# THE EXTREMIST ISLAMIST PRESENCE IN CANADIAN WEBSPACE: AN EMPIRICAL STUDY

By

Neil Thomson, Ryerson University, October, 2006

Project Paper

presented to Ryerson University and York University

In partial fulfillment of the

Requirements for the degree of Master of Arts

In the Program of

Communication and Culture

Toronto, Ontario, Canada, 2006

## DECLARATIONS

I hereby declare that I am the sole author of this thesis or dissertation.
I authorize Ryerson University to lend this thesis or dissertation to other institutions or individuals for the purpose of scholarly research.

_____ (signature)

I further authorize Ryerson University to reproduce this thesis or dissertation by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

_____ (signature)

## ABSTRACT

The Extremist Islamist Presence in Canadian Webspace: An Empirical Study
Master of Arts, 2006
Neil Thomson, Communication and Culture,
Ryerson University and York University

This paper outlines the results of a two month study in which a series of extremist Islamist websites - registered, hosted or given datacentre services by Canadian internet companies - were empirically observed. The results of this project are inserted into a framework which explores the misuse and wrongful application of the 'terrorist' signifier to substate or nonstate activities, discerns between the purported use of the internet by extremist Islamist organizations for destructive means and the real use of the internet by such groups, and suggests a number of conclusions based on prior administrative responses to the extremist Islamist use of the internet. The full results of this project can be viewed at http://www.stormloader.com/members/nordicfury.

## ACKNOWLEDGEMENTS

I would like to thank my supervisor Greg Elmer, for the excellent feedback he was able to provide through our many, Friday afternoon group presentations. This went a long way toward helping me with the basis for this project. My secondary readers Amin Alhassan and Patricia Mazepa also provided extensive and much needed feedback on this project as well.

Olatokunbo Olaleye and Chris Cachia were instrumental in helping me get through this, even when I was close to abandoning the project entirely. And my mother, most of all, kept me afloat throughout this entire ordeal, despite all of my moaning and complaining.

## DEDICATIONS

This project is dedicated to my mother, Joanne, without whom I wouldn't even have been able to eat, and my sister Jane, who so often helped me revise and refine my writing style in the early part of my degree. This project is – most of all – dedicated to my father – gone but not forgotten, you always lift me out of desperation when I feel isolated and alone.

## LIST OF FIGURES

## LIST OF APPENDICES

# I. INTRODUCTION

The arrival of the 'information age' has witnessed a significant restructuring of control over the management of transnational information flows. Spurred on by the phenomenal proliferation of NICT's[1] at the close of the twentieth century and given wind by our progression into a global, networked economy in which some believe the primary resource will be information (Toffler, 1970, Nasbitt, 1982, Negroponte, 1995), a considerable redistribution of authority has seen non-traditional stakeholders - namely substate and non-state actors - rising to challenge the dominance previously enjoyed over the information environment by state and corporate actors (Leistyna, 2005). This challenge has resulted in the tipping of the "political balance away from the state and toward activists" (Perry & Sindayen, 2001), and has led some to posit the information environment as a primary site of struggle wherein state and non state actors will battle – ultimately - for control over the right to manage public perception of international events (Zanini, in Jones, 2004).

Foremost among transpirations impelling this struggle has been the establishment of the internet. Developed in 1969 as the ARPANET - a U.S. Department of Defense Advanced Research Projects Agency (ARPA) initiative - and formally opened to civilian and commercial interests in 1985, the internet first came into wide-scale use by the general public after the invention of the World Wide Web by Tim Berners-Lee in 1990 (Galloway, 2004, Naughton, 2002). "In less than ten years," the internet became "indispensable to many people in their daily lives" (Hoffman et al, 2004, p. 37) and is now viewed by some as a precondition for the functionality of affairs in the Western world. With a 2006 estimate putting the total number of world internet users at 694

[1] New Information and Communication Technologies

million – or 14 percent of the world's population (Australian, 2006, p.32) compared to 38 million at the end of 1994 (dns.net, 1998), the assertion that "the adoption rate of the Internet has exceeded that of earlier mass communication technologies by several magnitudes" (Hannemyr, 2003) finds little dispute, as does the inference that the global explosion in internet usage has allotted sections of the world's population greater leverage over local and international political processes.

Since its inception, the internet has provided a "global voice to radically excluded groups" (Dartnell, 2006, introduction) resulting in the dissemination of "information and culture that exists beyond the means of control of the dominant order" (Kahn and Kellner in Leistyna, 2005, p. 218). Instrumental in the development of new forms of resistance, the internet has become a means to empowerment for a plethora of organizations existing beneath or outside of the state, allowing subversive groups to challenge elite definitions of reality by gaining a greater control over their own message (Van de Donk et al, 2004).

In many ways, the internet can be thought of as essential to the pursuit of counter-hegemonic, information-related initiatives. Whereas the Mexican Zapatista movement of Southern Mexico and the Falun Gong organization in (and outside of) China have both made use of the internet to provide an information front to their respective struggles (Van de Donk et al, 2004), the Revolutionary Association of the Women of Afghanistan (RAWA) maintains an online presence to fight for human rights and social justice on the Central Asian continent. Environmental groups – such as Greenpeace - have generated websites seeking to bring public attention to issues such as toxic waste and genetically modified organisms, while activist groups such as those responsible for organizing the Seattle protests of 1999 have proven the internet to be a forum through which

communication, counter-information and organization are made possible (Van de Donk et al, 2004).

It is clear that the internet has become a significant vehicle for the facilitation of affirmative sub state and non-state activities. In its ability to provide publics and counter publics with a method for subverting official information channels, it has allowed dissenting groups to conduct "...discussion, interconnections and struggles on a global level in ways that challenge and often bypass both the nation-state and its creations" (Cleaver, 1997, n.p.) and has generated postulations that the internet may the first emancipatory, public sphere capable of giving rise to global, revolutionary activity (Van de Donk et al, 2004).

At the same time as facilitating the pursuit of positive activities by sub state and non-state actors – however - the internet also provides a voice for factions seeking different aims. The idea that "The activists one finds on the net are not all necessarily democratic in character..." (Van de Donk et al, 2004, foreword) underscores the reality that, just as the internet has become a platform for groups committed to emancipatory, or forward-looking ideals, it has also become a social space for those opposed to progressive initiatives.

As opposing assemblages "...characteristically see different possibilities in the usage of a given technology..." (Burnett and Marshall, 2003, p.127), the employment of the internet for "...both progressive and reactionary causes by an abundance of groups" (Kahn and Kellner in Leistyna, 2005, p. 218) is not surprising. With the websites of neo-Nazi groups, right-wing militias, religious fundamentalists and an assortment of other antagonistic groups found on the internet (Yagil, 2002), notions of the 'information

superhighway' as a space reserved for constructive activism are problematized – as opposed to a forum solely populated by left-leaning and populist ideals, the internet can instead be seen as multiplicitous, an environment marked by a host of noble – as well as condemnable - challenges to the official control of global information flows (Kahn and Kellner in Leistyna, 2005)

At present, perhaps the most significant of groups using the internet for aims not considered 'progressive' are those that can be classified under the rubric of 'extremist Islamism'. Regarded "by knowledgeable observers to have the largest presence on the web" (Swartz, 2005, p.03b) among subversive groups, the extremist Islamist internet population, in terms of websites "...has rocketed to 4,350 from a dozen in 1997" (Swartz, 2005, 03b). According to Gabriel Weimann, professor of communications at the University of Haifa in Israel, the extremist Islamist presence on the internet now makes up about 70 percent of the almost 4,700 extremist sites in operation worldwide (Weimann, 2006). Revelatory of the degree to which extremist Islamist groups are "...increasingly using the internet and websites to promote their causes" (Kahn and Kellner in Leistyna, 2005, p. 225), Weimann's postulation indicates a significantly higher rate of IT adoption among extremist Islamist organizations than other radicalist groups, and promotes an understanding of the fact that extremist Islamist organizations have successfully moved to cyberspace where they now have a platform from which to extend their reach transnationally.

## II. INTENT OF PAPER

What this paper intends to do is to elucidate the findings of a two-month research project in which a series of extremist Islamist websites – hosted, housed or registered by Canadian internet companies – were observed. The overall project – one intended to create a background understanding of the presence of extremist Islamist sites in Canadian webspace - will be fit into a framework intended to explore the extremist Islamist use of Canadian registrars, service providers or datacentres and the motives of Canadian state actors – the Federal Government, Canadian intelligence, law enforcement – in countering the use of Canadian webspace by extremist Islamist groups.

The choice to examine the extremist Islamist use of the world wide web as opposed to – for example – the use of the internet by white, ethnonationalist extremist groups or ecological extremist groups stems from a desire to document a contemporary and ill-understood phenomenon. Extremist Islamism, the current phase in what Walter Laquer defines as "The Age of Terrorism"[2], is a widely discussed topic about which many misconceptions exist, just as the extremist Islamist use of the internet is an emerging area of investigation prone to erroneous beliefs. A study of how extremist Islamist groups are employing the services of Canadian ISP's is not only warranted because of its potential to grant insight into a current trend, but even more so because of its ability to provide – for academics, researchers and students – an exploration of how cyberspace is becoming a forum for collectivity and dissent, just as it evolves into an arena of surveillance and policing.

[2] The 'Age of Terrorism' signifies the different phases – throughout the 19th century to the present – in which specific extremist groups have been sensationalized by governments and the media for the purpose of galvanizing public condemnation and indignancy (Laquer, 1977).

This initiative will begin with a short explanation of the terminology to be used in this report as well as the rationale behind the use of the chosen terminology. Following this section, this paper will then delve into the question of "what is terrorism", explaining who defines terrorism, what the term is used for and finally, why the term must be abandoned in light of its overbroad and problematic nature. An exploration of the extremist Islamist use of the web – both fictional and factual - will then be undertaken. This will provide a contrast between the portrayal, by state and corporate actors, of 'cyber-terrorism' as the dominant agenda behind the extremist Islamist use of cyberspace, versus some of the ways in which extremist Islamist groups actually use the internet. Finally, the project itself will be detailed in terms of its intent, methods, results and implications. The paper will end with an investigation into the final results of the project, and the extremist Islamist use of Canadian webspace and the administrative response to it will be placed into context.

At the conclusion of this paper, I hope to provide – for the reader – not only an awareness of which extremist Islamist websites are being hosted by Canadian internet companies and why. As this report adjourns, I also intended to infer that new laws and policies toward existing technologies in Canada – while supposedly being implemented, in part, to track extremist Islamist activities on the web – are actually being used for other purposes, most significantly, the attempt to place a stranglehold over the online environment. The extremist Islamist employment of Canadian internet companies and the resultant attack on internet freedoms by the Canadian security establishment – it will be concluded – can be viewed in the context of an asymmetric struggle for control over

the internet itself, the outcome of which may define the very future of the Canadian online world.

## III. TERMINOLOGY TO APPEAR IN THIS REPORT

Prior to any exploration of a topic as contentious as international extremist activity, one's choice of terminology must be based on cautious deliberation and selective interpretation. The following section – intended to detail terms to be used in this report, will elucidate the definitions of specific terms. As well, explanations will be provided as to the choice of particular idioms.

This list is not to be considered all inclusive – the likelihood is present that certain terms, while self-evident to many readers, will not appear as such to others. As well, certain terms will be left out for the reason that their explanation will be considered unnecessary.

In this report, the term *extremist Islamist* will be used to indicate those groups who hold Islam as a political system as well as a religion, who seek to remodel state governance based on a strict interpretation of Sharia law, and whose advocacy for direct, militant action against perceived 'anti-Islamic' forces puts them at odds with the hegemonic powers of the Western world as well as the mainstream of their own faith.

The first part of this term, the word 'extremist', will be employed – in the context of this report – to describe subversive, Islamist groups which espouse extremist viewpoints and which may or may not endorse specific acts of violence. The word 'Islamist' will be used with the understanding that Islamism is a "...political ideology rooted in interpretations of Islam" (Nassar, 2004, p. 87) and does not represent the mode of thinking of the majority of the world's Muslims. It is hoped that the use of the 'extremist Islamist' marker – in this report - will draw a separation between the Islamic

faith and Islamist militancy, with the result that the reader will be able to discern between a religion of millions and the actions of a few.

