hacked.

During the same conflict, but concerning different players, US defense officials said on November 8<sup>th</sup> 1999 that the Pentagon refrained from unleashing an all-out computer attack on Serbia, because they were uncertain about the legal implications of launching the world's first cyberwar. They claimed that, in theory, they had the capacity to hack Milosevic's bank account and plunder Serbia's financial system. Furthermore, in May 1999, the Pentagon issued a fifty-page booklet of guidelines for waging cyberwar called 'Assessment of International Legal Issues in Information Operations', which the Defense Department had been preparing since the first cyber-offensive used in Haiti in 1994. The report considers that information operations would be legal 'weapons' in the traditional law of war, thus rendering cyberattacks on civilian targets like universities or financial infrastructure a war crime. John Arquilla, a cyberwar expert at the Naval Postgraduate School in California, and Martin Libicki, a researcher on cyberwarfare for the Rand Corporation think-tank in Washington, both think that the Pentagon spied on Serbian computers, but did not attack them for strategic reasons.<sup>700</sup>

Despite these instances of cyberwarfare, the real novelty of the use of the internet during the Kosovo conflict was the amazing amount of emails sent to news

---

<sup>699</sup> 'Serb hackers on the rampage', BBCOnline, 14/4/00

organisations from the people in the region. As Chris Nuttal comments, '[i]f someone could write a program quickly enough, it should be possible to collate them from all over the Net and automatically build up an interactive map of Yugoslavia linking to accounts of the bombings town by town.'<sup>701</sup>

The Kosovo conflict is considered the first major conflict where cyberwarfare was used. NATO admitted that its website was blocked due to a bombardment of automated requests for information. During the bombing campaign, NATO web servers were subjected to sustained attacks by what NATO suspected were hackers in the employ of the Yugoslav military.<sup>702</sup> The attacks, which included 'ping saturation' (denial of service attack where a target computer is overwhelmed with ping requests) and email viruses which brought NATO servers to a halt for a number of days. The attacks caused serious disruptions in the communication infrastructure of the organisation.

## ISRAEL-PALESTINE

The increasing importance of cyberconflict is indeed very evident when it reflects conflicts belonging to the real world. In October 2000, Israeli and Palestinian hackers engaged in adversarial hacking when the prolonged peace talks between the two parties broke down. Until the beginning of November 2000, groups

---

<sup>700</sup> Borger, J: 'Pentagon kept lid on cyberwar in Kosovo', Washington Guardian, Guardian Unlimited, 9/11/99

<sup>701</sup> Nuttal, C: 'Kosovo – the Internet war', BBC online, 16/4/99



supporting either side in the conflict limited their online activities to defacements and Denial of Service attacks against websites affiliated with the Palestinian movement or Israeli nationalists. One example was when an Israeli flag, Hebrew text and a piano recording of 'Hatikva', the Israeli national anthem, appeared on the Hezbollah home page.<sup>703</sup> Also, Palestinian hackers created a website called Wizel.com - a host for a FloodNet attack, a type of attack which reloads a targeted web page several times, rendering the site inoperable. The reaction was a sustained counterattack from pro-Palestinian 'cybersoldiers' from the US. The websites of the Israeli Army, Foreign Ministry and Parliament, among others, were attacked. Targets also included financial institutions, as a result of which, e-commerce sites crashed and there was an economic impact reflected in the Israeli stock market.<sup>704</sup>

The situation escalated in the first days of November 2000, when an anti-Israeli hacker attacked the website of one of Washington's most powerful lobbying organisations, the American-Israeli Public Affairs Committee (Aipac). Fred Cohen, a computer-security professor, commented at the time: '[w]hen you talk about war, you are talking about turning off the constraints that hold back people. You have people who want to break into computers, and now they have an excuse - they can do it for a cause'.<sup>705</sup> The hackers published critical emails downloaded from Aipac's own databases and credit card numbers and email addresses of

---

<sup>702</sup> Messmer, E: 'Serb supporters sock it to NATO and U.S computers', Network World, 5/4 /99

<sup>703</sup> Hockstader, L: 'Pings and e-arrows fly in Mideast cyber-war', Washington Post online, 27/10/00

<sup>704</sup> *ibid.*



Aipac members. After the FBI was informed, the members of the organisation, including a Republican Senator, were advised to cancel their credit cards and monitor their accounts. The hackers wrote that '[t]he hack is to protest against the atrocities in Palestine by the barbaric Israeli soldiers and their constant support by the US government'.<sup>706</sup> Aipac spokesman Kenneth Bricker said at the time that the hackers downloaded credit card numbers and about 3,500 names and web addresses from people who had contracted Aipac's website. The broadest list of the organisation's 55,000 members was stored in a separate computer system and was not compromised.

The Israelis were not slow to retaliate. According to MAGLAN, an Israeli information warfare research lab, an Israeli supporter, 'Polo0', posted Palestinian leaders' cell phones numbers, as well as information about accessing the telephone and fax systems of the Palestinian Authority, plus 24 different websites, 15 IRC channels and an IRC server through which the Palestinian movement communicates. Analysis by iDefense, a security monitoring agency, considered a number of key players in the cyber conflict. On the Israeli side the wizel.com creators, a.israforce.com, Smallmistake and Hizballah attacked Palestinian sites.

On the Palestinian side there is Unity, a Muslim extremist group, one of the forerunners of what is referred to as e-jihad or cyberjihad. Unity attacked the Tel Aviv Stock Exchange. Later they announced that their strategy was four-phased.

---

<sup>705</sup> Lemos, R: 'Hactivism: Mideast war heats up', zdnet.com, 6/11/2000

<sup>706</sup> 'Israeli lobby group hacked', BBCOnline, 3/11/00

Phase one included crashing official Israeli government sites, phase two hit the Bank of Israel and phase three targeted the Israel ISP infrastructure, Lucent and Golden Airlines, and an Israeli telecommunications provider. They also said that they would not realise phase four, the destruction of e-commerce sites, but added: '[w]e warn the Zionists and their supporters that any attempt to touch any Anti-Zionist site will be faced with phase four of the cyberwar - causing millions of dollars in transactions'.<sup>707</sup> Unity also claimed in an email in February 2001 to have successfully attacked AT&T in retaliation for the company doing business - as a back-up in case of emergency - with the Israeli Defense Force, claiming to have blocked the site for seventy-two hours in a particular hit.<sup>708</sup>

What distinguishes this cyberconflict from past ones is that it has moved beyond being a game controlled by a few highly-specialised hackers into being a full-scale action involving thousands of Israeli and Arab youngsters sending racist and occasionally pornographic emails to their opponents while circulating for their supporters a range of website addresses with simple instructions on how to crush the enemy's electronic fortresses.<sup>709</sup> One site offered a menu of targets to attack, including the sites of Hezbollah, the Palestinian National Authority, Hamas and a dozen others.<sup>710</sup> The site encouraged users to click on the targets they would like to disable and offered a set of simple instructions for executing the assault. The whole process did not take more than a minute or two and generated multiple and

---

<sup>707</sup> Gentile, C: 'Hacker war rages in Holy Land', Wired News, 8/11/00

<sup>708</sup> Galvin, J: 'Cyberwars bring real world conflict to the Web', ZDNet, 20/2/01

<sup>709</sup> Hockstader, L: 'Pings and e-arrows fly in Mideast cyber-war', Washington Post online, 27/10/00



high-speed attacks. IDefense's director of intelligence production Ben Venzke thinks that the Palestinians won this particular battle in cyberspace, because according to him, there are people on the Palestinian side trying to learn how to hack overnight to join the effort.<sup>711</sup>

The political crisis in the beginning of 2002 in the Middle East spawned another increase in defacement attacks on Israeli Web servers. Israel was the victim of 10 out of 15 significant web defacements in the Middle East over the first two weeks of April 2002 according to security consultancy mi2g. Mi2g reported Israeli websites with the 'il' domain were defaced 413 times in 2001- up 220 per cent from the year before - and Israel has been the biggest victim of web defacements over the past three years, suffering 548 of the 1,295 attacks in the Middle East. The most active anti-Israeli hacker group claims to be Egyptian and started its activities just after 9/11.<sup>712</sup>

## INDIA-PAKISTAN

Also, sympathisers on both sides of the Kashmir conflict (in northwestern India) have used cyberattacks to disrupt each other's computer systems and to disseminate propaganda. One of the first moments of cyberwarfare in the region was reported on October 16, 1998 by the Indian news agency PTI. Suspected Pakistani intelligence operatives had hijacked the Indian Army's only website,

---

<sup>710</sup> *ibid.*

<sup>711</sup> Hershman, T: 'Israel discusses "Inter-Fada"', Wired News, 29/6/01.



‘Kashmir: A Paradise’, which gives the Indian view on Kashmir. The site was set up a month earlier as counter-propaganda to the dozens of sites supporting Muslim Kashmiris seeking independence. The hackers had put up information on alleged torture of Kashmiris by the Indian security forces. The attack came at the time when Indian and Pakistan began talks in Islamabad in an effort to ease tensions. The Pakistani hackers dedicated the ‘new’ site to ‘all the Kashmiri brothers who are suffering the brutal oppression of the Indian army’.<sup>713</sup> The photographs of the site were overwritten with the slogans: ‘Stop the Indians’ and ‘Save Kashmir’. Pictures showing Kashmiris allegedly killed by Indian forces were posed under headings such as ‘massacre’, ‘torture’, ‘extra-judicial execution’ and ‘the agony of crackdown’. A government statement said the hackers changed the site parameters so that visitors were diverted to a different server.

Among the propaganda on the site, there was also a guest-book where visitors can leave comments. Two typical responses from the opposing sides were: ‘[t]his website is very biased and very unfair to the Pakistani point of view. This is just a whole charade by the Indians and 80% of it is absolutely untrue!’ (Pakistani), and ‘[a] whole hearted salute for my brothers fighting for our country with a religious maverick enemy’ (Indian).<sup>714</sup>

---

<sup>712</sup> Leyden, J: ‘Middle East conflict spills over into cyberspace’, the Register, [www.mi2g.com](http://www.mi2g.com).

<sup>713</sup> ‘Indian Army website ambushed’, BBC online, 16/10/98

<sup>714</sup> Nuttal, C: ‘India opens virtual front in Kashmir’, BBC online, 5/10/98

In March 2000, the cyberconflict escalated when a group of Pakistani hackers defaced 600 websites and temporarily took over government and private computer systems. The majority of the sites were hacked after the Pakistanis broke into IndiaLinks, India's largest internet service provider. The team responsible, the 'Muslim On Line Syndicate', were described by their spokesperson as a group of nine ranging from 16 to 24 years of age.<sup>715</sup> Their spokesman also described their operations as taking control of a server, then defacing the site, after they have no more use for the data or the server. Their message was: '[w]e hope to bring the Kashmir conflict to the world's attention... We wish that our Muslim brothers will be given the right to choose, as was promised them half a century ago'.<sup>716</sup>

The number of Pro-Pakistani defacements of Indian websites has increased dramatically between 1999 and 2001: 45 in 1999, 133 in 2000 and 275 by the end of August 2001.<sup>717</sup> However, the assault on Pakistani sites has not been as successful. There were reports that Indian hackers have repeatedly tried to hack the Pakistani newspaper *Dawn*, without any result. Nevertheless, they have left messages to their Pakistani counterparts like 'keep your hands off Indian sites', threats of 'breaking the Internet backbone' of Pakistan and claims that 'India is the superpower of Information Technology'.<sup>718</sup>

---

<sup>715</sup> Hopper, I: 'Kashmir conflict continues to escalate on line', CNN.com, 20/3/00

<sup>716</sup> *ibid.*

<sup>717</sup> 'Pro-Pakistan hackers deface centre's venture capital site', The Statesman, 21/8/01

<sup>718</sup> Joseph, M: 'Both sides hacked over Kashmir', wired, 23/12/00

More recently, an email worm in March 2003 appeared to be yet another salvo in a yearlong war between Indian and Pakistani hackers. According to the Indian Snakes, authors of the worm known as Yaha, it was written to retaliate against Pakistani hackers, who the Snakes said were defacing websites in India. Yaha variants have been around the net for over a year. It began its life as a standard mass-mailer worm. Political messages first appeared in its E variant, released in June 2002, which attempted to launch elementary Denial-of-Service attacks against the Pakistani government's primary website. Yaha.Q attempted to launch a Denial-of-Service attack against five Pakistani sites, changing user settings on infected machines and containing a number of messages directed at Pakistani hackers, other virus writers and an anti-virus researcher.

Virus writers often use their creations to make a point, but very few are overtly political. Another example of a politically-motivated virus attack was the Lion worm of 2001, which was, according to its author, intended to chastise Japan over the issue of Japanese textbooks that implied that the Japanese occupation of China and Korea was justified and beneficial to the occupied countries.<sup>719</sup>

## **US-CHINA**

Another example of ethnoreligious cyberconflict is the Sino-American cyberconflict which emerged during an international diplomatic incident. A US



spy-plane made an emergency landing on Chinese soil on April 1<sup>st</sup> 2001 after colliding with a Chinese fighter jet over the South China Sea, in a collision which killed the Chinese pilot. After this incident, Chinese hackers vowed to attack US sites, a threat which led hackers in the US to retaliate. According to UK computer security firm Mi2g, the Honkers Union of China hacking groups defaced 80 websites and the Americans defaced more than 100 during April 2001.<sup>720</sup> China's remote sensing satellite ground station was overwritten with a picture of a mushroom cloud, while in the US, the White House historical association was plastered with Chinese flags as were the departments of Health, Navy, Labour and the House of representatives' email servers.

On May 9<sup>th</sup> 2001, Chinese hackers boasted they had defaced 1,000 US websites, but called a truce to the conflict. A statement by the Honker Union of China said that, having attacked 1,000 sites, they had reached their goal, and that any attack from that point on had no connection with them. Their American counterparts broke into hundreds of Chinese sites, leaving messages such as, '[w]e will hate China forever and will hack its sites'.<sup>721</sup> After a meeting online between the Honkers Union and the Chinese Red Guest Network Alliance, it was decided that their attack would last a week, ending on May 7<sup>th</sup>, the two-year anniversary of the bombing of the Chinese embassy. They decided to keep the destruction of business websites to a minimum and attack government websites instead. They said that the point of the attack was to encourage people in the US to protest

---

<sup>719</sup> Delio, M: 'Virus uses netizens as pawns', wired, 13/3/03

<sup>720</sup> Left, S: 'Chinese and American hackers declare "cyberwar"', Guardian unlimited, 4/5/01

against their government and demand peace between nations. One hacker said: '[t]he U.S. wants the world to go to war. All people cherish peace, but the mildew dog government of the U.S. wants war. We will attack to send a message to the people of the U.S., to tell them we are all one, but they must stop their government from destroying the world'.<sup>722</sup>

Attacks that were discussed on an Internet Relay Chat during their meeting included defacing websites, emailing viruses to U.S. government employees and flooding computers with garbage data. A US hacker collective dubbed Project China left this message on a Chinese site: 'Get ready to meet a strike force with strength the world has never seen before! We are going for all-out cyberwarfare on your gov.cn boxed and every box that you fucks haven't secured!'.<sup>723</sup> The Xinhua News Agency reported at the time that U.S hackers had defaced the websites of the provincial governments of Yichun, Xiajun and Beijing, the Deng Xiaoping Universities, as well as the Samsung and Daewoo Telecom sites in South Korea. A South Korean government security agency blamed the Sino-US cyberwar for the 164 cyberattacks on South Korean websites that had occurred during that time. Computer analysts said that American and Chinese hackers were using Korea to get into rival countries' computer systems without revealing their identities, because S.Korea has extensive links with both countries.

---

<sup>721</sup> 'Chinese hackers halt Webwar, say 1,000 U.S sites defaced', Globe Technology, 10/5/01

<sup>722</sup> Delio, M: 'It's cyberwar: China vs US', Wired news, 30/4/01

<sup>723</sup> Left, S: 'Chinese and American hackers declare cyberwar', Guardian unlimited, 4/5/01



Interestingly, the Chinese government has been quite open about its future strategic military objective. In the spring 2001 issue of *China Military Science Journal*, a member of the Chinese Committee of Science, Technology and Industry of the System Engineering Institute wrote,

We are in the midst of a new technology in which electronic information technology is the control technology. The technology provides unprecedented applications for the development of new weaponry... Military battles during the 21<sup>st</sup> century will unfold around the use of information for military and political goals.<sup>724</sup>

This is hardly surprising. As we have seen in section 4.2, the Chinese government has placed heavy and detailed regulations on the internet, has arrested 25 people the past two years due to their online activities, has closed down thousands of internet cafes, and has blocked thousands of sites. Reportedly, elements of the government have also hacked sites belonging to dissident groups.

## **AI-QAIDA ON THE WEB**

The size and the structure of the internet provides virtual sanctuary. The internet provides the glue that links groups that operate within the ancient modes of organic order – religious, tribal, etc. that form the backbone of the physical world sanctuary, with the modern world's operational environment. However, the

---



internet is more than merely a communications medium, it is a place of sanctuary in itself.<sup>725</sup>

Most militant groups now rely on the web to recruit new adherents. Terrorist groups rely increasingly on internet chat rooms, more anonymous than traditional websites. Gabriel Weiman, a professor at University in Haifa in Israel, began tracking terrorist-related web sites eight years ago, he found 12; today there are more than 4,500.<sup>726</sup>

The web's growing centrality in Al-Qaida-related operations has led such analysts as former CIA director John E. McLaughlin to describe the movement as primarily driven today by 'ideology and the Internet'.<sup>727</sup> The web's shapeless disregard for national boundaries and ethnic markers fits exactly with bin Laden's original vision for Al-Qaida, which he founded to stimulate revolt among the worldwide Muslim ummah, or community of believers.

It was said that the Hamburg cell around Muhammad Atta, one of the presumed suicide pilots, was systematically using the internet to organise the 9/11 attacks.<sup>728</sup> For security reasons, these individuals rarely used their private PCs from home, but more often visited internet cafes. The US intelligence agencies came to this

---

<sup>724</sup> Chepsiuk, R: (2001) 'Get ready for cyberwars', ncmonline, 23/8/01.

<sup>725</sup> 'Global guerrillas and temporary autonomous zones', forwarded from [e-resistance@yahoogroups.com](mailto:e-resistance@yahoogroups.com), posted on 20/8/04, accessed 27/12/04

<sup>726</sup> Coll, S and Glasser, S: 'Terrorists turn to the web as base of operations', Washington Post, 7/8/05, accessed 16/8/05

<sup>727</sup> *ibid.*

conclusion when they arrested the alleged mastermind of the attacks, Abu Zubayda, and put his personal computer through the hoop. In it, they found a large number of encoded messages – the last ones having been sent on Sept. 9. Vince Cannistraro, the former head of the CIA's counter-intelligence unit once said: 'Internet communications have become the main communications system among Al-Qaida around the world because it's safer, easier and more anonymous if they take the right precautions, and I think they're doing that'.<sup>729</sup>

In November 2001, as the Taliban collapsed and Al-Qaida lost its Afghan sanctuary, Osama bin Laden biographer Hamid Mir watched 'every second Al-Qaida member carrying a laptop computer along with Kalashnikov' as they prepared to scatter into hiding and exile.<sup>730</sup> On the screens were photographs were photographs of Sept. 11 hijacker Mohamed Atta. With laptops and DVDs, in secret hideouts and neighbourhood internet cafes, young coding jihadis have sought to replicate the training, communication, planning and preaching facilities they lost in Afghanistan with countless new locations on the internet. Al-Qaeda suicide bombers and ambush units in Iraq routinely depend on the web for training and tactical support, relying on the internet's anonymity and flexibility to operate with near impunity in cyberspace. In Qatar, Egypt and Europe, cells affiliated with Al-Qaeda that have recently carried out or seriously planned bombings have relied heavily on the internet. Al-Qaida's innovation on the web

---

<sup>728</sup> Aliefudien: 'Al-Qaeda, big brother, and cyberspace', Tehran Times, 26/12/04

<sup>729</sup> *ibid.*

<sup>730</sup> Coll, S and Glasser, S: 'Terrorists turn to the web as base of operations', Washington Post, 7/8/05, accessed 16/8/05



‘erodes the ability of our security services to hit them when they are most vulnerable, when they are moving’, as Michael Sheuer, former CIA chief of the unit that tracked bin Laden explains. ‘It used to be they had to go to Sudan, they had to go to Yemen, they had to go to Afghanistan to train. An Al-Qaida operative ‘no longer has to carry anything that is incriminating. He doesn’t need his schematics, he doesn’t need his blueprints, he doesn’t need anything that is incriminating’. Everything is posted on the web or ‘can be sent ahead by encrypted Internet, and it gets lost in the billions of messages that are out there’.

731

Al-Qaida militants have defied a crackdown and the loss of senior leaders in Saudi Arabia by using the internet to win over new recruits in Osama bin Laden’s birthplace.<sup>732</sup> Despite the killing of top contributors, including one of its leading web magazine editors Issa Saad bin Oshan, the group has continued to publish its two widely distributed magazines regularly for the past year. Paul Eedle, a London based analyst who closely follows Qaeda sites explains it as follows: ‘This shows how a small group can continue a campaign using the Internet. Before the days of the Internet a group would pretty much fade from view if they were reduced in numbers like Al-Qaida in Saudi Arabia’.<sup>733</sup>

The group ‘Al-Qaida in Mesopotamia’ after an attack on a hotel in central Baghdad, released an internet statement claiming credit, while one group even

---

<sup>731</sup> *ibid.*

<sup>732</sup> Reuters: ‘Al-Qaida defies Saudi manhunt with high web profile’, 16/11/04, accessed 18/11/04



released its own videotape of the bombing, along with statements explaining why and how it chose that target. Within hours, all of it was appearing not only in Arabic websites and chat rooms, but also on television stations and even in some Western news reports.<sup>734</sup>

It's an all too familiar ritual, hours after an attack on an American convoy or an Iraqi police patrol, a brief statement begins appearing on Islamist web sites claiming it was carried out by fighters loyal to Abu Musab al-Zarqawi.<sup>735</sup> Everyday messages appear on the web offering encouragement to resistance fighters. Zarqawi's group started an internet magazine, complete with photographs and 43 pages of text. According to Michael Doran, a professor of Near East Studies at Princeton university who monitors traffic on Islamist web sites and chat rooms the magazine is partly a reaction against the Arab state media, which often misrepresent terrorist attacks like any other Qaeda-linked web publications. Other Islamist groups are joining the effort, including one calling itself the Jihadist Information Brigade.

Maaskar al-Battar (al-Bataar Training Camp), a jihadi online publication, with motivational material interwoven with military training input, which has ceased publication was aimed at building a jihad culture among Muslim youth and to equip them to fight against those who have 'invaded the Islamic world'. With

---

<sup>733</sup> *ibid.*

<sup>734</sup> Worth, R.F: 'Jihadists take stand on web, and some say it's defensive', The New York Times, 13/3/05

<sup>735</sup> *ibid.*

Maaskar al-Battar, training to become a jihad was available at the click of a mouse. The first issue drew attention to the convenience of online training it provided. 'Oh Mujahid (holy warrior) brother, in order to join the great training camps you don't have to travel to other lands...Alone, in your home or with a group of your brothers, you too can begin to execute the new program. You can all join the al-Battar Training Camp'.<sup>736</sup> Al-Khansa, a magazine aimed exclusively at women and named after a woman poet who was a close associate of Prophet Mohammed, aimed at motivating women to participate more actively in the jihad. Jihadi online publications are not just about getting matter, putting together content and posting it on the internet. They are also concerned about survival, which is determined not so much by funding and circulation as it is about evading counter-terror experts. They constantly move URLs and change addresses regularly, sometimes embedding themselves within other websites to evade detection. Another jihadi online publication named Dhurwat al-Sanam, Arabic for the 'highest or more virtuous belief/insight' has been posted by the official spokesman of Al-Qaida in Iraq.<sup>737</sup>

Imam Samudra, charged with engineering the devastating Bali nightclub bombings, published a jailhouse autobiography justifying the Bali attacks, which killed 202 people it wasn't surprising. What was a surprise was that into the back of the book is a chapter entitled ' Hacking, Why Not?'. There Samudra urges

---

<sup>736</sup> Ramachandran, S: 'Jihad's latest 'rag' hits the internet', Asian Times, [www.atimes.com](http://www.atimes.com), 31/5/05

<sup>737</sup> *ibid.*



fellow Muslim radicals to take the holy war into cyberspace by attacking US computers, with the particular aim of committing credit card fraud, called 'carding'. The chapter then provides an outline on how to get started. Samudra is among the most technologically savvy members of Jamaah Islamiah, an underground Islamic radical movement in Southeast Asia that is linked to Al-Qaida. He sought to fund the Bali attacks in part through online credit card fraud, according to Indonesian police. 'This is hacking for dummies. But in this day and age, you don't have to be an expert hacker to have a tremendous impact', comments Evan F. Kohlman, a US consultant on international terrorism who reviewed the chapter. Kohlman and other cyberterrorism experts say the kind of fraud preached by Samudra is becoming increasingly attractive as a source of funding for Al-Qaida operatives in several regions of the world.<sup>738</sup>

Three internet cafes, including one located in downtown Riyadh, have been raided by security officials in a move to track down on terrorists who have been using public cafes to exchange information, post terror messages and issue treats to organisations, government agencies and nations.<sup>739</sup> Arif Ziauddin, manager of one of the raided cafes, stated that many terror suspects have turned to cyberspace to communicate with their accomplices since the May 12 2003 bombings in Riyadh.

