7
Civil society, the Internet and terrorism

Case studies from Northern Ireland

Paul Reilly

The rapid penetration of information and communication technologies in advanced industrialised societies has created new opportunities and dangers for governments and civil society. Civil society can be defined as the 'space of uncoerced human association and also the set of relational networks formed for the sake of family, faith, interest and ideology that fill this space' (Walzer, 1995:7). The Internet can bestow a degree of organisational coherence upon those groups outside the political establishment. These groups are often unable to orchestrate a campaign of political protest using the conventional mass media, which typically reflect the interests of larger sections of civil society. Terrorism can be defined as violence used to articulate a political message. Contemporary terrorists use the Internet like marginalised elements of 'civil' society to communicate with sympathetic diasporas, disseminate propaganda and issue statements unfettered by the ideological refractions of the mass media. This chapter will argue that terrorist utility of the Internet has two dimensions. Terrorists will use the Internet to communicate 'overtly' like other civil society actors. They will use websites to increase organisational coherence and to expound their political ideologies. Terrorist organisations may also use the Internet for 'covert communication'. They will use information and communications technologies to plan and perpetrate acts of terror. This chapter analyses several websites linked to Northern Irish terrorist organisations, to gauge whether websites related to political actors deemed 'uncivil' by many will vary significantly in form from other societal groups using the web. The study suggests that websites relating to terrorist groups not only do not differ markedly from those of 'civil' groups, but also do not seem to offer any new dimension of terrorist threat.

Cyberoptimism vs. cyberpessimism

There are three main conceptions of the relationship between civil society and information and communications technologies. The 'cyberoptimist' model argues that computer-mediated communication (often referred to as CMC in the literature) will facilitate forms of communication, interaction and organisation that undermine unequal status and power relations (Spears and Lea, 1994:428). On the Internet, social context will be reduced in or around a message transmitted from sender to receiver (p. 431). The main beneficiaries of the reduction of social context in communication transactions would be nation-states in the developing world. The Internet can provide a degree of 'organisational coherence' to these political actors who ordinarily are incapable of 'punching above their weight' in the international community. Governments could use the databases to aid the more equitable distribution of resources in economically deprived regions. Information and communication technologies also could facilitate more sophisticated methods of democracy within advanced industrialised states. Low electoral turnouts could be partially remedied by the utility of electronic voting systems similar to the 'teledemocracy' piloted in California in the 1980s (Barber, 1984:275). 'Dialogic' democracy, in which citizens debate political issues with those who hold diametrically opposing views, could be facilitated by electronic bulletin boards. Giddens asserts that in an ethnically divided society such as Northern Ireland, the creation of a public arena could help resolve controversial issues and constrain violence (Giddens,

1995:16). Terrorist organisations often receive support from constituencies who feel that their perceived grievances are not recognised by their respective governments. The cyberoptimist model suggests that new technological innovations (such as bulletin boards and email) could allow these constituents to have their voices heard. This could potentially reduce the number of supporters—as well as future members—of terrorist organisations.

Inequalities in access to information and communication technologies militate against the cyberoptimist position and towards the cyberpessimist position. Cyberpessimists assert that the Internet will reinforce the gap between rich and poor as well as between activists and the disengaged (Norris, 2001:12). Statistics from the Organization for Economic Cooperation and Development (OECD) reflect the dominance of the First World in terms of Internet usage. An estimated 54.3 per cent of Americans use the Internet regularly compared to a mere 0.4 per cent of the population in Saharan Africa (Manrique, 2002:7). This First World hegemony is reflected in the predominance of English as the vernacular of cyberspace. This suggests that the so-called 'fourth generation rights' are being denied to developing countries in which English is not the common tongue. These rights include the right to information and the right to communicate (Council of Europe, 1997:39). The indigenous mass media facilitate the exercise of these rights more effectively than the Internet in developing countries. The Internet has not levelled the playing field for global political actors. However, Norris asserts that the Internet retains the potential to amplify the voice of 'less resourced insurgents and challengers' (2001:239).

The prospects for dialogic democracy using information and communications technologies would appear slim. Electronic bulletin boards devoted to political themes fail to promote deliberative political debate. People choose to post to groups that contain others with similar political ideologies to their own. This is illustrated by a survey of political Usenet groups in which only 9.3 per cent of leaders posted messages to ideologically dissonant groups (Hill and Hughes, 1997:13). People cannot be compelled to use the Internet to increase their comprehension of complex political issues. Political activity online remains a minority interest in the shadow of popular pursuits such as entertainment and sport. Both cybersceptics and cyberpessimists project that the Internet will alter inequalities of political power and wealth. The cybersceptic viewpoint is perhaps the most apposite conception of how information and communications technologies have altered power relations within nation-states. Norris (2001) asserts that the potential of the Internet has not yet had a dramatic impact on the realities of 'politics as usual' (p. 13). It is too early to assess whether information and communications technologies will have a lasting effect upon patterns of political organisation and behaviour.

How do civil society actors use the Internet?