The term *Canadian webspace* will be employed in this report to connote any Canadian service provider, datacenter or registrar providing – knowingly or unknowingly – services to extremist Islamist groups. In the context of this paper, a necessary separation will be drawn between *registrars, service providers and datacentres*, noting that each of these terms indicates a different type of service being rendered to a specific client. The term *Canadian Internet Companies* will similarly be used in this report to describe those ISP's (internet service providers) in Canada allotting expertise or services to extremist Islamist groups.

In this paper, the term *Registrar* will be used to indicate an internet company providing a registration service – that is, registering the domain name (such as www.khilafah.net) - of a client for a fee.

The term *Service Provider* will connote any internet company hosting a client's website on their servers.

The term *Datacentre* will be employed to describe a company housing a large amount of data on multiple servers, including – but not limited to – websites and online software programs.

The term *Cyber-terrorism* appears in this paper solely on the basis of describing how online 'terrorism' has been traditionally conceived of. 'Cyber-terrorism', which indicates the malicious use of the world-wide web to disrupt or attack essential services or critical infrastructure (Yagil, 2002), will be used to provide a backdrop for a discussion

on the true use of the web by extremist Islamist groups, and will be used only to note incorrect conceptions of online extremism.

Finally, in this report, the term *Terrorism* or any of its variants will only appear in single quotation marks. This is partially because – as will be detailed later – terrorism is a problematic, floating signifier, a term too overbroad and general to be of any real use in the elucidation of extremist thought and action. The term 'terrorist' will only be used in the context of citing the quotations of other authors, and will not appear in this report as a significant marker in my descriptive lexicon.

It is hoped that – with these terms having been extrapolated from the outset – the reader of this report will be able to better navigate through this paper with a minimal level of confusion. It is also hoped that the potentially contentious nature of this project will be mitigated through an understanding that the terms chosen herein are meant to be sensitive to the beliefs of academics, social activists, and most of all, Muslims worldwide. It is my expectation that highly loaded and disputed terms can be kept to a minimum, or at the very least, put into context, so that an objective and unbiased look at both the extremist Islamist use of Canadian webspace as well as the administrative response to it can be undertaken.

## IV. WHAT CONSTITUTES AN 'EXTREMIST ISLAMIST WEBSITE'?

The question of what constitutes an 'extremist Islamist website' is one that needs to be addressed – at this point - not solely on the basis of the perception that such sites are a recent addition to the internet landscape (Weimann, 2006), but also because of the fact that no concrete attempts have been made, to my knowledge, to elucidate the definition of an 'extremist Islamist website' to date. As the study of Islamist activity vis-à-vis the internet is itself a new field of enquiry, the lack of an attempt to define what constitutes and extremist Islamist website – in literary circles – is not unexpected. With this notion in mind, I will offer the following, working definition.

For the purpose of this essay, an extremist Islamist website will be defined as a communication module through which extremist Islamist groups can broadcast, network, recruit and plan, and which allows such groups to create an idealized, virtual space for members and supporters. The designation of a website as extremist Islamist will be based on the following criteria:

- Its affiliation with a group federally designated as 'extremist' under Canadian law
- Its intent being that of a propaganda - as opposed to a news - conduit
- Its content being decidedly slanted in favour of the extremist Islamist perspective

The idea of classifying certain sites into the category of 'extremist Islamist' is problematic, partially because categorization is largely contingent on one making a value judgement about what constitutes an 'extremist Islamist website'. Even more problematically, the grouping of a series of websites under the 'extremist Islamist' label could be viewed as beneficial to state and corporate actors wishing to recreate a power structure over the internet similar to that which exists in real life. In this sense, the idea of providing a concrete definition of an 'extremist Islamist website' is complicated,

although for the purpose of this paper it is the term must be provisionally defined in order to avoid confusion, and in hopes of providing future researchers with a platform on which to eventually reach some kind of a consensus as to the fundamentals which constitute the term.

## V. WHAT IS 'TERRORISM'

### A. Definitional Struggles

The term 'terrorism' has long been considered "...an extremely difficult concept to define" (Mullins, 1997, p.11). Owing to capricious treatments of the descriptor, a precise explication of what constitutes the 'terrorism' signifier has never been solidified. There is no universally agreed-upon definition of the term (Weimann and Wynn, 1994). According to Nacos (2006), the definition of terrorism has been applied (by governments, security forces, academics and researchers) so inconsistently that its precise delineation – even among governmental departments - varies to the point of incongruity. Terrorism – it can be stated - is a floating signifier of the highest severity, its meaning dependent upon "...who you are and why you are bothering to define it" (Tuman, 2003, p. 11), its use rooted in selective interpretations of what constitutes 'a terrorist act'.

### B. History

The term "Terrorist" first appears in the English lexicon at the end of the eighteenth century in revolutionary France (Weinberg, 2005). The architects of the execution of Louis XVI and the subsequent Jacobin 'reign of terror' (1793-1794) are described by the English author Edmund Burke as 'thousands of those hell hounds called terrorist', unleashed upon the people of France (Laquer, 1977). At the end of the nineteenth century, the term 'terrorism' is widely used again, this time by European and American heads of state in describing the actions of revolutionary anarchists purportedly linked to a vast, worldwide, anti-state conspiracy (Tuman, 2003). In Russia, the Narodnaya Volya (1878-1881) revolutionary group - credited with the assassination of Tsar Alexander II – earns the 'terrorist' label (Thackrah, 1987). And in the twentieth

century, groups with aims ranging from the struggle for working class rights to socialist revolutionaries to right-wing paramilitaries are all grouped – at one time or other – under the rubric of 'terrorism'.

## C. Use and Misuse of the term 'Terrorism'

At present – there are postulations that the signifier of 'terrorism' can be applied to almost any political, religious or ideologically motivated undertaking (Conway, 2002). The notion that the term "...has been used in so many different senses as to become almost meaningless, covering almost any, and not necessarily political, act of violence..." (Laquer, 1977, p.11) underscores recognition – by many academics – that the 'terrorist' label is a blanket term used to generalize the activities of a vast number of substate and non state actors, and not a specific marker useful in elucidating the actions of any specific group. 'Terrorism' is viewed – among prominent authors, scholars and academics - as a value-laden generalization, its meaningful use negated by its inherent abuse at the hands of those in positions of authority.

Paradoxically, those who most frequently abuse the term 'terrorism' are those who are most likely to provide definitions for it (Laquer, 1977). Government officials, who are "...in more advantageous position than other political actors to confer the 't' word on groups or withhold it..." (Nacos, 2006, p. 19), create working definitions of terrorism as much for their own internal communications as to provide a platform on which to confer disadvantage onto societally undesirable elements. Consider some of the following definitions of 'terrorism', provided by the Canadian legal and security establishments:

The Canadian criminal code defines terrorism as an action that is:

> "taken for political, religious or ideological purposes and intimidates the public concerning its security, or compels a government to do something, by intentionally killing, seriously harming or endangering a person, causing substantial property damage that is likely to seriously harm people or by seriously interfering with or disrupting an essential service, facility or system."
>
> (canada.justice.gc.ca, 2001)

Under this definition of 'terrorism', the act of 'terror' is committed – on ideological, political or religious grounds - to intimidate the public or to force the hand of the government by causing serious harm to persons or property. This definition – although assumedly intended to criminalize acts of violence and destruction - remains vague enough in its wording so as to apply to lawful acts such as strikes and labour protests.

CSIS, the Canadian Security and Intelligence Service, meanwhile, defines 'terrorism' as:

> "activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state"
>
> (csis.gc.ca, 1985)

This definition moves beyond intimidation and violence to include those who support the threat of violence, against both persons or property. This definition also recognizes the transnational nature of 'terror' as it defines, as an act of 'terrorism', any international undertaking of opportunistic violence against Canadian interests. Under this definition of 'terrorism', actions not in favour of Canada within a foreign state – including the support of those who speak out against Canadian interests – could conceivably be considered an act of terrorism. Again, the vague wording of this definition broadens its scope to cover a wider range of people than those whom one would normally consider 'terrorists'.

It is clear that the 'terrorism' signifier allows governments to label certain sub state or non state actors 'subversives', in the process demonizing undesirable groups and publics. More importantly - however – is the notion that the lack of a universal definition for the term 'terrorism' allows states to apply the 'terrorist' label while refuting charges that the activities they themselves engage in are 'terrorist' in nature (Hartman, 2002). Just as states define 'terrorism' to distinguish between illegitimate violence and dissent practiced by those who oppose the state from their own "legitimate" form of violence (Olivero, 1998), states also refuse to accede to internationally agreed-upon consensuses on what defines 'terror' in order to abrogate accountability for the commission of what could be termed 'acts of state terrorism' (Conway, 2002). In their paradoxical use of the terrorism signifier, states take a contradictory stance regarding 'terrorist' activity, and in doing so, lead to accusations that the real goal – in defining 'terrorism' – is not really to fight 'terror', but to create a convenient label with which to offload responsibility for the majority of the world's violent activities on to a subordinate group (Hartman, 2002).

The term 'terrorism' – as a value laden concept without any real academic merit – is thus at best a general label used to encompass a wide range of political, religious or ideologically motivated activities and at worst a net ensnaring a variety of subversive as well as lawful, civil groups in its grasp. In its vague and overbroad nature, 'terrorism' is little more than "...a semantic technique employed by government spokespersons to change the subject, a slick way of transforming the victims of injustice into its perpetrators" (Weinberg, 2005, p. 1). In this sense, the transposition of the 'terrorist' label is less about separating lawful groups from unlawful groups, and more about ostracizing certain, sub state actors from the state itself.

## D. Conclusions

It is partially because of the ambiguities associated with the term 'terrorism' that the application of this title to specific political, religious or ideologically motivated actions should be done cautiously in academia. Absent a clearly delineated, international consensus of what defines 'terrorism', the risk remains that the 'terrorist' label could be applied to indigenous guerrilla operations, movements for national liberation, foreign actions against despotic governments or even legal strikes at home (Conway, 2002). The independent use of the term 'terrorism' – in any serious academic study - should be based on a working definition informed by an examination of a multitude of existing definitions, and should be achieved through a precise and clear wording intended to create a minimal level of uncertainty as to who the intended target of the particular definition is.

Furthermore, when applying the 'terrorist' label in any serious examination of sub state or non-state activity, one must be made aware that many scholars ultimately view 'terrorism' "...as a political label rather than a meaningful research concept" (Nassar, 2004, p.17) and that the term operates in domain which exists outside of the realm of legitimate academic study. Because 'terrorism' is a descriptor which so frequently works to the advantage of state actors - a signifier commonly employed to castigate certain sub state and non state groups for violent activities while exonerating the state from blame for similar deeds – its applicability to rational, academic discourse is questionable at best and it should therefore be used only in the context of the work of others.

Taking into account pointed criticisms of the terrorism marker, traditional struggles in defining the term, its ambiguities and its abuse at the hands of authorities, it

should be clearly understood why this report refuses to use the term 'terrorism' on its own to connote any form of sub state or non state militant activity. Subjective and loaded, the 'terrorism' marker is not only contentious, but hazardous - when used improperly, the term can lead to damaging criticism from well established experts in the 'terrorism' field[3], and – in my opinion - can ultimately discredit any academic study hoping to make a serious examination of the extremist Islamist phenomenon.

[3] One must be selective when considering experts in the 'terrorism' or 'terrorology' field. This field has been criticized on the basis that – although it has been marked by the work of informed and noted scholars such as Walter Laqueur – it has also seen works by administratively inclined authors such as Benjamin Netanyahu. See - http://www.nuclearspin.org/index.php/Terrorology_and_political_violence.