---

<sup>738</sup> Sipress, A: 'An Indonesian's prison peep takes war into cyberspace', Washington Post Foreign Service, 14/12/04

<sup>739</sup> Khan, Ghazanfar Ali M: 'Terror crackdown leads to cybercafes', [www.arabnews.com](http://www.arabnews.com), 18/1/05



On June 1 2004, al-Qaida terrorists conducted one of their most spectacular operations – a brutal assault on the Saudi oil town of Khobar, replete with seek-and-destroy missions targeting non-Muslims and gun battles with security forces.

<sup>740</sup>An internet post by a man who calls himself Fawaz Bin Muhammad al-Nashmi, posted on June 3 to a forum called Al-Qal'ah (the Fortress) recounts a heroic 'battle' in which he along with comrades set out to cleanse the Arabian peninsula of infidels. The posting resembles a Hollywood action film. Although al-Qaida adherents are commonly described as having a medieval world view, their rhetoric and self-image owe as much to blockbuster movies and *Mortal Kombat* as to epic tales of seventh-century Islam. Al-Nashmi uses the word 'ilj' to refer to the non-Muslim he and his comrades murder, which means an unbeliever. It has become a jocular pejorative for US soldiers, and Al-Nashmi uses it interchangeably with 'cafir', the standard put-down for an infidel. As improbable as it is that these events occurred as he describes them, his idealized narrative presents them as they appear to the mind's eye of Al-Qaida. The pool of potential recruits teems with young men adrift amid feelings of humiliation and powerlessness, eager for a world view that answers their questions, and hungry for action. In his account of a blood-soaked day, al-Nashmi gives them what they lack – power over life and death, a mission to rid the world of enemies, and violence as the path to deliverance.

---

<sup>740</sup> Kimmage, D: 'Al-Qaida's next action hero', 16/6/04, <http://slate.msn.com/id/2102487>

Efforts at undermining Al-Qaida's virtual operations, networking, mobilisation, propaganda, recruiting and fundraising are many and in fact various research centres, university and think tanks have been funded or prepare proposals for funding on several counterterrorism projects. For instance, documents obtained by the Electronic Privacy Information Centre through a Freedom of Information Act show that the US Central Intelligence Agency and the National Science Foundation collaborated to fund researchers developing software to electronically spy on internet chat rooms. The project is described as the 'fully automated surveillance system for data collection and analysis in internet chat rooms to discover hidden groups'.<sup>741</sup>

A new generation of software called Starlight 3.0, developed for the Department of Homeland Security by the Pacific Northwest National Laboratory (PNNL), can unravel the complex relationships between people, places, and events.<sup>742</sup> Anticipating terrorist activity requires continually decoding the meaning behind countless emails, web pages, financial transactions, and other documents, according to Jim Thomas, director of the National Visualization and Analytics Centre (NVAC) in Richland, Washington. In September 2005, NVAC, a division of the PNNL, will release its Starlight 3.0 visual analytics software, which graphically displays the relationships and interactions between documents containing text, images, audio, and video. Starlight quadruples the number of documents that can be analyzed at one time –from the previous 10,000 to 40,000

---

<sup>741</sup> Indymedia: 'CIA behind automated chat room spying scheme', [www.indymedia.org](http://www.indymedia.org), 15/12/04

<sup>742</sup> Gartner, J: 'A vision of terror', [www.technologyreview.com](http://www.technologyreview.com), 10/5/05



– depending on the type of files. It also permits visualizations to be opened simultaneously, which allows officers for the first time to analyze geospatial data within the program.

Moreover, British chief police officers are asking the UK government for new powers that would allow them to attack terrorist websites.<sup>743</sup> Ken Jones, chairman of the ACPO Terrorism and Allied Matters Committee said that the evolving nature of the current threat from international terrorism demands that those charged with countering the threat have the tools they need to do the job. But a representative of Spy.org.uk, a civil liberties advocacy web site, in an email to silicon.com, wrote: ‘Who exactly is going to define what a terrorist website is? There are none of these hosted in the UK, so the targets must be abroad...The only people who seem to have a legal hacking law at the moment are the Australians, but it does not appear that they have dared use it against overseas targets.

Other legal issues are also controversial. The case of Babar Ahmad, who after being arrested under our draconian and catch all Terrorism Act, and released without charge, presumably for lack of actual evidence, has been arrested in London in order to be extradited to the USA. He is accused of running a website in the USA, which apparently supported the Taleban in Afghanistan and some rebels in Chechnya in Russia. Neither of these were at the time or are now,

---

<sup>743</sup> Illet, D: ‘UK cops want to attack terrorism web sites’, silicon.com, published on ZDNet News, 25/7/05, accessed 16/8/05



proscribed terrorist organisations in the United Kingdom, yet this British citizen is in the process of being extradited to a foreign country the USA, regarding possible actions in a third and fourth country i.e Afghanistan.<sup>744</sup>

---

<sup>744</sup> 'Global guerrillas and temporary autonomous zones', forwarded from [e-resistance@yahoogroups.com](mailto:resistance@yahoogroups.com), posted on 20/8/04, accessed 27/12/04

## 5.2 Ethnic Cyberconflicts

So far I looked at the Israeli-Palestinian, Indian-Pakistani and US-Chinese cyberconflicts, which are considered to be ethnoreligious cyberconflicts. The next section looks at various cyberconflicts that are more ethnic in character, namely China-Taiwan, China-Japan and Colombia (more of an internal conflict), in order to include empirical evidence and discussion of different types of cyberconflict.

After Taiwanese president Teng-Hui talked about a two-state theory to describe the relationship between China and Taiwan in what was perceived by many as a declaration of independence, Chinese hackers attacked many of the Taiwanese government's websites. The hackers during the first week of August 1999 filled the pages with political slogans and warnings to the 'separationists'. On the rebound, Taiwanese hackers attacked Chinese government sites, with hack attempts succeeding. The interesting part was that Taiwanese hackers added many liberal elements to their hacking such as music (pop songs and the national anthem), animations and comments citing popular culture.

The Taiwanese authorities warned that hacking even a Chinese site is illegal and that hackers would be prosecuted. The response from a representative of Taiwanese hackers was that their movement was an autonomous action against

any kind of information warfare invasion, and a dismissal of the government's countermeasures as unethical.<sup>745</sup>

Also, in February 2000, Chinese hackers launched an attack against major Japanese companies. The reason for this was what they perceived as Japan's hard line against China. They left messages such as 'Down with Japanese militarism' and 'Kill all Japs'.<sup>746</sup> Japan more recently has been targeted twice. During the first week of April 2001, pro-Korean hackers attacked Japanese organisations responsible for the approval of a new history book. The textbook glossed over atrocities committed by Japan during World War II and the occupation of China and South Korea. The attackers were mainly Korean students, who crashed several websites belonging to Japanese organisations, including Japan's education ministry, the Liberal Democratic Party and the publishers of the book. Then in August 2001, pro-Chinese hackers defaced several sites belonging to Japanese companies after Japan's Prime Minister visited a controversial war memorial, the Yasukuni Shrine.<sup>747</sup> Chinese hackers have demonstrated their willingness to use cyberspace as a platform for protests and patriotic nationalism – though this is not to say that other nationalities have not been doing the same. Similarly, in Malaysia between April 1999 and April 2000, there were 89 hacker attacks on 60 government agencies, including sensitive data-carrying targets like the treasury,

---

<sup>745</sup> Jame, F: 'China, Taiwan in web hacking "war" ', ZDNet, 10/8/99

<sup>746</sup> *ibid.*

<sup>747</sup> 'Chinese hackers attack Japanese websites over the Shrine visit', Agence France Presse, 14/8/01



public works, social security and immigration, along with major non-government sites such as Malaysian Airlines.

Japan has bolstered the defence of its computer systems in the face of a surge in cyberattacks believed linked to anti-Japanese sentiment in Asia during the spring of 2005. Government officials were reluctant to publicly pin the attacks on Chinese and South Korea hackers because of the difficulty of identifying their source, but the attacks coincided with violent anti-Japanese protests in China. This actually fuels the argument that 'real' conflicts have the tendency to transfer online to the extent that cyberconflicts and hackattacks can be used as a barometer for real life conflicts. Cyberattacks hit Japan's National Police agency, Self-Defence Forces and the Defense and Foreign Ministries, other businesses and a Tokyo war shrine criticised in Asia for honouring convicted war criminals. An official in Tokyo's Yasukuni Shrine, which honors war criminals among Japan's 2.5 million war dead, said on condition of anonymity that the site was hit with 15,000 attacks per second.<sup>748</sup> Experts say the recent flow of internet intrusions marks a shift from 'kid's play' hacking to organized, full-scale, politically motivated assaults. 'People have discovered that they can conduct "digital demonstrations" at any time. It's almost unthinkable that a huge flock of Chinese people could come to Japan and hold a protest. But digitally is possible',

---

<sup>748</sup> Lateline News: 'Digital demonstrations in China spark concern in Japan', <http://news.muzi.com/11/english/1362332.html>, 11/5/05, accessed 1/7/05

comments Itsuro Nishimoto, A SecureNet service, a division of Internet security LAC.<sup>749</sup>

## COLOMBIA

After the Revolutionary Armed Forces of Colombia (FARC) hijacked a commercial plane and kidnapped a senator at the end of February 2002, the government called off peace talks and decided to send troops to reclaim a Switzerland-sized territory it conceded to the rebels in 1998. While there were battles on the ground, another crucial battle was being fought in cyberspace to influence public opinion.

On their multi-lingual website, FARC condemn the government's move, rally their foreign supporters and swear to fight to the finish. FARC commandos wrote in a press release published on their site the day after President Andres Pastrana ended negotiations in a televised speech, '[o]nce more the Colombian oligarchy impedes the dialogue that would allow the structural, economic, political, social and military changes that Colombia requires to escape the profound crisis that liberal and conservative governments have historically mired in'.<sup>750</sup> They continued in an online editorial: '[w]hile there is no definite solution to the great injustices suffered by our people, while resources are spent on war and not peace,

---

<sup>749</sup> *ibid.*

<sup>750</sup> Scheeres, J: 'Colombia's cyber (un)civil war', Wired news, 4/3/02

we will continue forward in the conquest of power for the construction of the New Colombia'.<sup>751</sup>

2005 was the first year in more than a decade that no Colombian reporters were killed. However, the statistic, while welcome, was due more to the increased caution being practiced by journalists rather than an improvement in the country's situation. From a journalistic perspective, this is cause for concern because it appears to have resulted in a self-censorship that has rendered serious investigative journalism virtually non-existent and led to a distorted portrayal of Colombia's conflict.

Reporters are fearful of the reactions of right-wing paramilitaries and leftist guerrillas to the stories that they report. Paramilitaries from the United Self-Defense Forces of Colombia (AUC) are prominent in Puerto Asis and other towns in Putumayo, while the Revolutionary Military Forces of Colombia (FARC) guerrillas control many of the rural areas. Due to their fear of the armed groups, local journalists in Putumayo practice what they call 'social journalism', in which they focus on social and political stories that do not involve the armed groups.<sup>752</sup>

---

<sup>751</sup> *ibid.*

<sup>752</sup> Leech, G: 'Scared into silence', [www.columbiajournal.org](http://www.columbiajournal.org), accessed 14/1/05



### **5.3 Is the internet a tool for conflict resolution or an escalating factor?**

The examples of ethnoreligious and sociopolitical cyberconflict show that cyberattacks follow actual conflict, and are therefore closely linked with the real world. Also, cyberspace can be used as a battleground for future warfare, as some experts argue. On the other hand, in the pursuit of potential positive uses of the internet as a tool for communication and conflict resolution between opposing sides in a conflict, the Palestine-Israeli conflict emerges as a constructive example.

One of the initiatives taken to promote cooperation in the Middle East region through the internet is the Middle East Virtual Community (MEViC). MEViC ([www.mevic.org](http://www.mevic.org)) seeks to create a virtual community of academics and intellectuals in order to foster cooperation, collaboration in research, communication and understanding in the region. The organisation currently has participants from Palestine, Egypt, Jordan, Israel, the Gulf, Turkey and Morocco. Working as individuals, they have been able to bypass political and institutional constraints that have been characteristic of the region. As Dachan puts it, '[t]he singular aspects of computer mediated communication are particularly relevant to creating the kind of community and discussion groups dealing with the issues related to regional conflict, and should serve as an important component of

community based diplomacy'.<sup>753</sup> Moreover, such a community has the potential for creating strong dialogue, especially when there is a group of committed individuals, limited by neither time nor space, and having the capacity to plan and organise, to access regional research centers and to use online document delivering systems.

Another interesting attempt at dialogue is an internet community called the Middleast Abrahamic Forum (MEAF). On the homepage of the community, it is mentioned that the forum is devoted to interfaith dialogue between the three Abrahamic traditions, Islam, Christianity and Judaism. The first seven months of the life of this community are described by its founder and manager Mohamed Mosad.<sup>754</sup> The values emphasised by the majority of members included stressing the importance of unity between the different religions. The forum participants exchanged ideas reflecting the beliefs common to the different religions. Then, they moved to discussing the value of dialogue itself and its ethics, and, while they became more convinced of the differences between them, they remained committed to a search for peaceful coexistence. Mosad writes that although there were threads calling for a debate to prove which religion is the right one or reminding the dreamy members of the conflictual aspects of reality, participants in the forum still managed to develop a common language.<sup>755</sup>

---

<sup>753</sup> Dachan, M: 'Internet usage in the Middle East: Some political and social implications', Department of Political Science, The Hebrew University of Jerusalem.

<sup>754</sup> Mosad, M: 'The web community: A social movement in cyberspace?', Department of sociology, American university of Cairo.



Also, Mosad is interested in the individual and collective identities of the MEAF virtual community. Responding to a thread raising the question of 'who are we', the members defined themselves in terms of nationality, ethnicity, religion, gender, age, and political position. Some shaped their identity in opposition to an 'Other'. Some spoke with 'I', others with 'we'; some were talking as members of a community, while others were representing different identities from outside. It is useful to include here Mosad's comment that identity becomes an issue when one's status quo is threatened. He argues that, in this particular community, people felt threatened in two situations. Firstly, they felt threatened when facing the political situation or international media coverage from outside the community, when this operates in a way which threatens a person's particular identity (e.g. defending Muslims from being called terrorists after a suicide bombing). Secondly, they became defensive when their identity was threatened by an inside alternative. For instance, when a Jewish member said that Jerusalem should belong to the three traditions, some Jewish members stressed their Israeli identity and their critic's American one.<sup>756</sup>

As far as their collective identity is concerned, Mosad explains that, when receiving a new member, the old ones replied in a sense of 'we welcome you', and, when dealing with a rebelling member, the rest of the members would show solidarity against him/her. It did not matter what religion s/he was or which

---

<sup>755</sup> Mohamed Mosad: 'The web community: A social movement in cyberspace?', Department of sociology, American university of Cairo.

<sup>756</sup> *ibid.*



country s/he was from; every member responded in the same way to refute him/her, and when the member would not be convinced politely, they would start to attack the opponent in his/her thread, showing solidarity with their community. Even more interestingly (since, as Mosad notes, a collective identity is not simply the drawing of a cognitive boundary; it is also an emotion), many of the members started a good friendship via phone-calls and emails, and when they would notice an absence of an active member, they would send messages to check on him.

The power-game turned out to be a game for information. Social movements, instead of exercising a physical action, acted so as to control the way information would be interpreted. That is why communities like these are becoming important as initiatives in regional conflicts. An example was when the MEAF community participated in a campaign to stop the demolition of Palestinian homes, where members of the community bombarded the Israeli PM, the general secretary of the UN and the then US Secretary of State Madeline Albright.

A third effort in the same region to build communication bridges through the internet was initiated by the Project for Arab-Jewish Dialogue of the Program in Conflict Resolution at Bar-Ilan University with Palestinians counterparts from the Bethlehem-Hebron area. Participants from Bar-Ilan University and Beit Ommar village participated in an experimental email dialogue for approximately two

months during the late spring of 1998.<sup>757</sup> Eight participants on each side were paired up and given instructions to introduce themselves to each other and describe a Muslim or Jewish holiday and conduct clarifications with each other on this topic. The organising parties had to overcome major technical difficulties, namely, to install the first email location in Beit Ommar. Due to the success of this first dialogue, a second one was attempted, this time focusing directly on two holidays, Ramadan and Rosh Hashanah. The email effort was meant to explore possibilities for precise data transmission and comprehension across the Israeli-Palestinian divide, as well as to facilitate the positive relationship-building necessary for both conflict resolution and effective coactivity. Eight participants from both sides took short examinations on the two holidays before and after the email exchange, and concluded the two-month cycle with actual face-to-face workshops. An example of their email messages follows.

An Israeli student wrote:

I learned that Ramadan is one of the five foundations of Islam, and that every Moslem has to fast for the whole month of Ramadan, in which the Quran was given to Mohammad on the night of the 27<sup>th</sup>. I didn't quite understand what do you do during the days of the fasting, are there any special thing you do during

---

<sup>757</sup> Mollov, B, Schwartz, Steinberg, G and Lavie, C: 'The Impact of Israeli-Palestinian intercultural dialogue: Virtual and face to face', Bar-Ilan University, [www.mevic.org/papers/mollovvirtual.html](http://www.mevic.org/papers/mollovvirtual.html)

the day? Special prayers? Special places to go to? Another question: Do all Moslems fast on this month or just the very religious ones...<sup>758</sup>

His Palestinian partner responded:

It is so nice to hear from you, and it was a nice time that we spent at Bar-Ilan University. Regarding your questions: we spend time during the day in Ramadan as usual, we go to work normally, and we pray the five prayers but we add in the last prayer an extra prayer and during these prayers we read the whole Quran during the month... Not all Moslems fast, but we can say most of them. I would like to ask what does Rosh Hashanah symbolize? And how many days do you celebrate?<sup>759</sup>

During the two-month email cycle, in total 65 messages were exchanged and the organisers were impressed by the richness of the message content and the social information exchanged. Furthermore, while both groups performed poorly in their exams prior to the dialogue, with the Israelis scoring 58% and the Palestinians 51%, after the dialogue the Palestinians increased their knowledge to 73% and the Israelis to 61%. Palestinian results can be partly explained due to the fact that Israeli communication styles place less emphasis to social interaction and talk straight and to the point, that is to say, Arab participants acquired greater amounts of information from their Israeli partners than vice versa.<sup>760</sup>

---

<sup>758</sup> *ibid.*



Despite these efforts of reconciliation, there is a cyberbattle for hearts and minds in the Israeli-Palestinian conflict. Examples include the pro-Palestine Electronic Intifada ([www.electronicintifada.com](http://www.electronicintifada.com)), a site that encourages media activism and features daily reports from the Palestinian territories, while in the pro-Israel camp there is the New York-based Israel Support Group (ISG) ([www.israelsg.com](http://www.israelsg.com)), which hosts a comprehensive site with news, video reports, and activist guides.<sup>761</sup> One of the largest Islamic websites, IslamiCity ([www.islamicity.com](http://www.islamicity.com)), reaches about 50 million people a month and features polls, TV and radio broadcasts, and religious guidance. Similarly, Middle East news Online ([www.middleeastwire.com](http://www.middleeastwire.com)) partners with 120 content providers worldwide and uses a network of reporters to disseminate information about the entire region. 'The impact of the Internet on the media is that they are hearing from people on both sides of the conflict', comments Rania Awwad, a representative for Palestine Media Watch ([www.pmwatch.org](http://www.pmwatch.org)).<sup>762</sup> Also, the Middle East Media Research Institute (MEMRI) ([www.memri.org](http://www.memri.org)) uses the web to monitor Arab media for anti-Israel content. All this cyberactivism means that journalists are subject not just to increased scrutiny, but also to massive lobbying campaigns.

Some observers worry that the proliferation of independent websites, media monitors and lobbying campaigns will have a polarizing effect on the conflict. "Muslims get news from a Muslim perspective. Jews get news from their

---

<sup>759</sup> *ibid.*

<sup>760</sup> *ibid.*

<sup>761</sup> Foreign Policy: 'Net Effect: The Middle East's e-war', July/ August 2002

<sup>762</sup> *ibid.*

perspective. There is a gap in understanding what is happening in the conflict”, says IslamiCity’s Mohammed Abdul Aleem.<sup>763</sup>

### *Conclusion*

In ethnoreligious cyberconflicts, when an anti-Israeli activist attacks the Aipac site, an Israeli sets up a website of targets to attack, when Pakistanis attack India’s largest internet service or when Chinese and American nationalists hack each other, the use of the internet is different from that found in sociopolitical cyberconflicts. The parties in ethnoreligious cyberconflicts mostly do not use the internet in order to mobilise support or influence public opinion. They use it as a weapon, like throwing stones.

Cyberconflict should not be dismissed as just a series of catfights between computer geeks. Mi2g Chief executive, DK Matai, has argued that cyberwarfare could be used as a barometer for political tensions around the world. ‘The tense situation in the Middle East is reflected in both covert and overt hack attacks’.<sup>764</sup>

In addition, cyberconflict is a phenomenon that includes a variety of actors with different characteristics, many of whom cannot be easily distinguished as either terrorist or activist in nature. Accordingly, the political game between parties in

---

<sup>763</sup> *ibid.*

<sup>764</sup> ‘Israel under hack attack’, BBCOnline, 16/4/2002

an ethnoreligious conflict or among social activists engaged in a sociopolitical one is neither clear, nor fully developed at this early stage.

Nonetheless, it is important to emphasise that we are discussing two different kinds of cyberconflict and that they should be treated as distinct. The groups in sociopolitical cyberconflicts initiate a newsworthy event by putting the other side to the defensive, sending stories for the whole world to see, rendering information uncontrollable or mobilising support by promoting an alternative frame for the event. On the other hand, in ethnoreligious cyberconflicts, the opposing parties tend to use the internet as a weapon. While they might initiate events, they fail to promote an alternative frame. They simply attack the enemy or defend their electronic territory.

This means that cyberconflict needs to be monitored, and the actors and practices involved in such conflict need to be researched and evaluated. It is important that we increase our understanding of the nature and trajectories of conflict with an internet component, for a number of political reasons. These include improving conflict resolution and mediation strategies, and developing ways of bringing cyberwar activities under the purview of international agreements governing conflict.

This section looked at ethnoreligious and ethnic cyberconflicts, in particular, cyberconflicts between Israelis and Palestinians, Indians and Pakistanis, and



Americans and Chinese, as well as incidents in South-East Asia, Colombia and Kosovo and attempts at conflict resolution using the internet as the platform.

The integrated theoretical framework proposed in section 2.4 urges us to focus on the following parameters when looking at ethnoreligious cyberconflicts:

### 3. Ethnoreligious Cyberconflicts:

a. Ethnic/religious affiliation, chauvinism, national identity, b. Discourses of inclusion and exclusion, c. Information warfare, the use of the internet as a weapon, propaganda and mobilisational tool, d. Conflict resolution depends on legal, organisational framework, number of parties issues, distribution of power, values and beliefs.

In the Israeli-Palestinian cyberconflict, we see the use of national symbols when hacking websites, such as the Israeli flag, Hebrew text and even a recording of the Israeli national anthem on the Hezbollah home page. This explicitly urges us to look at issues of national identity, nationalism and ethnicity (see 3a). Secondly, the language used by hackers, as for instance in the AIPAC hack ('[t]he hack is to protest against atrocities in Palestine by the barbaric Israeli soldiers and their constant support by the US government'), relies on an 'us' and 'them' mentality, where Israelis and their American supporters are portrayed as barbaric, reflecting discourses of inclusion and exclusion (see 3b). Thirdly, the internet in

ethnoreligious cyberconflict became a battleground and was used as a weapon by both sides, and full-scale action by thousands of Israeli and Palestinian youngsters involved both racist emails (see 3a ,3c) and circulating instructions on how to crush the enemy's website (see 3c).

Similarly, in the Indian-Pakistani cyberconflict, the Indian Army's website was set up as a propaganda tool, and hacked pictures of alleged tortures of Kashmiris by Indians were placed on the site, in a similar propaganda tactic (see 3c). Also, the internet was used as a weapon, when the worm Yaha was released by Indian hackers (see 3c). In terms of national identity and discourses of exclusion and inclusion, the following is telling: '[a] whole hearted salute for my brothers fighting for our country with a religious maverick enemy' and '[w]e wish that our Muslim brothers given the right to choose, as was promised them...' In both sentences, religion is mentioned (religious affiliation), the word 'brothers' (collective identity and solidarity), and 'our country' and a promised land (see 3a, 3b and 3c).

