Cyber Terrorism – Electronic Activism and the Potential Threat to the United Kingdom

A.Wareham and S.M.Furnell

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

The recent rise of anti-terrorist action in response to deemed terrorist organisations has been a major international concern, prompting military action as well as domestic reforms by the United Kingdom since the attacks of 2001. In addition to the physical threat of terrorist activities, the utilisation of computer systems and services to promote a further threat has also become a point of significant interest. Dubbed 'Cyber terrorism' by government groups, media agencies and specialist software and hardware manufacturers the potential risk of 'e-activism' has seemingly increased, most notably of all due to widespread adoption of the Internet.

However, it is relevant to ask what we actually know about 'cyber terrorism', and whether it actually poses a realistic threat to the United Kingdom. This paper discusses the various aspects of activism online, utilising analysis of cited attacks to examine the methods and impact of direct pressure at both the corporate and national level.

Keywords

Electronic Activism, Cyber Terrorism, Terrorism, Activism, Hacktivism, UK Threats, Intimidation & Influence

1 Introduction

The issue of cyber terrorism has grown considerably in the public eye since the events of 9/11, the issue of security and the potential for the spread of Internet-based threats receiving further attention as the issue of 'home grown' activism continues in the current public media. The motivation of such threats is not purely limited to religious idealism; the considerations of moral, ethical and political standpoints have their own parts to play, with examples of such efforts giving rise to this current paper.

The presence of activism on the Internet is a problem that requires more than simply analysing the potential technical attack methods, with considerations on social factors, legal issues and present legislation, the current UK defence policy to electronic attack and numerous other factors. We shall briefly look at a few core areas in order to draw a more informed opinion.

2 The Reach of Electronic Activism

Since its inception, the Internet has been a natural conduit for the exchange of ideas, evolving from the early ARPANET into a global phenomenon. The widespread acceptance of the web into the public spectrum has created a universal resource for business, community support, education, finance and the handling of the affairs of government; a link to the outside world which is becoming increasingly important in everyday life.

So what does this essentially offer online groups who wish to promote themselves and their ideals, and who may find it difficult to do so due to the exposure of potentially illegitimate activities? The rise of 'public' Internet provides a number of opportunities for any group who wishes to centralise their activities online, both in terms of services and environment:

- *Operations Support* - The ability to build and maintain the necessary 'command network' from which to operate as a cohesive group, a consideration especially important when considering the large global geographical and transnational spread of potential large-scale efforts.

- *Anonymity* - The ability to "hide in the anonymity of cyberspace" (Jones, 2005), allowing potential planning, co-ordination and actions to be overlooked until the goal has been completed.

- *Personal 'Safety'* - The ability to use considerations of anonymity from which to operate, a potential benefit and incentive to less 'driven' orchestrating groups or lone individuals.

- *Publicity* - The ability to publicise objectives, viewpoints and motivations for the purpose of informing, persuading and the incitement of propaganda, coupled with the maintaining of a desired 'public image' to validate or support operations and ideals.

- *Financing* - The ability to maintain continued operations through continued financing, through both donations and the utilisation of legal or illegal credit transactions

2.1 The Community

The Internet has a substantial capacity to further and support community elements in commerce, entertainment and academia, with social networking sites and privately managed communities forming to focus on innumerable topics of interest. The majority of these groups offer a benign and harmless outlet for the free exchange of ideas. However, the online community can offer its own potential dangers, and the ways in which services can be utilised depend largely on the needs of the group in question. For many the ability to publicise information regarding their goals and