Civil society organisations have used information and communication technologies in a conservative fashion to date. Environmental non-governmental organisations (NGOs) have essentially transferred their existing methods online, treating the Internet as another media tool. For example, they have chosen not to use 'electronic civil disobedience' techniques utilised by small extremist elements such as the Electro-Hippies (Denning, 2001:73). Websites are used for recruitment, fundraising, issuing press releases and advertising the core values of environmental NGOs. Sites such as GreenNet link pressure groups across the globe through transnational advocacy networks (GreenNet, http://www.gn.apc.org/). These

umbrella sites amplify the impact of smaller like-minded NGOs that might otherwise struggle to make their voices heard in the international community (Norris, 2001:187). It could be argued that other civil society organisations have failed to realise the potential for deliberation and protest offered by the Internet. Civil rights organisations have been slow to facilitate political debate among citizens or between citizens and the government. For example, while there were already 5 million regular African American Internet users (Lekhi, 2000:78), civil rights organisations such as the National Association for the Advancement of Colored People (NAACP) did not appear to be using the mobilising potential of the Internet. Rather, the NAACP maintained 'glossy' impressive websites promoting their activities (www.naacp.org). The NAACP site epitomised the hegemony of style over substance in the constitution of most civil society websites. The site provided no facility for deliberation amongst African Americans at that time (Lekhi, 2000:85), although the site was providing a forum for discussion on the Internet by 2005. The experience of civil society groups and political parties suggests that the Internet may not live up to the hype embodied by the cyberoptimist paradigm. Only small sub-state actors at the periphery of the political establishment have used the Internet to facilitate genuine political deliberation in the vein of the 'dialogic democracy' espoused by Anthony Giddens (1995:16). Less institutionalised organisations such as the Cartoon Rights Network have created opportunities for political debate and participation through bulletin boards on their websites (http://www.interplus.ro/smileclub/). The Internet can have a critical multiplier effect for civil society organisations via improvements in organisational linkage, bureaucratic efficiency and the advertisement of core values to a potentially worldwide audience. However, the Internet does not provide a critical mass for these organisations. People use the Internet as a private viewing box and therefore cannot be compelled to visit the websites of transnational advocacy networks or terrorist organisations (Noveck, 1999:30). The Internet does not increase the life expectancy of these sub-state groups. The attention of the conventional mass media, financial resources and grassroots activism are still critical to the sustenance of civil society organisations.

The Internet, civil society and semi-authoritarian states

It is in semi-authoritarian states that the Internet has precipitated tangible political change to date. The Internet can focus the attention of the international community upon the plight of oppressed sub-state actors within semi-authoritarian regimes. Oppressed groups can communicate with the Western mass media and sympathetic solidarity networks worldwide via 'mirror' sites in foreign territories. China, with the largest population on the planet, faces enormous challenges from global expansions in information and communication technologies as they increase the speed and volume of information that elites deliver to its citizens. These economies of scale might come at a high political cost for the Chinese authorities. Increased public utility of information and communication technologies will lead to increased exposure to foreign news websites, free from the ideological dogma of the Chinese political elite. An increasing number of exile groups will be able to brief their fellow citizens with information about what is really happening within the state (Noveck, 1999:49). China has responded to this threat by erecting electronic firewalls, which block access to websites that highlight human rights abuses by the Chinese government. Citizens who wish to access the Internet have to apply to open email and Internet accounts through Public Security Bureaus (Deibert,

2002:148). Access might be the only method through which the state can clamp down on this so-called 'cyberdissidence'. Firewalls can be easily sidestepped using proxy servers that reconnect users to sites officially blocked by the state (Deibert, 2002:153).

The Chiapas uprising in Mexico in 1994 exemplified the potential of the Internet as a weapon against semi-authoritarian states. A group of guerrillas staged an insurrection in opposition to Mexican government discrimination against the indigenous people of the Chiapas province (Ferdinand, 2000:13). Support for the movement and its leader, the enigmatic 'Subcomandante' Marcos, was mobilised on newsgroups such as Chiapas95 and sympathetic Internet sites hosted by US universities. This online mobilisation led to increased international scrutiny of the Mexican government and an end to their policy of repression in the region (Ferdinand, 2000:13). While not representing a coup d'état via cyberspace, the lessons of Chiapas for the political elites of semi-authoritarian states were clear. Sub-state political activists in semi-authoritarian states can attract a multitude of sympathisers worldwide utilising the public spaces of the Internet. At the same time, NGOs can help to expose human rights violations via the Internet and, in turn, the NGOs can lobby Western decision makers to take decisive action against oppressive states. The Internet can provide information even when repression reaches extreme levels. In Zimbabwe, NGOs such as Human Rights Watch have sustained a 'drip feed' of information to Western news agencies and governments alike despite President Robert Mugabe's decision to detain and expel Western journalists from the country.[1]