In the rest of the examples, similar links can be made with the proposed framework. Again this is clear in the discourse used: 'We will hate China forever and will hack its sites' (US-China), 'Down with Japanese militarism, Kill all Japs' (China-Japan), 'Welcome to the web page of the biggest liars and killers, Long Live Serbia', (Kosovo-Serbia). In all of these cases, a nation is identified as the

enemy by nationality and appropriate adjectives are used to create the inclusion/exclusion effect (see 3a, 3b).

The conflict resolution component in the framework (see 3d) is included due to the attempts at such resolution through the internet. The three examples (MEViC, MEAF and the Project for Arab-Jewish Dialogue) place emphasis on community-based diplomacy, interfaith dialogue (which reflects the importance of exchanging ideas reflecting the common beliefs between different religions), and building a positive relationship as a platform for resolution.

The internet as a medium:

a. Analysing discourses (representations of the world, constructions of social identities and social relations), b. Control of information, level of censorship, alternative sources, c. Wolsfeld: Political contest model among antagonists: the ability to initiate and control events, dominate political discourse, mobilise supporters, d. Media effects on policy (strategic, tactical, representational).

In Colombia and Kosovo the internet was used as a medium for disseminating information to the extent that, in the latter conflict, a commentator has said that if one was to collate the amount of emails sent to news organisations, one would build up an interactive map of Yugoslavia linking to accounts of bombing town by town. Online news organisations like the Electronic Intifada and the Israeli



Support Group also represent alternative sources for the explanation of conflict (see 4b), can be used for propaganda and mobilisation, and reflect a political contest between Israelis and Palestinians to dominate political discourse (see 4b).

The Al-Qaida network and its ideology relies more on common religious affiliation and kinship networks than strict national identity, which fits well with the borderless and network character of the internet (3a). Secondly, the internet has been used as a primary mobilisational tool (3c), before the 9/11, especially after the break down of cells in Afghanistan, Saudi Arabia and Pakistan. On the internet Al-Qaida is replicating recruitment and training techniques and evading security services, because they cannot be physically intercepted due to the virtuality of their networks. The internet is used as a propaganda tool via electronic magazines, training manuals and general recruitment sites (3c), as well as a weapon for financial disruptions aiming at financing operations, or stealing data and blueprints.

On the organisational aspect and in order to avoid confusion, it is crucial to note that Al-Qaeda is quite a unique case in point, because as an ethnoreligious actor in a cyberconflict, although expected to be more hierarchical - like the hackers in Israeli-Palestinian cyberconflict and use the internet more as a weapon and not as a resource - is instead networked in comparison to the rest of the ethnoreligious cyberconflicts and uses the internet in all sorts of resourceful ways. A possible explanation for this is two fold: Firstly, their ideology does not rest on national

identity, so it is open to international networking through religion and kinship/family and secondly, they are not left with any other choice but to use the internet in resourceful ways, because they are not legitimate and they are not going to be given a chance at conflict resolution.

This chapter attempted to describe some cases of ethnoreligious cyberconflict, to understand their operation, to examine the current methods and weapons used and link these examples with the proposed integrated theoretical framework. The conclusion I came to is that the knife can cut both ways. On the one hand, evidence suggests that cyberconflicts can spill over to the real world with information warfare becoming a threat to governments and businesses. On the other hand, the inexpensive, easy-to-use and interactive style of the medium can provide significant assistance in bringing opposing sides together who would otherwise not communicate due to spatial, political, religious or other differences. The next chapter examines the effect of the internet on the March 2003 Iraq conflict.

## **Chapter 6: The effects of the internet on the 2003 Iraq war**

In the particular case of post-September 11 information warfare, the assertions of US unity by the Bush administration have resulted in a context in which public statements directed to the international community are interpreted as representative of the US as a political entity and not just the utterances of a particular individual in the current administration.<sup>765</sup>

Before and during the March 2003 Iraq war, information technologies, and particularly the internet, inspired several groups belonging to all sorts of different backgrounds and ideologies to voice their opinion on the war and in certain instances to engage in symbolic hacking against opposing groups or institutions. But still, the principal originality of this conflict was the effect of the internet on war coverage. This section looks at three levels of the internet's role in the conflict: its effect on the organisation and spread of the peace movement, its impact on war coverage and the issue of war-related cyberconflicts.

Before delving deeper, it would be helpful to explain again that with the advent of the internet, new forms of conflict have emerged, not directly linked with information warfare but rather, connected to a more subtle form of societal

---

<sup>765</sup> Walls, A.T: 'The image of unanimity: The utility of the promotion and disparagement of cultural and social unanimity as a form of context manipulation in information warfare in the



netwar<sup>766</sup>, where new social movements, ethnic groups and terrorists use the internet to organise, acquire resources and attack 'the other side'. Despite the high-tech name, the groups involved have quite traditional political goals - power, participation, democracy, alternative ideologies - using, however, a postmodern, interactive medium.

There are two types of cyberconflict. The groups in sociopolitical cyberconflicts (for example, the peace and anti-globalisation movements) initiate a newsworthy event by putting the other side on the defensive, sending stories for the whole world to see, rendering information uncontrollable and mobilising support by promoting an alternative frame for the event. On the other hand, in ethnoreligious cyberconflicts (such as Israeli-Palestinian hacking and Indian-Pakistani activity), the opposing parties tend to use the internet as a weapon. While they might initiate events, they fail to promote an alternative frame. They simply attack the enemy or defend their electronic territory.<sup>767</sup> Thereby, I analyse the different kinds of cyberconflict in the context of international conflict theory for ethnoreligious cyberconflict and social movement theory for sociopolitical cyberconflict, while keeping in mind that this takes place in a new media environment, using media theory.

---

aftermath of the attacks of September 11, 2001', *Journal of Information Warfare*, (2002) 2,2: pp.119-127

<sup>766</sup> Arquilla and Ronfeldt (2001) *Networks and Netwars*, Rand: California.

<sup>767</sup> Karatzogianni, A: 'The politics of cyberconflict', *Journal of Politics*, February 2004, vol. 24 (1), pp. 46-55

The most recent opportunity to apply this theoretical framework arose with the recent war in Iraq. There the distinction (ethnoreligious/sociopolitical) worked quite well. There was sociopolitical CC before the war, starting with the peace groups organising demonstrations and events through the internet, and, while the tension was mounting, there were hackings between anti-war and pro-war hacktivists (sociopolitical), but also between pro-Islamic and anti-Islamic hackers (ethnoreligious). The most interesting part was the effect of the internet on war coverage. The war itself was dubbed as the first internet war, and the use of 'blogs' helped ordinary people to become involved in reporting the war and presenting an alternative by means of independent media, avoiding the restraints the corporate media face, namely censorship and the demands and politics of advertisers.<sup>768</sup>

---

<sup>768</sup> 'Some critical media voices face censorship', Media Advisory, Fair and Accuracy in Reporting, 3/4/03

## **6.1 The internet's role in the organisation of anti-war protests**

The importance of the internet in the organisation of political groups is not new. However, in this particular conflict, its effects were for the first time indicative of the full potential of the new medium in politics. In the months preceding the actual war in Iraq, we witnessed a plenitude of phenomena on, off and because of the internet that in previous international conflicts were only embryonic. Anti-war groups used email lists and websites, group text messages and chatrooms to organise protests, making politics more accessible to an unprecedented number of people from all backgrounds, who normally would not or could not get so involved.

In fact, anti-war protests in world capitals were impressive, whenever they actually made it to the newsrooms. In world capitals, people of all ages and nationalities took to the streets to demonstrate against the possibility of a war with Iraq. In only one weekend of February 15th and 16<sup>th</sup> 2003, or F-15 in activist parlance, about 10 million people protested globally against the war, rendering them the biggest peace protests since the Anti-Vietnam War protests of the 1960s/70s.<sup>769</sup> In the US, the two biggest demonstrations took place in San Francisco and Washington. The disparity of protestors, where London is a case in point, is a sign that the antiwar movement has gone mainstream thanks to hundreds of anti-war websites and mailing lists. The internet speeds up



organising, doing in months what took years in the Vietnam era.<sup>770</sup> As historian and columnist Ruth Rosen explains in *The San Francisco Chronicle*, '[n]ever before in human history has an anti-war movement grown so fast and spread so quickly. It is even more remarkable because the war has yet to begin. Publicized throughout cyberspace, the anti-war movement has left behind its sectarian roots and entered mainstream culture'.<sup>771</sup>

More astonishingly, millions of people all over the world were protesting the possibility of a war that had not even started yet. According to Sarah Sloan, an organiser with International ANSWER, the internet played a very significant role, because 'it made a major difference in getting our message out there especially because the mainstream media is not covering the anti-war movement'. The internet also allowed protests to go international, with protestors in 32 countries holding demonstrations. 'There is no way the event would have been international without the Internet'.<sup>772</sup> The same is being suggested by Rayman Elamine, organiser with Direct Action to Stop the War, an umbrella organisation for a number of antiwar groups based in San Francisco Bay Area. 'Groups wouldn't have been able to do some of the logistical and other planning without the aid of the Internet for getting the message out'.<sup>773</sup> Alistair Alexander from the Stop the War Coalition in England has commented in a Guardian article that the web 'has

---

<sup>769</sup> Gumbel, A: 'Global peace movement is alive and kicking', *The Sunday Independent*, 16/3/03

<sup>770</sup> Max, S, a Manhattan based trainer of community activists for 30 years, quoted in 'Cyberspace spurs activism too', *Corydon Ireland, Democrat and Chronicle*.

<sup>771</sup> As quoted in Kahney, L: 'Internet strokes anti-war movement', *wired*, Jan/21/03, accessed 20/3/03

<sup>772</sup> As quoted in Kahney, L: 'Internet strokes anti-war movement', *wired*, Jan/21/03

<sup>773</sup> As quoted in Glasner, J: 'Protests to start when war does', *wired*, 19/3/03

allowed Stop the War to connect with people in a way politicians have failed to do. The much hyped age of online politics has finally arrived'.<sup>774</sup>

Indeed there is no end to practitioners and theorists alike concerning the possibilities of the medium in the organisation of the anti war movement. Kahney, for instance, mentions the United for Peace website, which includes news, contacts of activist groups and travel arrangements to the protests from 3000 different cities. 'Before the Internet people felt blacked out by the media, because it doesn't represent their views. Now because of the Net, they feel like they are part of a movement. They are no longer isolated. It helps mobilise people, gets them to move'.<sup>775</sup> Howard Rheingold, a well-known researcher in the field, has similar views. 'Instead of having some hierarchical top-down coalition, it's possible to have loose coalitions of small groups that organise very quickly'.<sup>776</sup>

In fact, the distinguishing characteristic of these groups is their disparity and their full use of networking, where we witness 'a mass mobilisation without leaders – a digital swarm'.<sup>777</sup> In other words, it exhibits the characteristics of a rhizome:<sup>778</sup>

---

<sup>774</sup> Alexander, A: 'Britain's biggest political protest was mobilised on the web', The Guardian, 19/2/03

<sup>775</sup> As quoted in Kahney, L: 'Internet strokes anti-war movement', wired, Jan/21/03,

<sup>776</sup> As quoted in Glasner, J: 'Protests to start when war does', wired.

<sup>777</sup> Lance Bennet, University of Washington, quoted in 'Internet may mobilise largest protests ever seen, Professor predicts', [www.ascribe.org](http://www.ascribe.org), 17/3/03

<sup>778</sup> Deleuze, G and Guattari, F: (1987) *A Thousand Plateaus*, Athlon: London.



What they (virtual networks) fostered was a form of interaction that preserved the integrity and autonomy of the constituent parts. No group was subject to the will of another. No group had to recognise one as a leading group or as the 'vanguard' of the movement. There was no need for bureaucracy, permanent staffs, officials, 'leadership', or even premises, beyond somewhere to house a server. Here was a form of interaction that denied the need for the very institutional and logistical framework that had for a century defined the terms and conditions of political activism.<sup>779</sup>

I receive the same impression when looking at these protests, which were very graphically reported as

[n]ot just the usual left-liberal suspects with their tie-dyes and political correct slogans, but Spanish-speaking bus drivers, public health workers, suburban mothers and their children, blue-collar production line workers, lawyers and Republican-voting executives. Also unprecedented is the participation of the big labour unions, who were notoriously quiet during the Vietnam war...<sup>780</sup>

Thus the internet has become more than just an organising tool. It can be argued that, by allowing mobilisation to emerge from free-willing amorphous groups, rather than top-down hierarchies, the net has changed protests in a more fundamental way. 'It took four and a half years to multiply the size of the

---

<sup>779</sup> Tormey, S: (2004) *Anti-capitalism: A Beginner's Guide*, Oneworld: Oxford, p. 65.

<sup>780</sup> Gumbel, A: 'Global peace movement is alive and kicking', the Sunday Independent, 16/3/03



Vietnam protests twenty fold. This time the same thing has happened in six months', Todd Gitlin, sociology professor at Columbia has commented.<sup>781</sup>

Virtually, the evidence of this is seen in the growing number of web-pages supporting or criticising the war. For instance, [Moveon.org](http://Moveon.org), a political website with 650,000 subscribers based in Silicon Valley, raised \$400,000 through 10,000 or more individual donations to remake the 1960s 'Daisy' anti-nuclear war ad.<sup>782</sup> Also, online groups promote and offer updates on protests, list event information, use chatrooms, conferences and email lists and offer special updates on the conflict ([www.notinourname.net](http://www.notinourname.net), [www.stopwar.com](http://www.stopwar.com) etc). These include religious sites, with examples ranging from the catholic church ([www.vatican.va](http://www.vatican.va)) and the US conference of Catholic Bishops ([www.usccb.org](http://www.usccb.org)) to Jewish and Muslim sites such as the aforementioned IslamiCity.<sup>783</sup> The National Council of Churches provides a grassroots toolkit on its site, which puts it this way: '[h]ere is a grassroots tool, roughly based on the Sherrod Brown Amendment, that activists can use to request information from their member of Congress on Iraq'.<sup>784</sup>

In Europe, anti-war groups are using the internet to organise protests outside US military bases and to organise protests generally, in countries such as Germany

---

<sup>781</sup> Lee, J: 'How the protesters mobilized', New York Times, 23/2/03

<sup>782</sup> Kahney, L: 'Internet strokes anti-war movement', wired, Jan/21/03

<sup>783</sup> Webb, C: 'Religious groups go online for peace', Washington Post. The article mentions: [www.quaker.com](http://www.quaker.com), [www.afsc.org](http://www.afsc.org) (American friends service committee), Unitarian movement [www.uua.org](http://www.uua.org), Presbyterian church ([www.pcusa.org](http://www.pcusa.org)) world council of churches ([www.wcc-coe.org](http://www.wcc-coe.org)), the Washington based group Churches for Middle East peace ([www.cmep.org](http://www.cmep.org)), [www.peaceprayer.com](http://www.peaceprayer.com). American Jews [www.peacenow.org](http://www.peacenow.org), [www.jewishpeacefellow.org](http://www.jewishpeacefellow.org), [www.jewishpeacethread.com](http://www.jewishpeacethread.com), [www.peacelobby.org](http://www.peacelobby.org), Muslim sites [www.ymca.org](http://www.ymca.org), [www.icna.com](http://www.icna.com), [www.mpfweb.org](http://www.mpfweb.org).

([www.resistthewar.de](http://www.resistthewar.de)), Britain ([www.reclaimthebases.org.uk](http://www.reclaimthebases.org.uk), [www.peaceuk.net](http://www.peaceuk.net)), France ([www.mvtpaix.org](http://www.mvtpaix.org)) and Spain ([www.pazahora.org](http://www.pazahora.org)). Internationally, there are sites originating from Australia, South Africa, Egypt and also the global Independent Media Center ([www.indymedia.org](http://www.indymedia.org)) which is linked to worldwide anti-war coverage or sites like 'The Campaign Against Sanctions in Iraq' ([www.casi.org.uk](http://www.casi.org.uk)).<sup>785</sup>

Not surprisingly, those supporting the war rallied around the flag online too. Organisations supporting the war used message boards, weblogs, online petitions and email to rally support for using force to disarm Iraq, from sites such as [grassfire.net](http://grassfire.net).<sup>786</sup>

More interestingly, there was a 'Virtual March' on Washington where tens of thousands of people bombarded the switchboard of the White House and other US government offices with protest calls and emails, halting much business in the capital. The coalition of 32 organisations which organised the action claimed that more than 400,000 people registered to participate in the campaign. Meanwhile,

---

<sup>784</sup> *ibid.*

<sup>785</sup> Webb, C: 'Overseas the Internet is rallying point for antiwar activists', Washington Post, 17/1/03

<sup>786</sup> Webb, C: 'Rallying around the flag online', Washington Post, 14/3/03  
Others sites supporting the war:: [www.citizensunited.com](http://www.citizensunited.com), [www.freerepublic.com](http://www.freerepublic.com), <http://defenseofamerica.org>, [www.leatherneck.com](http://www.leatherneck.com), [www.coldfury.com](http://www.coldfury.com), [www.defendamerica.com](http://www.defendamerica.com) which is sponsored by the department of defense, features news and information about the US war on terrorism and preparations for the Iraq war. Pro-war Bloggers: [www.thesafetyvalve.com](http://www.thesafetyvalve.com) [www.andrewsullivan.com](http://www.andrewsullivan.com), [www.scrappleface.com](http://www.scrappleface.com).



700 theatre groups in 42 countries led coordinated readings of the Aristophanes' anti-war comedy *Lysistrata*.<sup>787</sup>

Yet, there is not optimism everywhere one turns. Stewart Nusbaumer, coordinator of Veterans Against the War, makes a somewhat valid point. 'On the one hand, [the internet] gives you larger numbers of people. But I've also noticed it's not great for a specific demonstration somewhere. I get emails from people who say: I live 2,000 miles away'.<sup>788</sup> Still, there is recognition that the internet has been important in the growth of the movement.. 'It has been invaluable in sharing information. With a growing constituency in the US becoming convinced the American Media is not giving an honest or complete picture, people have turned to alternative sources online, notably the European press'.<sup>789</sup>

The strength the internet gives these type of movements is that it preserves the particularity of distinct groups and causes, while greatly facilitating the creation of networks of the like-minded:

As well as preserving a distinct space or presence, groups could make common cause with other groups that shared their values. This could be achieved either through a simple 'links' page which indicated which groups they felt some sense

---

<sup>787</sup> Kahney, L: 'Internet strokes anti-war movement', wired, Jan/21/03, accessed 20/3/03, 'Internet may mobilise largest protests ever seen', Professor predicts, [www.ascribe.org](http://www.ascribe.org), 17/3/03

<sup>788</sup> Glasner, J: 'Protests to start when war does', wired

<sup>789</sup> Gumbel, A: 'Global peace movement is alive and kicking', the Sunday Independent, 16/3/03



of common cause with or through more elaborate networks, sites and mechanisms that acted as an umbrella organisation all of its own.<sup>790</sup>

On the other hand, there are weaknesses in this kind of politics, since it could be argued that the leaderless and dispersed nature of online activism is ineffective, in that it ultimately fails to reach the vast majority of the world, where many activists in developing countries have little or no access to the internet or ICTs in general.

---

<sup>790</sup> Tormey, S: (2004) *Anti-capitalism: A Beginner's Guide*, Oneworld: Oxford.

## 6.2 The internet's effect on media coverage

The internet was influential in the media coverage of this war for a variety of reasons, some touching on the simple fact that more people are online now than in the last war in Iraq, others emerging because technology has advanced to include instant messaging, audiovisual imagery, file sharing etc. Still, what made the difference in this conflict was that the media environment was in such a ripe state for alternative reporting of the conflict, mainly because Americans (as well as the rest of us) searched online for news they could not find at home. An indicative example is that as early as January 2003, according to *Wired News*, half the 1.3 million visitors to the Website for Britain's *Guardian* and *Observer* newspapers were from the Americas.<sup>791</sup>

This part of the discussion looks at three main aspects of the internet's impact on war coverage: the integration of the internet into mainstream media, the effect of online material challenging official government sources and mainstream media, and the 'blogging' phenomenon, whereby everybody can be a journalist on the Net.

'You are combining the speed of television with the depth of print. This could define how future wars are covered', Mitch Gelman, executive producer of CNN, the media network that defined the coverage of the 1991 Gulf War, has

commented.<sup>792</sup> The web pages of all major media networks were well prepared for the integration of the internet in their coverage of the war. CNN itself planned for a war-tracker page, continuously featuring live reports from the frontline, 3-D charts that track bombs dropped, Iraqi casualties and defections and interactive maps of the battlefield, troop movements and terrain. ABCnews planned for fixed cameras on locations in Kuwait and Qatar 24 hours. MSNBC.com said that chat rooms and satellite transmitters that run off car cigarette lighters would be used, CBSNews.com would offer free video, maps and backgrounds and reporters with online notebooks and video feeds, and FoxNews would include the War on Terror page with a correspondent tracker and video clips from the front.<sup>793</sup> As for the BBC's online coverage, it competed remarkably with its American counterparts. On the downside, many independent news operations on the internet have slimmed down or disappeared altogether since the info-bubble burst in 1999.<sup>794</sup>

Despite all the available tools, a large number of media watchdogs, journalists and audiences have protested the unchallenging position of the mainstream media towards both the decision to go to war and in terms of the actual coverage during the war. As a result, the internet itself was used not only to mobilise international civil society as explained above, but also to offer alternative coverage of the conflict. There are different lines of development here: the US government's troublesome if not 'bombastic' relationship with the media, American media

---

<sup>791</sup> Kurtz, H: 'Webloggers, signing on as war correspondents', Washington Post, 22/3/03

<sup>792</sup> Swartz, J: 'Iraq war could herald a new age of web-based news coverage', USA Today, 18/3/03

<sup>793</sup> *ibid.*



mostly following the government line with patriotic fervor, Americans turning to non-US sources by using the internet, and the rest of the world discovering the unpredictable and amazing effect of the internet on coverage, and the potential for first-hand eyewitness accounts via emails and blogging.