## VI. CYBERTERRORISM – FACT AND FANTASY

### A. Introduction

Defined by Denning (2000) as "the convergence of terrorism and cyberspace" (n.p.), the term 'Cyberterrorism' represents the idea that extremist groups will leverage computer and information systems in order to provide a substantial attack on data networks, critical infrastructure and essential services (O'Day, 2004). Born out uncertainties brought on by the networking of transportation systems, public utilities, homes, businesses and educational institutions (Embar-Seddon, 2002), the 'cyberterrorist' concept presupposes the existence of groups or individuals whose proficiency with computer technologies will be coupled with a violent, political agenda to create a cyber nightmare (Lezner and Vardi, 2004) for Western institutions and citizens. In its suppositions of a world imperilled by vulnerable infrastructure, unchecked information systems and technologically adept insurgents, the idea of 'cyberterrorism' is both a potent propagandist vision as well a symbol of traditional, Western suspicions of the power afforded to subversive groups – especially extremist Islamist organizations - by new technologies (Ehrlich and Dworzecka, 1998).

### B. History

Coined in the 1980s by Barry Collin, senior research fellow at the Institute for Security and Intelligence in California (Conway, 2002), the 'cyberterrorism' moniker first enters the public consciousness via depictions in popular culture. Formed in the wake of early 'hacking' incidents – the discovery of 'phone phreaking' in the 1960's[4], the

[4] 'Phone phreaking' refers to a subculture of people who – in the late 1960's – experimented with various methods of placing free, long distance phone calls

intrusion into the AT&T mainframe systems in 1981[5], the arrest of 'computer outlaw' Kevin Mitnick[6] - acclaimed films "War Games" (1983) and "Sneakers" (1992), William Gibson's novel "Neuromancer" (1984) and the television series Max Headroom (1987) all forward visions of a future in which information technology systems are employed for malicious or subversive ends. Images of 'hacking' and cyber-crime become prevalent through depictions in film, television and popular literature, just as the notion of 'cyberterrorism' is fermented in the imagination of the public. In the 1982 film 'Tron', a powerful super computer remarks "Do you have any idea how many outside systems I've gone into? I was planning to hit the Pentagon next week." (Disney, 1982).

The entry of the 'cyberterrorism' concept into mainstream thought soon follows. In 1991, contemporaneous to writer Winn Schwartu describing the prospect of an "electronic pearl harbour" arising from the malicious use of information technology (Schwartu, 1991), a report produced by the National Research Council entitled *Computers at Risk* states, "The modern thief can steal more with a computer than a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than a bomb." (National Research Council, 1991, p.7). 'Cyberterrorism', allegedly made possible through the linking of computer systems to the world-wide-web, suddenly emerges as a threat on the agendas of national governments, security agencies, federal think tanks and computer experts (Conway, 2002). With journalists labelling the perceived risk from malicious hackers a 'Cyber-war' (Hoffman, 1999, p.C1) or 'Existential Terrorism' (Becher, n.d.), and the alleged campaign to attack targets in and through cyberspace

[5] Ian Murphy was convicted in 1981 of hacking into AT&T's mainframe computer system and changing internal clocks (Delio, 2001).

[6] For information on the pursuit and eventual arrest of Kevin Mitnick, see Tsutomu Shimomura's 1996 book *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw-By the Man Who Did It* (New York: Hyperion Books).

being called a 'Cyber Jihad' (Bunt, 2003), the Washington-based Centre for Strategic and International studies raises the spectre that 'cyberterrorism' could be exceptionally devastating for the Western world, stating - in a 1998 report - that the threat from cyberterrorism represents no less than "a Digital Waterloo" (Centre for Strategic and International Studies, 1998).

## C. Government and Media Depictions of Cyberterrorism

At present, 'cyberterrorism' is portrayed – by national governments - as "the darkest downside of the information revolution" (Arquilla, Ronfeldt and Zanini, 2000, p.179). Where state actors infer that "...the number of actors with the ability to utilize computers for illegal, harmful and possibly devastating purposes is on the rise" (fbi.gov, 2004, n.p.), and it is declared inevitable that malicious sub state and non state actors – namely extremist Islamist groups - will employ the internet as an offensive weapon (Zanini in Jones, 2004) the idea is surreptitiously pushed that networked attacks on Western infrastructure, services and information systems are imminent. The claim that "It is only a matter of time before there is a convergence between those with hostile intent and techno-savvy..." (gwu.edu, 2000) underscores a mode thinking which suggests the necessity of preparing for a "...true cyber attack on information systems by terrorists" (Vatis in Kirkland, 2002, n.p.).

Inferences that new modes of assault will be opened up to sub state and non state actors simultaneous with the advent of new technologies (csis.gc.ca/en/publications/perspectives/200111.asp, 2002) are essential to lawmakers and national security agencies. Employing such inferences, state actors posit the potential of damaging 'cyber-attacks', instil – in public thought - the idea that subversive groups

gravitating toward new technologies will utilize such technologies solely for disruptive, destructive or deadly means, and facilitate the eventual movement toward a greater amount of administrative control over the online environment.

Following the lead of national governments, major media outlets also advance notions that attacks on major facets of the industrialized world via the internet are an inherent possibility. Driven by a concentrated sphere of corporate ownership closely aligned with elite interests (Herman and Chomsky, 1988), many media outlets reflect governmental views on the idea of 'cyberterrorism', inferring to mass audiences that "disruptive computer attacks that could result in injuries or deaths are no longer a matter of conjecture" (Wallace, 2001, p.3A). The idea that "The unimaginable is looking ever more plausible" (Lezner and Vardi, 2004, p.70) is indicative of the way in which elements of the media view the 'looming threat' of 'cyberterrorism'. Cyber attacks are broadcast by the media as an inescapable reality, a phenomenon guaranteed to "strike at the heart of any Western economy" (Ellsmore, 2002).

State and corporate actors heavily emphasize the possibility of 'cyberterrorist' attacks, in the process parlaying a vision of an information technology future dominated by increasing assaults on critical infrastructure, essential services and the internet itself. Seeking to shape public perception of the threat level represented by 'cyberterrorism', state and corporate actors suggest that it is necessary to expect – given the history of the malicious use of information technology[7] – that sub state and non state actors will make use of information technology in the future to inflict damage, financial ruin and significant casualties on sections of the industrialized world (Weimann, 2006).

[7] Vegh (2002) has suggested that computer hacking – which has a relatively benign but fairly lengthy history - has been historically viewed as inseparable, in many government and security circles (such as the American NSA) from cyberterrorism.

## D. Reality of Cyberterrorism Threat

In their strong emphasis of the 'cyberterrorist' threat, state and corporate actors not only create currents of disinformation which blur the distinction between 'cyberterrorism' and other forms of networked activity – such as 'hacktivism'[8] (Vegh, 2002), but also problematize the public's understanding of the extent to which 'cyberterrorism' actually affects daily life[9] (Lia, 2005). With the reality present that a major act of 'cyberterrorism' has yet to happen (Conway, 2002), and the claim that cyberterrorist incidents currently hover at zero per annum (Poulsen, 2001), postulations of cyberterrorism as an endangerment to the functionality of Western life begin to appear questionable and unconvincing.

Some have inferred that the alleged threat posed by 'cyberterrorism' may be significantly less than what state and corporate discourse on the matter would suggest. While Lia (2005) posits the unlikelihood of substate and nonstate actors attacking infrastructural targets through cyberspace, Jones (2005) forwards the idea that "Mounting an attack against computers systems is beyond the skills of terrorists" (p.5). Journalist Lee Gomes sees 'cyberterrorism' as "More marketing ploy than a real threat" (2001, p. B1). And Dorothy Denning, professor in the Department of Defense Analysis at the Naval Postgraduate School in Monterey, California, intimates that "Not only does cyberterrorism not rank alongside chemical, biological, or nuclear weapons, but it is not anywhere near as serious as other potential physical threats like car bombs or suicide bombers." (in Green, 2002, p.9).

---

[8] Hacktivism can be thought of as the confluence of 'hacking' and activism or 'hacking' for political means. See http://thehacktivist.com/hacktivism.php.

[9] A 2001 study found that 75 percent of Internet users worldwide believed 'cyberterrorists' would soon "...inflict massive casualties on innocent lives by attacking corporate and governmental computer networks" (Poulsen, 2001, n.p.).

Countering dominant assertions about 'cyberterrorism' by the majority of state and corporate actors, many view the phenomenon as an "unlikely threat" (Lewis in Clarke, 2004, p.148) to the physical world. Richard Clarke, former Cyber-security advisory to U.S. President George Bush, admits, in 2002, "...we have not seen the traditional terrorist groups using cyberspace for malicious, offensive activity" (Mogull, 2002), indicating a growing wariness of the concept's usage even among some administrative interests.

As opposed to an imminent threat to Western infrastructure, services and citizens, 'cyberterrorism' would be better thought of as an "alarmist vision... useful in order to mobilize public opinion and political will" (Lia, 2005, p. 174). An as-of-yet unrealized fear propagated by federal governments and the media, the spectre of "cyberterrorism" instils apperceptions of imminent 'cyberattacks' in the minds of global publics (Poulsen, 2001) and leads to the conception of scenarios in which infrastructural damage, internet failures and wide scale loss of life all figure prominently. This has the effect of leading to surreptitious calls for a higher level of online policing and – as will be detailed later – aids in "preparing the ground for an attempt a at bureaucratic empire-building via internet regulation" (Conway in Clarke, 2004. p. 181).

State and corporate actors – in their exploitation of the 'cyberterrorism' phenomenon - not only infer that new technologies can only be used for disruptive or destructive means by militant sub state groups, but mask an understanding of the true use that extremist groups make of the internet every day (Weimann, 2006). As the following section will demonstrate, far from utilizing information technologies for disruptive or destructive means, extremist Islamist groups are making use of the internet in innovative

and self-beneficial ways, in the process creating an environment which eschews the idea of "cyberterrorism" and leads us to believe that an active, IT infrastructure is much more beneficial to extremist Islamist groups than a one destroyed by incessant 'cyber-attacks'.

## VII. The Extremist Islamist use of the Internet

### A. Introduction

An understanding of the degree to which extremist Islamist organizations have become "technologically sophisticated" (Walters, 2005, p.11) presently permeates discourse on the subject of 'technology and extremism' (Clarke, 2004). Formed partially as a reaction to the perception – by state and corporate actors – of extremist Islamist groups as "...backward looking... anti-science and anti-technology" (Tremayne, 2006, p.1), this new recognition of extremist Islamist technological proficiency sees journalists, academics and administrative interests coming to accept that extremist Islamist groups have become "adept at using modern technology for their own ends" (http://www.nato.int/docu/review/2004/issue3/english/military.html). The understanding of extremist Islamist groups as amicable to new technologies posits the ability of these collectives to adapt to new innovations such as cell phones, laptop computers and digital video cameras (Clarke, 2004) and recognizes "a decidedly unprimitive" (Booth and Dunne, 2002, p. 298) use of technologies by such groups. Popular perceptions of Osama Bin Laden carrying around a satellite phone with which to facilitate intra-organization communications are significant – the penetration of this media-reinforced image into the public imagination demonstrates a growing recognition of the link between extremist Islamist organizations and advanced technologies.

As journalists, academics and administrative interests build an understanding of the significance of new innovations to extremist Islamist groups, a parallel understanding of how the internet has become a technology of paramount importance to such organizations is formed. Said to be initially seen – by extremist Islamist groups such as

Hamas and Hizballah – as offering a "level playing field" with the West (Nacos, 2006, p.228), the internet is employed by such organizations prior the awareness of the international community (Gunaratna 2003, p.103). Moving "from physical space to cyberspace" (Coll and Glasser, 2005, A01), extremist Islamist organizations migrate to the net in significant numbers – by 2000, virtually all extremist Islamist groups have "established their presence on the internet" (Weimann, 2004, p.2). Extremist Islamist organizations begin to leverage the internet "for perception management and propaganda" (Zanini in Jones, 2004, p.167), and in the process prove the internet to be a tool through which previously unrealized goals – namely the transnational extension of their reach – can be met (Weimann, 2006).