Terrorist organisations and the Internet

The dichotomy of 'civil' and 'uncivil' sub-state actors on the Internet relates to the transparency of their activities. Non-governmental organisations such as GreenNet typically use information and communication technologies in a one-dimensional 'overt' manner (GreenNet, http://www.gn.apc.prg). The group uses the Internet to facilitate communication, disseminate propaganda and recruit new members. 'Uncivil' actors such as terrorists use the Internet in a two-dimensional manner. The first dimension is identical to the functions of the websites of civil society actors. Terrorists often portray themselves on websites as oppressed civil society actors, in a similar vein to the Chiapas paradigm. They rarely make reference to their 'military' campaigns, choosing instead to focus upon their perceived grievances. Terrorist organisations have an asymmetric relationship with the traditional mass media. The media can survive without terrorism and have the power to determine which atrocity is reported. The Internet allows the terrorist rather than the editors to decide whether their activities are 'newsworthy'. Terrorist organisations can issue statements free from the ideological refraction of the mass media via the Internet. In using their own vocabulary, the terrorist can attribute a degree of legitimacy to their activities. Emotive words such as 'freedom fighter' and 'state oppression' permeate solidarity sites of organisations such as the Basque separatists Euskadi Ta Askatasuna (ETA).[2] However, people cannot be compelled to visit these websites. People who access these websites are likely to be members of the organisation itself, or sympathetic to its ideology.

The second dimension of the terrorist utility is of a covert nature. Terrorists use information and communication technologies to fund, plan and execute acts of terrorism against nation-states and their citizens. The attacks on New York and the Pentagon (11 September 2001) tragically illustrated this covert utility of the Internet. Subsequent investigations into the attacks revealed that the terrorists had used email and the Internet to coordinate and plan the hijackings (Pew Internet and American Life Project, 2001). Some terrorist groups have followed the lead of transnational corporations, organising themselves into decentralised networks. Theoretically, network-based terrorist organisations should not be defeated through decapitation as they are based around the idea of 'leaderless resistance'

(Tucker, 2001:1). Network-based groups such as Hamas are gradually replacing old hierarchical groups such as the Popular Front for the Liberation of Palestine in the Middle East. However, it should be noted that network-based terrorist organisations are not a product of the information age. The Palestinian Liberation Organization (PLO) was formed as a network of smaller Palestinian groups as early as 1964. However, the restructuring of terrorist hierarchies into networks has been facilitated by technological innovations such as email. There are other examples of covert utility of these new technologies. Bomb-making instructions can be distributed in the form of CD-ROMs to members worldwide. Intelligence can be gathered using information and communications technologies. The Ulster Loyalist Information Service has provided a secure email facility enabling sympathisers to submit information about leading Republicans or rival Loyalist factions.[3] Groups such as the Ulster Freedom Fighters in Northern Ireland have used the Internet to select potential targets. In March 2001, a message on an 'Ulster Loyalist' website urged the Limavady Ulster Freedom Fighters to go to a named bar where it claimed that members of the Provisional Irish Republican Army regularly visited.[4] Although this particular example came to the attention of the press, the scale of such covert utility of the Internet is difficult to assess. Most terrorist-related Internet sites such as Red Hand Commando carry disclaimers stating that their sites are for information purposes only (http://www.freewebs.com/red-hand/, accessed 14 June 2004). It is only when terrorist operations are foiled (or exposed in the conventional mass media) that this malevolent utility of the Internet is revealed.

Information and communication technologies provide a new medium through which the terrorist can attack the nation-state. States increasingly use information and communication technologies to store and disseminate information. These information systems as manifestations of state power are potential terrorist targets. Cyberterrorism can be defined as 'the unlawful attacks and threat of attacks on computers, networks and information stored therein when done to intimidate or coerce a government or its people in furtherance of political objectives' (Denning, 2000:1). The Liberation Tigers of Tamil Eelam (LTTE) have used 'cyber-terror' as a means of creating a new front in their conflict with the Sri Lankan authorities. In 1996, LTTE e-bombs hit several websites of Sri Lankan diplomatic missions, creating a virtual blockade (Zanini and Edwards, 2001:44). The paralysis of the Sri Lankan missions marked a propaganda coup for the insurgent Liberation Tigers of Tamil Eelam. The methods used by 'cyber-criminals' (hackers) and 'cyber-terrorists' (terrorists on the Internet) are similar. Both hackers and terrorists manipulate the content of popular websites to spread their names to a larger audience (Denning, 2001:72). The website www.attrition.org contains 'mirrors' of 'hacked' official government and corporate websites (www.attrition.org, accessed 24 October 2002). However, it should be noted that statistics from the Information Warfare Database show that such incidents are more likely to be perpetrated by hackers than terrorist organisations.[5] Sites such as the Californian Republican Assembly Caucus have been defaced by cyber-vandals. Personal messages and cartoon graphics were the most popular calling cards used by the hackers (www.attrition.org). So far, terrorists have not demonstrated that they have the necessary skills to effectively hack government sites. The difference between the terrorist and hacker is usually overlooked by nation-states. It is politically expedient for nation-states to assert that all hacking incidents are perpetrated by cyber-terrorists. Internet restrictions are less likely to be resisted if the public believes that the Internet is a haven of 'perverts and terrorists' (Moore, 1999:42). Cyber-terrorism receives more headlines in the conventional mass media than the covert utility of email or bulletin boards by terrorist organisations.