Let us now examine these developments one by one. As far as the US administration is concerned, even though it made it clear there would be no censorship, it made it very difficult for war correspondents that were not embedded with their troops to get non-official stories out. On the other hand, embedded journalists were controlled by the military. 'We will tell you what you can report from the speech afterwards', an army media organiser told journalists on their first day as embedded correspondents with 1<sup>st</sup> Fusiliers Battle Group.<sup>795</sup>

Embedded journalists in Iraq topped 800 at the height of the combat in 2003, but their number has since dropped to the double figure. Five journalists have been kicked out of embed slots for reporting secure information.<sup>796</sup> Most US journalists do not leave their hotels, and in some cases, even their rooms are located in heavily fortified compounds in and around the Green Zone, the US military's Baghdad enclave. Their reporting is based in large parts on handouts from the US occupation officials or material gained while 'embedded' with US military units, is supplemented by on-the-spot accounts and interviews obtained by Iraqi

---

<sup>794</sup> Noted by David Carlson, professor in media journalism in the University of Florida, quoted in 'Media plot online war coverage', Reuters, 6/3/03

<sup>795</sup> Tomlin, J: 'Censored in the desert', Press Gazzete, 16/5/03

<sup>796</sup> Strupp, J: 'Five embeds booted out of Iraq in recent months, [www.editorpublisher.com](http://www.editorpublisher.com), 7/1/05

‘stringers’, who risk their lives for a fraction of the salary paid to their Western counterparts.<sup>797</sup> Colonel Steve Boylan, a spokesman for the US military forces, acknowledged that some of the detained journalists have been ‘held for several months’. None of them have been formally charged with any crime or even presented in court.<sup>798</sup>

This ‘difficulty’ demonstrates itself in the fact that the largest single group of war correspondents appears to have been killed by the US Military. As Philip Knightley, writer of *The First Casualty: The war correspondent as Hero and Myth Maker from Crimea to Kosovo*, puts it, ‘[t]he figures in Iraq tell a terrible story. Fifteen media people dead, with two missing, presumed dead. If you consider how short the campaign was, Iraq will be notorious as the most dangerous war for journalists ever’.<sup>799</sup>

In a single day on April 8 2003, a US missile hit an al-Jazeera office, killing a Jordanian journalist, and a US tank fired a shell at the Palestine Hotel, killing two more. Al-Jazeera offices in Basra were shelled on April 2 and a car clearly marked as belonging to the same station was shot at by US soldiers a day before the Palestine Hotel incident. International journalists and press freedom groups have condemned the attacks on the press corps in Iraq. ‘We can only conclude

---

<sup>797</sup> *ibid.*

<sup>798</sup> Van Auken, B: ‘US imprisons Iraqi journalists without charges’, [www.wsws.org](http://www.wsws.org), 7/5/05, accessed on [www.uruknet.info](http://www.uruknet.info) 7/8/05

<sup>799</sup> Knightley, P: ‘Turning the tanks on the reporters’, 14/6/03, *The Guardian*



that the US Army deliberately and without warning targeted journalists'.<sup>800</sup> 'We believe these attacks violate the Geneva conventions'.<sup>801</sup> The attacks on journalists 'look very much like murder', Robert Fisk of the London *Independent* reported on March 3, 2003.<sup>802</sup>

Eason Jordan, CNN's chief news executive, suggested at the World Economic Forum in Switzerland that some of the 63 journalists killed in Iraq had been specifically targeted by US troops.<sup>803</sup> Jordan quickly backed off his suggestion, but constant exposure from political weblogs led to his resignation. A year before that, he had admitted that CNN withheld news of atrocities taking place in Iraq under the regime of Saddam Hussein because the network was afraid it might lose access to the country. Echoing the same claim, the president of the 35,000-member Newspaper Guild asserted US troops deliberately are killing journalists in Iraq.<sup>804</sup>

Furthermore, with 600 correspondents, including about 150 from foreign media, accepting the Pentagon offer to be embedded with military troops, one would expect satisfying coverage. But even when embedded reports not consistent with the official Pentagon line appeared, they were not taken up from American

---

<sup>800</sup> Reporters Without Borders

<sup>801</sup> Committee to protect journalists in a letter to Defense Secretary Donald Rumsfeld, 8/9/03

<sup>802</sup> Fair and Accuracy in Reporting, [www.fair.org](http://www.fair.org) has a wealth of information on this, these quotes are from 'Is Killing part of the Pentagon policy?', 10/4/03

<sup>803</sup> World Net daily: 'US troops killing journalists, [www.globalresearch.com](http://www.globalresearch.com), 20/5/05, accessed 7/8/05

<sup>804</sup> World Net Daily: 'President of Newspaper Guild Echoes Claim of Ex-CNN Exec' 19/5/05, [www.costalpost.com](http://www.costalpost.com), accessed 21/9/05



media.<sup>805</sup> A look at some examples helps explain why more and more people turned to the internet for information on the war. A *Washington Post* article on William Branigin's eyewitness account describing the killing of civilians outside the Iraqi town of Najaf, where military procedures may not have been properly followed, was not picked up from the *New York Times*, which instead ran a story presenting the official line: 'Failing to Heed Warning, 7 Iraqi Women and Children Die'.<sup>806</sup>

Such uncritical coverage is hardly surprising, since several national and local media figures in the US had their work jeopardised, either explicitly or implicitly, because of the critical views they expressed on the war. Veteran war correspondent Peter Arnett was fired by NBC after giving an interview to Iraqi TV, Henry Norr was suspended without pay from the *San Francisco Chronicle* for using his sick day to get arrested in an anti-war protest and Phil Donahue's talkshow was cancelled, in what the MSNBC argued in an internal memo leaked to the All your TV website on 25 February 2003 would be a 'difficult face for NBC in a time of war... He seems to delight in presenting guests who are anti-war, anti-Bush and skeptical of the administration's motives'.<sup>807</sup>

---

<sup>805</sup> 'Official story vs eyewitness account', 4/4/03, [www.fair.org](http://www.fair.org), also see another incident considering Robert Fisk's report on evidence that civilians were killed by US strikes: 'Journalist's evidence that US bombed market ignored by US press', 4/4/03, [www.fair.org](http://www.fair.org)

<sup>806</sup> 'Official story vs eyewitness account', 4/4/03, [www.fair.org](http://www.fair.org)

<sup>807</sup> 'Some critical media voices face censorship', 3/4/03, [www.fair.org](http://www.fair.org)

Again, this is to be expected in a media environment where official sources dominate US network newscasts and dissent is considered immoral.<sup>808</sup> Nearly two-thirds of all sources, 64 per cent, used in news programs were pro-war, while 71 per cent of US guests favored the war. Anti-war voices made up only 10 per cent of all sources, just 6 per cent of non-Iraqi voices and a miserly 3 per cent of US sources. Viewers were more than six times as likely to see a pro-war source as one who was anti-war, and with US guests alone, the ratio increases to 25 to 1.<sup>809</sup> 'Given how timid most US news organisations have been in challenging the White house position in Iraq, I am not surprised if Americans are turning to foreign news services for a perspective on the conflict that goes beyond freedom fries', *Wired News* quotes former *Newsweek* contributing editor Deborah Branscum as saying. He continues:

Although it's true that anyone with a website can publish news, it's still the established media players, such as newspaper publishers, that attract the largest

---

<sup>808</sup> For more on this and inter-media politics see: Younge, G: 'Now dissent is "immoral"', *The Guardian*, 2/6/03; Kennedy, D: 'The GOP attack machine: All who are not Bushies are evil', *phoenix.com*, 6/6/03; Lazare, D: 'The New Yorker goes to war', *The Nation*, 2/6/03; Vann, B and North, D: 'Panic and hysteria reign at the New York Times', [www.wsws.org](http://www.wsws.org); McQuaig, L: 'Bush unchallenged by media', *Toronto Star*, 25/5/03; The following articles from [www.fair.org](http://www.fair.org): Rendall, S: 'Dissent, disloyalty and Double Standards: Kosovo doves denounced Iraq war protest as anti-American', May/June 2003; Naureckas, J: 'Wolf Blitzer for the Defense (Department): Making sure the official line is the last word', January/February 2003; 'In Iraq crisis, networks are megaphones for official views', 18/3/03; Solomon, N: 'Media war: Obsessed with tactics and technology', 27/3/03.

<sup>809</sup> For more analysis see Rendall, S and Broughel, T: 'Amplifying officials, squelching dissent: FAIR study finds democracy poorly served by war coverage', *Extra!*, May/June 2003. The news programs studied were ABC World News Tonight, CBS Evening News, NBC Nightly News, CNN's Wolf Blitzer reports, Fox's Special Report with Brit Hume, and PBS's Newshour with Jim Lehrer.



share of an online audience, it's also true that more people are using the Internet as their primary news source, the same handful of companies run these sites.<sup>810</sup>

The '100 Orders' penned by former US administrator in Iraq L.Paul Bremer include Order 65 passed March 20 2004 to establish an Iraqi communications and media commission. This commission has powers to control the media because it has control over licensing and regulating telecommunications, broadcasting, information services and all other media establishments. The media commission sent out an order asking news organisations to 'stick to the government line on the US led offensive in Fallujah or face legal action'.<sup>811</sup> It would be a worthwhile undertaking to look at <http://www.iraqbodycount.net/resources/Fallujahh/index.php>, which archives three hundred selected news stories on the April 2004 siege of Fallujah.

In an article in the Guardian Dahr Jamail, an unembedded journalist in Iraq, noted that refugees from Fallujah told him that 'civilians carrying white flags were gunned down by American soldiers. Corpses were tied to US tanks and paraded around like trophies'.<sup>812</sup>

American documentary film-maker Mark Manning returned from Fallujah after delivering supplies to refugees. Manning was able to secretly conduct 25 hours of videotaped interviews with dozens of Iraqi eyewitnesses. In an interview with a

---

<sup>810</sup> Chris Murray, legislative counsel for Consumers Union quoted in Glasner, J: 'Media more diverse? Not really', wired news 30/5/03



local newspaper in the US, Manning recounted how he was told grisly accounts of Iraqi mothers killed in front of their sons, brothers in front of their sisters, all at the hands of American soldiers. He also heard allegations of wholesale rape of civilians, by both American and Iraqi troops. Manning said he heard numerous reports of the second siege of Fallujah [November 2004] that described American forces deploying – in violation of international treaties – napalm, chemical weapons, phosphorous bombs, and ‘bunker-busting’ shells laced with depleted uranium.<sup>813</sup>

A Los Angeles Times scoop (3/6/04) revealed that one of the most enduring images of the war – the toppling of the statue of Saddam Hussein in a Baghdad square on April 9, 2003, was a US Army psychological warfare operation staged to look like a spontaneous Iraqi action: ‘As the Iraqi regime was collapsing on April 9, 2003, Marines converged on Firdos Square in central Baghdad, as was widely assumed from the TV images – who decided to topple the statue, the Army report said. And it was a quick thinking Army psychological operations team that made it appear to be a spontaneous Iraqi undertaking’.<sup>814</sup>

As Gardiner sums it up:

---

<sup>811</sup> Jamail, D: ‘Media repression in “Liberated” Land’, [www.dissidentvoice.org](http://www.dissidentvoice.org), 18/11/04

<sup>812</sup> Steel, J and Jamail, D: ‘This is our Guernica’, The Guardian, 27/4/05

<sup>813</sup> Welsh, N: ‘Diving into Fallujah’, Santa Barbara Independent, 17/3/05, [www.independent.com/cover/Cover956.htm](http://www.independent.com/cover/Cover956.htm)

<sup>814</sup> Fair.org: ‘The return of PSYOPS: Military’s media manipulation demands more investigation’, Media Advisory, [www.fair.org](http://www.fair.org), 12/3/04

Among the fabricated stories was the early surrender of the commander and the entire 51<sup>st</sup> Iraqi mechanized division. We were told of an uprising in Basra – it did not happen. We were told on White House and State Department web sites that Iraqi military has formed units of children to attack the coalition – untrue. We were told of a whole range of agreements between the French and Iraq before the war over weapons – false. We were told Saddam had marked a red line around Baghdad and that when we crossed it Iraq would use chemical weapons – completely fabricated.<sup>815</sup>

Again, in ‘psy-op’ terms, on the evening of October 14, a young Marine spokesman near Fallouja appeared on CNN and made a dramatic announcement. ‘Troops crossed the line of departure’, 1<sup>st</sup> Lt. Lyle Gilbert declared, using a common military expression signalling the start of a major campaign. ‘It’s going to be a long night.’<sup>816</sup> CNN, which had been alerted to expect a major news development, reported that the long-awaited offensive to retake the Iraqi city of Fallujah had begun. In fact, the Falloujah offensive would not kick off for another three weeks. As Mazetti explains, Gilbert’s carefully worded announcement was an elaborate psychological operation –or ‘psy-op’- intended to confuse insurgents in Falloujah and allow US commanders to see how guerrillas would react if they believed US troops were entering the city, according to several Pentagon officials.<sup>817</sup>

---

<sup>815</sup> Gardiner, S: ‘The enemy is us’, [Salon.com](http://Salon.com), 22/9/04

<sup>816</sup> Mazzetti, M: ‘PR meets Psy-Ops in War on Terror’, [www.latimes.com](http://www.latimes.com), accessed 24/1/05

<sup>817</sup> *ibid.*



A report by the Defense Science Board, a panel of outside experts that advises Defense Secretary Donald Rumsfeld, concluded that a 'crisis' in US 'strategic communications' had undermine American efforts to fight Islamic extremism worldwide. The study cited polling in the Arab world that revealed widespread hatred of the United States throughout the Middle East. A poll taken in June by Zogby International revealed that 94% of Saudi Arabians had an 'infavorable' view of the United States, compared with 87% in April 2002. In Egypt, the second largest recipient of US aid, 98% of respondents held an unfavourable view of the United States.<sup>818</sup>

In May 2004, photos of Iraqi prisoners being humiliated by US soldiers popped up all over the web as the internet once again proved to be the place millions of people turned to get information on a big story. While American newspapers were careful in how many and which prisoner photos they printed, lots of websites posted as many images as they could find in great graphic detail. Among the sites were [www.thememoryhole.org](http://www.thememoryhole.org) and [www.globalsecurity.org](http://www.globalsecurity.org), a global think tank, which posted the full text of the army's report into the Abu Ghraib abuse and other documents on the Iraq prison scandal. Among the many activist sites covering the prison scandal were ElectronicIraq ([electroniciraq.net](http://electroniciraq.net)) and [AlterNet.org](http://AlterNet.org). Weblogs also posted exhaustive commentary on the naked pictures that were first publicised on CBS's '60 Minutes II'. English-language website al-Jazeera ([english.aljazeera.net](http://english.aljazeera.net)) published more subdued coverage such as a photo gallery

---

<sup>818</sup> *ibid.* For more on the poll, visit [www.zogby.com](http://www.zogby.com)



showing Muslims protesting outside the prison and a survey of site visitors in which 62 per cent of the 72,840 respondents said they suspected that abuse of Iraqi prisoners was routine.<sup>819</sup>

Paul Taylor explores the extent to which the 'mental atmosphere' of the Abu Ghraib prison reflects more widespread values within the western mediascape that has become increasingly synonymous with our idea of public discourse.<sup>820</sup> As Taylor very intelligently puts it, Baudrillard's notion of the ecstasy of communication was implicitly acknowledged by Donald Rumsfeld who complained that it was much harder nowadays to control information sent back home by soldiers serving overseas. Unlike conventional letters in which the censors can black out the offending parts, Rumsfeld bemoans the fact that US soldiers were 'running around with digital cameras and taking these unbelievable photographs and then passing them off, against the law, to the media, to our surprise'.<sup>821</sup>

Specifically in the light of Abu Ghraib, Sontag points out that although 'trophy' pictures have been taken in many previous military and social conflicts, these particular photographs:

---

<sup>819</sup> Walker, L: 'Iraq prison scandal at its most graphic', Washington Post, 9/5/04

<sup>820</sup> Taylor, P: 'The pornographic barbarism of the self-reflecting sign', fwd in email, undated.

<sup>821</sup> Sontag, S: 'What have we done?', The Guardian G2 Section, 13/5/04, as quoted in Taylor, P: 'The Pornographic barbarism of the self reflecting sign'. Also look her work Sontag, S: (2003) *Regarding the Pain of Others*, Farrar, Strauss and Giroux.

...reflect a shift in the use of pictures – less objects to be saved than evanescent messages to be disseminated, circulated...now the soldiers themselves are all photographers – recording their war, their fun, their observations of what they find picturesque, their atrocities – and swapping images among themselves, and emailing them around the globe, it was all fun. And this idea of fun is, alas, more and more – contrary to what Mr. Bush is telling the world – part of the “true nature and heart of America”.<sup>822</sup>

It is worth mentioning how online newspapers operate here. With the net able to supply information almost instantly, newspapers had little choice but to put everything they publish every day up on the internet in the hope of keeping people on their site and returning to their site the next day. The struggle has always been how to make money by charging for the content while also keeping as many people as possible visiting the site to make it attractive to advertisers with the ever-present back-of-the-mind fear that free and diverse online content will stop people buying printed newspapers.

According to K. McCarthy, newspaper websites and their content have gradually become split into six areas: First, news stories which are free and will always be. After a week, though, these stories become archive stories and access to them may be charged for. Second, columnists and opinion pieces news items that are exclusive and identifiable to the individual paper. Third, email services - giving people a concise rundown of stories that are likely to interest them direct to their

---

<sup>822</sup> Sontag, S: ‘What have we done?’, The Guardian G2 Section, 13/5/04 quoted in Taylor as



inboxes. Fourth is the digital facsimile of the printed newspaper - whether in internet-standard jpeg images, PDF files or using some proprietary software. And finally there are the add-ons: crosswords, competitions, games, etc.<sup>823</sup>

To continue, MoveOn.org, already mentioned for its successful anti-war efforts, concluded the same in a recent advertising campaign, which featured media mogul Rupert Murdoch under the banner, '[t]his man wants to control the news in America', claiming that Murdoch's News Corp, Disney, Viacom, GE and AOL Time Warner control 75 per cent of the total television audience and 90 per cent of the television news audience for broadcast and cable in the United States.<sup>824</sup> Under this light it is worrying that the Federal Communications Committee is considering scrapping decades old regulation that have kept one or two companies from dominating news.

In the first week of the war, internet traffic ran at twice the usual rate, according to ComScore Media Metrix. The at-work audience reached 36.5 million people on that particular Wednesday, almost matching the home audience of 37.1 million. Yahoo.com was among the places where usage skyrocketed. The volume of traffic to its news selection jumped 600 per cent on Thursday and Friday and CNN.com had the most traffic of all news sites: 9 million visitors. MSNBC was next with 6.8 million. The website of Britain's BBC drew nearly half a million visitors from the US alone on the Sunday of the same week, 60 percent more than

---

before

<sup>823</sup> McCarthy, K: 'This is the future of online newspapers', posted 9/7/03



usual. The BBC site drew a worldwide audience of 3.1 million visitors on Sunday, while the top news site, CNN, drew 4.3 million.<sup>825</sup> Traffic also increased rapidly on anti-war websites, where on average, three leading protest sites ([www.antiwar.com](http://www.antiwar.com); [www.unitedforpeace.org](http://www.unitedforpeace.org); [www.stopwar.org.uk](http://www.stopwar.org.uk)) drew 160 per cent more traffic than they did four weeks previously.<sup>826</sup> Also, according to Hitwise's media alerts service, which trawls 11,000 articles daily (covering the top 300 global news and media sites), 40 per cent of articles that week related to the war against Iraq. For the week ending 22 March, news websites accounted for a 22.47 per cent share of all web traffic in the UK, an increase of 9 per cent.<sup>827</sup>

Moreover, three-quarters of online Americans (77 per cent) have used the internet in connection with the war in Iraq. More than half of the nation's 116 million adult internet users have used email to communicate or learn about the war.<sup>828</sup> According to the PewInternet study 17 per cent of online Americans say their principal source of news is the internet and in the days before the war broke out, 37 per cent of internet users got news on a typical day. Interestingly, war opponents are slightly more likely than supporters to report intensified internet use.

---

<sup>824</sup> Glasner, J: 'Media more diverse? Not really', wired news 30/5/03

<sup>825</sup> Walker, L: 'Casting a wider net for world news', Washington Post, 26/3/03

<sup>826</sup> Walker, L: 'Web use spikes on news of war', Washington Post, 21/3/03

<sup>827</sup> Europemedia.net: 'War dominates the Web', report

<sup>828</sup> Rainie, L, Fox, S and Fallows, D: 'The Internet and the Iraq war: How online Americans have used the Internet to learn war news, understand events and promote their views', Pew Internet and American Life Project, [www.pewinternet.org](http://www.pewinternet.org)

Another contribution of the internet to this war was in the form of 'blogs'. Blogging is an easy and fast way for personal publishing on the web. Some examples are indicative of the potential for citizen journalism. During extensive flooding, CNN and the BBC and others received powerful firsthand accounts by email long before camera crews and correspondents were on the scene. The email newsgathering was vivid and also included colour stills which were posted into website galleries hours before newspapers published their accounts.<sup>829</sup> To a lesser extent, blogging was experienced during the NATO bombing of Belgrade in 1999.

In South Korea, OhmyNews, which publishes 200 stories a day, mostly written by more than 26,000 registered citizen journalists, has 2 million daily readers and has been widely credited as helping elect South Korea's new Prime Minister.<sup>830</sup> By some measures, South Korea is the most wired country in the world, with broadband connections in nearly 70 percent of households. Around election time OhmyNews was registering 20 million page views per day. The service averages about 14 million visits daily, in a country of only about 40 million people.

---

<sup>829</sup> Cramer, C: 'How the net will play a key role in this war', The Observer, 9/3/03. Also, there is an interesting quote on interactivity of the medium by Nigel Chapman, the deputy director of the BBC World service in Lawson, A: 'War prompts text message boom', The Guardian: 'Suddenly text messaging appears to have moved on from personal communication to personal statement...New technologies are giving us a level of interaction with our audiences that we have never seen before'. According to the same article the volume of text messages to the broadcaster has grown tenfold since March to a total of 6,000. Talking point, the show that enables listeners to quiz world leaders has received more than 160,000 emails from listeners commenting on the war. BBC Arabic version of Talking point in its launching day received 3,000 emails.

<sup>830</sup> Kahney, L: 'Citizen reporters make the news', [www.wired.com](http://www.wired.com), 17/3/03



In June 2003, Iranian blogs gave voice to dissidents ([www.hoder.com](http://www.hoder.com), [www.iranian.com](http://www.iranian.com)) while a growing network of Iranian-American media outlets have been aiding the student-led protests. In another instance, bloggers reported alternative news from a G8 meeting.<sup>831</sup> During the Iraq conflict, a blogger called Salam Pax<sup>832</sup>, blogging from Baghdad ([Dear\\_raed.blogspot.com](http://Dear_raed.blogspot.com)), and Christopher Allbriton, A New York based veteran journalist ([Back-to-iraq.com](http://Back-to-iraq.com)), have been profiled in many news stories. Reporters of *Time* magazine, the BBC and other leading news outlets had their own blogs. Kevin Sites, a CNN correspondent, posted pictures, audio and commentary on his website from the Kurdish section of Iraq. CNN asked Sites to suspend the blog.

The effect blogging had on coverage might not have been profound in this war<sup>833</sup>, but it is an indication perhaps of where war coverage might be going.

For all the saturation coverage of the invasion of Iraq, this has become the first true Internet war, with journalists, analysts, soldiers, a British lawmaker, an Iraqi exile and a Baghdad resident using the medium's lightning speed to cut the fog of

---

<sup>831</sup> Theodoulou, M: 'Proliferating Iranian weblogs give voice to taboo topics', Christian Science monitors, 23/6/03; Dobbs, M: 'Iranian exiles sow change via satellite', Washington Post, 25/6/03; Curiel, J: 'North American media help Iran protests grow', San Francisco Chronicle 20/6/03; Batista, E: 'Bloggers report alternative news from G8', wired, 4/6/03

<sup>832</sup> The Iraqi blogger was later revealed to be the interpreter of Slate Journalist Peter Maas, White, C: 'Iraqi blogger revealed', dot journalism, 12/6/03. Salam Pax's site featured in hundreds of news stories, including pieces by MSNBC, the BBC, the New York times and the Washington post. The bandwidth demands caused by the ensuing stampede of visitors overwhelmed servers, to the extent that Taylor Suchan who runs Industrial Death Rock and Pyxz.com out of Texas, said he directed the links from the original photos to a parody image out of frustration, after trying contacting both Pax and Blogger, but received no response. The images on Suchan's servers are being viewed on average at least 140,000 times a day (Delio, M: 'Iraq Blog: Hubbub over a headlock', wired, 26/3/03)



war. The result is idiosyncratic, passionate and often profane, with the sort of intimacy and attitude that are all but impossible in newspapers and on television.<sup>834</sup>

Kurtz also cites law professor Glenn Reynolds, whose site, InstaPundit.com, saw a surge in traffic as the Iraq crisis has heated up, doubling to 200,000 hits a day.

The most interesting thing about the blog coverage is how far ahead it is of the mainstream media. The first hand stuff is great. It's unfiltered and unspun. That doesn't mean it's unbiased. But people feel like they know where the bias is coming from. You don't have to spend a lot of time trying to find a hidden agenda.<sup>835</sup>

Because of their personal nature, weblogs have served as a great filter for the pro- and anti-war lobbies, but apart from the now globally famous Iraqi blogger Salam Pax, very few of these sites actually gives new information. The wire services, broadcasts and newspapers have the most journalists close to the fighting and are able to fire reports off instantly through TV, radio and the web. And this is perhaps where electronic media have made the biggest difference. The BBC's very successful rolling weblog of all correspondents in the Gulf and the US

---

<sup>833</sup> The PewInternet survey on how online Americans use the internet and the Iraq war shows that blogs are gaining a following, but are not yet a source for the majority of users. Some 4% of online Americans report going to blogs for information and opinions. ([www.pewinternet.org](http://www.pewinternet.org))

<sup>834</sup> Kurtz, H: 'Webloggers, signing on as war correspondents', Washington Post, 22/3/03

<sup>835</sup> *ibid.*

carried a mention of the missile hitting the Baghdad marketplace before it made it to air.<sup>836</sup>

However, the global internet audience is still in its earliest stages. Only about 5 per cent of the world's population can access the internet, according to Nielsen/Net Ratings. It is hard to fathom what will happen to world opinion should net use reach 50 per cent or more.<sup>837</sup> Notably, UN Secretary-General Kofi Annan, before the World Electronic Forum, a summit of world leaders in December 2003, said that the focus should be on expanding internet use and reaffirming media freedoms and the rights of ordinary people to stay informed.

The information summit centred on whether the United Nations should have more control on the internet, since the key decisions are made by a private, US-based organisation of technical and business experts known as the Internet Corporation for Assigned Names and Numbers (ICANN), and as well as who will pay for getting more poor nations online. The broadcasters asserted that the future is not only online, since radio and TV will remain dominant means of mass communication in many poor countries for decades.<sup>838</sup> One of the main areas of conflict was over who should pay for technology projects in the developing world. African nations have been rallying behind a proposal from Senegal to set up a new 'digital solidarity fund'. Many industrialised nations are wary of

---

<sup>836</sup> Bell, E: 'The blogs of war', *The Observer*, 30/3/03

<sup>837</sup> Walker, L: 'Web use spikes on news of war', *Washington Post*, 21/3/03

<sup>838</sup> 'Kofi Annan: Keep media free!', *wired*, 9/12/03

creating a new UN fund, instead supporting investment by private companies and redirecting existing fund.<sup>839</sup>

---

<sup>839</sup> 'Discord at digital divide talks', BBC online, 29/9/03



### 6.3 The impact of the war on the internet itself

The possibility of war with Iraq and the actual war caused cyberattacks between pro-islamic/anti-islamic hackers (ethnoreligious cyberconflict) and pro-war/anti-war hackers (sociopolitical cyberconflict).<sup>840</sup> Despite the official US government warning against patriotic hacking,<sup>841</sup> the most notorious incident occurred when the al-Jazeera website was knocked offline by an American web designer. In an incident originally thought to be perhaps an inability of the site to deal with traffic,<sup>842</sup> the site was disabled by hackers for long periods of time. The Arabic news broadcaster's domain name was redirected to patriotic web pages or porn sites.<sup>843</sup> According to Ballout, an employee of Network Solutions was tricked into giving the culprit a confidential password that allowed the hacker to temporarily

---

<sup>840</sup> For more on this distinction look at Karatzogianni, A: 'The politics of cyberconflict', *Journal of Politics* February 2004, vol. 24 (1), pp. 46-55

<sup>841</sup> 'Government warns "Patriotic hackers" against cyberattacks on Iraqi interests', 12/2/03, Associated Press

<sup>842</sup> Knight, W: 'Key Arab news station knocked offline', new scientist.com cites P.Huggins a security expert interpreting as such, which goes to show how problematic internet security diagnosis can be.