## B. Decentralization

At present, the internet is seen as attractive to extremist Islamist groups primarily due to its decentralized nature (Galloway, 2004). A network made up of interconnected computer networks, lacking a central administration and based on the omni-directional - as opposed to vertical - movement of data (Preston, 2004), the internet allows extremist Islamist groups to share information in methods which bypasses state and corporate control (Arquilla, Ronfeldt and Zanini, 2000). As many extremist Islamist organizations have adopted the 'leaderless resistance' principle in which small cells lacking a central command conduct operations independent of each other (Weimann, 2006), the internet provides a unifying structure which permits cells of such organizations to communicate, network and organize while remaining fluid and independent (Arquilla, Ronfeldt and Zanini, 2000). Preparations for the September 11th hijackings, in which a series of independent agents "used the internet and used it well" (Dick in Conway, 2002) to

communicate, organize and plan for a series of large-scale attacks, are indicative of the extent to which the internet allows decentralized organizations to function in a networked manner.

The internet has changed extremist Islamist networks "from those of strong, central control to ones with no clear centre of control" (Jones, 2004, p. 141). It has allowed for the decentralization of extremist Islamist operations, and in the process has led such groups to become more fluid and independent. The "network of networks" has been beneficial in other ways to such groups, however. In order to better grasp the ways in which extremist Islamist organizations profit from the internet, the following exploration will examine some of the most significant areas of extremist Islamist internet usage.

## C. Communication and Organization

Extremist Islamist organizations – first and foremost – make use of the internet "as a tool for intra-group communications" (Lewis in Clarke, 2004, p.148). Operating independently of one another, often over long distances and across remote terrain (Gunaratna, 2002), extremist Islamist groups use the internet to share "complex information ... over a geographically dispersed area" (Anderson in Clarke, 2004, p.158) and to provide a high level of intra-organizational contact. Utilizing the internet, Extremist Islamist organizations benefit from an increased ability to quickly disseminate large amounts of data and are able to maintain quantitatively improved communications within their organizational structures (Weimann, 2006). The purported, internet-based communications between Iraqi insurgent Abu Musab Al-Zarqawi and the 'Al-Qaeda' network prior to his 2006 death demonstrate the degree to which the internet has

facilitated "more dialogue between members" (Zanini and Edwards in Arquilla and Ronfeldt, 2001, p. 36) of extremist Islamist organizations. These communications are said to have helped in the delivery of communiqués and orders to Zarqawi, ultimately leading to a solidification of the 'Al-Qaeda in Iraq' leadership structure (Brisard, 2005).

Extremist Islamist organizations also utilize the internet to communicate to potential supporters. Understanding the importance – to operational success - of mobilizing bases of popular support (Tuman, 2003), extremist Islamist groups reach out to followers and agreeable publics through the use of websites, chat rooms and online databases. In addition to authorizing websites which merchandise t-shirts, flags, badges, videos and audio-cassettes to interested parties (Weimann, 2006), extremist Islamist groups leverage the internet to provide sympathetic audiences with text and imagery designed to affect their sensibilities (Lia, 2005, p. 175). Extremist Islamist groups communicate current activities, struggles and successes to allies through the internet and draw supporters into their daily operations in the process (Yagil, 2002).

The extremist Islamist use of the internet for the purpose of communicating with international, 'enemy publics' is also worth noting (Weimann, 2004). As the internet provides extremist Islamist groups with a way to reach mass audiences (Nacos, 2006) coupled with "direct control over the content of their message" (Zanini in Jones, 2004, p. 168), such groups can broadcast potentially uncensored text, images and video to international viewers. According to Weimann (2006), it is often unclear whether or not extremist Islamist communications via the web are destined for hostile populations, although many extremist Islamist websites do feature English language sections of their sites as well as easily accessible – often graphic – footage and imagery intended to reach

an enemy audience. In May of 2004 – for example - an extremist Islamist website hosted a video featuring the beheading of American contractor Nicholas Berg. Accompanying this video, a headline read, "Sheik Abu Musab Zarqawi slaughters an American infidel with his hands and promises Bush more" (Filkins et al. 2004), a message clearly intended to reach – and to intimidate – a foreign populace.

## D. Recruitment and Indoctrination

Bruce Hoffman (2004) has indicated that the longevity of militant organizations is based partially on their "ability to recruit, to mobilize and to animate both actual and would-be fighters, supporters and sympathizers" (p. 8). Factual if we consider the cases of Palestine's 'PFLP'[10] and Peru's 'Shining Path'[11], Hoffman's line of thought appears to be shared by many extremist Islamist organizations.

Where traditional methods of recruitment are problematized through physical distance and external disruption (Gunaratna, 2002), extremist Islamist groups turn to the internet to draw the attention of willing individuals toward their organizations (Yagil, 2002). Over the internet, extremist Islamist organizations facilitate a virtual environment for the indoctrination of members into their groups (Yagil, 2002), "recruit and mobilize supporters to play a more active role in (their) activities or causes" (Reynalds, 2006) and ultimately "bridge the gap from the isolated potential mujahed to the global jihad" (Sageman, 2004, p.163). Extremist Islamist organizations provide access to "thousands

[10] The Popular Front for the Liberation of Palestine (PFLP) is a Marxist-Leninist, anti-Israeli militant organization formed in 1967. It gained notoriety in the 1960's and 1970's for several high profile aircraft hijackings but is now an organization largely secondary to other militant groups such as Hamas due to declining membership. *Source: Yonah, A. (2003). Palestinian secular terrorism : Profiles of Fatah, Popular Front for the Liberation of Palestine, Popular Front for the Liberation of Palestine-General Command and the Democratic Front for the Liberation of Palestine. Ardsley, New York, U.S.A.: Transnational Publishers.*

[11] Peru's 'Shining Path' guerillas – a Maoist organization formed in the late 1960's – succeeded in conducting numerous militant campaigns around Peru but eventually collapsed partially due to a lack of popular support. *Source: Palmer, D.S. (1994). The Shining Path of Peru. New York: St. Martin's Press.*

of books, articles, communiqués and fatwas" (Lia, 2005, p. 175) for the benefit of potential recruits. They also facilitate large, online databases catering to interested supporters. The introduction to an 'al Qaeda' training manual – published on the internet in 2004 - states the following:

> "Because many of Islam's young people do not yet know how to bear arms, not to mention use them, and because the agents of the Cross are hobbling the Muslims and preventing them from planning for the sake of Allah – your brothers the Mujahideen in the Arabian Peninsula have decided to publish this (online) booklet to serve the Mujahid brother in his place of isolation ... " (worldnetdaily.com, 2004, n.p.).

Some have suggested that – in addition to "seeking converts using the full panoply of web site technologies" (Weimann, 2006, p. 118), extremist Islamist organizations may also use clandestine means to recruit potential members. Such organizations could – for example – "note which type of propaganda receive the most browser hits" and resultantly "tailor a message for a particular audience" (Zanini in Jones, 2004, p. 168). These suggestions don't appear to carry much weight, but are worth considering due to the influx of data mining and other web surveillance technologies easily available over the internet.

Ultimately, statements which posit the internet as the 'ideal recruiting tool' for extremist Islamist organizations (Ariza, 2006) are predicated on the perception of the internet as open, disorganized and 'chaotic'. Because the internet is viewed as a largely unregulated forum in which activists can anonymously converse, share information and collaborate (Van de Donk et al, 2004), authors, researchers and journalists postulate the ease with which extremist Islamist organizations utilize cyberspace to extend their reach to potential members, to bring new individuals into their organizational structures and to

foster an environment in which recruiting for their causes can proceed "unabated" (Ariza, 2006).

## E. Virtual Community Building

In his 2000 book, "Virtually Islamic", author Gary Bunt wonders to what extent the virtual communities[12] of the internet – specifically those communities populated by citizens of the Islamic faith – have become transcendent forums blurring the realities of actual, physical life. Viewing cyberspace as an abstract, illusory world with the potential of implanting artificial perceptions in participants, he questions whether or not the internet has developed into an "electronic space casting Islam in an idealized light" (p.1) and attempts to gauge the ramifications of such a possibility. Interesting if we consider that extremist Islamist groups are said to be creating "virtual sanctuaries" (O'Brien in Jones, 2004. p. 141) for their activities on the world-wide web, Bunt's queries shift our attention to the part that the internet is potentially playing in giving rise to an idealized space for extremist Islamist activities.

Some postulate that chat rooms, bulletin boards and other interactive forums of the internet may be fertile ground for the development of virtual communities "just, egalitarian, full of opportunity, unified in an Islam purged of national peculiarities and devoid of corruption, exploitation and persecution" (Sageman, 2004, p. 161). Absent the physical bonds and face to face contact characteristic of real life experience, virtual communities may provide extremist Islamist groups with a social space in which to create idealized and slanted interpretations of the Islamic faith, may allot such groups a platform on which to "glorify the heroes and martyrs of the movement's cause" (Nacos, 2006, p.

[12] Virtual communities are communities in which participants communicate and interact primarily through the use of IT, and in which face-to-face communications are infrequent and rare. (Rheingold, 1993).

230) and could potentially give such groups a module with which to push participants toward the attainment of unrealistic and unattainable goals.

The notion of an 'extremist Islamist virtual public sphere' has – in my opinion – not been properly addressed in literary works dealing with the topic of extremist Islamist activity on the internet. A further exploration of this facet of extremist Islamist internet usage is probably warranted in the future, not only because of its absence in the literature, but even more so due to the fact that it may be the creation of idealized virtual communities – by extremist Islamist groups – which allows the facilitation of other aspects of extremist Islamist internet usage.

## F. Conclusions

Ultimately, extremist Islamist groups – having become technologically proficient in the use of NICT's – employ these technologies for various purposes. While extremist Islamist groups facilitate communication and organization through the data-transfer capabilities of the internet, they also utilize the World Wide Web, chat groups and online databases to reach potential supporters and recruits. Employing the internet to form egalitarian and corruption-free 'virtual communities', extremist Islamist groups build idealized versions of real-life societies, and exhort members and followers to achieve unrealistic and largely unattainable goals in the life-world. And making use of the internet's distributed structure, extremist Islamist groups remain in close contact and "accomplish everything they need to do together without ever being co-present in the same location" (Baba in Hyland et al, 2005, p. 120).

The internet – in its complex and multi-faceted nature - has allowed extremist Islamist groups to remain functional in a world where they face significant challenges to

their daily operations. It has given such groups a way to overcome physical obstacles, to build and grow, and to expand into areas of the world – such Great Britain[13] - where a strong, Islamist presence was previously not evident. Utilizing the internet, extremist Islamist groups have been able to create a visible, online presence for themselves around the world, and more importantly, have raised the profile of the 'extremist Islamist employment of the internet' to the point where it has become a legitimate - and significant – area of study.

[13] Britain is home to the Finsbury Park Mosque in which controversial (and now jailed) imam Abu Hamza al-Masri preached regularly (bbc.co.uk, 2006) Muslim Cleric Omar Bakri Muhammad – who until 2005 resided in Britain – is quoted as stating "the life of an unbeliever has no value. It has no sanctity." (theage.com.au, 2004).

## VIII. THE PROJECT

### A. Intent of project

At the outset, my project was intended to identify a series of extremist Islamist websites operating in Canadian webspace, to plot the location of these websites (based on the geographical position of the registrars, service providers or datacenters hosting them) on an interactive map, and to track the disappearance, reappearance or change in physical location of any of these sites over a period of two months. During the two month period of observation, the intention was also made to take note of the layout of the chosen websites sites and to track significant changes in content and format, although this idea was later dropped due to the difficulty of interpreting site contents and due to the fact that initial scans of the websites in my project revealed such sites as having little relevance – in terms of content – to the Canadian state.

The reasoning behind this project was twofold. Firstly, it was considered imperative to demonstrate – to students, academics and researchers - the presence of extremist Islamist websites within Canadian webspace. Noting claims that Canada has become "a potential target" for extremist Islamist activity (csis.gc.ca/en/newsroom/backgrounders, 2002) and that extremist Islamist groups have begun to set up operations on Canadian soil (Bell, 2004), there was a perceived need to provide a visual representation of any extremist Islamist websites being serviced by Canadian internet companies. The alleged, plot – by a group of "like-minded Islamists" (Van Rijn, 2006, n.p.) - to attack various Canadian targets in June of 2006 was claimed to have been internet-facilitated, and thus the timing was correct for a project which would

explore the aims of extremist Islamist groups being serviced by Canadian internet companies.

