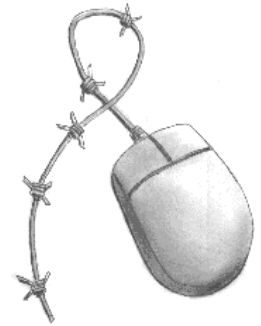


GreenNet CSIR Toolkit Briefing no. 15

New Terrorism Legislation

How new terrorism legislation may criminalise the work of protest groups



Written by Paul Mobbs for the
GreenNet Civil Society Internet Rights Project, 2002.
<http://www.internetrights.org.uk/>

Terrorism (whether organised by "internal" groups or those in other states) can be a threat to any country. It is justifiable to have legislation which can police the threat to society that terrorism represents.

In the wake of the September 11th attacks on New York and Washington, however, many states are introducing new, wide-ranging powers relating to terrorism. Canada¹, the USA² and France³ are among states who are planning to introduce such powers, or who have done so. A significant part of these powers focus on the use of the Internet.

A central aspect of these new laws is that they redefine terrorism, to cover a broader range of activities than previous legislation. Security services, such as the Federal Bureau of Investigations in the USA, have also begun to describe the activities of some grassroots protest groups - such as *Reclaim the Streets* - as terrorism⁴.

In the UK, the Home Office definition of certain types of action as posing "extreme" problems for public order will have a powerful influence on how recent, draconian anti-terrorism laws (introduced before and after September 11th) are used against those in civil society who protest against government policy. New legislation has widened the scope for using terrorist investigations against campaign groups and individuals dissenting from local or national government policy.

This new UK legislative framework (principally made up of the Terrorism Act 2000, the Regulation of Investigatory Powers Act 2000, The Police Act 1997 and the Security Services Act 1996, all of which we discuss in more detail below) is not specifically intended to assist "*the maintenance of order*", but to address, over and above the use of violence for a political cause, any action that "*seeks to change the mind of government*".

The implementation of this new anti-terrorism framework may prove useful in anticipating how international anti-terrorism laws will develop; many of these new laws are intended to implement international agreements, such as the *Cybercrime Convention*⁵ recently agreed by the Council of Europe.

¹See Wired, 19th October 2001 - <http://www.wired.com/news/conflict/0,2100,47734,00.html>

²See Wired, 12th October 2001 - <http://www.wired.com/news/print/0,1294,47522,00.html>

³See '*Lutte contre le terrorisme et controle de l'internet*' by Reporters sans Frontieres (in French) - <http://www.rsf.fr>

⁴*Statement for the Record* - Louis J. Freeh, Director Federal Bureau of Investigation - on the Threat of Terrorism to the United States before the United States Senate Committees on Appropriations, Armed Services, and Select Committee on Intelligence, 5th October, 2001 - available from the FBI's web site at <http://www.fbi.gov/congress/congress01/freeh051001.htm>

⁵*Cybercrime Convention* - <http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185&CM=1>

The problem with the new legislation is that the definitions of "terrorism" cover more than paramilitary or violent action and extend to actions that seek to challenge the power of the state. These new laws therefore endanger rights to public protest.

This briefing, therefore, deals with the potential impact of new anti-terrorism legislation on public protest, and in particular protest that is organised via the Internet or involves some form of direct action. We will do this by looking at the implementation of the *Terrorism Act 2000* in the UK.

The Terrorism Act 2000

The *Terrorism Act 2000*⁶ sought to update the law on terrorism to take account of recent political changes in Ireland, following a Government review of terrorism legislation⁷. But at the same time it widened the definition of terrorism to include actions that have traditionally been mechanisms of social change - direct action protests, for example. Many of the new laws proposed in other states, such as the USA, are very similar to the Terrorism Act. Some states are even using the new UK Act as a template for their own legislation.

For many years terrorism within the UK (excluding Northern Ireland, which has always had its own unique legislation) was dealt with under a variety of existing laws. Some of these laws date back to the nineteenth century and were originally drafted to deal with the Chartists, early trades unions, and other groups protesting for political and social change.

The Terrorism Act 2000 created new offences relating to the membership and support of specific proscribed terrorist organisations. The new Act proscribes certain groups involved with violence in Ireland, but allows for the Home Secretary (i.e. the Minister for the Interior, in European terms) to add further organisations to the list.