Terrorist organisations are likely to use the Internet to supplement their existing relationships with the mass media. Acts of cyber-terrorism themselves rely upon mass media reportage to permeate democratic polities. Cybercortical warfare can be defined as 'warfare'

conducted against minds or to change the will of an enemy (see Chapter 6). As Maura Conway points out, Hizbollah's 'cybercortical' campaign first came to prominence in 1999, when a story about mangled remains of slain Israelis published on a Hizbollah website caused a political row between the Israeli Defence Force and the families of several slain Israeli marines.[6] However, efforts to attract an American audience to their sites have so far proved less successful, despite the provision of an English-language facility on the three main Hizbollah websites. The existence of a website does not necessarily guarantee that more people will be exposed to the message and actions of the terrorist. The reaction of the conventional mass media to the exercise of 'hard power' (or 'big spectaculars') remains a more effective means of psychological warfare. People access the mass media in a very different fashion to the Internet. Television is a low-cost public medium available in virtually every household in advanced industrialised nations. Statistics also show that newspaper penetration in advanced industrialised nations remains high. In Northern Ireland, almost two-thirds of the adult population read at least one paper daily (Wilson, 1997:1). Media literacy can be described as a universal good in advanced industrialised democracies. Yet, while schools teach people to read and write—skills necessary to read the media—electronically mediated transactions require a new form of media literacy. The more people use information and communication technologies, the more fluent they become (Locke, 1999:219). Once people are literate in new information and communication technologies, they are likely to use the Internet as a private viewing box. The Internet cannot replicate either the shock value or the shared experience of real-time television images beamed live to millions of viewers.

Northern Irish terrorist organisations and the Internet

This chapter now turns to an examination of websites relating to Northern Irish terrorist organisations. The websites were selected with reference to the conclusions of the Independent Monitoring Commission Report (April 2004) and the UK Terrorism Act 2000.[7] Internet search engines geared to the British audience, including Google (www.google.co.uk) and Yahoo (www.yahoo.co.uk), were utilised to locate unofficial 'solidarity' sites. Solidarity sites were selected on the basis that they issued statements in support of or on behalf of proscribed Northern Irish terrorist organisations (see Table 7.1).

Organisational linkages

Republican organisations use the Internet effectively to communicate with local party activists and the mass media.[8] Each of the Republican groups examined provided correspondence details (including email addresses) for local activists (see Table 7.2). Members (and non-members) are invited to email departments within these organisations if they require any further information. Republican organisations also offer links to both domestic and international organisations. The Irish Republican Socialist Movement provides links to such diverse groups as the Popular Front for the Liberation of Palestine, Tupac Amaru and Jaleo.[9] Sinn Fein provides an email newsletter, the *Irish Republican Media*, via its website. This service grants the subscriber access to video and audio clips, Sinn Fein archives and exclusive interviews with the leadership (www.sinnfein.ie, accessed 10 April 2004). Subscribers also are given access to downloadable copies of the Sinn Fein newspaper *An Phoblacht/Republican News*. Similarly, the Irish Republican Socialist Movement and Republican Sinn Fein provide electronic versions of their publications, the *Starry Plough* and *Saoirse*.[10] Republican groups also use their websites to issue statements targeted at the conventional mass media. All of the Republican sites examined in this study had a 'Press Releases' section. In these sections, Republican groups post comments on local and international news stories. The Irish Republican Social Movement site issues statements on diverse issues such as the dedication of local hunger strike monuments, the Swedish-Kurdish Culture Association and statements from the proscribed Irish National Liberation Army

(www.irsm.org/statements/irsp/archive, accessed 12 April 2004). Republican groups use the Internet in a similar fashion to NGOs such as GreenNet. They use their sites to create more sophisticated bureaucracies, to promote solidarity with international organisations that share similar values, and to 'drip-feed' stories to the conventional mass media.

In contrast to Republican organisations, none of the Loyalist sites surveyed provide an email newsletter (see Table 7.3). Loyalist groups do not clearly identify their leadership on their websites. Loyalist organisations do not identify any current members of their organisation on their websites. Contact with these organisations is strictly limited to email correspondence with the webmaster. The Progressive Unionist Party is the exception, providing email addresses for both its leader David Ervine and its Chief Electoral Officer (www.pup-ni.org.uk, accessed 15 May 2004). Loyalist organisations do use the Internet to issue statements to the mass media. The Tullycarnet Ulster Political Research Group website issues press releases on grassroots issues, such as the redevelopment of a local park (www.tullycarnetuprg.ionichost.com, accessed 10 May 2004). The Orange Volunteers issue press releases via solidarity websites such as Loyalist Voice. The links provided by Loyalist sites provide the starkest contrast with their Republican counterparts. Republican websites provide links to groups engaged in struggles of 'national liberation', Irish diasporas as well as groups who share their Marxist principles. Diasporas in the United States provide crucial financial resources that sustain Republican organisations, so it is not surprising that Loyalist sites typically provide fewer links to diasporas or international solidarity organisations. The links provided on Loyalist sites are almost exclusively groups based in the United Kingdom. Loyalist Voice, for example, links 'exclusively' to websites such as the Yorkshire Loyalists and Cumbria Loyalists (http://free.freespeech.org/ovs/, accessed 10 May 2004). In sum, Loyalist organisations appear to use the Internet less effectively for organisational linkage.