<sup>843</sup> Users trying to log onto the al-Jazeera website in the US found a message that read 'hacked by Patriot, Freedom Cyberforce Militia', beneath the logo of the US flag (Deans, J: 'Hackers divert al-Jazeera users to US porn and patriot sites', *The Guardian*, 28/3/03). According to Ballout, an employee of Network Solutions was tricked into giving the culprit a confidential password that allowed the hacker to temporarily assume total control of Al Jazeera's domain (Delio, M: 'Hackers condemn Arab site hack', *wired* 31/3/03). Despite this social engineering tactic, at the time it was also reported that the likely technique was DNS poisoning, which fools traffic-directing computers across the Internet, similar to vandalising exit signs on an interstate to misdirect travelers. It is relatively difficult to defend against (Associated press: 'Hackers beat up on al-jazeera', AP, 27/3/03). Finally, in a plea agreement with the US Attorney's office, John William Racine, a 24-year old web designer admitted to tricking VeriSign subsidiary Network Solutions into giving him ownership of the aljazeera.net domain. He turned himself in to FBI agents on 26<sup>th</sup> of March, according to the plea agreement. He could have faced 25 years in prison, but if the judge agrees to the plea he is getting three years of probation and 1,000 hours community service ('Al-Jazeera hacker admits guilt awaits sentence', [www.silicon.com](http://www.silicon.com)).

assume total control of Al Jazeera's domain.<sup>844</sup> Al-Jazeera became the internet's number one search query for 48 hours, according to web portal Lycos. The reason was that people were hunting for video footage that al-Jazeera had aired of dead American soldiers and US prisoners being interrogated by their Iraqi captors - including gruesome images that American TV networks mostly declined to show. Most foreign news sources<sup>845</sup> noted that the US media had shown images of Iraqi prisoners before demurring on showing the American prisoners of war.<sup>846</sup>

Yet, this only gives a small taste of what really happened before and during the war. Cyberattacks were occurring as early as October 2002, debating virtually the situation in Iraq. London-based computer security firm mi2g said October 2002 was the worst month for digital attacks since its records began in 1995. It estimated 16,559 attacks were carried out on computer systems and websites during that month. But the computer security firm said the economic damage caused by the attacks is decreasing, reflecting a decline in the quality of targets chosen. According to mi2g, which monitors the hacking of websites, the number of attacks by groups opposed to action in Iraq, as well as Israeli attacks on Palestinians, rose tenfold that month. 'We have noticed that more and more Islamic interest hacking groups are beginning to rally under a common anti-US, UK, Australia, anti-India and anti-Israeli agenda. The most active hacking groups

---

<sup>844</sup> Delio, M: 'War worms inch across internet', wired, 21/3/03

<sup>845</sup> Walker, L: 'Casting a wider net for world news', Washington post, 26/3/03 writes: Typical was this report in Australia's Age which said US media 'had little hesitation in running graphical pictures of surrendering, captured, dead or dying Iraqi soldiers', and concluded: 'It was a powerful insight into the enormous sway that the Bush Administration and the Pentagon exert over the media's coverage of the Iraq war'.

<sup>846</sup> Walker, L: 'Casting a wider net for world news', Washington post, 26/3/03



are USG, with members from Egypt, Morocco and Eastern Europe, and FBH which is based in Pakistan'.<sup>847</sup> Unix Security Guards (USG) defaced nearly 400 websites in a single day with antiwar slogans written in Arabic and English, according to iDefense.<sup>848</sup>

When the war actually started, Zone-H, a firm that records and monitors hackings reported 20,000 defacements in the first week of the war. Hundreds of US and British business, government and municipal websites were defaced with anti-war messages, security experts reported. Seemingly within hours, more hawkish hackers went on the offensive against Arab sites. Roberto Preatoni, founder of Zone-H commented at the time: '[t]his is the future of protest. If you take down Al-Jazeera, every body around the world knows it. And you never have to leave your house'.<sup>849</sup>

As a result of the escalating conflict, thousands of websites were the target of Denial of Service attacks, defacement, worms and viruses.<sup>850</sup> According to F-Secure, another security firm, the majority of defacements were from anti-war hackers, with anti-war messages or images, including ones comparing the

---

<sup>847</sup> 'Islamic hackers step up attacks', BBC news, 29/10/03

<sup>848</sup> Krebs, B: 'Websites vandalised with antiwar messages', Washington Post, 20/3/03

<sup>849</sup> 'War attacks tit for tat', Reuters, 28/3/03

<sup>850</sup> Delio, M in 'War worms inch across internet', 21/3/03 reports that at least three email viruses that their authors claim they were released in response to the war made rounds on the Net. Virus writers often include messages tied to current concerns like war, or eternal human urges like lust, to get people to open infected attachments. In widest circulation is Ganda, a low security threat by most security firms. Once attachments with references to the current military action are opened on PCs running Windows, Ganda behaves like many other email worms, emailing itself to all the addresses in the affected machine's Outlook contact list. It also scans the machine for security software and shuts them down.



physical similarity between US president George Bush and a monkey, scrawled across various homepages. On the Sunday after the initial bombing, 10 Downing Street's website was inaccessible, having been the target of a distributed Denial of Service assault<sup>851</sup> and then in mid-June hackers put up a picture of President Bush carrying his dog, with Prime Minister Tony Blair's head superimposed on it.<sup>852</sup> 'At the moment we are tracking over a thousand such defacements, most with anti-war messages', commented Jason Halloway of F-Secure. 'I have never seen that level of political hacktivism before, nor so many defacements in such a short time'.<sup>853</sup>

Defacements and denial of service were accompanied by at least three war-related worms - Ganda, Lisa and Wanor - which shut down security, delete critical system files or erase hard drive data.<sup>854</sup> However, according to Symantec, most attacks, including one in October 2002 that brought down nine of the 13 servers that support the internet, cannot get around the fact that, when online traffic is disrupted or blocked in one place, it tends to flow through thousands of alternate channels instead.<sup>855</sup> With most netwarriors wanting the internet up and running, such attacks are symbolic and do not aim to bring down the net. Symantec itself has been in the centre of controversy a generous amount of times and in different cases –as mentioned throughout this thesis. In this particular antiwar cyberconflict, American online activist David Swanson says ISP Comcast, and

---

<sup>851</sup> 'Iraq invasion leads to massive increase in pro-war, anti-war hacker activity', europemedia.net, 1/4/03

<sup>852</sup> 'Britain's Labour Party website hit by hackers', Reuters, 16/6/03

<sup>853</sup> *ibid.*

security services company Symantec, blocked emails with 'www.afterdowningstreet.org' in the body of the email for a week. The emails were drawing attention to the so-called Downing Street memo, first published in the Times newspaper, which shows that the Iraq war was planned well in advance. A spokeswoman for Symantec said that a spam rule was created due to an increase in email traffic, but was later turned off for being too broad.<sup>856</sup>

Nevertheless, the truth of the story is that such activities are not appreciated by hackers, who in many instances have served as scapegoats for script kiddies<sup>857</sup> with moderate computer skills. Oxblood Ruffin, director of Hactivismo, a group that develops tools to circumvent censorship, has commented that 'the individual(s) who did this are committing a computer crime and causing censorship'.<sup>858</sup> Robert Ferrell, a security researcher, adds that '[m]ost of them have no clear grasp of the causes they are supposed to be supporting or fighting against. They just want to appear 'hacktivists', because that's a cool label to have'.<sup>859</sup> And Mark Loveless, a hacker working for US security software

---

<sup>854</sup> Krebs, B: 'Websites vandalised with antiwar messages', Washington Post, 20/3/03

<sup>855</sup> McMillan, R: 'Wartime internet security is business as usual', Washington Post, 27/3/03

<sup>856</sup> Symantec itself has been in the centre of controversy a generous amount of times and in different cases –as mentioned throughout this thesis. In this particular antiwar cyberconflict, American online activist David Swanson says ISP Comcast, and security services company Symantec, blocked emails with 'www.afterdowningstreet.org' in the body of the email for a week. The emails were drawing attention to the so-called Downing Street memo, first published in the Times newspaper, which shows that the Iraq war was planned well in advance. A spokeswoman for Symantec said that a spam rule was created due to an increase in email traffic, but was later turned off for being too broad.(Varghese, S: 'ISP "censored" anti-war email', Sydney Morning Herald, 27/7/05, accessed 2/8/05.)

<sup>857</sup> According to the New Hacker's Dictionary script kiddies do mischief with scripts and programs written by others, often without understanding the exploit, Delio, M: 'Hackers condemn Arab site hacked', wired, 31/3/03.

<sup>858</sup> Delio, M: 'Hackers condemn Arab site hacked', wired, 31/3/03.

<sup>859</sup> *ibid.*



company Bindview, put it this way: '[i]n a protest or activist scenario, one would hope that one's cause and message were strong enough that 'shouting down' the opposing viewpoint is considered unnecessary'.<sup>860</sup>

In fact, the US government used the internet for the first time in a campaign aimed at Iraqi email addresses, spamming recipients to contact the UN if they wanted to defect. Saddam responded by shutting down internet service providers.<sup>861</sup> The US action was quite a paradoxical venture, since only 12,000 of Iraq's 12 million people were online. Also the US was censoring troops' emails to family and friends to prevent leaks of sensitive information. Yet, the real potential of cyberwar for the US military probably lies in the military use of a highly secure intranet and wireless systems that speed audio, video and other data back to command and control systems, as noted by Winn Schwartau, a cyberwar expert.<sup>862</sup>

US diplomacy officially entered the electronic age with the completion of a two-year project to provide internet access to all US embassies and consulates, with some 44,000 foreign service officers and other embassy staffers able to access the web at Washington's more than 260 far-flung diplomatic missions from Afghanistan to Zimbabwe.<sup>863</sup> Accordingly, the US Department of State is well aware of the information warfare threat, as are the diplomatic departments of the

---

<sup>860</sup> 'War attacks tit for tat', Reuters, 28/3/03

<sup>861</sup> Cramer, C: 'How the Net will play a key role in this war', The Guardian, 9/3/03

<sup>862</sup> Tsuruoka, D: 'Internet, wireless to play key role in an Iraq war', yahoo news, 17/03/03

<sup>863</sup> 'US cyber-diplomacy now up and running', YahooNews, 29/10/03



top industrial nations. However, the extent of knowledge of the average diplomat and the staff of embassies and consulates around the world remains questionable.

It was also the first war 'in which thousands of hours of digital imagery will be shot of actual combat. A lot will be from unmanned aerial vehicles flying over the battlefield'.<sup>864</sup> As Der Derian notes, the Pentagon's current gospel is network-centric warfare,<sup>865</sup> an observation also found extensively in the work of Arquilla and Ronfeldt.<sup>866</sup> As Der Derian graphically puts it:

Command and control networks, like the air defense networks, will be taken out with missiles and possibly even electromagnetic pulse weapons. Prime time/cable networks will be red hot with war fever and coverage. NGOS will roll out humanitarian networks. Anti-war networks will send out marching orders. Soldiers, sailors and airman will email stories back home. This war will be started and ended by networks.<sup>867</sup>

---

<sup>864</sup> Keht Lee, CEO of East View Cartographic, a firm that sells satellite-generated maps and other digital imagery, quoted in Tsuruoka, D: 'Internet, wireless to play key role in an Iraq war', yahoo news, 17/03/03. Also, Associate Press also reported the possibility of the US military using 'e-bombs', which create a brief pulse of microwaves powerful enough to fry computers, blind radar, silence radios, and disable electronic ignitions in vehicles and aircraft. However, despite the e-bombs being classified, military analysts believe their range is a few yards at most ('E-bombs aims to stun Iraqi forces', AP, 19/3/03).

<sup>865</sup> McClellan, J: 'War on the Web', The Guardian, 19/2/03

<sup>866</sup> For more look at Arquilla, J and Ronfeldt, D: (2000): *Swarming and the Future of Conflict*, California: Rand. And Arquilla, J and Ronfeldt, D (eds.): (2001) *Networks and Netwars: The Future of Terror, Crime and Militancy*, California: Rand.

<sup>867</sup> McClellan, J: 'War on the Web', The Guardian, 19/2/03

## *Conclusion*

Following the integrated theoretical model proposed in section 2.4, we can make relevant links with the empirical analysis undertaken above. Interestingly, all the components of the framework are represented in this particular conflict. I will not get into the first component on the environment of real conflict, because it is explained more thoroughly in the theoretical sections, nor into the virtual conflict environment, because this is explained in general terms in chapter 3 and, for the Iraq War example, in section 6.3.

If we look for instance at the mobilisation structures (2a), they were greatly affected by the internet. The peace groups were organising demonstrations and events through the internet, to the effect that 10 million people protested against the war globally, with the net speeding up mobilisation remarkably. It helped mobilisation in loose coalitions of small groups that organised very quickly, at the same time preserving the particularity of distinct groups in network forms of organisation.

Moreover, the framing process (2b) was affected as well, since email lists and websites were used to mobilise, changing the framing of the message to suit the new medium. The language used to mobilise through the internet differs from traditional political discourse (for instance, speeches or texts in traditional media)

in that it can combine various technical media (video, satellite images, file-sharing) in a way that delivers on the one hand a richer message, but on the downside a sometimes hasty and crude, under-analytical political message. The political opportunity structure (2c) in this particular case can refer to the rise of alternative media (as we see below), but also to an opening of political space, and an opening of global politics to people who would not or could not get so involved before. In virtual terms, hacktivism (2d) was apparent in anti-war/pro-war hacking, anti-Islamic/pro-Islamic hacking and a Virtual March on Washington which had an impact on the city's communication infrastructure.

On the hacking front, the pro-Islamic/anti-Islamic hacking is an example of ethnoreligious cyberconflict and we can see the link with ethnoreligious affiliation and discourses of exclusion/inclusion (3a, 3b), if we consider the al-Jazeera hack from American hackers, and the movement of Islamic hackers united in a common anti-US, UK, Australia, anti-Indian and anti-Israeli agenda. Furthermore, the use of the internet as a propaganda and mobilisational tool (3c) is common to both sides (anti- and pro-war) through a considerable amount of websites advocating one view or another and mobilising, countermobilising and anti-mobilising against each other.

On the media front, it is clear that political discourse (4a) is constructed in the American mainstream media to mobilise support for the war as analysed above, since, for example, more than two-thirds of all sources in news programs were



pro-war. Very important is also the issue of alternative sources and censorship (4b). Due to the embedded system, journalists having their work jeopardised for not being 'patriotic' enough, and the American media generally following the government line, Americans and the rest of the world went online to find alternative news and first-hand eyewitness accounts via emails and blogging. The result was the integration of the internet into media coverage and the distribution of online material challenging official sources. The Wolfsfeld model (4c) is comfortably applied when we consider that the anti-war groups had the ability to initiate and control protest events and to mobilise supporters, but were not as successful in dominating political discourse. The media effects on policy (4d) are more technical than anything else, meaning there was instant 24-hour access to the war and the pressure that inevitably puts on any administration, but no actual debate or impact on policy, since the American media failed to question any decisions being taken by their government.

In the final analysis, the internet played a distinctive role in the spread of the peace movement, on war coverage and on war-related cyberconflicts, in relation to which we witnessed the full potential of the new medium in politics. In the months preceding the actual war in Iraq, we witnessed a plenitude of phenomena on and off the internet that in previous international conflicts were only embryonic. Anti-war groups used email lists and websites, group text messages and chatrooms to organise protests and in some cases to engage in symbolic hacking against the opposite viewpoint. The integration of the internet into

mainstream media, the effect of online material challenging official government sources and the mainstream media, and blogging, are an indication perhaps of where war coverage might be going when internet users exceed their present numbers.

The most interesting thing in a brief application of the CC theoretical framework is the level of censorship (2b) and the Wolsfeld model (4c). In terms of censorship the latest literature supports the idea that journalists were not only censored and manipulated (CNN incident), but also targeted in this conflict. Which brings us to whether the US could control information. Apparently through psy-ops, they could manipulate the conflict and control the media, especially the American mainstream ones (almost always submissive to the patriotic/nationalistic discourse after the 9/11) - (4a). Their mentioned inability to control inconsistencies and fiascos from 24 hour internet coverage, blogs and US soldiers using the internet to send pictures (as in Abu Graib prison incident) or to manipulate the American image in the Muslim world is nevertheless another issue. Accordingly, the anti-war movement succeeded in that respect at gradually building their own image of the Americans and their allies and framing their message (no WMD, dodgy dossiers, humanitarian concerns etc) (2b).

## **Conclusion**

This thesis addressed the problem of political conflicts in computer-mediated environments (cyberconflicts). Firstly, I questioned how modernist concepts like power, participation and democracy fit into a global postmodern medium, the internet, in an era of globalisation. Then I argued for and analysed three theories, media theory, social movement theory and conflict theory, as a way to understand the two kinds of conflict I identified (ethnoreligious and sociopolitical), thereby deriving and proposing an integrated analytical framework for cyberconflict. Thirdly, I proceeded with an analysis of the cyberconflict environment, by way of investigating the historical background for the phenomenon of cyberconflict, information warfare, cyberterrorism and internet security analysis.

In the empirical chapters, I analysed these two types of cyberconflict giving examples such as the Israeli-Palestinian, the Indian-Pakistani and the anti-war and anti-globalisation cyberconflicts, and including a discussion on cyberdissidents' conflicts with governments. The conclusions in the empirical chapters presented a possible application of my theoretical framework for cyberconflict to the empirical evidence, for an easier understanding of cyberconflict and its consequences for our political world.

Information communication technologies act as a force multiplier, enhancing power and enabling social actors to punch above their weight and attain a reach and influence previously denied to them. The groups that use the internet are able



to communicate messages to a wider audience than that reached by more traditional means of political communication. The promise of nearly unlimited information delivered to your monitor in mere seconds is a promise for a better democracy, since the internet can help to make us more active and more knowledgeable about government. However, this availability of unlimited information may inspire and indeed has inspired those who are already politically active, but it does not necessarily mean that the internet on its own will increase the attentive public.

As far as democracy is concerned, network technologies are increasingly used in public and political debates and communications, thus promoting dialogue between opposing parties - one of the elements of true democracy. New developments in governance such as deregulation, creating independent agencies, privatisation, and governing at a distance are factors resulting from ICTs. New uses of technology such as 'blogging' are the harbinger of a new interactive culture that could potentially change how democracy works, turning voters into participants rather than passive consumers. At the same time, however, technologies intruding upon privacy, surveillance and censorship may impede democratic liberties, due to their catastrophic effect on free speech and freedom of expression.

On the question of participation and the internet, providing greater choice and opportunity only solves the technical problems of participation - for example, that related to reducing the cost of involvement. It does not get to the heart of what

motivates citizens to move from a state of disengagement to one of salutary involvement in civic life. In other words, universal access is not sufficient for realising a democratic polity.

On the question of groups involved pursuing power, the internet offers opportunities for breaking down political hierarchies, while subverting the national boundaries that have helped in part to control flows of information. There is also a growing control of cyberspace by elites who are defined by their technical expertise, that is, the ability to alter the 'thingness' of technology that constructs online life, while the gap between the digital haves and the digital have-nots has been growing. Also, cyberspace appears as a place in which individuals can put aside many of the inequalities of offline life, simply because nobody knows if they are 'really' female, old or disabled. In a way, cyberspace can redefine problems such as the broadening and democratisation of decision-making procedures by removing the constraint of physical presence.

Furthermore, globalisation brings dramatic changes in the transactions and interactions taking place among states, firms and peoples in the world. It involves both an increase in cross-border transactions of goods and services and an increase in flows of images, ideas and people. In such a terrain, the internet seems to be forming a 'cybernation', where its initial subculture evolved a set of acceptable behaviors, a common history and a common identity of beliefs: free speech, protection of civil rights, privacy and freedom of expression, etc. With the



spread of the internet, there is scope for a newly international localism, which is finding expression in virtual communities, with some people going so far as to suggest that a new global cyberstate is forming.

When considering the postmodern nature of the internet, we would have to remind ourselves that the resistance of new media to modernity lies in their complication of subjecthood, their denaturalising of the process of subject formation, and their putting into question of the interiority of the subject and its coherence. The issue of identity is not merely of philosophical importance, but is also an issue of immense practical importance for the conduct of states, not to mention identifying the lines of flight from the status quo. Moreover, the shift from real to hyperreal occurs when we move from mere representation to simulation, a movement already existing in our virtual world. Once the internet moves closer to total connectivity, this metaphorical cyberspace could become the hyperreal - more real than the place it once simulated. The fact that many people believe virtual communities to be real places in which they live real experiences makes this blurring of the real and the unreal closer to Baudrillard's postmodern moment of hyperreal than to representation.

Searching for a satisfactory description of empirical cases of cyberconflict led to the use of a classification between two types of cyberconflict: sociopolitical and ethnoreligious. In order to explain the empirical evidence of 'cyberconflict', I proposed the integration of elements of social movement, conflict and media



theories into a single analytical framework for cyberconflict. I identified elements of social movement theory to discuss sociopolitical cyberconflicts, conflict theory to address ethnoreligious cyberconflicts and media theory as a component for both, deriving a single an integrated analytical framework for understanding cyberconflict.

In the social movement theory chapter, I identified elements of this theory relevant to new social movements using the internet to accomplish their goals of power, democracy and participation. More specifically, I analysed and used the classical resource mobilisation model of mobilising structures, framing processes and the political opportunity structure to analyse how these are affected by the use of the internet by new social movements.

New social movements are not new, but rather, are part and parcel of the dominant modern culture, which makes it difficult to think of movements as flowing as either from 'pre-modern' or 'postmodern' subcultures. However, the structure of NSMs - open, decentralised, nonhierarchical - makes them ideal for internetted communication. The movement is composed of adverse autonomous units that expend an important part of their resources on internal solidarity. A network of communication and exchange keeps the cells in contact with each other. Information and resources circulate in networks and leadership is not concentrated but diffuse. NSMs advocate direct democracy, self-help groups and cooperative styles of social organisation. The fewer and weaker the social ties to

alternative networks, the greater the structural availability for movement participation. Sociopolitical movements, such as the political dissidents in China, can test the limits of a system, pushing the system beyond the range of variations that it can tolerate without altering its structure.

Using conflict theory, I analysed the present situation of conflict between sociopolitical groups, as well as ethnoreligious ones. Neo-liberal governments and institutions face a counter-hegemonic account of globalisation, to which they have responded in a confused and often contradictory way. One of the interesting sides to the argument is that the information revolution is altering the nature of conflict by strengthening network forms of organisation over hierarchical forms. In contrast to the closure of space, the violence and identity divide found in ethnoreligious discourses, sociopolitical movements seem to rely more on networking and rhizomatic structures.

In media theory, the important questions were how information is released and why, how much censorship is taking place and what alternative sources of information are available. I asked these questions in my analysis of the anti-Iraq war/pro-war cyberconflict. The way the war is communicated is as important as the conduct of the war itself. Among many examples, the Moscow LiveJournal incident shows that individuals and protagonists can now send stories quicker than journalists, indicating that the media will have an independent capability to have access to future conflict arenas and to provide real-time visual and audio

coverage of battlefield events. This has consequences for news management by even very powerful states like the U.S.

The analyses of these theories led to an integrated theoretical framework with the following parameters to be looked at while analysing cyberconflicts.

1.Environment of Conflict and Conflict Mapping (real and virtual). The world system generates an arborescent apparatus, which is haunted by lines of flight, emerging through underground networks connected horizontally and lacking a hierarchical centre (Deleuze and Guattari). The structure of the internet is ideal for network groups (since it is a global network with no central authority) and has offered another experience of governance (no governance), time and space (compression), ideology (freedom of information and access to it), identity (multiplicity) and fundamentally an opposition to surveillance and control, boundaries and apparatuses. However, in ethnoreligious cyberconflicts, where the groups' systems of belief and organisation aspire to hierarchical apparatuses (nation, religion, identification with parties and leaders), this network form is not always evident. This is why there is a dual modality of cyberconflict: one rhizomatic and one hierarchical.