As well as creating new offences in relation to proscribed organisations, the Act also makes provision for the investigation of "terrorism" connected with groups other than those proscribed. This is a key area of concern.

If a group has been proscribed the Act provides for an appeals process whereby those concerned can argue that their actions do not constitute terrorism. But there is a significant threat to civil liberties in the very wide definition of terrorism and the sweeping powers of investigation against individuals that the Act establishes. It gives the state new powers to investigate the organisation and activities of protest groups - such as those campaigning on animal vivisection, against nuclear or chemical establishments, or taking direct action against damaging construction or development projects - and to prosecute those directing such campaigns.

The Act's definition of terrorism is so broad that it will cover many groups who use peaceful demonstration or direct action to achieve change.

Actions, or threats of action, by a group or person are defined as terrorism under Section 1 of the Act if:

- the action falls within subsection (2); and
- the use or threat is made for the purpose of advancing a political, religious or ideological cause; and
- the use or threat is designed to influence the government or to intimidate the public or a section of

⁶The *Terrorism Act 2000* - <http://www.hmso.gov.uk/acts/acts2000/20000011.htm>

⁷*White Paper on Terrorism Legislation* - <http://www.archive.official-documents.co.uk/document/cm41/4178/4178.htm>

the public.

This last point is the one that challenges civil liberties. Intimidating the public in order to influence the government is a traditional tactic of terrorism. But the ability to undertake action *designed to influence government* is the guarantee of a democratic society.

The use of the word *or* in the Act, rather than the words *by* or *through the means of* means that the two elements of the clause are logically separated. Action that seeks to influence government, but involves no threat, violence or intimidation against the public, also qualifies as terrorism.

It may be argued that most protest action is based on political or ideological grounds. Such protest action would be defined as terrorist "*action under subsection 2*" if it:

- involves serious violence against a person, or
- involves serious damage to property, or
- endangers a person's life, other than that of the person committing the action, or
- creates a serious risk to the health or safety of the public or a section of the public, or
- is designed to seriously interfere with or to seriously disrupt an electronic system.

Two of these conditions could relate to peaceful protests:

- *damage to property*: This clause could be used against direct action protests, such as roads protests. Other recent examples of such action are the campaign against the sale of Hawk jets to the Indonesian government, or the action by Greenpeace members against genetically engineered crop trials (for which those involved in these actions were acquitted in court).
- *disruption of electronic systems*: This clause could criminalise forms of online protest such as email lobbying or actions against Internet sites. Online actions promoted by protest groups do not breach computer misuse laws⁸ in the way they involve "changing or modifying computer systems". The Terrorism Act covers any group involved in online protest, however, if they can be said to have the potential to "disrupt" systems. The Act does not define the extent of what is meant by disruption; so even if an online action caused only minor inconvenience to its targets, it would constitute a disruption under the Act.

The other significant aspect of the Act is the powers it creates to investigate terrorism. Prior to the Terrorism Act, police forces investigated terrorist incidents and the security services investigated the terrorists themselves. The new Act creates new powers in relation to enable the investigation of:

- the commission, preparation or instigation of acts of terrorism,
- an act which appears to have been carried out for the purposes of terrorism,
- the resources of a proscribed organisation,
- the possibility of making an order to proscribe an organisation, or
- the commission, preparation or instigation of an offence under the Act.

This is a wide-ranging definition. The emphasis on investigation *before* a terrorist act takes place means that anyone falsely defined as being a terrorist under the definitions in section 1 could be subject to any of the investigation provisions of the Act without any substantial evidence. The suspicion of the police or the security services would be enough to warrant an investigation.

The powers of an officer to investigate terrorism are detailed in *Part IV* (sections 32 to 39) and *Schedule 14*

⁸ See GreenNet CSIR Toolkit Briefing no. 8 on *Computer Crime*.

of the Act. An "officer" may be a policeman, a customs officer or an immigration officer, or a member of the security services. As well as having powers of search with or without (the latter to be approved by a senior police officer in "urgent" cases) a warrant or on suspicion, the officer "*may if necessary use reasonable force for the purpose of exercising a power conferred on him by virtue of this Act*".