Justification of violence

The Internet allows Republican organisations to expound their core tenets and ideologies. The conventional mass media do not provide the necessary 'space' in which these groups can provide a detailed justification for campaigns involving political violence. Republican organisations broadly seek a 32-county socialist Irish republic as the solution to the Troubles, i.e. the historic conflict over British versus Irish rule for Northern Ireland. Consequently, Republican websites rarely refer to the political entity of Northern Ireland. Rather, the Irish Republican Socialist Movement refers to Northern Ireland as a 'colonial statelet' or the 'occupied six counties', denying the legitimacy of its position within the United Kingdom.[11] Republican websites depict their 'military activities' as morally justified in the context of Unionist political discrimination and British military aggression against their communities. In their 'History of the Conflict' section, Sinn Fein justifies the Provisional Irish Republican Army offensive of 1969 as a legitimate response to the 'Battle of the Bogside' in Derry, unionist 'pogroms' in Belfast and the introduction of internment without trial.[12] The implication of this version of events in 1969 is clear. Republican organisations consider themselves participants in a 'just war' on behalf of the Irish working classes against the British occupation of Ireland. Groups such as Sinn Fein and Republican Sinn Fein depict violence as legitimate when used as a last resort.[13] Eulogies for Republican terrorists killed during the Troubles permeate the websites of Republican organisations. Republicans use their Internet sites to provide their own history of the Troubles. They use their own frames to legitimise campaigns of political violence.

Loyalist groups also use the Internet to define their political ideologies. Loyalist organisations support the British presence in Northern Ireland and swear allegiance to the

British monarchy. The term 'Northern Ireland' is employed at regular intervals on all of the Loyalist websites examined for this analysis. Loyalist organisations choose instead to attack Republicans and the government of the Republic of Ireland (or the 'imperialist government of Eire') on their websites (http://www.ulisnet.com/main.htm, accessed 2 March 2003). Loyalist political violence is justified on the Internet by solidarity sites such as 'Loyalist Voice'. The genesis of groups such as the Red Hand Commandos is attributed to Republican attacks on members of the Loyalist community (http://www.freewebs.com/red-hand/, accessed 16 May 2004). Loyalist terrorist activity is defined as reactive or defensive in nature. This is very similar to the justification of Provisional Irish Republican Army violence that features on the Sinn Fein website. Loyalist political violence is not discussed or justified on the 'official' Loyalist websites. The Progressive Unionist Party website does not provide a history of the Ulster Volunteer Force or Red Hand Commandos. The Progressive Unionist Party asserts that they only provide 'political analysis' to the leadership of the Ulster Volunteer Force or the Red Hand Commandos (www.pup-ni.org.uk, accessed 15 May 2004). The Tullycarnet Ulster Political Research Group similarly does not offer any comment on current Ulster Defence Association activity. This 'ideology-lite' website instead highlights Ulster Political Research Group activities in the Tullycarnet area, such as the organisation of discos for local teenagers (www.tullycarnetuprg.ionichost.com, accessed 10 May 2004). The website does not expound on the ideology of the organisation, nor define it as 'Loyalist'.

However, the assertions of these groups on their websites are negated by the recent Independent Monitoring Commission report into paramilitary activity. The International Monitoring Commission concluded that both the Ulster Political Research Group and the Progressive Unionist Party were directly linked to the proscribed Ulster Defence Association and Ulster Volunteer Force respectively.[14] These groups thus use their websites to deliberately blur the distinction between civil and 'uncivil' society. This is achieved not just by the rhetoric these groups employ, but also by the information they do not disclose on their websites. These groups do not use their websites to illuminate their links to political violence. They use their websites to portray themselves solely as community activists and political parties.

Fundraising and recruitment

Republican organisations use the Internet in a similar fashion to NGOs in their efforts to recruit members and raise funds. Membership of these organisations is open to applicants worldwide. Only Republican Sinn Fein stipulates that applicants must live in Ireland, Wales, Scotland or England (www.rsf.ie, accessed 18 May 2004). The procedure for joining each of these Republican organisations is identical. Online application forms are provided by each Republican organisation, to be submitted by the applicant along with a current telephone number and email address. This mirrors the online recruitment section of 'civil' groups such as the National Association for the Advancement of Colored People (www.naacp.org, accessed 2 March 2003). Potential recruits to Republican organisations are advised that they will be contacted by the organisation in due course. The Irish Republican Socialist Movement and Sinn Fein also solicit donations using an online application form. The Irish Republican Socialist Movement provides bank details for people who wish to contribute to their 'Fighting Fund'.[15] Republican groups are savvy in their utility of the Internet to aid recruitment and fundraising. These sites claim that they do not solicit resources for proscribed terrorist organisations; rather the 'Fighting Fund' is to sustain the Irish Republican Socialist Movement's *Starry Plough*. People visiting these sites are asked to join political parties such

as Republican Sinn Fein. They are not invited to apply to become members of proscribed terrorist organisations such as the Continuity Irish Republican Army.