aspirations, if only in a few brief paragraphs, is a basic component of web presence; perhaps even their main or only point of contact with the 'outside world'. A further necessity for many established communities is a need to authenticate users in order to view more pertinent information of interest, commonly in the form of membership or some other standardised process so that access to key services can be achieved. The same considerations also are in existence when considering the issue of activism, the balance of organisation and co-ordination processes with the presentation of intended material for the general public, whilst ensuring that sensitive and potentially incriminating information is secured. The overall cost provisions in terms of infrastructure are for the most part negligible, with tools such as IRC, phpBB and instant messaging systems providing flexible and free options for communication. The introduction of secure data using such tools as PGP adds further credence to the management of 'closed' community environments, systems which can cause significant headaches for policing and the security services. As a case in point, in 2006 the Serious Organised Crimes Agency (SOCA) found itself essentially foiled by the use of encryption during the raid on an ID theft ring, the estimated time to break the encryption "taking 400 computers twelve years to complete" (Espiner, 2006).

2.2 Influence and Intimidation – the Power of 'Reality'

The ability to influence the viewing audience effectively is a significant issue when considering the nature of electronic activism. The ability to 'prove' or 'disprove' specific information, as well the legitimising of actions, provides activists a certain amount of validity to justify intent, such as the committing of actions that may otherwise be viewed to be entirely inappropriate in the public spectrum.

Influence Type	Approach	Influence Strategy
Propaganda	Wide-scale	Sociological principles reinforcing cultural or social values
Persuasion	"Personal"	Psychological principles and arguments

Table 1 : A table denoting the differences between the two primary classifications of influence (Hutchinson, 2007)

Hutchinson (2007) explains the basic considerations of *propaganda* and *persuasion* in the common presentation of ideas, the subtle difference between the two methods highlighted in Table 1. The processes of each are self evident in numerous online publications and on a range of media, with services such as *YouTube* providing an ideal host to portray supportive material to capture the global audience. The ability to create 'realities' through the submission of convincing and relevant material allows for the swaying of public opinion, enhanced further by the provision of community groups to strengthen given perceptions. Arguably this is not a new concept; indeed the reinforcement of values, ethical principles, ideology and given

arguments can be seen in virtually every current mainstream religion and Government across the globe. The main difference we can see when considering electronic activism is that the adoption of full media web services allows for the presentation of emotionally driven material that can both support activist efforts and separate the target from perceived legitimate protection.

2.3 Utilisation of electronic activism in offensive scenarios

The following is a brief review of two separate acts against corporate and national entities, in order to highlight the scope and capability of electronic activism.

2.3.1 National Considerations - The Estonian Dispute

An example that highlights the potential threat of a national attack is provided by events in April and May 2007, which demonstrated the potential impact of activism on a national scale. The relocation of a Soviet war memorial in the City of Tallinn sparked a high profile conflict with both the Russian Federation and ethnic Russians living within Estonia; the apparent catalyst for the later attacks on Government services and infrastructure. The attack sustained for a number of weeks, with Table 2 emphasising the range frequency of attacks committed during a monitored period.

Attacks	Destination	Address or owner	Website type
35	"195.80.105.107/32″	pol.ee	Estonian Police Website
7	"195.80.106.72/32″	www.riigikogu.ee	Parliament of Estonis website
36	"195.80.109.158/32″	www.riik.ee	Government Information website
		www.peaminister.ee	Estonian Prime Minister website
		www.valitsus.ee	Government Communication Office website
2	"195.80.124.53/32″	m53.envir.ee	Unknown/unavailable government website
2	"213.184.49.171/32″	www.sm.ee	Ministry of social affairs website
6	"213.184.49.194/32″	www.agri.ee	Ministry of agriculture website
4	"213.184.50.6/32″		Unknown/unavailable government website
35	"213.184.50.69/32″	www.fin.ee	Ministry of finance website
1	"62.65.192.24/32″		Unknown/unavailable government website

Table 2 : Figures highlighting a range of targeted websites over a captured period (Nazario, 2007)

The thought that Estonia is heavily dependent on the Internet to support government, civil and financial institutions is indeed concerning, considering that Estonians "pay taxes online, vote online, bank online (and that) their national ID cards contain electronic chips" (Applebaum, 2007). This means that an effective *Denial of Service*

attack increases in the potential effect on a target as the sophistication of the target increases (a concerning trend due to a similar embracing of technology in the UK).