There is a general requirement that officers investigating terrorism must act in accordance with *relevant codes of practice*. These codes of practice must be approved by Parliament; they interpret the Act and guide the work of those involved in terrorist investigations. However, although officers are required to work in accordance with the code, the Act does not hold them liable for criminal or civil proceedings⁹ for any breaches of the code. This is a cause for concern; in the absence of proper penalties for breaches, officers might depart from the code whenever they find it convenient. If a breach of the Code is demonstrated, however, this failure can be used as evidence in criminal proceedings.

The arrest and detention of suspects is defined in *Part V* of the Act. Section 41 permits a police officer to *arrest without a warrant a person whom he reasonably suspects to be a terrorist*. The police may stop and search a person whom they reasonably suspect to be a terrorist to discover whether he has in his possession anything which may constitute evidence that he is a terrorist.

Authorisations for stop and search do not have to be given to police officers in writing. A senior police officer can issue verbal authorisation and confirm it in writing as soon as is reasonably practicable. A person detained under section 41 (unless detained under any other power) must be held for forty-eight hours from the time of arrest. They can be released within forty-eight hours only if, on review of their case, there is no cause to detain them. These reviews must be carried out at least every twelve hours.

The powers created for investigating terrorist suspects, especially the powers of search and detention, are a clear threat to civil liberties if not used with care. The ability to detain for forty-eight hours without access to legal assistance could lead back to the sorts of miscarriages of justice seen in the 1970s and 1980s, in relation to Irish terrorism, if as a result detainees are pressured into incriminating themselves or others.

Other significant powers in the Act relate to the *collection of information*, and the power to require a *reasonable explanation* for the possession of an article:

- Section 58 of the Act makes it an offence to collect or make a record of information of a kind likely to be useful to a person committing or preparing an act of terrorism, or to possess a document or record containing information of that kind. There is no definition or explanation of precisely what kind of documentation might be useful to terrorists, and the section applies to both paper and electronic documents. A person may be charged with this offence alone, even if the police have no clear evidence that they are involved with any terrorist action.
- Section 13 of the Act allows those investigating terrorism to obtain a court order to require a person who is subject to investigation, or from whom evidence has been seized, to provide a "reasonable explanation" for the possession of those items. There is a legal penalty for not providing an explanation, or providing a false or misleading explanation.

In the past, the possession of certain types of information has been used to support the prosecution of certain offences. In essence, the possession of information has always been ancillary to the act the police were investigating (see reference to the *GAndALF* case below).

The new Act changes this to make possession a specific offence. The offence of "possession" under section 58 can also be investigated and prosecuted in its own right too. Section 40 of the Act on "suspected terrorists" includes reference to section 58, and hence possession of information; information taken from the Internet and monitored under the powers provided by the RIP Act, for example, could be investigated.

⁹Section 101(6) of the Terrorism Act 2000

The police could arrest people without a warrant (under section 41 of the Act), or obtain warrants to search premises for evidence, to bring a prosecution under section 58. The use of section 13 as part of these investigations could also be used to gain further evidence by self-incrimination.

This presents new opportunities for the state to harass or intimidate members of the public. Information on the construction of explosive devices, or information on the structures on terrorist organisations, is one thing. *Information of a kind likely to be useful to a person committing or preparing an act of terrorism*, however, might be something far more innocuous.

These sections emphasise that possession is an offence unless the person charged proves that they had a "reasonable excuse" for possession. As such, it criminalises knowledge.

An example of how these powers might be used is the trials of activists for "conspiracy with persons unknown", and in particular the trial of the *Gandalf Six*¹⁰. Members of the *Green Anarchist Magazine*, and the *Animal Liberation Newsletter*, were charged with "conspiracy" with "persons unknown" to commit criminal damage. This was based upon their reporting of incidents of criminal damage against animal experimentation laboratories or construction sites. The case included the possession of material relating to the planning and execution of criminal damage - one of the group had a copy of the *Anarchists' Handbook*. The *Anarchists' Handbook* is widely available, has an ISBN number and can be ordered from bookshops. Even so, it was still used as evidence for the prosecution.

The Anti-Terrorism, Crime and Security Act 2001

In the wake of the September 11th terrorist attacks, the UK Government decided that the new anti-terrorism framework created during 2000 was insufficient. This led to the hurried preparation and rushing through Parliament of the *Anti-Terrorism, Crime and Security Act 2001*¹¹. The Act is not a specific set of measures intended to address a specific threat - it has been described as a mish-mash of measures cleared out of the cupboards of Whitehall mandarins, and which use the media panic created around the September 11th attacks to justify their implementation, with as little public debate as possible through an expedited Parliamentary process¹².