2. Sociopolitical Cyberconflicts: The impact of ICTs on: a. Mobilising structures (network style of movements using the internet, participation, recruitment, tactics, goals), b. Framing Processes (issues, strategy, identity, the effect of the internet



on these processes), c. Political opportunity structure (the internet as a component of this structure), d. hacktivism.

3. Ethnoreligious Cyberconflicts: a. Ethnic/religious affiliation, chauvinism, national identity, b. Discourses of inclusion and exclusion, c. Information warfare, the use of the internet as a weapon, propaganda and mobilisational resource d. Conflict resolution, which depends on the legal and organisational framework, the number of parties and issues, the distribution of power, and the content of values and beliefs.

4. The internet as a medium: a. Analysing discourses (representations of the world, constructions of social identities and social relations), b. Control of information, level of censorship, alternative sources, c. Wolsfeld: Political contest model among antagonists: the ability to initiate and control events, dominate political discourse, mobilise supporters, d. Media effects on policy (strategic, tactical, and representational).

The political environment of the internet is analysed not in terms of the internet as a mass medium in the traditional sense, but rather, as a significant new resource used by the opposing parties in a conflict. My approach involves analysing the use of the internet by the parties in a conflict (endogenously) and not just theorising about how the media influence the political outcome of a conflict (exogenously). What was evident from the beginning was that major political and military

conflicts are increasingly accompanied by a significant amount of online activity. Furthermore, cyberattacks are escalating in volume, sophistication and coordination.

The third chapter of my thesis illustrated the environment of cyberconflict placing emphasis on hackers, security experts and internet security analysis. Hacking can potentially perform a variety of benevolent services to the security industry constantly pushing forward the limits of computer security, being an important from of watchdog counter-response to the use of surveillance technology and data gathering by the state. At the same time there is a knowledge gap between computer security and computer underground. There is a scarcity of theoretical knowledge surrounding computer security with various calls for more hands-on experience of security to supplement more formal theory.

A further part of the cyberconflict environment is cyberterrorism: computer-based attacks intended to intimidate or coerce governments or societies in pursuit of goals that are political, religious or ideological. According to Arquilla and Ronfeldt, conflicts increasingly revolve around knowledge and the use of soft power. This would come about with the help of information-age ideologies in which identities and loyalties shift from the nation-state to the transnational level of global civil society. Additionally, netwar is referred to as the low, societal type of struggle, while cyberwar refers more to the heavy information warfare type.

After introducing the technical environment of cyberconflict, I proceeded to describe and analyse specific cases of political conflicts online and link these with the integrated analytical framework. Firstly, I looked at sociopolitical cyberconflicts. Sociopolitical cyberconflicts could be seen as taking two forms, the first being when proper hackers attack virtually chosen political targets, and the second occurring when people organise through the internet to protest or carry through email a political message. Sociopolitical CCs seem to rely heavily on decentralised networks and indicate the use of rhizomatic structure, following the structure of NSMs as discussed above.

Cyberconflicts can act as a 'barometer' of real life conflicts and can reveal the nature and the conflict of the participating groups. The protagonists in sociopolitical cyberconflicts fight for participation, power and democracy. In the case of the anti-globalisation and the anti-capitalist movement, what we see is an alternative programme for the reform of society, asking for democracy and more participation from the 'underdogs', be they in the West or in the developing world. In the anti-war movement, which is a single-issue movement, the demand is for a change in power relations in favor of those that believed the war to be unjustified. In new social movements, networking through the internet links diverse communities such as labour, feminist, ecological, peace and anti-capitalist groups with the aim of challenging public opinion and battle for media access and coverage. Groups are being brought together like a parallelogram of forces following a swarm logic, indicating a web of horizontal solidarities to which



power might be devolved or even dissolved. The internet encourages a version of the commons that is ungoverned and ungovernable either by corporate interests or by leaders and parties.

An early example of hacktivism is the Seattle anti-WTO mobilisation at the end of November 1999, which was the first to take full advantage of the alternative network offered by the internet. The anti-WTO protesters were able to initiate a newsworthy event, putting the other side on the defensive. Using the internet, they could send stories directly from the street for the whole world to see, rendering the flow of information uncontrollable. Thirdly, they were able to mobilise support by promoting an alternative frame for the event.

Dissidents against governments are able to use a variety of internet-based techniques (email lists, email spamming, BBS, peer-to-peer and e-magazines) to spread alternative frames for events and a possible alternative online democratic public sphere. An example of dissidents' use of the internet is spamming e-magazines to an unprecedented number of people within China, a method which provides recipients with 'plausible deniability'. Also, file-trading networks like Kazaa and Gnutella can help dissidents communicate, since they have no central source and are hard to turn off.

Ethnoreligious cyberconflicts primarily include hacking enemy sites and creating sites for propaganda and mobilisational purposes. I provided empirical evidence

and analysis of such conflicts (Israeli-Palestinian, India-Pakistan, China-US, Taiwan-China-Japan, Kosovo, Colombia). In ethnoreligious CC, despite the fact that patriotic hackers can network, there is a greater reliance on traditional ideas, such as the protecting the nation or fatherland and attacking for nationalist reasons. The Other is portrayed as the enemy, through very closed, old and primordialist ideas of belonging to an imagined community.

The brief section on conflict resolution on the internet looks at attempts and experiments and concludes that the internet is a helpful tool that fosters cooperation and dialogue between opposing sides in a conflict, bringing individuals and groups together that would otherwise find it difficult to meet. The three examples I examine (MEVic, MEAF and the Project for Arab-Jewish Dialogue) place an emphasis on community-based diplomacy, interfaith dialogue, and building positive relationship as a platform for resolution.

In the Israeli-Palestinian cyberconflict, we see the use of national symbols when hacking websites, like the Israeli flag, Hebrew text and even a recording of the Israeli national anthem on the Hezbollah home page. This explicitly draws attention to issues of national identity, nationalism and ethnicity. Also, the language used by hackers relies on an 'us' and 'them' mentality, where Israelis and their American supporters, or else Palestinians and Muslims, are portrayed as barbaric, reflecting discourses of inclusion and exclusion. The internet in this cyberconflict became a battleground and was used as a weapon by both sides, and

full-scale action by thousands of Israeli and Palestinian youngsters involved both racist emails and circulating instructions for how to crush the enemy's websites.

Similarly, in the Indian-Pakistani cyberconflict the Indian Army's website was set up as a propaganda tool, and hacked pictures of alleged tortures of Kashmiris by Indians were placed on the site, in a similar propaganda tactic. Also, the internet was used as a weapon, when the worm Yaha was released by Indian hackers. In particular discourses, religion is mentioned (religious affiliation), the word 'brothers' (collective identity and solidarity), and 'our country' and a promised land. In the rest of the examples, similar links can be made with the proposed framework.

In analysing the March 2003 Iraq conflict, I looked at the internet's role in the conflict: its effect on the organisation and spread of the movement, its impact on war coverage and war-related cyberconflicts. These last involved hacking between anti-war and pro-war hacktivists (sociopolitical CC), but also between pro-Islamic and anti-Islamic hackers (ethnoreligious CC).

If we look for instance at the mobilisation structures, they were greatly affected by the internet, since the peace groups were organising demonstrations and events through the internet, mobilising in loose coalitions of small groups that organise very quickly and preserving the particularity of distinct groups in network forms of organisation. Moreover, the framing process was affected as well, since email



lists and websites were used to mobilise, changing the framing of the message to suit the new medium. The political opportunity structure in this particular case refers to alternative media, but also to an opening of political space, or an opening of global politics to people who would not or could not get so involved before.

This thesis identifies a duality of cyberconflict, where ethnoreligious cyberconflicts are mapped as representing/defending loyalties of hierarchical apparatuses and sociopolitical cyberconflicts are empowering network forms of organisation. The thesis also promotes the argument that actors in ethnoreligious CC need to operate in a more *network* fashion, if they are fighting network forms of terrorism or resistance. Actors in sociopolitical CC need to operate in a more *organised* fashion, if they are to constructively engage with the present global political system or parts of that system. Conflict resolution will be possible, only when hierarchical apparatuses become more networked and rhizomatic groups become more conscious of the rest of their hosting network. Ultimately, what this 'reversal' argument calls for is twofold: Firstly, in sociopolitical cyberconflicts, the need to strengthen the organisational structures and informal weak connective structures these non-hierarchical movements normally have. As Tarrow explains the most effective forms of organisation are based on partly autonomous and contextually-rooted local units linked by connective structures, and coordinated by formal organisations. Secondly, the information revolution is favoring and strengthening networked organisational designs, often at the expense of hierarchies. As Arquilla and Ronfeldt argue and the 9/11 demonstrated, states

need to wake up to this fact and realise that networks can be fought effectively only by flexible network-style responses.

The impact of information technology on political conflict cannot be ignored. The form of the internet itself - a global network with no central authority - has offered another experience of governance (no governance), time and space (compression), ideology (freedom of information and access to it), identity (multiplicity) and fundamentally an opposition to surveillance and control, boundaries and apparatuses. New information-age ideologies could be easily arguing for a transfer of virtual social and political structures to real life world, reversing for once the existing process of imitating real life in cyberspace. The internet is not a medium. It is 'another' place. In this environment, cyberconflicts are complex conflicts involving social movement, conflict and media components, which in this thesis are combined to derive an integrated theoretical framework to explain this novel and exciting phenomenon.

## Bibliography

Allen, T and Hudson, K (eds.): (1996) 'Introduction' in *War, Ethnicity and the Media*, South Bank University: London.

Anderson, B: (1991) *Imagined Communities*, 2<sup>nd</sup> edn, Verso: London.

Anderson, J.W: (1998) *Arabizing the Internet*, The Emirates Occasional Papers, no30, The Emirates Center for Strategic Studies and Research.

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

Arquilla, J and Ronfeldt, D: (1997) *In Athena's Camp: Preparing for Conflict in the Information Age*, Rand: California.

Arquilla, J and Ronfeldt, D: (2000) *Swarming and the Future of Conflict*, Rand: California.

Arquilla, J and Ronfeldt, D: (2001) (eds.) *Networks and Netwars: The Future of Terror, Crime and Militancy*, Rand: California.

Barrett, N: (1996) *The State of the Cybernation*, Kogan Page: London.



Barthes, R: (1993) *Mythologies*, Vintage: London.

Baudrillard, J: (1983) *Simulations*, Semiotext: New York.

(1988) *The Ecstasy of Communication*, Semiotext: New York.

(1993) *The Transparency of Evil*, Verso: New York.

(1988) *Selected Writings*, ed. Mark Poster, Polity Press: Cambridge; Stanford University Press: Stanford.

(1995) *The Gulf War Did Not Take Place*, Indiana University Press: Bloomington, Ind.

Bhabha, H: (1994) *The Location of Culture*, Routledge: New York.

Bell, D and Kennedy, B (eds.): (2000) *The Cybercultures Reader*, Routledge: London and New York.

Bennett, W.L: (2004) 'Communicating Global Activism' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York.

Berton, P et.al: (1999) *International Negotiation*, St. Martin's Press: New York.

Bloom, W: (1990) *Personal Identity, National Identity and International Relations*, Cambridge University Press: Cambridge.

Boucher, J, Landis, D and Clarke, AK (eds.) (1987) *Ethnic Conflict: International Perspectives*, Sage: London and New York.

Broadbendt, L: (1985) *War and Peace News*, Glasgow University Media Group, Open University Press: Milton Keynes.

Brown, R: 'The Contagiousness of Conflict: E.E. Schattschneider as a theorist of the information society', *Information, Communication and Society*, 5:2 2002

'Mobilizing the Bias of Communication: Information Technology', Political Communications and Transnational Political Strategy, American Political Science Association Convention, Washington DC, 30 August- 3 September 2000

'Conceptualizing the Impact of Communication Technologies on World Politics: Space, Time, and Mobilization', International Studies Association Conference, Washington DC 17-21 February 1999

Browning, G: (1996) *Electronic Democracy*, Wilton: London.

Brint, S: (1984) 'New class and cumulative trend explanations of the liberal attitudes of professionals', *American Journal of Sociology*, 90, pp.30-71

Burton, J: (1997) *Violence Explained: The Sources of Conflict, Violence and Crime and their Prevention*.

Cairns, E: (1997) *A Safer Future*, Oxfam Publications: England.

Campbell, D: (1992) *Writing Security*, Manchester University Press: Manchester.

Campbell, D: (1998) *National Reconstruction: Violence, Identity and Justice in Bosnia*, University of Minnesota Press: Minneapolis.

Campbell, D: (1999) 'Violence, Justice and Identity' in Edkins, J, Persram, N and Pin-Fat, V (eds.) *Sovereignty and Subjectivity*, Lynne Rienner: Boulder, London.

Castells, M: (2000) *The Rise of the Network Society*, vol.1 of The Information age: Economy, Society and Culture, 2<sup>nd</sup> edn, Blackwell: Oxford.

Cebrian, J.L: (2000) *La Red (The Net)*, translated in Greek, Staxy: Athens.

Chanteur, J: *From War to Peace*, Westview Press: Boulder.



Chapman, R: 'Hyperlinks and HyperProtestantism: The Internet as a postmodern epistemological shift', Lincoln Trail College, Robinson, Illinois, undated

Chase, M and Mulveron, J: (2002) *You've Got Dissent! Chinese Dissident Use of the Internet and Beijing's Counterstrategies*, Rand: California.

Chayko, M: (2002) *Connecting: How we form Social Bonds and Communities in the Internet Age*, State University of New York Press: New York.

Chernaik, W, Deegan, M, and Gibson, A: (1996) *Beyond the Book: Theory, Culture, and the Politics of Cyberspace*, Office for Humanities Communication Publications, no 7, The Centre for English Studies, University of London

Chesters, 'Shape shifting: Civil society, complexity and social movements', *Anarchist Studies*, 11, 1

Clemens, E: (1996) 'Organizational Form as Frame: Collective identity and political strategy in the American labor movement, 1880-1920', in McAdam, D, McCarthy, J and Zald, M (eds.): *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Structural Framings*, Cambridge University Press

Cohen, J.L: (1985) 'Strategy or Identity: New theoretical paradigms and contemporary social movements', *Sociological Research*, 52, pp.663-716.

Cornell, S and Hartmann, D (1998) *Ethnicity and Race: Making Identities in a Changing World*.

Dachan, M: *Internet Usage in the Middle East: Some Political and Social Implications*, Department of Political Science, The Hebrew University of Jerusalem, undated.

David, M.W and Sakurai, K: 'Combating Cyberterrorism: Improving analysis and accountability', *Journal of Information Warfare*, (2003) 2, 2: 15-26.

Davis, R: (1999) *The Web of Politics*, Oxford University Press: Oxford.

De Armond, P (2001) 'Netwar in the Emerald City: WTO Protest Strategy and Tactics' in Arquilla, J and Ronfeldt, D (eds) *Networks and Netwars: The Future of Terror, Crime and Militancy*, Rand: California.

De Fleur, M and Ball-Rocchach, S: (1982) *Theories of Mass-communication*, 4<sup>th</sup> edn, Longman: New York and London.

Deleuze, G and Guattari, F: (1987) *A Thousand Plateaus*, The Athlone Press: London.

Denning, D: (2001) 'Activism, Hacktivism and Cyberterrorism: The Internet as a tool for influencing foreign policy' in Arquilla, J and Ronfeldt, D (eds) *Networks and Netwars: The Future of Terror, Crime and Militancy*, Rand: California.

Dery, M: (1993) *Flame Wars: The Discourse of Cyberculture*: Duke University Press.

Diamond, L and Plattner, M: (1994) *Nationalism, Ethnic Conflict and Democracy*, the John Hopkins University Press: Baltimore and London.

Dodge, M and Kitchin, R: (2001) *Mapping Cyberspace*, Routledge: London and New York.

Eder, K: (1985) The 'new' social movements: moral crusades, political pressure groups or social movements?', *Sociological Research* 52, pp. 869-901.

Edwards, A: (2004) 'The Dutch women's movement online' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York.



Emery, E: 'The postmodern desert: Solitude and community in cyberspace',  
Preconvention papers, The American Benedictine Academy,  
[www.osb.org/aba/aba2000/emery.html](http://www.osb.org/aba/aba2000/emery.html)

Everard, J: (2000) *Virtual States*, Routledge: London and New York.

Fairclough, N: (1995) *Media Discourse*, Arnold: London and New York.

Ferdinand, P (ed.: (2000) *The Internet, Democracy and Democratization*, Frank  
Cass: London and Portland.

Fink, J: (1999): *Cyberseduction: Reality in the Age of Psychotechnology*,  
Prometheus: New York.

Foucault, M: (1979) *Discipline and Punish*, Prentice Hall: London.

Foucault, M: (1980) *Power/Knowledge*, Harvester Wheatsheaf: New York and  
London.

Freeden, M: (1996) *Ideologies and Political Theory: A Conceptual Approach*,  
Clarendon Press: Oxford.

Gadet, F: (1986) *Sassure and Contemporary Culture*, Hutchinson: London.

Galtung, J: *Peace by Peaceful Means: Peace and Conflict, Development and Civilisation*, Prio, Sage: London and New York.

Gamson, W and Meyer, D: (1996) 'Framing political opportunity' in McAdam, D, McCarthy, J and Zald, M (eds.): *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Structural Framings*, Cambridge University Press: Cambridge,

Grewlich, K: (1999) *Governance in 'Cyberspace'*, Kluwer Law International: The Hague, London and Boston.

Guisnel, J: (1997) *Cyberwars*, Plenum Trade: New York and London.

Hall, S: (1997) 'The Local and the Global' in A. McClintock et.al: *Dangerous Liaisons: Gender, Nation and Postcolonial Perspectives*, University of Minnesota: Minneapolis.

Hardt, M and Negri, A: (2000) *Empire*, Harvard University Press: Cambridge, MA and London.

Held, D: (1995) *Democracy and the Global Order*, Polity Press: Cambridge.

Heim, M: (1993) *The Metaphysics of Virtual Reality*, Oxford University Press: Oxford.

Held, D and McGrew, A: (2000) *The Global Transformation Reader*, Polity Press: Cambridge

Hill, K and Hughes, J: (1998) *Cyberpolitics*, Rowman and Littlefield: Lanham

Hindess, B: (1999) *Discourses on Power: From Hobbes to Foucault*, Blackwell: Oxford.

Higgins, J: 'Peace Profile: Paulo Freire', *Peace Review* 9:4 (1997), 571-577

Hintjens, H: 'When identity becomes a knife', *Ethnicities Journal*, Sage: London.

Horowitz, D: 'Structure and strategy in ethnic conflict', paper presented at *The Annual Conference on Development Economics*, Washington D.C., April 20-21, 1998.

International Centre against Censorship: *Forging War: The Media in Serbia, Croatia and Bosnia-Herzegovina*, May 1994



Howarth, D: (2000) *Discourse*, Open University Press: Buckingham and Philadelphia.

Howarth, D., Norval, J. and Stavrakakis, Y (eds): (2000) *Discourse Theory and Political Analysis: Identities, Hegemonies and Social Change*, Manchester University Press: Manchester and NY.

Ignatieff, M: (2000) *Virtual War: Kosovo and Beyond*, Chatto and Windus: London.

Jabri, V: (1996) *Discourses on Violence: Conflict Analysis Reconsidered*, Manchester University Press: Manchester.

Jenkins, J.C: 'Resource Mobilization Theory and the study of Social Movements', *Annual Review of Sociology*, vol. 9 (1983), pp. 527-553

Joinson, A: *Understanding the Psychology of Internet Behaviour*, Macmillan: Palgrave.

Jones, S (ed.): (1999) *Doing Internet Research*, Sage: Thousand Oaks, London and New Delhi.

Jordan, T: (1999) *Cyberpower: The Culture and Politics of Cyberspace and the Internet*, Routledge: London and New York.

Kahn, R and Kellner, D: 'New media and internet activism: from the "Battle of Seattle" to blogging', *New Media and Society*, 6 (1), Sage: London and Thousand Oaks.

Karatzogianni, A: 'The Politics of Cyberconflict', *Journal of Politics*, 2004 vol. 24 (1), pp.46-55.

Karim, H.K: 'Diasporas and their communication networks: Exploring the broader context of transnational narrowcasting', draft, Carleton University, Ottawa.

Keane, J: (1996) *Reflections on Violence*, Verso: London and New York.

Khalizad, Z, White, J.P, Marshall, W: (1999) *The Changing Role of Information Warfare*, Rand: California.

Khan, A: (1996) *The Extinction of Nation States: A World without Borders*, Kluwer Law International: The Hague, London and Boston.

Kidd, D: 'Indymedia.org.' in McCaughey, M and Ayers, M (eds.) (2003) *Cyberactivism: Online Activism in Theory and Practice*, Routledge: New York and London

Klandermans, B: 'Mobilisation and participation: Social-psychological expansions of resource mobilization theory', *American Sociological Review*, vol.49 (Oct.1984), pp 583-600.

Klandermans, B: (1994) 'Transient identities? Membership patterns in the Dutch peace movement' in Larana et al: *New Social Movements: From Ideology to Identity*, Temple University Press: Philadelphia.

Klandermans, B and Goslinga, S: (1996) 'Media discourse, movement publicity, and the generation of collective action frames: Theoretical and empirical exercises in meaning construction' in McAdam, D, McCarthy, J and Zald, M (eds.): *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Structural Framings*, Cambridge University Press: Cambridge

Knightley, P: (2000) *The First Casualty: The War Correspondent as Hero and Myth-maker from Crimea to Kosovo*, Prion: London.



Kriesi, H: 'New social movements and the new class in the Netherlands', *American Journal of Sociology*, vol.94, no. 5 (Mar.1989), pp.1078-1116.

Kroker, A and Weinstein, M: (1994): *Data Trash: The Theory of Virtual Class*, St.Martin's press: New York.

Laclau, E (ed.): (1994) *The Making of Political Identities*, Verso: London and NY.

Laclau, E and Mouffe, C: (1985) *Hegemony and Social Strategy: Towards a Radical Democratic Politics*, Verso: London and NY.

Lebert, J: 'Wiring human rights activism' in McCaughey, M and Ayers, M (eds.) (2003) *Cyberactivism: Online Activism in Theory and Practice*, Routledge: New York and London.

Le Grignou, B and Patou, C: (2004) 'ATTAC(k)ing expertise' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York

Lesser, I, Hoffman, B, Arquilla, J, Ronfeldt, D, Zanini, M, Jenkins, B.M: (1999) *Countering the New Terrorism*, Rand: California.

Levy, P: (1995) *Qu'est-ce que le Virtuel?*, Editions La Decouverte, translated in Greek, 1999, Kritiki: Athens.

Libicki, M and Shapiro, J: (2001) *Strategic Appraisal: The Changing Role of Information Warfare*, Rand: California.

Loader, B (ed): (1997) *The Governance of Cyberspace*, Routledge: London and New York.

Loader, B (ed.): (1998) *Cyberspace Divide: Equality, Agency and Policy in the Information Society*, Routledge: London.

Lukes, S: (1970) *Power: A Radical View*, McMillan: London and Basingstoke.

Mansbach, R: (2000) *The Global Puzzle*, 3<sup>rd</sup> edn., Houghton Mifflin: Boston.

Mansell, R: (2001) *Inside the Communication Revolution*, Oxford University Press: Oxford.

Margolis, M and Resnick, D: (2000) *Politics As Usual*, Sage: Thousand Oaks, London and New York.

Mattelart, A and Mattelart, M: (1992) *Rethinking Media Theory*, University of Minnesota Press: Minneapolis.

McAdam, D, McCarthy, J and Zald, M (eds.): (1996) *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Structural Framings*, Cambridge University Press: Cambridge.

McAdam, D: (1996) 'The framing function of movement tactics: Strategic dramaturgy in the American civil rights movement' in McAdam, D, McCarthy, J and Zald, M (eds.): *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Structural Framings*, Cambridge University Press: Cambridge.

McCarthy, J et al: 'Images of protest: Dimensions of selection bias in media coverage of the Washington demonstrations 1982 and 1991', *American Sociological Review*, vol 61, no3, Jan 1996, pp 478-499

McCarthy, J and Zald, M: 'Resource mobilization and social movements: A partial theory', *The American Journal of Sociology*, vol.82, no6, May 1977, pp.1212-1241.

McCaughey, M and Ayers, M: (2003) *Cyberactivism: Online Activism in Theory and Practice*, Routledge: New York and London.



McGregor, B: (1997) *Live, Direct and Biased? Making Television News in the Satellite Age*, Arnold: London and New York.

McKenna and Bargh, J: (1998) 'Coming out in the age of the Internet: Identity, demarginalization through virtual group participation', *Journal of Personality and Social Psychology* 75, pp.681-694.

McNay, L: (1994) *Foucault: A Critical Introduction*, Polity Press: Cambridge.

Melucci, A: (1989) *Nomads of the Present: Social Movements and Individual Needs in Contemporary Society*, edited by John Keane and Paul Mier, Temple University Press: Philadelphia.