The sheer fact that the Estonian government brought the issue before NATO as a legitimate attack on its sovereignty highlights the validity and seriousness of the incident, not merely as an annoyance but most certainly as a full blown attack in its own right. The response from NATO Secretary General was that of voiced condemnation over the incident (Estonian Government, 2007), although further action was not clearly identified.

2.3.2 Corporate Considerations - Huntingdon Life Sciences

Animal research and testing has long attracted the attention of animal rights activists on both a national and transnational level. One such group, the *Stop Huntingdon Animal Cruelty* activist group (Affiliated with the international group PETA), has been involved on numerous occasions with illegal activity, primarily in terms of physical actions such as the storming of target offices and direct intimidation methods of targeted personnel.

Analysis of legal case reports from March and May 2004 highlights a variety of offences against the HLS facility and its personnel, with the documents demonstrated a joint campaign of both physical and technical threats to continued operations. The usage of phone, fax and email blockades, the interruption of mobile phone services and the harassment of affiliates were identified as the primary forms of technical attack, and although extremely basic, these methods proved enough in conjunction with physical efforts to drive away a number of investors. Indeed, the intended "impacting (on) Huntingdon's bottom line" (QB, 2004) as voiced by one of the defendants was an important part of many of the highlighted public comments, with the viewpoint of potential prison sentencing being "a small price to pay". (QB, 2004). This highlights understandable concerns over legal steps when attempting to deal with persistent or repeat offenders, especially when considering that one of the defendants in the reviewed cases highlighted legal action as being "laughable because we will find a way around it" (QB, 2004).

3 Defending the Realm

The primary recourse against actions committed has been that of the law, specifically in the case of terrorism (and thereby potentially most applicable to defined activism) three laws in particular, namely the *Terrorism Act 2006*, the *Prevention of Terrorism Act 2006*, and the *Anti-Terrorism, Crime & Security Act 2001*. Table 3 highlights the powers that these deliver, with the Terrorism Act in particular referencing *Internet* activities. This is a significant tool when combating potential aggressive forms of electronic activism, referencing key issues that (especially in terms of the HLS example) can be applied to situations where a particularly aggressive threat may be present. Further to the list in the Table, the RIPA Act 2000 further requires the handover of all keys and information relating to encrypted data for investigation, with a potential prison sentence for up to 5 years should there be any issues of

National Security (Home Office, 2007). As highlighted by the example of encryption employed against SOCA investigations, this may not be a large enough incentive should the potentially discovered information lead to a greater sentence. However, this covering period provides a mechanism to legally charge and detain potentially disruptive or dangerous elements.

Act	Focus
Terrorism Act 2006	Designed to combat: • Planning of Terrorist Acts • Encouragement of Terrorism • Dissemination of Terrorist Publications • The Training of Terrorists
Prevention of Terrorism Act 2006	Designed to: • Impose sanctions on specific suspects including the introduction of control orders • *Note: carried out in accordance to the EHCR and authorised directly by the Home Secretary*
Anti-Terrorism, Crime & Security Act 2001	Designed: • Combat Terrorist funding operations • Extend police powers

Table 3 : An overview of key UK anti-terrorism laws

3.1 The Structure of National Defence

The overall defence of UK infrastructure and interests is largely under the jurisdiction of the Home Office, assisted by independent groups such as the Joint Intelligence Committee (JIC) in the development of a suitable overall strategy. This structure is illustrated in Figure 1.

The four core groups that deal with the main body of the UK infrastructure and assets (CSIA, 2007) are as follows:

- CESG: a cabinet body catering primarily to the advisory of government groups and departments,
- CSIA: an arm of GCHQ which primarily focuses on the protecting of national information systems,
- CPNI: an arm of MI5 which focuses on protecting the UK's infrastructure from Electronic Attack

- SOCA: a progression from the now defunct National High Tech Crime Unit which deals with primarily high level crime / high impact crime.