Secondly, there was a desire to present interested parties – scholars, students and academics - with an easy way to conceive of the scope of extremist Islamist websites operating under Canadian internet companies. With preliminary research indicating that no attempt had yet been made to geographically chart extremist Islamist websites active in Canadian webspace, and noting that a visual representation of active, extremist Islamist websites would be more effective than – for example – a simple written description of the placement of these sites, it was decided to choose a format which would privilege the visual over the written.

It was hoped that the format chosen for this initiative – the idea of presenting extremist Islamist websites (active in Canadian webspace) in a visual, geographically placed fashion - would provoke a high level of inquisition and discussion. As the topic of extremist Islamist activity within Canada is currently highly debated, and as the recognition is emerging that extremist Islamist groups are making use of the internet for various purposes on a global scale, it was felt that this project could possibly ignite a debate over the reasons behind why extremist Islamist websites are or might not be operating in Canadian webspace. The aim of this project was not to be contentious per-se, but as it was believed that a certain level of debate would lead to possible elucidations regarding the existence of extremist Islamist websites in Canadian webspace, it was felt that the format chosen for the project was correct.

Ultimately, the real reason behind the development of this project was not to investigate the aims of, methods utilized by and benefits incurred by extremist Islamist

groups using the internet – this had already been done in depth, notably by Weimann (2006), Nacos (2004), Last (2005) and others. The real value in this project was to present members of the public – namely students and ordinary citizens – with a first look at the extension, to Canadian webspace, of the extremist Islamist phenomenon, a phenomenon which has spread onto the internet in recent years, making its presence felt on a global scale.

## B. Method of Pre-Preparation

Prior to the commencement of this project's observation phase, a series of extremist Islamist websites operating in Canadian webspace had to be identified. The idea was undertaken to make use of the 'tracking terrorism.com', 'Internet Haganah' and 'siteinstitute.org' websites, three sites with major databases pertaining to extremist Islamist websites. Using the "Who Is" search engine, located at www.whois.org, dozens of sites listed in the databases of these sites were scanned for ownership. The result was the discovery that 32 extremist, Islamist websites were registered, hosted or given datacentre space by Canadian internet companies. After this initial phase was done, I could successful move onto the next phase, the actual plotting of the sites on an interactive map.

## C. Plotting of sites and use of Google Earth

After the initial period of pre-preparation which identified a series of extremist Islamist websites being serviced by Canadian internet companies, the choice was made to plot the found sites on Google Earth, an interactive mapping program said to be able to provide "high-resolution satellite imagery of 20 percent of the Earth's surface" (Claburn, 2006, p. 18). Google Earth was chosen on the basis of it being dynamic, user-friendly

and flexible. As well, Google Earth represented an evolving platform – it was felt that, if this project was to continue past the end of the allotted two month observation period, it could potentially benefit from future technical additions to the Google Earth program. Using Google earth would offer the potential of sharing this project with a global audience, and would provide a way to allow users a direct view of extremist Islamist website activity within Canadian Internet companies.

The plotting process began by looking up the geographic addresses of the Canadian internet companies providing services to the found sites. This was done easily by examining the company websites themselves. *Appendix A* lists the names and addresses of Canadian internet companies found to be providing services to extremist Islamist websites. After this, the physical addresses of these companies were noted, and – using several online maps – matches were made between the companies and their actual physical location[14]. The dynamic map in Google Earth was referenced with these matches. 'Placemarks' indicating the physical location of respective Canadian internet companies hosting extremist Islamist websites were then plotted in Google Earth.

Figure 1: Temporary Placemark - Webserve Canada, Vancouver, B.C.

[14] Google Earth provides the viewer with a visualization of physical terrain, but at the time of writing, does not support street names and addresses.

After this step, placemarks were plotted on the Google Earth Map linking extremist Islamist websites with their respective Canadian registration, hosting or datacenter companies. Relevant information was included with each placemark, such as the name of the website, its group affiliation (for example, Hamas, Palestinian Islamic Jihad, etc), and the datacenter, service provider and hosting company servicing it. Where applicable, an image from the site itself was also linked to provide the viewer with a quick site-identifier. Google Earth was beneficial in these regards because it provided a dynamic way of having a text box appear – when clicking on placemarks - which would allow the viewer to see all information about the chosen websites.

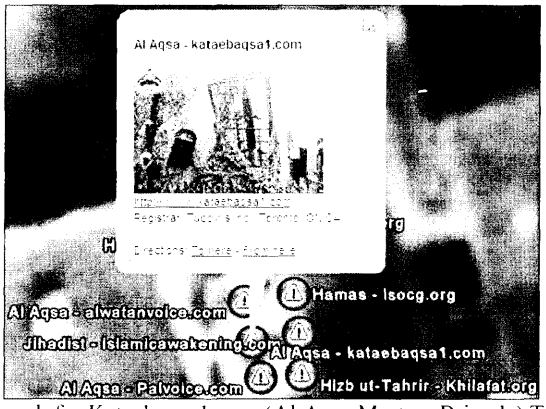

Figure 2: Placemark for Kataebaqsa1.com (Al Aqsa Martyrs Brigade) Tucows, Toronto

Overall, Google Earth was deemed the right program to use for this project. While its public display capabilities provided potential viewers with an easy visualization of the scope of extremist Islamist websites operating in Canadian webspace, its server capabilities[15] and ease of manipulation were of great benefit to my aims, and showed promise for the possibility of this project being easily transferred to a more in-depth researcher in the future.

## D. Results of Research period

[15] Google Earth allows the user to treat a specific project like a website – using this program, one can store information and make it publicly available.

The observation phase of my project formally commenced after the plotting of the 32 extremist Islamist websites – found during the pre-preparation stage of this initiative – on the Google Earth Map. I had expected, prior to the beginning of the project, to find many more sites operating in Canadian webspace, but the realization that 32 extremist Islamist websites were being serviced by Canadian internet companies was significant in and of itself. Sites affiliated with Islamist groups Al Aqsa Martyrs Brigade, Hamas, Hizballah and Hizb ut-Tahrir were all found and plotted – Appendix B lists these groups and their respective backgrounds.

By week two of this project, I began to see the first evidence of site movement, as several observed sites went offline. While two sites in my study became inactive in this week, a third was replaced with an error message possibly indicating that the site administrator had been locked out. Two other sites now re-directed to another site as well. Appendix D lists the results of week 2 of my study.

Week three of the project saw one additional site disappear, bringing the total of sites having disappeared since the start of the observation period to four. However, another site also appeared in week three – this site was discovered through an additional examination of the databases at the Internet Haganah website. This meant that the total number of active sites– in my study – remained at 29. At this point, I began to wonder chiefly why Tucows Ltd. of Toronto was providing registration services to so many sites, as by the third week, 15 sites were active under the services of Tucows. Appendix E lists the results of week three of my study.

Week four saw the disappearance of a site that had appeared only a week earlier, but also saw the reappearance of two other sites which had previously disappeared. This

brought the total number of sites active in my study back up to 30. I began to question postulations – by experts such as Weimann (2004) – about the rapid fluctuation of extremist Islamist websites. If such sites were frequently moving from server to server to avoid being shut down, or continually going on and offline for various reasons (Weimann, 2004), my expectation at this point was that I should have already witnessed this phenomenon. Instead, I was witnessing a series of sites which appeared to remain static. Appendix F lists the results of week four of my study.

Week six of my study followed a disappointing week five in which nothing of significance had happened. In week six, I again noticed the movement of sites, as two more extremist Islamist websites became inactive. In this week, an interesting turn of events saw two sites change direction – the ikhwan.net and al-multaqa.net sites no longer re-directed to www.hassanalbana.org – instead, al-multaqa.net and hassanalbana.org now re-direct to ikhwan.net. This was probably due to site ownership – my postulation here was that several different domain names had likely been registered by the same group so that, in the event of one site being shut down, information could quickly be moved to another site. Appendix H lists the results of week six of my study.

Week seven of my study saw another new site come online. This site was again found through searches of new sites listed in the Internet Haganah database. This meant that there were 29 sites in total still active in my study. Appendix I lists the results for week seven of my study.

At week eight – the final week of my study - two more sites became inactive. This meant that – at the end of my observation period, while there were seven sites which were not operational, 27 total sites remained active. I had expected – at the outset of my

project – to see a much larger fluctuation of sites. As well, I had anticipated the rapid movement of sites between different servers – what occurred was well below my expectations. Nonetheless, I saw this as significant – these results alone were to inform some of the conclusions of my project. Appendix J lists the results for week 8 of my study.

## E. Makeup of Observed Sites

During the initial planning stages of this project, the question arose as to how to accurately connect alleged extremist Islamist websites with their purportedly associated groups.[16] Challenging and thought provoking, this question became one requiring a critical level of attention. With the integrity of this project largely dependent upon the precise designation of a series of websites as 'extremist Islamist' and with the knowledge present of a possible margin of error concerning the proper identification of found sites[17], a method of determining the association between uncovered websites and related extremist Islamist groups was deemed imperative.

It was decided that the best way to cement the relationship between found sites and their suspected authors would be – firstly - through a research process revealing identifiers (emblems, color schemes, statements) common to the groups in this study. The signs, symbols and aesthetic preferences of organizations such as Hizballah and Hamas would be noted, their various stances on issues and important statements taken into account. This would be followed by a thorough examination of the sites in this study to see if the imagery, colors and terminology used on such sites bore any relation to the

[16] Relying solely on outside sources to positively identify active, extremist Islamist websites was deemed inappropriate for this study – to cement the relationship between suspected websites and their alleged authors, a more in depth level of investigation was necessary.

[17] One of the primary questions initially asked – by observers of this project – concerned the possible misidentification of ordinary, Arabic-language websites as Islamist in orientation.

conventions utilized by their allegedly associated organizations. Finally, site contents would be recorded based on a standard set of criteria, and comparisons would be made by cross referencing positively-identified extremist Islamist websites against sites affiliated with similar groups. Following this method, it was believed that not only would a greater level of assurance regarding proper website identification be achieved, but that as well, common threads unifying the different websites of singular groups would be seen. The following section details the last part of the process described above, with special emphasis on common imagery, color scheme and terminology threads running through similarly affiliated sites.

### E.1 Imagery

At the adjournment of the website content investigation phase of this project, it was firstly concluded that the sites observed in this study could be positively matched to their allegedly affiliated groups through identifying imagery. Possessing splash banners bearing group logos, pictures and diagrams intended for identifiable audiences and photographs appearing as almost endemic to specific interpretations of Islamist extremism, many of the sites surveyed in the context of this initiative pictorially reflected the authorship of particular, extremist Islamist organizations.

One of the primary types of observed imagery aiding in the proper designation of found sites during this initiative came in the form of group crests or emblems. Displaying logos identical – or similar to – official logos used by groups such as Al-Aqsa and Hizballah, the majority of the websites investigated during this project provided clear, outward signifiers of group orientation and ownership. The majority of Hizb ut-Tahrir websites, for example, displayed the characteristic black flag with white lettering

symbolic of that group, while most sites allegedly affiliated with Hamas were marked with a variation on that group's official insignia. Logos, crests and emblems were generally embedded in colourful and image-rich banners located at the top of the intro page of most websites in this study; this combination was likely intended to instil – in target audiences – an immediate understanding of site affiliation and authenticity.

Revealing photographs also acted as markers tying numerous sites in this study to their suspected owners. Featuring images strongly reflecting the operational mandates of allegedly affiliated groups, the majority of websites examined in this initiative provided clear, pictorial evidence linking them to specific, extremist Islamist beliefs, operations and actions. Supposed sites of the Al-Aqsa Martyrs' Brigades, containing photographic combinations of important personalities[18], known martyrs and Palestinian militants brandishing rocket propelled grenades, were complimented in this study by the apparent web pages of Hizb ut-Tahrir, whose sites provided images of group-related meetings, protests and demonstrations. Websites linked with Hamas - a group whose primary operations are directed towards the funding of educational institutions, health centres and similarly-related charity projects - were unsurprisingly adorned with images of schools, hospitals and community centres under construction. And a host of independent sites in this study featured images of armaments, Islamist militants, anti-Israeli emblems and other related elements, all of which acted as indicators of such sites being tied to the operations of known, extremist Islamist groups.