Mercer, D, Mungham, G and Williams, K: (1987) *The Fog of War: The Media on the Battlefield*: Heinman: London.

Mermin, J: 'Television news and American intervention in Somalia: The myth of a media driven foreign policy', *Political Science Quarterly*, vol.112, no 3, Autumn 1997, pp 385-403.

Milone, M.G: 'Hactivism: Securing the national infrastructure', *The Business Lawyer*, vol. 58, issue 1, Chicago, November 2002.

Minear, L, Scott, C and Weiss, T (1994): *The News Media, Civil War and Humanitarian Action*, Lynne Rienner: Boulder and London.

Minkoff, D: 'The sequencing of social movements', *American Sociological Review*, vol.62, no5 (Oct.1997), pp. 779-799.

Morse, M: (1998) *Virtualities: Television, Media Art and Cyberculture*, Indiana University Press: Bloomington and Indianapolis.

Moss, J (ed.): (1998) *The Later Foucault*, Sage: London.

Mouffe, C: (1993) *The Return of the Political*, Verso: London and NY.

Mouffe, C: (2000) *The Democratic Paradox*, Verso: London and NY.

Mosad, M: *The Web Community: A Social Movement in Cyberspace?*, Department of Sociology, American university of Cairo.

Mueller, C: 'International press coverage of East German protest events', *American Sociological Review*, vol. 62, no5, (Oct.1997), pp.820-852

Mulveron, J and Yang, R: (1999) *The People's Liberation Army in the Information Age*, Rand: California.

Murray, T: (2004) 'New media art and rhizomatic in-securities', Ctheory.net

Myers, M: (2001) 'Collective identity.org: Collective identity in online and offline feminist activist groups', thesis submitted to the Virginia Polytechnic Institute for the degree of Masters of Science in Sociology.

Negroponte, N: (1995) *Being Digital*, Hodder and Stoughton: London.

Nip, J: (2004) 'The Queer Sisters and its electronic bulletin board' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York,

Nunes, M: (1995) *Baudrillard in Cyberspace: Internet, Virtuality, and Postmodernity*, Style 29.

Offe, C: (1985) 'New social movements: Challenging the boundaries of institutional politics', *Sociological Research*, 52, pp.817-68.

O'Hara, K: 'The internet: a tool for democratic pluralism?', *Science as Culture* 11:2, 2002, 287-98



Olofsson, G: (1988) 'After the working class movement? An essay on what's "new" and what's "social" in the new social movements', *Acta*, 31. pp.15-34.

Pateman, C: (1970) *Participation and Democratic theory*, Cambridge University Press: Cambridge.

Poster, M: (1995) *The Second Media Age*, Polity Press: Cambridge.

Poster, M: 'Cyberdemocracy: Internet and the public sphere', University of California, Irvine, [www.humanities.uci.edu/mposter/writings/democ.html](http://www.humanities.uci.edu/mposter/writings/democ.html)

Rheingold, H: (1991) *Virtual Reality*, Secker and Warburg: London.

(1994) *The Virtual Community: Surfing the Internet*, Minerva: London.

(2002) *Smart Mobs: The Next Social Revolution*, Perseus publishing.

Ronfeldt, D, Arquilla J, Fuller, G.E, Fuller, M: (1998) *The Zapatista Social Netwar in Mexico*, Rand: California.

Rothstein, R.L: (1999) *After the Peace*, Lynne Rienner: Boulder, London.

Richardo, N: 'New social movements: a critical review', *Annual Review of Sociology*, vol.23 (1997), pp. 411-430

Rosenkrands, J: (2004) 'Politicizing *Homo economicus*' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York.

Rucht, D: (1996) 'The impact of national contexts on social movement structures: A cross-movement and cross-national comparison' in McAdam, D, McCarthy, J and Zald, M (eds.): *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Structural Framings*, Cambridge University Press: Cambridge

Rucht, D: (2004) 'The quadruple "A": Media strategies of protest movements since the 1960s' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York

Salter, L: (2003): 'Democracy, social movements, and the Internet' in McCaughey, M and Ayers, M: *Cyberactivism: Online Activism in Theory and Practice*, Routledge: New York and London

Scott, A: (1990) *Ideology and the New Social Movements*, Unwin Hyman: Boston.

Simons, J: (1995) *Foucault and the Political*, Routledge: London and NY.

Shaw, M: (1996) *Civil Society and Media in Global Crises: Representing Distant Violence*, Pinter: London and New York.

Shimeall, T, Dunlevy, C, Williams, P: *Intelligence Analysis for Internet Security: Ideas, Barriers and Possibilities*, Certo Analysis Center, Carnegie Mellon University, May 2001.

Slevin, J: (2000) *The Internet and Society*, Polity Press: Cambridge.

Smith, M and Kollock, P: (1999) *Communities in Cyberspace*, Routledge: London and New York.

Snow, D, Zurcher, L and Olson, S.E: 'Social networks and social movements: A microstructural approach to differential recruitment', *American Sociological Review*, vol. 45, no5 (Oct. 1980), pp. 787-801.

Snyder, D and Kelly, W: 'Conflict intensity, media sensitivity and the validity of newspaper data', *American Sociological Review*, vol. 42, no1 (Feb 1977), pp.105-123.

Sola Pool de I: (1990) *Technologies without Boundaries*, Harvard University press: Cambridge.



Sterling, B: (1992) *The Hacking Crackdown: Law and Disorder on the Electronic Frontier*, Viking: London

Tarrow, S: 'National Politics and Collective action', *Annual Review of Sociology*, vol. 14 (1988), p.421-440.

(1983) 'Struggling to reform: Social movements and policy change during cycles of protest', *West. Soc. Pap.* no15, Cornell University: Ithaca, NY.

'Aiming at a moving target: social science and the recent rebellion in Eastern Europe', *Political Science and Politics*, vol.24, no1 (Mar.1991), p. 12-20

(1998) *Power in Movement: Social Movements and Contentious Politics*, Cambridge University Press: Cambridge

(1996) 'States and opportunities: The political structuring of social movements' in McAdam, D, McCarthy, J and Zald, M (eds.): *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Structural Framings*, Cambridge University Press: Cambridge

Taylor, Phil: (1992) *War and the Media Propaganda and Persuasion in the Gulf war*, Manchester University Press: Manchester and New York

Taylor, Paul: (1999) *Hackers*, Routledge: London and New York.

Taylor, Paul and Jordan, T: (2004) *Hacktivism and Cyberwars: Rebels with a cause?*, Routledge: London

Taylor, V and Whittier, N (1992) 'Collective identity and lesbian feminist mobilization', pp.104-29 in *Frontiers of Social Movement Theory*, edited by A.Morris and C. Mueller, Yale University Press: New Haven.

Thomas, D and Loader, B (eds): (2000) *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*, Routledge: London and New York.

Thiel, S: 'The online newspaper: A postmodern medium', *The Journal of Electronic Publishing*, University of Michigan Press, 4/01.

Tidwell, A.C: (1998) *Conflict Resolved?* Pinter: London and New York.

Tilly, C: (1978) *From Mobilization to Revolution*, Addison-Wesley: Reading, MA.

(1984) 'Social movements and national politics', in *State-making and Social Movements*, ed. C. Bright and S. Harding, Michigan University Press: Ann Arbor, pp.297-317.

Toffler, A: (1980) *The Third Wave*, Morrow: New York.

Torring, J: (1999) *New Theories of Discourse: Laclau, Mouffe, Žižek*, Blackwell: Oxford.

Tormey, S: (2004) *Anti-capitalism: A Beginner's Guide*, Oneworld: Oxford.

Touraine, A: (1985) 'An introduction to the study of social movements', *Sociological Research*, 52, pp.749-88.

Tsagarousianou, R, Tambini, D and Bryan, C (ed.): (1998) *Cyberdemocracy: Technology, Cities and Civic Networks*, Routledge: London and New York.

Turner, R and Killian, L (1972) *Collective Behavior*, Prentice Hall: Englewood Cliffs, NJ.

Van de Donk, W, Loader, B, Nixon, P, Rucht, D: (2004) *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York.



Van Dijk, T: (1997) *Discourse as Social Interaction, discourse Studies: A multi-disciplinary introduction*, vol 2, Sage: London

Van Aelst, P and Walgrave, S: (2004) 'New media, new movements?' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York

Vatis, M (2001) 'Cyberattacks during the war on terrorism: A predictive analysis', Dartmouth: Institute for Security Technology Studies, Dartmouth College.

Vegh, S: 'Classifying forms of online activism' in McCaughey, M and Ayers, M (eds.) (2003) *Cyberactivism: Online Activism in Theory and Practice*, Routledge: New York and London

Wang, F: 'Subscribing to democracy through the Internet', *JAHC*.

Walls, A.T: 'The image of unanimity: The utility of the promotion and disparagement of cultural and social unanimity as a form of context manipulation in Information Warfare in the aftermath of the attacks of September 11, 2001', *Journal of Information Warfare*, (2002) 2,2:119-127

Waterman, P: (2001) *Globalization, Social Movements and the New Internationalisms*, Continuum: London and New York.

Webb, K et al: (1983) 'Etiology and outcomes of protest: New European perspectives', *American Behavior Science*, 26, pp.311-31.

Wellman, B et al.: 'Computer networks as social networks: Collaborative work, telework, and virtual community', *Annual Review of Sociology*, vol 22 (1996), 213-238.

Whittier, N: 'Political generations, micro-cohorts and the transformations of social movements', *American Sociological Review*, vol. 62, no 5 (Oct.1997), pp760-778.

Wilhelm, A: (2000) *Democracy in the Digital Age*, Routledge: New York and London.

Wright, S: (2004) 'Informing, communicating and ICTs in contemporary anti-capitalist movements' in Van de Donk, W, Loader, B, Nixon, P, Rucht, D: *Cyberprotest: New Media, Citizens and Social Movements*, Routledge: London and New York

Wolfsfeld, G: (1997) *Media and Political Conflict*, Cambridge University Press: Cambridge.

Zald, M: 'Culture, ideology and strategic framing' in McAdam, D, McCarthy, J and Zald, M (eds.): *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Structural Framings*, Cambridge University Press: Cambridge

Zittrain, J and Elderman, B: 'Empirical Analysis of Internet filtering in China', Berkman Center for Internet and Society, Harvard Law School, last updated 20/3/03



## Web Sources:

- Abdel-Latif: 'Cyber-struggle: Islamist websites versus the Egyptian state', Carnegie Endowment for International Peace, *Arab Reform Bulletin*, December 2004.
- Agence France Presse: 'Chinese hackers attack Japanese websites over the Shrine visit', 14/8/01
- Alexander, A: 'Britain's biggest political protest was mobilised on the web', *The Guardian*, 19/2/03
- Aliefudien: 'Al-Qaeda, big brother, and cyberspace', *Tehran Times*, 26/12/04
- AlwaysOn: 'Howard dean blogs, Gen. Clark and President Bush follow', 18/11/03
- American-Arab Anti-Discrimination Committee (ADC): 'Protest biased media coverage of Palestine and Palestinians', 13/11/04
- Amnesty International Press Release: 'China: Controls tighten as internet activism grows', 28/1/04
- Amnesty International: 'People's Republic of China: State control of the Internet in China', 26/11/02
- Asaravala, A: 'Treetop blogging protests logging', *wired.com*, 12/16/02
- Asaravala, A: 'Today's tech-dependent activists', *wired.com*, 28/08/03
- Asaravala, A: 'College questioning site's link', *Associated Press*, 28/9/02
- Ascribe.org: 'Internet may mobilise largest protests ever seen, Professor predicts', 17/3/03\
- Associated Press: 'US spies on chat rooms', *wired.com*, 11/10/04
- Associated Press: 'Google bows to Chinese censorship', [www.wired.com](http://www.wired.com), 25/9/04
- Associated Press: 'China's filters strong, subtle', *wired.com*, 14/4/05
- Associated Press: 'Is SCO hack a Linux attack?', *wired.com*, 27/08/03
- Associated Press: 'Are you too stupid to surf?', *wired.com*, 12/09/03
- Associated Press: 'New law used against "cybersquatter"', *msnbc.com*, 08/09/03
- Associated Press: 'Suspected virus author arrested', *wired.com*, 29/08/03
- Associated Press: 'Internet fraud spikes sharply', *wired.com*, 09/04/03
- Associated Press: 'The war in all its online glory', *wired.com*, 30/05/02
- Associated Press: 'Court approves more snooping', *wired.com*, 18/11/02
- Associated Press: 'Frankfurt: *nein* to neo-Nazi sites', *wired.com*, 20/12/02

Associated Press: 'Revised cybersecurity plan issued', wired.com, 07/01/03

Associated Press: 'Finns investigate bomb chat room', wired.com, 15/10/02

Associated Press: 'Ashcroft touts Patriot Act', wired.com, 21/08/03

Associated Press: 'Famed hacker turns himself in', wired.com, 09/09/03

Associated Press: 'Worm a sign of horrors to come', wired.com, 13/08/03

Associated Press: 'Revised cybersecurity plan issued', 7/7/02

Associated Press: 'Indictment due against hacker', 12/11/02

Associated Press: 'Few clues in worm whodunit'

Associated Press: 'Government warns "Patriotic hackers" against cyberattacks on Iraqi interests', 12/2/03

Associated press: 'Hackers beat up on Al-Jazeera', AP, 27/3/03

Associated Press: 'China dissidents thwarted on net', 27/8/02

Associated Press: 'E-bombs aims to stun Iraqi forces', 19/3/03

Assur, A: 'Bloggers are outwitting the mainstream and corporate media', [www.uruknet.info](http://www.uruknet.info), 24/5/04

Augman, R: 'The meaning behind the message of the RNC protests', <http://groups.yahoo.com/groups/smygo/message/5343>, accessed 16/10/04

Backgo: 'True democracy, fake democracy or no democracy', China Popular Marxist Liberal Left Ideology website.

Baker, P: 'Moral panic and alternative identity construction in Usenet', Department of Linguistics, Lancaster University, [www.ascusc.org/jcmc/vol7/issue1/baker.html](http://www.ascusc.org/jcmc/vol7/issue1/baker.html), undated, accessed 20/4/05.

Barton, J: 'Ukraine's domain in dot dispute', wired.com, 22/06/01

Batista, E, and K L Dean: 'Vague limits vex music traders', wired.com, 21/08/03

Batista, E: 'Bloggers report alternative news from G8', wired, 4/6/03

BBCnews: 'Blogs respond to London blasts', [www.bbc.co.uk](http://www.bbc.co.uk), 7/7/05

BBC: 'Chinese blogs face restrictions', [www.bbc.co.uk](http://www.bbc.co.uk), 16/6/05

BBC News: 'China's web surfers keep growing', [bbc.co.uk](http://bbc.co.uk), 22/07/03

BBC News: 'Discord at digital divide talks', 29/9/03

BBC News: 'Islamic hackers step up attacks', 29/10/03

BBC News: 'China jails web dissidents', [bbc.co.uk](http://bbc.co.uk), 29/06/03

BBC News: 'China censors online chat', [bbc.co.uk](http://bbc.co.uk), 15/08/03

BBC News: 'China blocks news not porn online', [bbc.co.uk](http://bbc.co.uk), 04/12/02

BBC News: 'The cost of China's web censors', [bbc.co.uk](http://bbc.co.uk), 23/09/02



BBC News: 'Bypassing China's Net Firewall', 3/11/04

BBC News: 'Computer worm targets Blair', [bbc.co.uk](http://bbc.co.uk), 08/09/03

BBC News: 'China online dissident charged', 24/9/03

BBC News: 'Israeli group hacked', 3/11/00

BBC News: 'Indian army website ambushed', 16/10/98

BBC News: 'War of words on the Internet', 25/10/98

BBC News: 'Serb hackers on the rampage', 14/4/00

BBC News: 'Israel under hack attack', 16/4/2002

Bell, E: 'The blogs of war', *The Observer*, 30/3/03

Bodeen, C: 'Search engine Google blocked in China', Associated Press, 3/9/02

Borger, J: 'Pentagon kept lid on cyberwar in Kosovo', *Washington Guardian*, Guardian Unlimited, 9/11/99

Boyle, J: 'Foucault in cyberspace: surveillance, sovereignty and hard-wired censors', [wcl.american.edu](http://wcl.american.edu), 1997

Bowles, W: 'Embedded in a media fantasy world: The case against objective reporting', [www.williambowles.com](http://www.williambowles.com), accessed 29/9/04

Bowles, W: 'Privatising propaganda', [www.williambowls.info](http://www.williambowls.info), 6/3/05

Butko, T.J: 'Revelation or Revolution: A Gramscian approach to the rise of political Islam', *British Journal of Middle Eastern Studies*, vol. 31, no1, May 2004.

Callinicos: 'Regroupment, realignment and the Revolutionary Left', [www.swp.org.uk/INTER/regroupmen.pdf](http://www.swp.org.uk/INTER/regroupmen.pdf)

CBS News: 'Video of Saddam's sons released', [cbsnews.com](http://cbsnews.com), 25/07/03

Chepsiuk, R: (2001) 'Get ready for cyberwars', *ncmonline*, 23/8/01

Chesters, G: 'ESF: Encounter or Representation', [www.indymedia.org](http://www.indymedia.org), 22/10/04

Delio, M: 'Hactivism and how it got there', [wired.com](http://wired.com), 12/7/04

Ching, F: 'The Internet dissidents', *Globe and Mail*, 22/5/03

CNETAsia: 'Malaysians enrol text messages for democracy', [zdnet.co.uk](http://zdnet.co.uk), 02/09/03

CNN.com: 'Experts warn of cyber security holes', [cnn.com](http://cnn.com), 19/06/02

Coll, S: 'In the Gulf, dissidence goes digital: Text messaging is new tool of political underground', *Washington Post Foreign Service*, 29/3/05

Collins, M: 'Flaming: The relationship between social context cues and uninhibited verbal behavior in computer-mediated communication', Fall 1992, [www.emoderators.com/papers/flames.html](http://www.emoderators.com/papers/flames.html)

Costello, S: 'Attrition.com stops mirroring hacked websites', *CNN.com*, 05/12/02



Cramer, C: 'How the net will play a key role in this war', The Observer, 9/3/03.

Cronauer, K: 'Activism and the Internet: Uses of electronic mailing lists by social activists, University of Columbia, web accessed undated

Cryan, P: 'Rightist bias in wire coverage of Colombia', [www.couterpunch.org](http://www.couterpunch.org), 1/12/04

Crypt Newsletter at [Sun.soci.niu.edu/~crypt](http://Sun.soci.niu.edu/~crypt)

Curiel, J: 'North American media help Iran protests grow', San Francisco Chronicle 20/6/03;

Dean, K: 'Schools rebuke music biz demands', wired.com, 01/08/03

Dean, K: 'Online anonymity comes under fire', wired.com, 26/04/03

Deans, J: 'Hackers divert al-Jazeera users to Us porn and patriot sites', The Guardian, 28/3/03

Delio, M: 'A gathering to hack the system', wired.com, 12/7/04

Delio, M: 'Hackers condemn Arab site hack', wired 31/3/03

Delio, M: 'It's Cyberwar: China vs US', Wired news, 30/4/01

Delio, M: 'Attrition offs its hacker monitor', wired.com, 29/06/02

Delio, M: 'Net analysis gets turbo boost', wired.com, 02/09/03

Delio, M: 'Did FBI bungle email evidence?', wired.com, 30/08/02

Delio, M: 'Flash mobs get a dash of danger', wired.com, 15/09/03

Delio, M: 'Viruses, worms: what's in a name?', wired.com, 15/09/03

Delio, M: 'So many holes, so few hacks', wired.com, 30/12/02

Delio, M: 'How much hack info is too much?', wired.com, 19/11/02

Delio, M: 'Terror turns real for horror site', wired.com, 18/10/02

Delio, M: 'Raided firm's software checks out', wired.com, 16/12/02

Delio, M: 'Blaster worm still making mayhem', wired.com, 30/08/03

Delio, M: 'This worm ain't gonna hurt', wired.com, 22/08/03

Delio, M: 'Net analysis gets turbo boost', wired.com, 21/08/03

Delio, M: 'Worm exploits weak link: PC users', wired.com, 13/08/03

Delio, M: 'Cyber-rights activists log a win', wired.com, 26/11/2002

Delio, M: 'Manhattan mob meets its maker', wired.com, 12/09/03

Delio, M: 'What Symantec knew but didn't say', wired.

Delio, M: 'Worm slowing, but still dangerous', wired, 28/1/04

Delio, M: 'The Internet is a very sick place', wired, 11/11/03

Delio, M: 'Do privacy fears allow terrorism?', wired.com, 3/4/03

Delio, M: 'Blogs opening Iranian society?', wired, 28/3/03

Delio, M: 'Virus uses netizens as pawns', wired, 13/3/03

Delio, M: 'Iraq blog: Hubbub over a headlock', wired 26/3/03

Delio, M in 'War worms inch across internet', wired, 21/3/03'

Denning, D: (2001) 'Is cyberterrorism next?' [www.ssrc.org/sep11/essays/denning/html](http://www.ssrc.org/sep11/essays/denning/html)

Diani, M: 'Social Movement networks virtual and real, paper for the conference 'A New Politics?', CCSS, University of Birmingham, 16-17 September 1999

Dobbs, M: 'Iranian exiles sow change via satellite', Washington Post, 25/6/03

Dot Journalism: 'Al-Jazeera launches English-language site', [journalism.co.uk](http://journalism.co.uk), 08/09/03

DotJournalism: 'Zimbabwe's daily news battles on- online', 18/11/03

Elliot, M and Scacchi, W: 'Mobilization of software developers: the Free Software Movement', August 2004, forthcoming in Information, Technology and People.

Europemedia.net: 'New website gets behind municipal wireless projects', [europemedia.net](http://europemedia.net), 09/07/03

Europemedia.net: 'Iraq invasion leads to massive increase in pro-war, anti-war hacker activity', 1/4/03

Europemedia.net: "Super-network" will combine internet, fixed-line and mobile', 14/04/03

Europemedia.net: 'Dutch professor calls for openness in IT security', [europemedia.net](http://europemedia.net), 19/05/03

Europemedia.net: 'Iran cracks down on internet journalists', 10/3/03

Fair and Accuracy in Reporting: 'Some critical media voices face censorship', Media Advisory, 3/4/03

Fair and Accuracy in Reporting: 'Journalist's evidence that US bombed market ignored by US press', 4/4/03, Fair and Accuracy in Reporting: 'Official story vs eyewitness account, 4/4/03, [www.fair.org](http://www.fair.org)

Fair.org: 'The return of PSYOPS: Military's media manipulation demands more investigation', Media Advisory, [www.fair.org](http://www.fair.org), 12/3/04

Farley, M: 'Dissidents hack holes in China's new wall', Los Angeles Times, [www.gis.net/~cht/dissidents.html](http://www.gis.net/~cht/dissidents.html).