The Act contains a diverse range of powers. But of particular concern are Parts 3, 11 and 13. What it is important to realise is that the provisions of this new Act are not limited to terrorism. Under the Terrorism Act 2000, the powers of the Act required that people 'qualify' as terrorist under Section 1 of the Act. This new Act does not have this restriction. Its powers could be used against terrorists. But they could equally be used against those engaged in disruptive protests, or other types of action where the police or security services can use the 'common purpose principle' (see next section) to justify their investigations.

Part 3 - 'Disclosure of information' (sections 17 to 20)

The Home Office's summary of the Bill¹³, given to Parliament during the debate on the new law, stated in relation to Part 3:

Part 3 and schedule 4 of the Bill contain provisions to remove current barriers which prevent

¹⁰The *Green Anarchist* and *Animal Liberation Front* trial - see <http://www.tlio.demon.co.uk/gandalf.htm> and the *Index on Censorship* feature at <http://www.indexonline.org/news/archives/UK2240798.htm>

¹¹The *Anti-Terrorism, Crime and Security Act 2001*- <http://www.legislation.hmso.gov.uk/acts/acts2001/20010024.htm>

¹²A paraphrasing of the comments of one of the opponents of the Act, Brian Sedgemoor MP, during its passage through the House of Commons during December 2001.

¹³See the Home Office's *Anti-Terrorism Bill* page - <http://www.homeoffice.gov.uk/oicd/antiterrorism/index.htm>

customs and revenue officers from providing information to law enforcement agencies in their fight against terrorism and other crime. They also harmonise many existing gateways for the disclosure of information for criminal investigations and proceedings.

The Bill creates a new gateway giving HM Customs and Excise and the Inland Revenue a general power to disclose information held by them for law enforcement purposes and to the intelligence services in the defence of national security. This is urgently needed to ensure that known criminals are brought to justice. For example, the provisions of the Bill would allow for information on a suspected terrorist financier's bank account to be passed to the police.

When the Act was published these objectives were given force by sections 17 to 20. Section 17 allows any public authority to disclose information to other authorities that they hold, providing they think it is justified. This is not a blanket provision - it relates only to the information held under the laws specified in Schedule 4 of the Act. But given that there are 53 separate laws mentioned in Schedule 4, ranging from telecommunications law to the licensing of goods vehicles, the scope of information that may be freely traded between different agencies is very wide.

Information could be moved between government agencies prior to this Act. But there was a clear procedure, and each case was considered on its merits. Part 3 of the Act effectively deregulates the procedure to allow the reading of information without the same oversight.

Part 11, 'Retention of Communications Data' (sections 102 to 107)

In actuality, Part 11 of the Act is not part of a post-September 11th agenda. It tidies-up an oversight in the *Regulation of Investigatory Powers Act 2000* which required companies to give access to their communications data, but did not require the back storage of this information for convenient use by the state. It is also a significant part of the *Cybercrime Convention*¹⁴, which long before September 11th was setting up systems to allow not only the monitoring of communications data by the state, but also the disclosure of this data between states. In no way can the government claim that the significance of communications data has become important to the security agenda post-September 11th.

The Home Office's summary of the Bill, given to Parliament during the debate on the new law, stated in relation to Part 11:

Communications data has been central to the investigation into the terrorist attacks on 11 September. Part 11 contains provisions to allow communications service providers to retain data about their customers' communications for access by law enforcement agencies and for national security purposes and to enable a code of practice to be drawn up in consultation with industry.

The code of practice will allow communications service providers to retain data about their customers' communications for access by law enforcement agencies...

The Regulation of Investigatory Powers Act 2000 sets out clear limits on the purposes for which the law enforcement, security and intelligence agencies may request access to data relating to specific communications. Mass trawls or "fishing expeditions" are NOT permitted. The Bill allows for a voluntary code of practice to support this. It has a reserve power to review these arrangements and issue directions if necessary. Reserve power is reviewable every two years. If still needed, it must then be reviewed by an affirmative order. As soon as the power is exercised, there is no need for further review.