Loyalist websites lack the sophistication of their Republican counterparts. These websites do not provide online application forms on their websites. Solidarity sites such as the Ulster Loyalist Information Service solicit resources from visitors to their sites. The ULISNET site requests that members donate (amongst other items) bulletproof vests, computers and Christmas gifts. The website states that the bulletproof vests are for 'obvious uses'.[16] This explicit reference to paramilitarism is the exception rather than the rule for Loyalist websites. The official Loyalist websites do not solicit resources via their websites. However, the Progressive Unionist Party and Tullycarnet Ulster Political Research Group do advertise membership on their websites. It should be noted that they do not advertise membership of proscribed paramilitary groups. Like their Republican counterparts, these organisations use their websites to recruit members to political, rather than military, organisations. The Progressive Unionist Party invites potential members to phone or email the webmaster in order to get an application form.[17] This suggests that members are still recruited on the basis of face-to-face interviews rather than over a relatively anonymous web linkage. Loyalist organisations, despite their lack of technological sophistication, use the Internet in a similar fashion to NGOs. For example, GreenNet uses similar methods of recruitment on its websites as volunteers are asked to email or telephone GreenNet if they are interested in positions advertised on the website.[18] Both civil and uncivil society actors are likely to favour recruitment strategies that include face-to-face interviews.

Conclusions

Organisations with historic links to terrorism use the Internet in a similar fashion to NGOs. The Internet will facilitate increased organisational coherence and communication across national borders. This analysis shows that Northern Irish organisations with historic links to paramilitary groups use similar methods of recruitment and organisational linkage to established NGOs such as GreenNet. Loyalist and Republican groups use their websites to portray themselves as legitimate members of civil society. It is the covert nature of terrorist computer-mediated communication that distinguishes it from NGOs. Terrorists use information and communication technologies to plan and perpetrate atrocities. The scale of this covert communication is extremely hard to estimate. The threat of 'cyber-terrorism' is vastly exaggerated by nation-states as a means of justifying Internet restrictions. Cyberoptimists assert that the Internet will alter power relations in favour of marginalised groups. Yet empirical evidence suggests that it is simply too early to determine how the Internet will affect power relations. A 'cybersceptic' approach should be employed by nation-states, when assessing the risk posed by 'cyber-terrorism' or 'cybercortical' warfare. The Internet is simply not an appropriate vehicle for compelling millions to identify with the causation and effect of political violence. Republican and Loyalist groups are likely to continue to use 'big spectaculars' as a central part of their strategy. Psychological warfare, a necessary component of ethno-nationalist terror, is effectively conducted through manipulation of the television news flash and the front pages of newspapers. The Internet will supplement the existing relationship between these groups and the mass media. As with NGOs, organisations with historic links to terrorist groups use their websites to deliver messages to their members, supporters, the media and occasionally their opponents. These messages are only placed in the public domain when they are reported by the conventional mass media. While it is possible that the Internet could increase the longevity of such outsider groups as the Provisional IRA, by improving organisational coherence and the ability to commune covertly in cyberspace, the Internet cannot replicate the shared experience of the

mass media. For terrorists, activities in the offline world are more likely to dictate their ability to survive or increase their political influence. Despite the government emphasis on cyber-terrorism, there is relatively little evidence of increased terrorist threat to citizens from the web pages of organisations linked to terrorism in Northern Ireland.