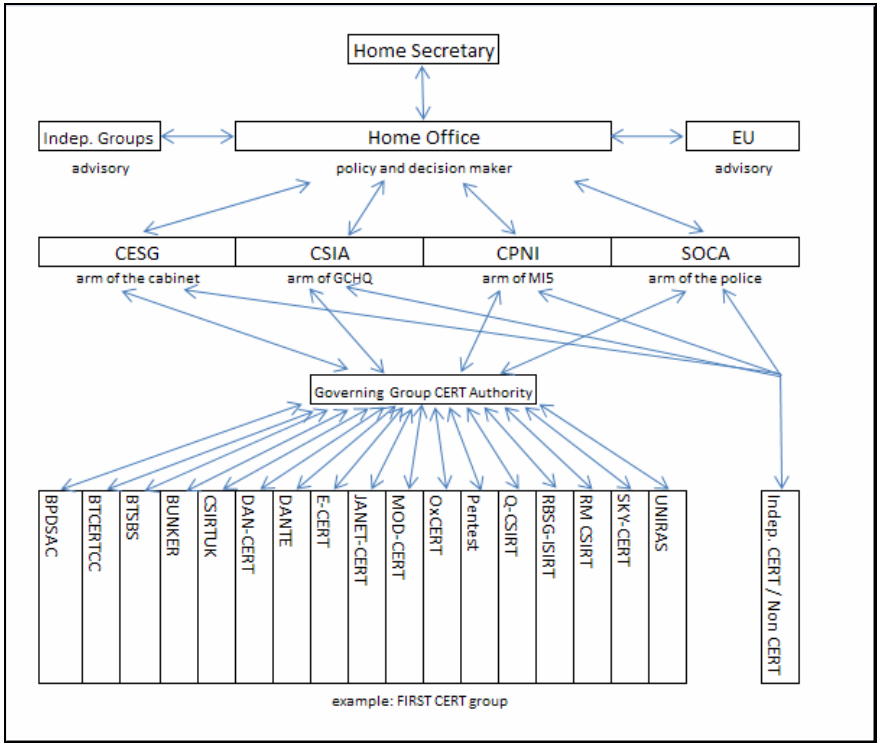

Figure 1 : A Basic Overview of UK Defence structure

These groups work together in order to protect against potential attack, as well as to ensure that information policy is maintained. Below these groups operate the various CERT and CSIRT teams that operate to protect key areas such as banks, infrastructure businesses, educational facilities or government concerns. These operate either independently or operate in mutually beneficial co-operative organisations such as FIRST. Overall this gives a reasonable level of infrastructural security, operating on a tiered basis in which each party can consult others for mutual support, development, education and protection whilst alleviating stress on Government groups.

4 Discussion and Conclusions

Overall, the considerations of activism highlight an embrace of basic attack methods in order to *deny* the target its communication capability, either in conjunction with defamation attacks as used in the Estonia, or by the usage of intimidation as prescribed by the events of the HLS case. The utilisation of electronic activism as a communication method provides opportunities for the conversion of others to a

similar way of thinking, facilitating both potential recruitment as well as an escalation of the impact of activities due to greater public support. The natural qualities of the Internet and the provision of free products and services mean that implementations for activist groups require little financial input, with the potential of utilising financial services such as *Paypal, Western Union* and even online virtual environments such as MMOGs (Massively Multiplayer Online Games) and *Second Life*. The nature and protection afforded by authenticated 'closed' community environments means penetration by law enforcement can be difficult, and even further impacted by the possibility of free encryption methods.