The collection and databasing of communications data is a very powerful intelligence tool. So long as the police or security services can collect the information, the systems already exist to store and match the

¹⁴Cybercrime Convention - <http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185&CM=1>

records to produce a highly detailed profile of a person's activities. However, there is no convincing body of evidence yet advanced to support the governments position that it will provide a qualitative improvement to law enforcement. In fact, the situation may arise where the 'presumption of innocence' in law is effectively abandoned as communications and other data is used to make the suspected offence match the evidence.

In many ways, we can compare the proposals on communications data to the proposals for closed-circuit television (CCTV) in the late 1980s. CCTV has had a debatable impact, in that it displaces rather than prevents crime, and has been responsible for some serious invasions of privacy due to the circulation or sale of tapes from CCTV operations. Likewise, the monitoring of communications data may result in those who deliberately wish to mask their communications finding technological means to avoid creating patterns - a good recent example being the means drug dealers have used recently to avoid detection using multiple, pre-paid mobile phones. Therefore, the only real targets of this legislation will be the public.

The issue that must be debated in relation to the use of communications data is not whether it is useful, but rather whether the databasing of all communications data, and its use potentially months or years after the events that created it, has an damaging impact on civil liberties. At the level of the single individual, communications data has specific meaning, and has limited application beyond the actions of the individual. But at the societal level, databases of communications data can be used to profile entire groups effortlessly by computer, and in turn this information could then be used to influence or harass those persons.

Part 13, 'Third pillar of the European Union' (sections 111/112)

The 'third pillar' of the EU is a new area of involvement where common issues involving domestic security are discussed at the European level. There are obvious benefits in working at the European level to tackle crime that is organised across the continent. But there are also dangers, in particular the differences of legal codes, and the interpretation of legal standards, between states.

The Home Office's summary of the Bill, given to Parliament during the debate on the new law, stated in relation to Part 13:

Measures on police and criminal judicial co-operation agreed by the JHA Council of the EU (third pillar) can currently only be implemented in the UK by primary legislation. This is time-consuming and does not allow the UK to respond promptly on an EU-wide basis to terrorist related measures. This clause would enable them to be implemented by secondary legislation, while still maintaining parliamentary control through the scrutiny process and through the affirmative resolution procedure that the secondary legislation would take. Measures agreed on European Community matters (for example the environment or the internal market) can already be implemented by secondary legislation.

The immediate impact of Part 13 will be enabling the introduction of new regulations governing 'Euro-warrants' - fast-track arrest and extradition warrants that will work between states within the European Union (EU). It means that new measures can be enacted via secondary legislation by the executive rather than having to be fully debated by the legislature. This has serious implications for civil rights. Unlike other areas of EU policy, such as trade or environmental standards, the deliberations of the EU on security and home affairs are not open to public scrutiny. At the same time the introduction of these measures by secondary legislation restricts the ability of law makers to scrutinise these measures at the national level too.

The Terrorism Acts and other related legislation

The Terrorism Act is not a stand-alone solution to the perceived problem of terrorists operating within society. Even before September 11th, the UK government had put into place a whole series of measures that sought to extend the rights of the state to monitor communications, and to investigate those who dissent from the policies of the state.

One of the new measures evolved during the 1990s was the principle of *common purpose*.

The *Security Services Act 1996*¹⁵ and the *Police Act 1997*¹⁶ made action by mass movements equivalent to that of serious criminals. The relevant clauses state that *conduct which constitutes one or more offences shall be regarded as serious crime* where it involves *conduct by a large number of persons in pursuit of a common purpose*. This may encompass traditional criminal activities, but it would also encompass the civil disobedience actions associated with social or environmental protests.

Under UK public order legislation, anyone intending to hold an assembly of twenty or more persons marching in a public place must notify the local police station seven days in advance before it can go ahead. A movement that held rallies without such notification would be liable to prosecution for an offence, and under the *common purpose* principle their activities could therefore be investigated as "serious crime".

Another significant change is the recent extension of surveillance laws under the *Regulation of Investigatory Powers (RIP) Act 2000*¹⁷. The RIP Act creates a legal framework for the use of surveillance and human operatives to monitor and infiltrate the activities of groups subject to "investigation". The RIP Act is directed towards those involved with "serious crime" and "terrorism". As noted above, in certain circumstances the activities of mass democratic movements can be classed as "serious crime". Under the Terrorism Act, the objective of "influencing government" could also class certain types of action, particularly where members of that movement engage in direct action, as terrorism. The terms of the RIP Act, therefore, bite both ways.