FirstMonday: 'LiveJournal as site of knowledge creation and sharing', [www.firstmonday.org](http://www.firstmonday.org), accessed 12/12/04

Foreign Policy: Net effect: 'The Middle East's e-war', July/ August 2002

Forth, R: 'Jihadists take stand on the web, and some say its defensive, The New York Times, 13/3/05



Frishberg, M: 'Local access: IT takes a village', wired.com, 27/05/02

Frishberg, M: 'Roll-your-own net TV takes off', wired.com, 21/07/-3

Gardner, J: 'Terror czar: the war is digital', wired.com, 11/09/02

Gentile, C: 'Hacker war rages in Holy land', wired news, 8/11/00

Gittings, J: 'Sense and censorship', wired, 17/9/02

Glasner, J: 'Security biz thrives on fear', wired.com, 16/04/03

Glasner, J: 'A Vote for less tech at the polls', wired.com, 19/11/

Glasner, J: 'Patriot Act legal attacks pile up', wired.com, 06/08/03

Glasner, J: 'Mobile junkies reshaping society', wired.com, 10/10/02

Glasner, J: 'Blackout a boon for backup tools', wired.com, 17/08/03

Glasner, J: 'Media more diverse? Not really', wired news 30/5/03

Glasner, J: 'Protests to start when war does', wired

Glave, G: 'Crackers call off war', wired, 8/1/99

Globe Technology: 'Chinese hackers halt webwar, say 1,000 U.S sites defaced', 10/5/01

Gorr, W: 'Cloudy, with a chance of theft', wired.com, Issue 11, 09/03

Graham, B: 'Bush orders guidelines for cyberwarfare', Washington Post, 7/2/03

Grebb, M: 'Windows, Unix still at risk', wired.com, 03/10/02

Greenspan, R: 'Education: reading, writing, pointing-and-clicking', internet.com, 14/08/03

Greimel, H: 'Psychiatry group hopes to probe Chinese mental wards for dissidents', Associated Press, 26/8/02

Guardian, 'Vietnam to monitor "reactionary" web use', Guardian Unlimited, 26/06/02

Gumbel, A: 'Global peace movement is alive and kicking', The Sunday Independent, 16/3/03

Hadar, L: 'Pseudo-events stir Mideast pot', [www.antiwar.com](http://www.antiwar.com), 12/3/05

Harding, D: 'Vigilantes fight back by hacking the hackers', *Metro*, 10 June 2004

Hasson, J: 'Surprising percentage of public fear cyberattacks', usatoday.com, 08/09/03

Hermida, A: 'Palestinian websites knocked offline', bbc.co.uk 06/05/02

Hershman, T: 'Israel discusses "Inter-Fada" ', wired, 29/6/01

Heskett, B: 'Who's benefiting from Net attacks?', [www.zdnet.com/zdnn](http://www.zdnet.com/zdnn), 05/02/02

Hockstader, L: 'Pings and e-arrows fly in Mideast cyber-war', Washington Post online, 27/10/00

Hood, Robin: 'Hacktivists use corporate credit cards to donate to humanitarian and civil liberties groups', [www.indynedia.org](http://www.indynedia.org), 29/8/04



Hopper, I: 'Kashmir conflict continues to escalate online', 20/3/00

Hines, M: 'Paper's anti-Bush ploy gets hacked, sacked', CNET News.com, 22/10/04

Information Society News: 'New wave of Chinese dissident arrests', 18/11/03

Indymedia: 'CIA behind automated chat room spying scheme', [www.indymedia.org](http://www.indymedia.org), 15/12/04

Indymedia: 'Hacktivism: A week of electronic disruption during the Republican National Convention', [www.indymedia.org](http://www.indymedia.org), 5/9/04

IMC: 'FBI took the hard drives of IMC servers in the UK', Pressrelease, 7/10/04, [www.indymedia.org](http://www.indymedia.org)

Jamail, D: 'Media repression in "Liberated" Land', [www.dissidentvoice.org](http://www.dissidentvoice.org), 18/11/04

Jame, F: 'China, Taiwan in web hacking "war"', ZDNet, 10/8/99

Jane's International Police Issues: 'Information warfare: the coming threat', 2/12/98

Jardin, X: 'P2P App's aim: defend free speech', wired.com, 29/10/02

Jesdanun, A: 'Computer infection snarls global network', newsday.com, 13/08/03

Joo-hee, L: Korea: Internet a key playing field for politicians, but has pitfalls', The Korea herald, 11/2/05

Jordan, J: (2001) 'Mapping hacktivism', Computer Fraud and Security.

Joseph, M: 'Tech king next Indian president?', wired.com, 03/06/02

Joseph, M: 'Both sides hacked over Kashmir', Wired News, 23/12/00

Jin, R: 'Korea: Roh adopts e-mail politics', The Korea Times, 11/7/05

Kattan, V: 'BBC reporting doesn't tell the whole story', electronicintifada.net, 29/3/05

Kahney, L: 'Futurist fears end of innovation', wired.com, 24/04/03

Kalathil, S, and T C Boas: 'The Internet and state control in authoritarian regimes: China, Cuba, and the counterrevolution', Carnegie Endowment, July 2001

Kahney, L: 'Internet strokes anti-war movement', wired, Jan/21/03

Kahney, L: 'Citizen reporters make the news', www.wired.com, 17/3/03

Kettmann, S: 'Europe's spin on web reporting', wired.com, 18/07/01

Kettmann, S: 'Make hate not anti-globalisation', wired.com, 13/07/02

Kettmann, S: 'Most hacking hides real threats', wired.com, 03/07/01

Kettman, S: 'Deep thinking on the "Inter-Fada"', wired.com, 10/1/01

King, B: 'Fear and lockdown in America', wired.com, 25/07/02

Kiss, J: 'Student jailed for web pics', [www.journalism.co.uk](http://www.journalism.co.uk), 14/10/04

Kiss, J: 'Bloggers rally to support voice of dissent in Iran', [www.journalism.co.uk](http://www.journalism.co.uk), 18/3/05

Kneen, C: 'Battle in Seattle', [interweb-tech.com](http://interweb-tech.com), 28/02/00

Knight, W: 'Key Arab news station knocked offline', [new.scientist.com](http://new.scientist.com)

Knightley, P: 'Turning the tanks on the reporters', 14/6/03, The Guardian

Ko, Y: 'Cyberwars in China', Far Eastern Economic Review, 03-10-03

Koppel, T: 'Impact of television on US Foreign policy', Congressional Hearing, 5

Koprowski, G: 'The Web: Iraqi blogs building free speech', United Press International, 6/10/04

Koprowski, G: 'The Web: The battle of the bloggers', [www.upi.com](http://www.upi.com), 23/3/05

The Korea Herald: 'Korea: Internet cannot substitute democratic process', 26/5/05, accessed [www.asiamedia.ucla.edu](http://www.asiamedia.ucla.edu)

Kotadia, M: 'Security researcher to be jailed for finding bugs in software?', ZDNet Australia, 11/1/05

Krebs, B: 'Websites vandalised with antiwar messages', Washington Post, 20/3/03

Kurtz, H: 'Dean defence forces: lobbying email at the enemy', [washingtonpost.com](http://washingtonpost.com), 13/08/03

Kurtz, H: 'Webloggers, signing on as war correspondents', Washington post, 22/3/03

Kuznetsov, S: 'Russia: dial "H" for hostage', [wired.com](http://wired.com), 30/10/02

Lasker, J: 'US Military's elite hacker crew', [wired.com](http://wired.com), 18/4/05

Lebowitz, R: 'Can Internet technology still revolutionize activism?', Digital Freedom Network

Leadbeater, C: 'The internet's way forward', Financial Times, [FT.com](http://FT.com), 4/12/04

Lee, J: 'How the protesters mobilized', New York Times, 23/2/03

Leech, G: 'Scared into silence', [www.columbiajournal.org](http://www.columbiajournal.org), accessed 14/1/05

Left, S: 'Chinese and American hackers declare "cyberwar"', Guardian unlimited, 4/5/01

Leister, B: 'Net brings together campaign supporters', News Hour media unit, 04/08/03

Leicester, J: 'Pentagon restricts overseas voters', Associated Press, yahoo news, 21/9/05

Lemos, R: 'Hactivism: Mideast war heats up', [zdnet.com](http://zdnet.com), 6/11/2000

Lemos, R: 'Attack on SCO's servers intensifies', [www.news.com](http://www.news.com), 11/12/03

Lenz, M W: 'Internet rejuvenates political movement', seacostonline.com, 15/08/03

Leonard, A: 'Will the Net save China?', [Salon.com](http://Salon.com), 21/3/02

Lettice, J: 'We seize servers, you can't complain', [www.theregister.co.uk](http://www.theregister.co.uk), 11/11/0

Levine, R: 'Neal Stephenson rewrites history', [wired.com](http://wired.com), Issue 11, 09/03

Leyden, J: 'Middle East conflict spills over to cyberspace', The Register, [www.mi2g.com](http://www.mi2g.com)

Lim, L: 'China to censor text messages', 2/7/04



Luard, T: 'Chinese activists evade web controls', BBCnews online, 30/1/04

Manila IndyMedia: 'Electronic civil disobedience and solidarity for Gelmart workers', [www.indymedia.org](http://www.indymedia.org), 10/1/05

Manjoo, F: 'Do Dots connect to police state?' , wired, 7/6/02

Mark, R: 'Internet voting improves participation', internet.com, 29/04/02

March, S: 'Battle in Seattle', interweb-tech.com, 28/02/00

March, S: 'Community organising on the Internet: Implications for social work practitioners', M.S.W, [www.interweb.com/nsmnet/docs/march](http://www.interweb.com/nsmnet/docs/march).

Matthews, W: 'Al-Qaeda cyber alarm sounded', wired, 25/7/02

Mayfield, K: 'Chronicling attacks on the web', wired.com, 04/10/01

Mazzetti, M: 'PR meets Psy-Ops in War on Terror', [www.latimes.com](http://www.latimes.com), accessed 24/1/05

McCarthy, K: 'This is the future of online newspapers', posted 9/7/03

McLaughlin, K: 'Internet prods Asia to open up', [www.csmonitor.com](http://www.csmonitor.com), 9/9/04

Meek, C: 'Milestone in online journalism', [www.journalism.co.uk](http://www.journalism.co.uk), 16/12/04

McClellan, J: 'War on the web', The Guardian, 19/2/03

McCullagh, D, and R Zarate: 'Hack a PC, get life in jail', wired.com, 27/02/02

McCullagh, D: 'Uncle Sam wants his geeks back', wired.com, 06/09/01

McGrath, D: 'Tunisian net dissident jailed', Associated Press, 13/7/02

McMillan, R: 'Wartime internet security is "business as usual"', Washington Post, 27/3/03

McWilliams, B: 'Dot-Mil hacker's download mistake', wired.com, 15/11/02

McWilliams, B: 'Fluffy Bunny no longer energized', wired.com, 29/07/02

McWilliams, B: 'Messages to al-Qaeda called fake', wired.com, 05/12/02

McWilliams, B: 'Leaked bug alerts cause a stir', wired.com, 20-03-03

McWilliams, B: 'Iraqis log on to voice chat', wired.com, 30/07/03

McWilliams, B: 'North-Korea's school for hackers', wired.com, 2/6/03

Meacher, M: 'The 9/11 attacks gave the US an ideal pretext to use force to secure its global domination', mail.com, 06/09/03

Messmer, E: 'Serb supporters Sock it to NATO and U.S computers', Network World, 5/4/99

Meyerson, H: 'The battle of Seattle', LA Weekly/interweb-tech.com, 28/02/00

Miami herald: 'Terrorists using the net to raise funds reach public', 3/4/01

Mintz, J: 'Al-Qaeda website points at new terrorist target Israel', Washington Post



Mollov, B, Schwartz, Steinberg, G and Lavie, C: 'The Impact of Israeli-Palestinian intercultural dialogue: Virtual and face to face', Bar-Ilan University-  
[www.mevic.org/papers/mollovvirtual.html](http://www.mevic.org/papers/mollovvirtual.html)

Mooney, P: 'China's big mamas vs. online dissidents', International Herald Tribune, 23/4/04

Moore, R.K: 'We the people, IndyMedia, and the neoliberal project',  
[www.globalresearch.ca](http://www.globalresearch.ca), 20/10/04

Morris, D and Langman, L: 'A better world is possible', [commondreamms.org](http://commondreamms.org), 5/4/03

Munson, C: 'Seattle Weekly trashes anti-globalization movement',  
[www.couterpunch.org](http://www.couterpunch.org), 30/11/04

Mustafa, W: 'Pakistan's netizens outsmart censors', wired, 4/6/03

Negroponte, N: 'Being wireless, wired.com', 24/09/02

Netto, A: 'Malaysia backtracks on its bloggers', <http://atimes.com>, accessed, 18/10/04

New Scientist: 'The 'blog' revolution sweeps across China', [www.newscientist.com](http://www.newscientist.com), 24/11/04

News.muzi.com: 'Digital demonstrations in

Newsbycountry.asp: 'UK web surfers prefer BBC, Guardian', [newsbycountry.asp](http://newsbycountry.asp), 15/04/03

Newsbytes: 'American companies fail to report intrusions', [www.nua.com/surveys/index](http://www.nua.com/surveys/index), 17/06/02

Nua Analysis: 'E-government gap widens', [nua.ie](http://nua.ie), 24/06/02

Nuttal, C: 'India opens virtual front in Kashmir', BBCOnline, 5/10/98

Nuttal, C: 'Kosovo – the Internet war', BBC online, 16/4/99

Oakes, C: 'Balkan war in domain attacks?', wired.com, 15/04/00

Ouyang Fei: 'Tapping into the TV system to broadcast truth clarification videos is a form of resistance against state-run terrorism', [www.clearwisdom.net](http://www.clearwisdom.net), 11/2004

OpenNet Initiative: 'Google search and cache filtering behind China's great firewall', [www.opennetinitiative.net](http://www.opennetinitiative.net), 30/8/04

Ortner, E: 'Worm suspect says case against him exaggerated', msnbc.com, 08/09/03

Penenberg, A: 'Site tracks political zeitgeist', wired.com, 1/9/04

Phrack Magazine, vol.8, no 54, Dec1998

Politics Online: 'The European Union student vote', [politicsonline.com](http://politicsonline.com), 27/06/02

Politics Online: 'The birth of a nation: online', [politicsonline.com](http://politicsonline.com), 16/05/02

Poulsen, K: 'Feds fear air broadband terror', wired.com, 11/7/05

Prosser, B T, and A Ward: 'Kierkegaard's "mystery of unrighteousness" in the information age', abdn.ac.uk, 24/05/02

Pruitt, S: 'EU approves creation of cybersecurity agency', IDG News Service, London Bureau.

Ragusa, R: 'Text messaging: let the US mobile marketing phenomenon begin', [www.bayoubuzz.com/political/articles/messaging\\_rand.htm](http://www.bayoubuzz.com/political/articles/messaging_rand.htm), 10/06/02

Rainie, L, Fox, S and Fallows, D: 'The Internet and the Iraq war: How online Americans have used the Internet to learn war news, understand events and promote their views', Pew Internet and American Life Project, [www.pewinternet.org](http://www.pewinternet.org)

Ramachandran, S: 'Jihad's latest 'rag' hits the internet', Asian Times, [www.atimes.com](http://www.atimes.com), 31/5/05

Raphael, C: 'Spinning media for government', [www.corpwatch.org](http://www.corpwatch.org), 10/2/05

Ratan, S: 'It's a flawed world after all', wired.com, 17/08/03

Rendall, S and Broughel, T: 'Amplifying officials, squelching dissent: FAIR study finds democracy poorly served by war coverage', Extra!, May/June 2003.

Rengi Neer: 'Symantec helps China crush freedom of information', [www.indymedia.org](http://www.indymedia.org), 14/11/04

Reporters Without Borders: 'President Gayoon cuts off Internet links with outside world', [www.rsf.org](http://www.rsf.org), 13/8/04

Reuters: 'Nepal scribes evade censors with blogs', [www.telegraphindia.com](http://www.telegraphindia.com), 23/3/05

Reuters: 'Iraq journo "held" in Fallujah', 18/11/04

Reuters: 'Hacker must live with parents', wired.com, 12/09/03

Reuters: 'AOL founder: censor the net? Ha!', wired.com, 24/04/00

Reuters: 'No Google for Chinese surfers', wired.com, 09/09/02

Reuters: 'Amazon fights brand "spoofing"', wired.com, 26/08/03

Reuters: 'New worm mocks "Billy" Gates', wired.com, 12/08/03

Reuters : 'Kremlin's new website stands up to hacker threats', reuters.com, 21/06/02

Reuters: 'China shuts down internet cafes', wired.com, 18/06/02

Reuters: 'US plans for online defence', 19/2/03

Reuters: 'Not just your average loser', 18/3/03

Reuters: 'Sasser worm suspect confesses', 8/5/04

Reuters: 'UK plans to extradite spammers', 30/10/03

Reuters: 'China locks up net dissident', 31/10/03



Reuters: 'Media plot online war coverage' , 6/3/03

Reuters: 'War attacks tit for tat', 28/3/03

Reuters: 'Britain's Labour party website hit by hackers', 16/6/03

Rozen, L: 'Forums point the way to jihad', wired.com, 07/08/03

Sandhana, L: 'I think, therefore I communicate', wired.com, 30/07/03

Savetibet.org: 'Chinese internet group found spying on Tibetan government computers', 28/10/03

Scahill, J: 'Indymedia and the text message jihad', [www.couterpunch.org](http://www.couterpunch.org), 9/9/04

Schechter, D: 'Miscovering anti-war protest', [www.zmag.org](http://www.zmag.org), 25/3/05

Scheeres, J: 'Spanish firms target file traders', wired.com, 01/08/03

Scheeres, J: 'Europeans outlaw net hate speech', wired.com, 09/11/02

Scheeres, J: 'Cuba bans PC sales to public', wired.com, 25/03/02

Scheeres, J: 'Lech Walesa: tech freedom fighter', wired.com, 19/06/02

Scheeres, J: 'Cautious Kabul dabbles with net', wired.com, 02/08/02

Scheeres, J: 'Net dissidents jailed in China', 24/2/04

Scheeres, J: 'Colombia's cyber (un)civil war', Wired news, 4/3/02

Scheeres, J: 'Progress report for net censors', wired, 22/6/04

Scheeres, J: 'Blair tagged as privacy threat', wired, 25/3/03

Shachtman, N: 'Terrorists on the net? Who cares?', wired.com, 20/12/02

Shachtman, N: 'The case for terrorism futures', wired.com, 30/07/03

Shachtman, N: 'Study makes less of hack threat', wired.com, 14/11/02

Shachtman, N: 'Hackers being jobbed out of work', wired.com, 30/08/02

Shachtman, N: 'Why countries make sites unseen', wired.com, 18/07/02

Shachtman, N: 'Sex sites sick of getting screwed', wired.com, 13/09/03

Shachtman, N: 'Urban combat takes street smarts', wired.com, 09-04-03

Shachtman, N: 'Spies attack White House secrecy', wired.com, 16/10/03

Shachtman, N: 'Hack attack gums up Authorize.Net', wired.com, 21/9/04

Shachtman, N: 'Hackers take aim at GOP', wired.com, 17/8/04

Silverman, J: 'Iran's most wanted: filmmakers', wired.com, 6/2/04

Singel, R: 'Net politics down but not out', wired.com, 2/2/04

Shankar Gupta: 'Bloggers protest possible FEC crackdown, [www.mediapost.com](http://www.mediapost.com), 10/3/05

Sherriff, L: 'China shuts 1,600 cybercafes', [www.theregister.co.uk](http://www.theregister.co.uk), 1/11/04

Schmelzer, P: 'Anarchy at the RNC', posted on Alternet, [www.infoshop.org](http://www.infoshop.org), 12/8/04



Simon, E: 'Soldiers' war blogs detail life in Iraq', Associated Press, 26/9/04

Singer, M: 'China's Google block sparks media group's protest', [www.internetnews.com](http://www.internetnews.com), 30/11/04

Singel, R: 'Congress expands FBI spying power', wire.com, 24/11/03

Sipress, A: 'An Indonesian's prison memoir takes war into cyberspace', Washington Post Foreign Service, 14/12/04

Sophos: 'Two British men charged in Trojan horse case, Sophos anti-virus comments', [sophos.com](http://sophos.com), 15/09/03

Starr, B and Shaughnessy, L: 'Pentagon sites: Journalism or propaganda?', [www.cnn.com](http://www.cnn.com), 5/2/05

Statesman (The): 'Pro-Pakistan hackers deface centre's venture capital site', 21/8/01

Stillman, L: 'Citizens of the world or citizens of a community: just where is the Internet heading?', [home.vicnet.net.au](http://home.vicnet.net.au), 06/05/03

Strupp, J: 'Five embeds booted out of Iraq in recent months, [www.editorpublisher.com](http://www.editorpublisher.com), 7/1/05

Strupp, J: 'Study: Media self-censored some Iraq coverage', [www.editorandpublisher.com](http://www.editorandpublisher.com), 19/3/05

Sturgeon, W: 'Italian police shut down piracy ring', CNET news.com, 16/6/03

Sutherland, J: 'Campus watch', wired, 7/10/02

Swartz, J: 'Iraq war could herald a new age of web-based news coverage', USA Today, 18/3/03

Swett, C: 'Strategic Assessment: The Internet', July 1995

Taggart, S: 'Irish eyes smile on dot-TP', wired.com, 08/03/02

Taira, C: '10 big stories the mainstream media missed', [www.lasvegascitylife.com](http://www.lasvegascitylife.com), 14/10/04

Talbot, D: 'Terror's server', technologyreview.com, February 2005

Taylor, P: 'The pornographic barbarism of the self-reflecting sign', fwd in email, undated

TechNews.com: 'Worldwide cyber-security breaches on the up', [www.nua.ie/surveys](http://www.nua.ie/surveys), 03/10/02

Terdiman, D: 'Dems hold the high ground online', wired, 23/4/04

Terdiman, D: 'Text messages for critical masses', wired.com, 12/8/04

Theodoulou, M: 'Proliferating Iranian weblogs give voice to taboo topics', Christian Science monitors, 23/6/03

Thomas, L: 'Electronic resistance: Young Iranians go digital in their quest for freedom', Summer 2004, fwd from Smygo list

Thompson, N: 'Machined politics', washingtonmonthly.com, 18/06/02

Tomlin, J: 'Censored in the desert', Press Gazzete, 16/5/03

TrendLabs Global Antivirus and Research Centre: 'Trend Micro weekly virus report' trendmicro.com, 12/09/03

Trotochaud, M and McDowell, R: 'The invasion of Falluja: A study in the subversion of truth', coomondreams.org, 22/1/05

'Trosky: The new course', www.marxists.org/archive/trosky/1923-nc/index.htm

Tsuruoka, D: 'Internet, Wireless to play key role in an Iraq war', yahoonews, 17/03/03.

Twist, J: 'Mobiles capture blast aftermath', BBCnews, [www.bbc.co.uk](http://www.bbc.co.uk), 8/7/05

USA Today: 'Groups campaign online against Burmese dictators', usatoday.com, 15/08/03

USA Today: 'Efforts to put government online could backfire', usatoday.com, 15-08-03

USA Today: 'US forces using Net to contact home', wired.com, 07/05/02

USA Today: 'Groups campaign online against Burmese dictators', undated

Van Handel, J L: 'Battle in Seattle', interweb-tech.com, 28/02/00

Venke, B: 'Information warrior', wired, 4/8/96

Verton, D: 'New cyberterror threatens AF', Federal Computer Week, 3/5/99

Villafania, A: 'Internet activists to hold virtual strike at Gelmart website', [www.inq7.net](http://www.inq7.net), 7/1/05

Witt, L: 'Finding truth on the internet', wired.com, 16/4/04

Wright, S: 'Pondering information and communication in contemporary anti-capitalist movements', ejournal The Commoner, accessed 2/8/05

Wagner, M: 'Fighting net censorship abroad', wired.com, 03/10/02

Wagner, J: 'Development news: airline database posted on defacement', internetnews.com, 05/12/02

Wagner, J: 'Development news: navy brass latest hacking victim', internetnews.com, 05/20/02

Wagner, M: 'Fighting net censorship abroad', wired.com, 3/10/02

Walker, L: 'Casting a wider net for world news', Washington Post, 26/3/03

Walker, L: 'Web use spikes on news of war', Washington Post, 21/3/03

Walker, L: 'Iraq prison scandal at its most graphic', Washington Post, 9/5/04

Walker, L: 'Casting a wider net for world news', Washington post, 26/3/03



Weaver, N: 'Warhol worms: The potential for very fast Internet plagues', University of California, Berkeley, 15/8/01

Webb, C: 'Religious groups go online for peace', Washington Post

Webb, C: 'Overseas the Internet is rallying point for antiwar activists', Washington Post 17/1/03

Webb, C: 'Rallying around the flag online', Washington Post, 14/3/03

Weinstein, L: 'Filters, laws won't clean up net', wired.com, 16/12/02

Weiss, J: 'Blogs' shake the political discourse', Globe News, 23/07/03

Wenzel, E: 'More privacy protections needed', Associated Press, 18/11/03

White, C: 'China is top of the gaggers', journalism.co.uk, 27/06/03

White, C: 'Iraqi blogger revealed', dot journalism, 12/6/03

Wilkinson, D H: 'The web and conflict theory', geocities.com, 27/05/02

Wired.com, 'Fighting the network war', wired.com, 29/06/02

Wired.com: 'Net dissidents jailed in China', 24/2/04.

Wired.com: 'Kofi Annan: Keep Media Free!', 9/12/03

Wired.com: 'Vietnam to monitor 'reactionary' web use', 26/6/02

Wired News Report: 'Microsoft braces for blister', wired.com, 17/08/03

Wired News Report: 'DoS attack maims web servers', wired.com, 23/10/02

Witt, L: 'Kerry net strategy now on voters', wired.com, 2/7/04

Wo-Lamp Lam, W: 'China pressured over net dissident', CNN.com, 9/11/03

Yahoo: 'MoveOn.org launches "recall no, democracy yes" campaign in California', yahoo.com, 08/09/03

YahooNews: 'US cyber-diplomacy now up and running', 29/10/03

Young, D: 'Chinese chatting up with numbers in cyberspace', reuters.com, 21-01-03

Zerbisias, A: 'Why are we dumbing down the news?', [www.commondreams.org](http://www.commondreams.org), 1/3/05

Zetter, K: 'Just say no to viruses and worms', wired.com, 11/09/03

Zetter, K: 'Security holes vex web host firm', wired.com, 05/09/03

Zetter, K: 'Blogs counter political plottings', wired, 5/5/04

Zetter, K: 'MoveOn moves up in the world', wired.com, 26/7/04

Zittrain, J, and B Edelman: 'Documentation of Internet filtering worldwide'.  
<http://cyber.law.harvard.edu/filtering>, 14/01/03

Zucchino, D: 'Internet helps corral protesters', Chicago Tribune, 4/9/04