### E.2 Color Scheme

Another interesting conclusion made at the adjournment of the website content investigation phase of this project was that the majority of sites investigated in this study

[18] Of these personalities, Yasser Arafat figured prominently. Al Aqsa is a known affiliate of Hamas.

could be connected to their allegedly affiliated groups through commonly-occurring color schemes. As it had been observed – through prior research – that most groups included in this study used specific color combinations as a hallmark of their public identities[19], it followed that such colors would be evident and recurring among many of the websites of such groups.

Websites indicated – by outside organizations such as Internet Haganah – to be connected with extremist Islamist groups were generally constructed in colors resembling those found in group logos, pictorials or communication-related materials. Suspected Hizb ut-Tahrir websites, for example, often appeared in the black and white of that group's official insignia, while the majority of Hamas websites were made up of the Green, red, white and black typifying both the official logo - and the association with the Palestinian state - of that group. In many cases, it appeared that color acted both as a signifier seizing the attention of target audiences as well as a visual device tying certain websites to a specific struggle – it was expected that the latter supposition would be given more weight by the eventual discovery and examination of a much larger amount of sites affiliated with groups seen in this study.

### E.3 Written Materials

One of the most significant findings of the website examination phase of this initiative concerned the identification of written materials – articles, pamphlets, statements – largely specific to certain extremist Islamist organizations. Using Google's free translation utility, as well as the Multi-Translate utility developed by Systran©, basic translations of the written contents of many observed sites were made – these translations were to reveal identifying terminology linking found sites to their supposedly affiliated

[19] The characteristic green on yellow, for example, reflecting the official colors of the Hizballah flag

groups. While it was assumed that much of the writing and terminology found on specific sites would be present on the websites of various, disassociated extremist Islamist groups, some terminology was group-specific enough to merit attention.

Among sites alleged to belong to the Al Aqsa Martyr's brigade, articles concerning the importance of martyrdom were complimented by calls for militant activities. One loosely translated phrase on a suspected Al Aqsa site indicated that "100 Martyrs are ready to attack the depth of the Zionists", while another, similarly affiliated site adorned photographs of deceased Al Aqsa members with glorifying descriptions of their individual sacrifices, many of which appeared related to suicide attacks. Sites claimed to be affiliated with Hamas contained textual references to initiatives undertaken in relation to schools and other charities – one site claimed to work on behalf of all Palestinians, "Especially the families of martyrs and prisoners, orphans and students of science and needy families." And along with writing concerning the dissolution of the Khilafah and articles proclaiming the need for the establishment of a worldwide caliphate, numerous Hizb ut-Tahrir related sites contained phrases calling for attacks on the West (an article found on one site states "We ask God Almighty to make the massive destruction") attacks on Israel and other, related militant activities.

Ultimately, the translation of written materials was an important key to drawing an association between found sites and their suspected authors. Through the conversion to English of written documents, familiar terms, phrases and idioms could be identified and linked to modus operandi of specific groups, and allegations of site ownership could be further bolstered. Contributing much to the verification of site identity, the translations methods used herein, however basic, proved invaluable - It was expected that

the inclusion in future endeavours of better translation methods along with the possible expansion of this project to include a greater number of observed websites would in turn produce more textual proof of site ownership.

## E.4 Conclusions

A thorough inspection of many sites involved in this study revealed common identifiers which – when cross referenced against the signs and symbols of extremist Islamist groups investigated in this initiative – helped to bolster links between observed virtual spaces and their alleged possessors. Undertaking a research process combining a knowledge of the traits of extremist Islamist groups with an empirical analysis of websites purported to belong to such organizations, it was found that – at the same time as laying the foundation for a method of verifying extremist Islamist website authenticity – common threads between similarly affiliated sites were being uncovered.

Very much for the infusion of an understanding of site affiliation into potential audiences, common identifiers may help to draw in interested individuals, while common threads may serve to provide a unified front for organizations with many, geographically dispersed factions. This may ultimately lead to visions – in sympathetic audiences – of stronger, larger, globally organized and cohesive extremist Islamist organizations. Future research endeavours – including possible audience impact surveys -will no doubt determine the impact that extremist Islamist groups are having on potential audiences – it is possible that extremist Islamist organizations may, through the makeup of their various sites, be very much geared toward seizing the attention and the sympathies of amicable publics.

## F. Conclusions about observation phase of Project

At the adjournment of the observation phase of this project, I was disappointed at what I viewed as a lack of high-yield results[20]. Against my predictions – informed by writers such as Weimann (2006) and Last (2005) - that observed websites would appear and disappear or change registrars, servers or datacentres on a weekly basis to avoid being shut down, most sites in this study changed very little in terms of their ISP location. The fact that 27 sites out of an initial total of 32 were still active at the end of my study demonstrated a failure to anticipate the immobility of extremist Islamist websites operating in Canadian webspace and indicated that certain other measures might have been taken prior to the study, such as the possible extension of this project to include the majority of North American webspace, as well as the inclusion of a wider number of groups in the project's observation phase.

A lack of dramatic results in this study did not – however – preclude the possibility that some important postulations could be made regarding the behaviour of the observed, extremist Islamist websites. The following conclusions, drawn from an examination of prior, extremist Islamist activity on the internet and external responses to this activity, were conceived out of a necessity of clarifying a phenomenon which remains – as of yet – under-investigated.

### F.1 Lack of Site Movement

At the outset of this project – noting that most of the websites in this study were associated with extremist Islamist groups now banned in Canada[21] - the expectation was present that many observed sites would quickly go offline, perhaps to be replaced with

[20] The term 'High-yield results' is meant to indicate findings which reveal a measurable level of peripheral elements surrounding a certain issue.
[21] See www.psepc.gc.ca/prg/ns/le/cle-en.asp

other sites which would themselves disappear. It was anticipated that, as Canadian security and policing agencies would not allow barred extremist Islamist groups to make use of Canadian webspace, a rapid closure of sites would be seen. The fact that this result did not occur and that very few observed websites went offline during the observation phase of my project is thus significant. This could – firstly - be attributed to the alleged difficulties associated with online regulation and control.

The internet – viewed by some as extremely difficult to regulate due to its decentralized nature (M.J., 1996), is often concurrently cited as being a medium which "does not allow for effective censorship against terrorism" (Lia, 2005, p.195). The claim that "terrorist activity online is hard to track down" (Lal, 2003, n.p.) underscores suppositions of a cyberspace beyond the realm of significant administrative control – this mode of thinking places subversive groups at the centre of sphere considered conducive to the anonymous activities of a range of substate and non-state actors.

Taking the alleged difficulties associated with internet regulation into consideration, it is possible that – in the context of this study – the ambiguous nature of the internet proved conducive to the observed, extremist Islamist websites staying online. Many of the websites observed in this study may have avoided being shut down out of an inability, or an unwillingness - on the part of Canadian law enforcement – to regulate them. As it is thought by many to be "difficult for hacktivists and governments alike to banish from the Net content they deem offensive" (Conway, 2002, n.p.), Canadian lawmakers, such as CSIS and the RCMP, may have considered - assuming their knowledge of the existence of the sites of observed in this study – the majority of online, extremist Islamist forums operational in Canadian webspace 'not worth shutting down'.

The fact that so few sites went offline during the observation phase of my project might also suggest that policing and security agencies in Canada prefer to keep most extremist Islamist websites online, as opposed to taking them down. Despite broad new powers allowing Canadian security and law enforcement agencies control over content housed by Canadian internet companies[22], organizations like CSIS and the RCMP may have wished many of the observed websites to remain active and may thus have limited the removal of these websites from the databanks of Canadian ISPs. According to Lewis (in Clarke, 2004), state actors "might gain more from penetrating hostile computer networks and unobtrusively observing them while they continue to operate" than they would get from disrupting them (p, 197). Leaving the majority of extremist Islamist websites online, Canadian security and policing agencies could potentially have been observing the activities of site visitors - as was said to have been done prior to the June 2006 arrest of an alleged "home-grown" cell of Canadian 'terrorists' (Shephard, 2006, n.p.) – and could have used such sites to identify facets of extremist Islamist organizations operating on Canadian soil.

One final theory which may help to elucidate why so few sites physically moved during the course of my project's observation phase is that which refers to the possible existence of 'dummy sites', extremist Islamist websites allegedly set up and run by law enforcement and intelligence agencies, specifically those of the United States[23]. According to this theory, certain, 'genuine looking' extremist Islamist websites could

[22] Bill C-74, the "Modernization of Investigative Techniques Act", also known as the Lawful Access act, allows Canadian security and intelligence agencies to request full information on subscribers from Canadian internet companies at any time, including name, address and telephone number. This act also requires Canadian internet companies to include information interception capabilities as they introduce new technologies (michealgeist.ca, 2005).

[23] Evidence supporting this theory is largely speculative – see http://www.informationclearinghouse.info/article4513.htm.

appear to operate for the benefit of Islamist groups and sympathizers while – in actuality – being run to track visitors and to fulfil various, propagandist aims (i.e., the releasing of incendiary videos of speeches by prominent Islamist figures at opportune times) on behalf of administrative interests.

At least one site in this study is rumoured – among internet forums and chat groups – to be a front for CIA activities. According to Shane (2003), "Jihad Unspun, an English-language site that appears to promote terror, may be a CIA creation, designed to find out who visits or orders videos glorifying bin Laden" (n.p.). The Jihad Unspun site, run out of a Vancouver-based internet service provider, appears as a contrast to most other, extremist Islamist websites in this study – employing a mixture of bold colors, attractive design motifs and stark images, the site appears as oddly professional, its juxtaposition of immediately recognizable figures and an 'Islamist friendly' layout highly suspect. This site, among others, merits further investigation, as does the 'dummy site' theory, as it might well be possible that a large number of seemingly 'extremist Islamist' websites are actually being run by domestic intelligence agencies.

### F.2 Site Movement

There were also some interesting results – in this study – regarding websites which did go offline. While some sites in this study appeared to go down for maintenance -such as the *fateh.org/news/index* website in week five of the observation period – other sites simply disappeared. Several observed websites reappeared, most notably the *khilafat.org* and *albadil.edaama.org* sites. And one site – *aqsavoice.net* - disappeared, only to be replaced by a page advertising such things as "intimate anonymous sex", "porn movies online" and "sexy muscle women".

It was suspected – at this point – that the domain name of the latter site may have been seized by a secondary party and the contents of the site replaced, as was done in the case of the *alneda.com* site, an alleged 'Al Qaeda' website seized by American hacker Jon Messner in 2002 (Di Justo, 2002). Taking into account the prevalence of 'internet vigilantes', groups of 'hackers' who specifically target perceived, extremist Islamist websites (Conway, 2002), the possibility was considered that this website had been 'hacked' and potentially brought under the control of another owner.

After one week, at which point the advertising page which had replaced the previous contents of the *aqsavoice.net* site disappeared, the DNS address of this site was run through the 'whois' service, located at www.whois.org . It was discovered that the site was no longer registered by Tucows Ltd. – its previous registrar. Furthermore, it was observed that the status of this site was now 'locked'. As a 'locked' status indicates that a site has been secured against seizure by outside parties, this gave further wind to the suspicion that this site had been taken over by a hostile party, and had eventually been regained by its previous owner.

### F.3 Clustering of Similarly-Affiliated Sites According to Service Provider

One interesting aspect of this study was the finding that – under certain Canadian ISP's - there was a prevalence of multiple sites affiliated with single, Islamist groups. For example, at the conclusion of the observation phase of this project, five sites associated with the Islamist group Hizballah were still active under Edmonton-based Tera-byte.com, while Peer 1 Network in Montreal was hosting several sites affiliated with the group Hizb-ut-Tahrir.