Redefining subversion and terrorism

The issue for civil society in the wake of the September 11th attacks is the ways in which definitions of terrorism and subversion are being widened to include social movements. The attacks on New York and Washington, and the subsequent bio-terrorism attacks on prominent US institutions, have led lawmakers to consider widening the definition of terrorism to something that may include single issue campaigns.

Previously, the activities of single issue groups were investigated within the bounds of ordinary criminal law. By redefining the activities of these groups, particularly those that target issues such as globalisation, anti-nuclear, animal experimentation or genetically modified crops, the state can devote extra resources to the investigation of such groups. It can do this with very little threat of legal action or disclosure, unlike ordinary criminal investigation, because of immunity granted it on the grounds of "national security".

In the USA, the FBI set out its position in relation to the definition of terrorism through a presentation to the Senate.¹⁸

¹⁵Section 2, *Security Services Act 1996* - <http://www.legislation.hmso.gov.uk/acts/acts1996/1996035.htm>

¹⁶Section 93, *Police Act 1997* - <http://www.legislation.hmso.gov.uk/acts/acts1997/1997050.htm>

¹⁷*The Regulation of Investigatory Powers Act (RIP) 2000* - <http://www.legislation.hmso.gov.uk/acts/acts2000/20000023.htm> See also the GreenNet CSIR Briefing No.3 on *Encryption and Electronic Signatures*, and No.13 on *Interception Capabilities*.

¹⁸Louis J. Freeh's statement to the US Senate - see reference 4 above

The FBI views domestic terrorism as the unlawful use, or threatened use, of violence by a group or individual that is based and operating entirely within the United States or its territories without foreign direction and which is committed against persons or property with the intent of intimidating or coercing a government or its population in furtherance of political or social objectives.

In relation to single-issue groups, it stated:

Special interest terrorism differs from traditional right-wing and left-wing terrorism in that extremist special interest groups seek to resolve specific issues, rather than effect more widespread political change. Special interest extremists continue to conduct acts of politically motivated violence to force segments of society, including, the general public, to change attitudes about issues considered important to their causes. These groups occupy the extreme fringes of animal rights, pro-life, environmental, anti-nuclear, and other political and social movements. Some special interest extremists - most notably within the animal rights and environmental movements - have turned increasingly toward vandalism and terrorist activity in attempts to further their causes.

Within this general description, the FBI still requires violence or property damage (albeit as undefined terms) to be part of the justification for taking action against a group.

Evidence of violence is not implicitly required in the UK, as noted in the guidance circular on the Terrorism Act 2000 issued to local authorities and police forces¹⁹:

The definition looks to cover acts that may not in themselves be violent but which nonetheless but have a significant impact on modern life...

Under the terms of the Terrorism Act, as we have seen, only the objective of *changing the mind of government* is required. This is a very broad definition. It strikes at the heart of one of the core principles within democratic society - that of freedom of expression. The Terrorism Act, and the explanatory circular quoted above, provides no clear guidance on what types of public expression are to be permitted - only on those which are to be investigated as demonstrating potentially "terrorist" intent.

Dealing with the new legislative framework

The Terrorism Act 2000 creates a new framework for dealing with terrorism in the UK. Its broader definition of terrorism will certainly cover various types of social and environmental protest.

It is likely that only a small number of campaign groups will be affected by the new Act (mostly those involving direct action for economic reasons, and in particular protests against animal industries and large multinational corporations). But the impact upon campaigns in general could be much wider, particularly if these actions prejudice public opinion, or intimidate members of the public from joining such campaigns.

The Act is likely to have a bigger effect on online action. This is because it defines the "disruption of networks" very vaguely. New laws relating to online actions criminalise many legitimate activities. The greatest impact of Terrorism Act may be to provide powers to investigate those working to develop campaigns opportunities via the Internet.

The chief concern is that certain types of protest will be targeted on the pretence of "terrorist investigations". If certain types of campaign groups are proscribed because of past actions, greater scope

¹⁹Home Office Circular 03/01 - *Terrorism Act 2000*. <http://www.homeoffice.gov.uk/circulars/2001/hoc0301.htm>

will exist for the state to associate others with the work of the more "extreme" groups.