Notes

1 Human Rights Watch, 'Zimbabwe', http://www.hrw.org/reports/2002/zimbabwe/ (accessed 21 February 2003).
2 Euskal Herria Journal—Navarre: A Basque Journal, http://www.contrast.org/mirrors/ehj/ (accessed 20 June 2004).
3 Ulster Loyalist Information Service, 'Projects', www.ulisnet.com/main.htm (accessed 2 March 2003). Please note this website is now offline.
4 'New Internet Terror Fear: Loyalists Are Using Web to Pick Targets', *Belfast Telegraph*, 15 March 2001.
5 Information Warfare Database, Terrorism Research Center, http://www.terrorism.com/iwdb/incidents.asp, (accessed 2 March 2003).
6 In 1999, a story emanating from a Hizbollah website claimed that a single coffin had been returned to Israel from Lebanon containing the body parts of several murdered Israeli marines. This caused a row between IDF officials and the families of the deceased.
7 Report issued by the Independent Monitoring Commission, 20 April 2004, available at http://www.news.bbc.co.uk/hol/shared/bsp/hi/pdfs/20_04_04_imcreport.pdf (accessed 22 April 2004); UK Terrorism Act 2000, www.homeoffice.gov.uk/terrorism/threat/groups/index.html (accessed 20 June 2004).
8 Websites were examined over a period of time from 2001 to 2004; these comments relate to how the websites appeared as of 2004.
9 Links in Solidarity, www.irsm.org/general/links (12 April 2004). Please note that Tupac Amaru is linked to the Peruvian terrorist organisation MRTA. Jaleo are a group of Andalusian Socialists.
10 Saoirse Online Newsroom, www.saoirse.rr.nu (accessed 14 April 2004); Electronic Starry Plough, www.irsm.org/irsp/starryplough (accessed 12 April 2004).
11 Irish Republican Socialist Committee, 'Thirty Years of Struggle', www.irsm.org/general/history/irsm20yr.htm (accessed 12 April 2004).
12 Sinn Fein, 'History of the Conflict 1968–1992', www.sinnfein.ie (accessed 15 May 2004).
13 'What is Irish Republicanism?', Ruairi O'Bradaigh, Republican Sinn Fein, www.rsf.ie (accessed 18 May 2004).
14 Report issued by the Independent Monitoring Commission, 20 April 2004, available at http://www.news.bbc.co.uk/hol/shared/bsp/hi/pdfs/20_04_04_imcreport.pdf (accessed 22 April 2004).
15 Electronic Starry Plough, http://irsm.org/irsp/starryplough/ (accessed 12 April 2004).
16 Ulster Loyalist Information Service, http://www.ulisnet.com/main.htm (accessed 2 March 2003). Please note this website is no longer available online.
17 Tullycarnet UPRG (accessed 10 May 2004).
18 GreenNet, 'Jobs and Volunteering', www.gn.apc.org/jobs.html (accessed 2 March 2003).

Table 7.1 Proscribed Northern Irish terrorist organisations

Group	*Political orientation*	*Estimated strength*	*Year formed*	*Pro/anti Good Friday Agreement*	*Website from organisation with closest political links*	*Unofficial (solidarity) website*
Continuity Army Council[1]	Republican	Under 50 active members	1996	Anti	Yes (as Republican Sinn Fein)	Yes
Cumann na mBan	Republican	No data available	1914	No data available	No	No
Fianna na hEireann	Republican	Unknown	1909	Anti	Yes	No
Irish National Liberation Army	Republican	Under 50 active members	1975	Anti	Yes (as Irish Republican Socialist Movement)	Yes
Irish People's Liberation Organisation[2]	Republican	No data available	1976	No data available	No	No
Irish Republican Army (also known as PIRA)	Republican	Several hundred active members	1970	Pro	Yes (as Sinn Fein)[3]	Yes
Loyalist Volunteer Force	Loyalist	50–150 active members, 300 supporters	1996	Anti	No	Yes
Orange Volunteers	Loyalist	20 active members[4]	1998	Anti	No	Yes
Red Hand Commandos	Loyalist	No data available	1972	Pro	No	Yes
Red Hand Defenders	Loyalist	Up to 20 active members	1998	Anti	No	No
Saor Eire	Republican	No data available	1931	No data available	No	No
Ulster Defence Association/Ulster Freedom Fighters	Loyalist	Few dozen active members	1971	Pro	Yes (as Ulster Political Research Group)	Yes
Ulster Volunteer Force	Loyalist	Few dozen active members	1966	Pro	Yes (as Progressive Unionist Party)	Yes

Sources: International Policy Institute (2004); Conflict Archive on the Internet, *Loyalist and Republican Groups*.

Notes:

1 Linked to Republican Sinn Fein, Continuity IRA and, according to some sources, Real IRA.

2 The Irish People's Liberation Organisation (IPLO) announced its dissolution in October 1992 following an internal feud.

3 Sinn Fein defines itself as a political organisation distinct from the IRA. However, the 2004 Independent Monitoring Commission Report found significant overlap in the two groups.

4 Security sources believe that Red Hand Defenders and Orange Volunteers are served by the same pool of volunteers.

Table 7.2 Functions of Republican websites

Group	*Website of organisation with closest political links*	*Justification of political violence*	*Press releases*	*Full membership available/ advertised*	*Donations*	*Email newsletter*	*Members-only section*
Continuity Army Council	Republican Sinn Fein, www.rsf.ie	Yes	Yes	Yes	No	Yes	No
Fianna na hEireann	Fianna na hEireann, http.//fianna.netfirms.com/	No	Yes	Yes	No	No	No
Irish National Liberation Army	Irish Republican Socialist Movement, www.irsm.org/	Yes	Yes	Yes	Yes	Yes	No
Irish Republican Army	Sinn Fein, www.sinnfein.ie	Yes	Yes	Yes	Yes	Yes	No

Source: Author's research.