The prevalence of similarly-affiliated sites under singular, Canadian ISP's could be due to Canadian ISP hosting policies, but could also be attributed – in some cases – to the range of services offered to potential clients. Certain Canadian ISP's could well appear more attractive to extremist Islamist groups than others due to benefits presented – Almina Multimedia of Toronto – for example –states on their website that "Our understanding of the Arabian Gulf and of Arabic culture ensures that we will be able to provide your organization with the extraordinary customer service and superior technical support it deserves". Partially headquartered in Dubai, Almina Multimedia offers services in both Arabic and English – their services may well be attractive to extremist, Islamist groups wishing to employ a user-friendly, easy accessible internet hosting company.

### F.4 Prevalence of Sites under Tucows

One final project finding involves the provision of services to numerous websites – in this study - by Tucows Ltd. of Toronto. In the final week of this study, Tucows appeared to be providing registration services to 13 observed sites, and was acting as a service provider for one additional site, making it the largest provider of services to extremist Islamist groups observed in my study.

The fact that Tucows provided services to a large number of extremist Islamist websites in this study could be partially explained by the size and business practices of the company itself. Tucows, which claims to be the "largest ICANN accredited wholesale domain registrar in the world" (tucows.ca, 2006), currently manages more than four million domain names (thehostingnews.com, n.d.) on a global basis. As most of Tucows business is done through 'domain name resellers' (tucows.ca, 2006), meaning the

company sells the majority of their domain names indirectly through second party agents located throughout the world, it is possible that the organization does not realize the extent to which extremist Islamist groups have begun to employ its services. Domain names could – under Tucows operational structure – be registered on behalf of the organization, but absent the organization's explicit permission.

### F.5 Final Thoughts

The results of this project – although not substantial – did allow for some important assumptions to be made. Where there was a certain degree of website movement, and certain sites were brought offline, changed or replaced, outside interference could have potentially been present. Sites that went offline and then returned could potentially have found new 'homes' in cyberspace, as Nacos (2006) indicates that sites sent offline "usually find alternative servers" (p. 232). And Canadian internet companies registering, hosting or providing datacentre services to sites might not have been aware of their involvement with extremist Islamist web content, due to various business practices and operational structures.

In the future, it would behove additional researchers to take the limited results of this project into account and to extend a similar project to a wider geographical base, as opposed to simply focusing on one content or territory. This would allow a much more substantial view on the internet-related activities of extremist Islamist groups, and more importantly, would help to give a more global picture of how extremist Islamist groups are operating within the confines of the internet and who is helping to shape, control and restrict their level of operation.

## IX. Responses to the Extremist Islamist use of the Internet

Frequently implicit - in literature dealing with the extremist Islamist use of the internet - is the inference that a lack of external scrutiny has allowed online activities by extremist Islamist groups to proceed with relative impunity. Proposing initiatives designed to curb the augmentation of extremist Islamist activities in cyberspace, authors such as Weimann (2006) and Nacos (2006) quickly posit that – in the absence of ostensible pressures - extremist Islamist groups have developed a "virtually unchecked ability to use the Internet to plan, promote, and propagate" (Abbey, 2004, p. 24) and that a high degree of technical mastery over the employment of the world-wide web by such groups has ensued as a result (Weimann, 2006). The notion that "Islamic extremists sometime run rings around us in cyberspace" (Kristof, 2005, A31) underscores a feeling, held by many authors examining the movement to the internet by Islamist groups, that the proficiency with which extremist Islamist organizations have made use of the internet stems from an historical lack of political will regarding the surveillance and curtailment of extremist Islamist cyber-activities. Online, extremist Islamist activity is – in the eyes of many – at least a partial product of complacency at official levels - writing about the growth of Islamist activity on the internet, one expert indicates that "a steady, stealthy indoctrination aimed at creating a whole new generation of jihadists" by extremist Islamist groups remains "scandalously ... unopposed" (Ulph in Morgan, 2006, p.1).

Suppositions of an internet posing few restraints to extremist Islamist groups not only highlight an inability of many authors, policy makers and national governments to comprehend the existence of obstacles to the extremist Islamist use of the internet, but as well belie an understanding of the presence of state and non state actors who monitor,

challenge and subvert the online actions of extremist Islamist groups on a daily basis. As challenges do exist to the extremist Islamist use of the internet, and as these challenges can be considered multifarious and varied, it is important to understand the ways in which substate and non-state individuals and groups, security and law enforcement agencies and state governments and administrative powers respond to the extremist Islamist use of the internet. While 'hackers' and 'cyber vigilantes' scour the world-wide web, frequently and unexpectedly attacking the home pages and databases of groups such as Hamas and Hizballah, lone wolf 'hacktivists' target well known, extremist Islamist websites, defacing and frequently rendering them inoperable for long periods of time. Privately-funded research institutes and non-governmental organizations such as the SITE institute examine the emergence of the Islamist ideology on the web from afar, drafting initiatives designed to constrain online, extremist Islamism from numerous angles. And lawmakers, security organizations and elements of federal governments surreptitiously monitor, track and, occasionally, – take action upon extremist Islamist websites, chat rooms and all other internet technologies employed by such groups. All of these responses can be considered in the context of an almost inevitable response to the perceived explosion of perceivably uncontrollable phenomenon, one which evokes feelings of apprehension, a sense of urgency, and more often than not the need for action in a multiplicity of substate, non-state and state actors.

## X. Conclusions

Far from being an isolated occurrence, the extremist Islamist presence on the internet has become a significant phenomenon, one which has spread to a multitude of international registrars, service providers and datacenters and which is now being witnessed on a global scale. Having moved into cyberspace in large numbers, extremist Islamist groups – such as Hizballah and Hamas – now employ various internet-based innovations for their purposes, including e-mail, chat rooms and online bulletin boards and presently utilize the internet to make possible a range of aims, such as communication, recruitment, organization and community building.

While the decentralized nature of the internet has allowed for dispersed, extremist Islamist organizations to remain in close contact while retaining a large degree of autonomy, the dynamic and seemingly unregulated online environment has permitted such groups to broadcast potentially uncensored messages to a global audience. The speed and efficiency of internet-driven transmissions has allowed extremist Islamist groups to rapidly convey substantial amounts of data between organizations and to potential members, and the ability to quickly publish data online has permitted these groups to easily make available text, images, audio and video at critical times. Extremist Islamist groups have come to rely on the internet for the fulfilment of a broad range of activities and aims, ultimately leading to assertions – by some – that such organizations have become strongly dependent upon this powerful – and indispensable – communicative medium (Last, 2005).

At the same time as understanding the potential which the internet has given extremist Islamist groups to more effectively conduct their operations – however - we

must also be aware of a "superhighway" of surveillance and internet policing which has developed largely as a response to the extremist Islamist use of the internet (Wade in Clarke, 2004, p.124). Formed partially out of a perception – by law enforcement and security agencies - that the internet provides extremist organizations, specifically extremist Islamist groups, with a potentially unchecked, global voice (Tuman, 2003), a new regime of internet regulation has seen the creation of laws and technologies designed to assist in the interception, surveillance and control of online content. This is leading to a fundamental challenge to the existing structure of the internet, and is laying the foundation for a shift into "a period where the secondary goal will be access and the primary goal will be security" (Light in Klotz, 2004, p.111).

This severity of this new regime of internet regulation and control should not be understated. While the 2001 Council of Europe Convention on Cybercrime[24] places "obligations on upon ISP's that, in effect, convert service providers into integral cogs in the apparatus of online law enforcement" (Huey and Rosenberg, 2004, p.1), Bill C-74, Canada's Lawful Access Act, forces Canadian internet companies to disclose all available personal information of "any subscriber to any of the service provider's telecommunications services" (parl.gc.ca, 2005) upon request by law enforcement. Anti-terrorism Bill C-36, in its "web of unprecedented investigative powers, broad offences and harsh punishment (Daniels, Macklem and Roach, 2001, p. 152) makes it a crime[25] to house the websites of banned, extremist Islamist groups, even unknowingly. And a host of other internet control and surveillance technologies – from intelligent filters to data-mining tools – combine to create an environment in which online freedoms and privacies

[24] Signed by Canada in 2001
[25] Punishable by between ten years and life in prison (Daniels, Macklem and Roach, 2001).

are being increasingly challenged, and in which the 'spectre' of online, extremist Islamist activity pales in comparison to methods used to challenge this activity.

Perhaps the most pressing part of the spread of online surveillance is that an apperception of how new policies, laws and technologies are being applied to the internet is lacking among the Canadian populace. A need to understand the ways in which new policies and new technologies "facilitate the erosion of privacy in unprecedented ways" (Austin in Daniels, Macklem & Roach, 2001, p.263) appears to be a low priority among Canadians - a recent poll – in which Canadians indicated the need for "tough new security measures" indicates that citizens of Canada have yet to grasp the extent to which security-related technologies and the policies behind them have penetrated Canadian webspace (Clark, 2005, n.p.).

Ultimately, we must understand that – as extremist Islamist groups increasingly gain a foothold on the internet, their presence will be met by new online surveillance and control measures. Security and policing agencies, wishing to both counter and monitor extremist Islamist activity within Canada, will make ready use of new policies, laws and technologies to delimit the ability of these actors to function within the online environment. This will no doubt lead to a significant struggle, one which will see extremist Islamist groups continually finding new and innovative ways to bypass official methods of information management, and one which will see further increases in the development and use of online surveillance and policing policies, methods and technologies by Canadian security and law enforcement. It will be the victor of this struggle – the one set of actors most able to leverage the internet for their own purposes - who will ultimately be in the best position to shape the future of the online world.

## Appendix A – Canadian Internet Companies providing Services to Extremist Islamist Group in this Study.

Almina Multimedia Services (now known as Amanah Tech Inc.)
*Provides network services and dedicated servers*
341 - 151 Front Street West
Toronto, Ontario, M5J 2N1
Tel: 1-416-603-9825
Fax: 1-416- 603-6587

Canaca.com, Toronto, O.N.
*Provides domain name resale and hosting services*
203 - 1650 Dundas Street East
Mississauga, Ontario, L4X 2Z3
Phone: 1-800-823-9410

Peer 1 Network, Montreal, Q.C.
*Provides dedicated hosting and Servers*
1512 - 1080 Beaver Hall
Montreal, Quebec, H2Z 1S8
Phone: 514-878-0080
Fax: 514-878-0085

Rackforce Hosting Inc., Kelowna, B.C.
*Provides wholesale hosting, network and datacenter services*
104 - 1708 Dolphin Ave,
Kelowna, BC, V1Y 9S4
Phone: 1-866-468-1151
Fax: 1-866-468-1156

Tera-Byte Dot Com, Edmonton, Alberta
*Provides shared hosting, dedicated servers and domain name registration services*
#900
10004-104 Avenue,
Edmonton, Alberta, T5J 0K1
Phone: 1-780-413-1868
Fax: 1-780- 413-1869

Tucows Ltd., Toronto, O.N.
*Provides domain sale and registration, hosting and software download services*
96 Mowat Avenue
Toronto, ON, M6K 3M1
Phone: 1-416- 535-0123
Fax: 1-416- 531-5584

WebServe Canada, Vancouver, B.C.
*Provides domain registration and hosting services*
235 - 1000 Roosevelt Crescent
Vancouver, BC, V7P 1M3
Phone: 1-604-904-0926
Fax: 1-604-904-0927

# Appendix B – Extremist Islamist Groups with Websites in this Study

## Al-Aqsa Martyrs' Brigade

The al-Aqsa Martyrs' Brigades is a militant, Palestinian group tied to Yasser Arafat's Fateh organisation. Formed at the outset of the second Palestinian Intifada (also known as the al-Aqsa Intifada), this group – made up of an unknown number of small cells - aims to drive Israeli settlers from the West Bank, Gaza Strip and Jerusalem, and to establish a Palestinian state. This is an organization which – at the same time as officially rejecting most of the aims of Islamist groups - utilizes Islam as a pretext for their struggle against the Israeli state.

The Al-Aqsa Martyrs' Brigade has conducted shootings and suicide operations against civilian and military targets in Israel and Palestine as well as attacks against Israeli settlements on the West Bank. The group is currently designated as a foreign 'terrorist' group under Canadian law.[26]

## Hamas

Hamas is a militant, Islamist, Palestinian group formed at the beginning of the first Palestinian Intifada in 1987. This group currently forms the democratically elected Government of Palestine.