The more aggressive forms of activism could be charged under anti-terrorism laws, with national infrastructure measures in place to counteract any wide-scale attack. However, these methods are for the most part reactionary responses rather than proactive methods, essentially waiting for the activist to make the first move. We have identified that legal consequences may not be a silver bullet to activist attacks, especially when the attacker feels that they report to a 'higher authority' based upon moral, ethical or religious grounds. The issue is compounded when considering that the previous head of MI5 Dame Eliza Manningham-Buller highlighted the nature of the UK's proactive surveillance activities, citing a lack of manpower in relation to the threat (BBC, 2006). Following the bombings of 2005, the question over the sacrificing of certain civil liberties highlighted the difficulty in balancing measured security with effective security over the general 'terrorist' threat.

We have identified that, although technical methods have been provided for, the issue of human-orientated attacks are a far harder issue to combat. The problems of intimidation and threats, although far smaller in terms of the potential target radius, can negate common methods of protection. With the focus of the attack on the user, the threat of disseminating personal information to friends, family and business relations in order to invoke an emotional response is a common tactic; and one that was used against key directors and target business partners within the HLS example. With the impracticality of segregation and the screening of emails and similar forms of contact (one of the only real defences against the human side of activism), an effective solution would seem to require a blend of protective considerations:

- The implementation of an effective security policy for staff, assets and information systems at both a corporate and government level,

- The confirmed civil and government enforcement of contraventions regarding either security breaches or acts of an activist nature,

- The assigning of responsibility to service providers for the usage of the services they provide

One of the best potential solutions to the issue of electronic activism is the alerting of consciousness and the enabling of dis-inhibitors; key principles initially defined in a UK Home Office report on the future of net crimes. The ability to influence the general public that the *action* of vigilantism (even if justified by some moral, ethical

or religious concept) is wrong will potentially offer a solution, either by directly influencing the potential activist or by inciting peer pressure through others to search for a more peaceful solution to grievances. Although this is an unlikely solution outside of the UK bar that of a global initiative, such steps could help on a more local level though the pacification of UK activist groups.

It is perhaps unsurprising that utilising the same tactics that threaten national interests also seemingly offer a potential solution to future attacks.

5 References

Applebaum, A (2007), "For Estonia and NATO, A New Kind of War", *The Washington Post*, 22 May 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/05/21/AR2007052101436.html (accessed 28/07/2007)

BBC (2006), "MI5 tracking '30 UK terror plots'", BBC News online, 30 November 2006, http://news.bbc.co.uk/2/hi/uk_news/6134516.stm (accessed 19/07/2007)

CSIA (2007), "Key organisations", Central Sponsor for Information Assurance, Cabinet Office, http://www.cabinetoffice.gov.uk/csia/key_organisations (accessed 12/08/2007)

Espiner, T. (2006), "ID theft gang thwarts police with encryption", ZDNet News, 18 December 2006, http://news.zdnet.co.uk/security/0,1000000189,39285188,00.htm (accessed 17/10/2006)

Estonian Government (2007), "NATO Secretary General to the President of the Republic: the alliance supports Estonia", Government Communication Office Briefing Room. 3 May 2007. http://www.valitsus.ee/brf/?id=283225 (accessed 27/07/2007)

Home Office (2007), "Frequently Asked Questions", Regulation of Investigatory Powers Act, http://security.homeoffice.gov.uk/ripa/encryption/faqs/ (accessed 28/08/2007).

Hutchinson, W. (2007), "Using Digital Systems for Deception and Influence", in *Proceedings of the International Symposium on Human Aspects of Information Security & Assurance (HAISA 2007)*, Plymouth, UK, 10 July 2007, pp79-86.

Jones, A. (2005), "Cyber Terrorism: Fact or Fiction", *Computer Fraud and Security*, June 2005, pp4 – 7.

Nazario, J (2007), "Estonian DDoS Attacks: A summary to date", 17 May 2007, Arbor Networks, http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date (accessed 27/07/2007)

QB (2004), EWHC 493 *'Chiron Corpn Ltd and Others v Avery and Others'*, section 21