Table 7.3 Functions of Loyalist websites

Group	*Website of organisation with closest political link*	*Justification of political violence*	*Press releases*	*Full membership available/ advertised*	*Donations*	*Email newsletter*	*Members-only section*
Loyalist Volunteer Force	Ulster Loyalist Information Service,[1] www.ulisnet.com	Yes	Yes	Yes	Yes	No	No
Orange Volunteers	Loyalist Voice, http://free,freespeech.org/ovs/	Yes	Yes	No	Yes	No	No
Red Hand Commandos	Red Hand Commandos, http://www.freewebs.com/red-hand/[2]	Yes	No	No	No	No	No
Ulster Defence Association/ Ulster Freedom Fighters	Tullycarnet Ulster Political Research Group, http://www.tullycarnetuprg.ionichost.com/	No	Yes	Yes	No	No	No
Ulster Volunteer Force	Progressive Unionist Party, www.pupni.org.uk	No	Yes	Yes	No	No	No

Source: Author' s research.
Notes:
1 Site no longer online.
2 Site states that it is merely for information purposes and does not support the views of the Red Hand Commandos.

References

Barber, B. (1984) *Strong Democracy: Participatory Politics for a New Age*, London: University of California Press.

Conflict Archive on the Internet (CAIN) Loyalist and Republican Groups. Online. Available http://cain.ulst.ac.uk/issues/violence/paramilitaryhtm (accessed 10 June 2004).

Council of Europe (1997) *Cultural Rights, Media and Minorities,* Strasbourg: Council of Europe Press.

Deibert, R.J. (2002) 'Dark Guests and Great Firewalls: The Internet and Chinese Security Policy', *Journal of Social Studies* 58, Spring: 143–159.

Denning, D. (2000) 'Cyberterrorism, Global Dialogue'. Online. Available http://www.cs.georgetown.edu/~denning/publications.html (accessed 10 March 2003).

Denning, D. (2001) 'Cyber Warriors: Rebels, Freedom Fighters and Terrorists Turn to Cyberspace', *Harvard International Review* 23 (2), Summer: 70–75.

Ferdinand, P. (ed.) (2000) *The Internet, Democracy, and Democratization,* London: Frank Cass.

Giddens, A. (1995) 'The New Context of Politics: New Thinking for New Times', *Democratic Dialogue*. Online. Available http://www.democraticdialogue.org/publications.htm (accessed 2 March 2003).

Hill, K.A. and Hughes, J.E. (1997) 'Computer-mediated Political Communication: The USENET and Political Communities', *Political Communication* 14:3–27.

International Monitoring Commission (2004) *International Monitoring Commission Report,* 20 April. Online. Available http://www.news.bbc.co.uk/hol/shared/bsp/hi/pdfs/20_04_04_imcreport.pdf (accessed 22 April 2004).

International Policy Institute (2004) *Terrorist Group Profiles.* Online. Available www.ict.org.il/inter_ter/orgdat (accessed 10 June 2004).

Lekhi, R. (2000) 'The Politics of African America Online', in Ferdinand, P. (ed.), *The Internet, Democracy, and Democratization,* London: Frank Cass.

Locke, T. (1999) 'Participation, Inclusion, Exclusion and Netactivism: How the Internet Invents New Forms of Democratic Community', in Hague, B.N and Loader, B.D. (eds), *Digital Democracy Discourse and Decision Making in the Information Age,* London: Routledge.

Manrique, C.G. (2002) 'The Internet and World Politics in an Age of Terror', Paper presented at the American Political Science Association annual meeting, Boston, MA.

Moore, R.K. (1999) 'Democracy and Cyberspace', in Hague, B.N. and Loader, B.D. (eds), *Digital Democracy Discourse and Decision Making in the Information Age,* London: Routledge.

Norris, P. (2001) *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide,* New York: Cambridge University Press.

Noveck, B.S. (1999) 'Paradoxical Partners: Electronic Communication and Electronic Democracy', in Hague, B.N. and Loader, B.D. (eds), *Digital Democracy Discourse and Decision Making in the Information Age,* London: Routledge.

Pew Internet and American Life Project (2001) 'How Americans Used the Internet after Terror Attack', 15 September, Washington, DC: Pew Internet and American Life Project. Online. Available www.pewinternet.org (accessed 27 September 2002).

Spears, R. and Lea, M. (1994) 'Panacea or Panopticon: The Hidden Power in Computer Mediated Communication (CMC)', *Communication Research* 21 (4): 427–459.

Tucker, D. (2001) 'What's New about the New Terrorism and How Dangerous Is It?', *Terrorism and Political Violence* 13, Autumn: 1–14.

Walzer, M. (1995) *Towards a Global Civil Society, International Political Currents,* Volume 1, Oxford: Berghahn Books.

Wilson, R. (1997) 'The Media and Intrastate Conflict in Northern Ireland', *Democratic Dialogue,* July. Online. Available http://www.democraticdialogue.org/publications.htm (accessed 2 March 2003).

Zanini, M and Edwards, J.A. (2001) 'The Networking of Terror in the Information Age', in Arquilla, J. and Ronfeldt, D., *Networks and Net wars: The Future of Terror, Crime, and Militancy,* Santa Monica, CA: Rand Corporation.