Although this might not result in prosecutions, it could restrict the work of campaign groups; this may indeed be one of the objectives of this new legislation. For those who may be subject to this Act - which means anyone involved in direct action, or other types of physical or online protest - there is little opportunity for stopping the implementation of the Act.

The Act can now be challenged, however, on a case-by-case basis through:

- *Campaigners understanding the legal processes and their rights.* This includes not just the Act but also the codes of practice that accompany it.
- *Networking information on the Act.* Action in the UK has produced useful support for peace and roads protests that enabled those arrested to challenge their arrest and detention (compensation claims against the police forces involved for the wrongful use of relevant laws now run into millions of pounds). Similar work could be done on the Terrorism Act.

Challenging the use of the Act in the courts could be the best way forward. The lack of clear definitions within new laws, in the UK and elsewhere, open opportunities to refine their interpretation by bringing cases against the state. Only in this way, perhaps, can the most offensive parts of this new wave of legislation (in particular the extension of terrorism powers to civil society groups) be challenged and perhaps overturned.

At the global level, it is vital for everyone that the implications of proposals for new or amended anti-terrorist legislation are publicised and their impact monitored.

Further work

This briefing has been written in the context of the legal framework currently in force in the UK. If you live outside the UK you will need to make yourself aware of the procedures operating in your own country. Key points you will need to find out are:

- What steps has the state taken, following September 11th, to redefine "terrorism", and the type of action that may be investigated as terrorism?;
- How is it proposed to implement the Council of Europe's Cybercrime Convention? (if at all - not all states may ratify the Convention because of its civil liberties aspects);
- Has the state changed the controls over communications data, and more important will telecommunications or other service providers be required to store all communications data for a number of years to allow the detailed tracking of a suspect's actions?

You should also contact any civil liberties organisations operating in your country. They may be able to provide you with much of the information you need on laws relating to terrorism and protest action.

The GreenNet Internet Rights Project

GreenNet²⁰ is the UK member of the Association for Progressive Communications²¹ (APC), and is leading the European section of the APC's Civil Society Internet Rights Project²². The primary goal of this project is

²⁰GreenNet - <http://www.gn.apc.org/>

²¹APC - <http://www.apc.org/>

²²CSIR Project - <http://rights.apc.org/>

to provide the resources and tools necessary to defend and expand space and opportunities for social campaigning work on the Internet against the emerging threats to civil society's use of the 'Net. This involves developing ways and means of defending threatened material and campaigning, as well as lobbying to ensure a favourable legal situation for free expression on issues of public interest.

Until recently, the social norms of Internet communities, together with a very open architecture based on supporting these norms, regulated the Internet, and was responsible for its openness. The main forces of regulation now, however, are the business sector and government legislation. Corporations and governments are pressing for fundamental changes in legislation and in the architecture of the Internet. Unless challenged, these moves could radically change the nature of the 'Net, making it a place of oppressive controls instead of freedom and openness. It is in this context that APC's Internet Rights project is being developed.

This briefing is one in a series²³ that document different aspects of work and communication across the Internet. Although written from the perspective of the UK, much of its content is applicable to other parts of Europe. There is continuing work on these issues, as part of the European project. If you wish to know more about these briefings, or the European section of the APC Civil Society Internet Rights Project, you should contact GreenNet. You should also check the APC's web site to see if there is already a national APC member in your country who may be able to provide local help, or with whom you may be able to work to develop Internet rights resources for your own country.

Free Documentation License:

Copyright © 2001, 2002 GreenNet and Paul Mobbs. Further contributions and editing by Gill Roberts and Karen Banks. The project to develop this series of briefings was managed by GreenNet and funded by the Joseph Rowntree Charitable Trust. (<http://www.jrct.org.uk/>).

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.1 or any later version (see <http://www.gnu.org/copyleft/fdl.html> for a copy of the license).

Please note that the title of the briefing and the 'free documentation license' section are protected as 'invariant sections and should not be modified.

For more information about the Civil Society Internet Rights Project, or if you have questions about the briefings, contact ir@gn.apc.org.

²³<http://www.internetrights.org.uk/>