Hamas – whose 1988 charter calls for Israel's detruction and replacement with an Islamic Palestinian, state - has been responsible for attacks against Israeli civilian and military targets since 1990. Hamas has been one of the main groups involved in the planning and carrying out of a wave of suicide bombings which have struck Israel since the commencement of the second Palestinian Intifada in 2000. The group is currently designated as a foreign 'terrorist' group under Canadian law.[27]

## Hizballah

Hizballah is a militant, Islamist, Lebanese group closely linked to Iran. Formed in 1982 as a response to the Israeli invasion of Lebanon, Hizballah's main objective is the elimination of Israel and the liberation of Jerusalem. This group seeks the establishment of an Islamic state in Lebanon, and is active in the current political process in Lebanon.

Hizballah has been credited with numerous militant attacks on targets in Lebanon, Israel and throughout the world. This group is responsible for the bombing of the US Marine barracks in Beirut in 1983 as well as attacks on Israeli targets in Argentina and Brazil. The group is currently designated as a foreign 'terrorist' group under Canadian law.[28]

## Hizb-ut-Tahrir

Hizb-ut-Tahrir is an Islamist, political group operational in several countries (including Australia, Bangladesh, and Great Britain). This group advocates the establishment of a global Caliphate (a state ruled by a strict interpretation of Islamic Law) and supports the declaration of Jihad against the state of Israel.

Hizb-ut-Tahrir has condoned suicide bombings against Israeli civilian targets. It is currently banned in many countries around the world, but is currently not designated as a foreign 'terrorist' group under Canadian law.[29]

---

[26] Sources: N.A. (2003). Profile: Al-Aqsa Martyrs' Brigades. *Retrieved July 29, 2006 from http://news.bbc.co.uk/2/hi/middle_east/1760492.stm.*

Mannes, A. (2004). *Profiles in terror : The guide to Middle East terrorist organizations.* Toronto: Rowman and Littlefield.

[27] Source: Levitt, M. (2006). *Hamas : Politics, charity, and terrorism in the service of jihad.* New Haven, C.T., U.S.A.: Yale University Press.

[28] Source: Harik, J.P. (2004). *Hezbollah : The changing face of terrorism.* London: I.B. Tauris.

[29] Source: Mannes, A. (2004). *Profiles in terror : The guide to Middle East terrorist organizations.* Toronto: Rowman and Littlefield

# Appendix C

For the last week, I have been doing continuous searches for extremist, Islamist websites operating under Canadian ISP's using the Google, Excite and Yahoo search engines – noting that these are some of the most popular and well known engines and available and would probably yield the best results. This hasn't really proved fruitful... I turned to websites Internet Haganah (www.haganah.us), siteinstitute.org and trackingterrorism.com, sites which track extremist, Islamist websites, to provide some insight into which sites are being operated by which extremist, Islamist groups,. I have found 32 active sites. I have plotted all of my sites on my interactive map and have commenced the process of documenting the movement of these websites in Google earth.

Already, my results are as follows:

32 sites in total active
1 mirror site

### In Edmonton, A.B.:

**Sites affiliated with Hizballah:**
aljarha.org *(Datacentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
al-nour.net *(Datacentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
alrassoul.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
alemdad.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
daralislamia.com *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
maahadalmahdi.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*

### In Kelowna, B.C.:

**Sites affiliated with Hizballah:**
nasrollah.net *(Datacentre: Rackforce Hosting Inc.)*

### In Montreal, Q.C.:

**Sites affiliated with Hizb-ut-Tahrir:**
hilafet.org *(Datacenter: Peer 1 Network)*
al-waie.org *(Datacenter: Peer 1 Network)*
khiafah.net *(Datacenter: Peer 1 Network)*

### In Toronto, O.N.:

**Sites affiliated with the Al Aqsa martyrs brigade:**
fateh.org *(Registrar: Tucows Inc., Service Provider: Tucows, Inc.)*
alwatanvoice.com *(Registrar: Tucows Inc.)*
kataebaqsa1.com *(Registrar: Tucows Inc.)*
palvoice.com *(Registrar: Tucows Inc., Service Provider: Tucows, Inc.)*

**Sites affiliated with Hamas:**
isocg.org *(Registrar: Tucows Inc.)*
alkotla.com *(Registrar: Tucows Inc..)*
aqsavoice.net *(Registrar: Tucows Inc.)*
Islamso.org *(Registrar: Tucows Inc.)*

**Sites affiliated with Hizb ut-Tahrir:**
khilafat.org *(Registrar: Tucows Inc)*
hizb-ut-tahrir.info *(Registrar: Tucows Inc., Service Provider: Tucows, Inc.)*

albadil.edaama.org *(Datacentre: Almina Multimedia)*

**Other sites:**
alhawali.com *(Datacentre: Almina Multimedia)*
islamicawakening.com *(Registrar: Tucows Inc.)*
alsakifah.org *(Registrar: Tucows Inc.)*
tasjeelat.net *(Registrar: Tucows Inc.)*
as-sahwah.com *(Registrar: Tucows Inc.)*
ikhwan.net *(Registrar: Tucows Inc.)*
jamaat-islamia.org -> mirror site for www.islamicawakening.com *(Registrar: Tucows Inc.)*
al-multaqa.net (Registrar: Tucows Inc.)
d3wa.net (Service Provider: Canaca-com Inc.)

**VANCOUVER:**

**Sites affiliated with Hizb ut-Tahrir:**
Khilafah.com *(Datacentre: WebServe Canada, Webhost: WebServe Canada, Service Provider: Web Serve Canada)*

**Other sites:**
jihadunspun.com *(Datacentre: WebServe Canada, Webhost: WebServe Canada, Service Provider: Web Serve Canada)*

I am somewhat surprised at this point to see that there are not more extremist Islamist websites active in Canadian webspace, noting all the American talk over Canada being a "hotbed of Islamic extremism". That said, I've read somewhere that the majority of the world's "terrorist" websites are hosted in the United States anyways, so this seems a bit of hypocrisy on the part of the United States.

Interesting to see how many of these sites are being hosted by Tucows of Toronto... I'll have to take a look to see why this is. The one mirror site I've found, hosted by Tucows (jamaat-islamia.org) points back to Islamicawakening.com, another site hosted by the same company. Tucows is certainly popular with extremist Islamist groups.

So, the Al Aqsa Martyrs brigade, Hamas, Hizballah and Hizb ut-Tahrir and possibly a few other groups all operate pages in Canadian webspace.

# Appendix D

After the first week of monitoring the extremist Islamist websites I have set out to examine, I have now gathered the first evidence that such sites tend to appear, disappear and change location weekly. However, out of 32 sites which were active in week one, 29 of these sites are still active, suggesting the 'coming and going' of these sites is not as pronounced as I had initially thought. Tucows is still hosting the majority of the extremist Islamist websites in Canadian webspace, with 13 sites still active. The reason this might be is because of the combination of two facts:

a) Tucows is one of the world's bigger registrars
b) They do most of their business through international resellers

I intend to call Tucows this week and ask them what their policy is regarding content. This might shed more light on the prevalence of extremist Islamist sites registered by them.

My week two results are as follows:

29 sites in total active
3 sites de-activated
1 mirror site
2 re-directs

### In Edmonton, A.B.:

**Sites affiliated with Hizballah**:
aljarha.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
al-nour.net *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
alrassoul.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
alemdad.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
daralislamia.com *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
maahadalmahdi.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*

### In Kelowna, B.C.:

**Sites affiliated with Hizballah:**
nasrollah.net *(Datacentre: Rackforce Hosting Inc.)*

### In Montreal, Q.C.:

**Sites affiliated with Hizb-ut-Tahrir:**
hilafet.org *(Datacenter: Peer 1 Network)*
al-waie.org *(Datacenter: Peer 1 Network)*
khiafah.net *(Datacenter: Peer 1 Network)*

### In Toronto, O.N.:

**Sites affiliated with the Al Aqsa Martyr's Brigade:**
fateh.org ----> DEACTIVATED
alwatanvoice.com *(Registrar: Tucows Inc.)*
kataebaqsa1.com *(Registrar: Tucows Inc..)*
palvoice.com *(Registrar: Tucows Inc., Service Provider: Tucows, Inc.)*

**Sites affiliated with Hamas:**
isocg.org *(Registrar: Tucows Inc.)*
alkotla.com *(Registrar: Tucows Inc..)*

aqsavoice.net ----> DEACTIVATED
Islamso.org *(Registrar: Tucows Inc.)*

**Sites affiliated with Hizb ut-Tahrir:**
khilafat.org ----> DEACTIVATED --------->

*SITE GIVES FOLLOWING MESSAGE WHEN VISITED:*
*"Warning: mysql_connect(): Access denied for user: 'admin1korg@erbium.webserverdns.com' (Using password: YES) in /home/khilafat/public_html/Connections/DBCon.php on line 9*
*Access denied for user: 'admin1korg@erbium.webserverdns.com' (Using password: YES)"*

hizb-ut-tahrir.info *(Registrar: Tucows Inc., Service Provider: Tucows, Inc.)*
albadil.edaama.org *(Datacentre: Almina Multimedia)*

**Other sites:**

alhawali.com *(Datacentre: Almina Multimedia)*
islamicawakening.com *(Registrar: Tucows Inc.)*
alsakifah.org *(Registrar: Tucows Inc.)*
tasjeelat.net *(Registrar: Tucows Inc.)*
as-sahwah.com *(Registrar: Tucows Inc.)*
ikhwan.net – re-directs to www.hassanalbana.org *(Registrar: Tucows Inc.)*
jamaat-islamia.org -> mirror site for www.islamicawakening.com *(Registrar: Tucows Inc.)*
al-multaqa.net – redirects to www.hassanalbana.org (Registrar: Tucows Inc.)
d3wa.net (Service Provider: Canaca-com Inc.)

## In Vancouver, B.C.:

**Sites affiliated with Hizb ut-Tahrir:**
Khilafah.com *(Datacentre: WebServe Canada, Webhost: WebServe Canada, Service Provider: Web Serve Canada)*

**Other Sites:**
jihadunspun.com *(Datacentre: WebServe Canada, Webhost: WebServe Canada, Service Provider: Web Serve Canada)*

Two sites have become inactive at this point – fateh.org and aqsavoice.net. A third, khilafat.org, gives a strange error message, "Access denied for user: 'admin1korg@erbium.webserverdns.com" – suggesting that – for whatever reason – this site has been shut down and the administrator locked out. Someone might have gotten hold of this site, taken it down and locked the owners out... Not sure yet. Apparently there are hackers who specialize in shutting down these types of websites.

Jamaat-islamia.org remains a mirror site for www.islamicawakening.com. Also, two sites - ikhwan.net and al-multaqa.net - now seem to re-direct to www.hassanalbana.org, a site hosted by _____. Both of these sites appear to fall into the 'other sites' category, as does www.hassanalbana.org. I expected to see more of this re-direction of multiple sites to a single address as this project progresses.

# Appendix E

This week's results proved to be much like those of week two. This week I have seen less site movement, re-direction, etc. however. Again – much to my surprise, most of the sites I started watching at the beginning of week one have remained up and active. None of these appear to be 'changing their skin', so to speak, either – this seems to be flying in the face of claims that extremist, Islamist websites change format as quickly as they change location.

My results for week three are as follows:

29 sites in total active
1 site de-activated
3 Sites inactive
2 mirror sites
1 re-direct

### In Edmonton, A.B.:

**Sites affiliated with Hizballah**:
aljarha.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
al-nour.net *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
alrassoul.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
alemdad.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
daralislamia.com *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
maahadalmahdi.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*

### In Kelowna, B.C.:

**Sites affiliated with Hizballah:**
nasrollah.net *(Datacentre: Rackforce Hosting Inc.)*

### In Montreal, Q.C.:

**Sites affiliated with Hizb-ut-Tahrir:**
hilafet.org *(Datacenter: Peer 1 Network)*
al-waie.org *(Datacenter: Peer 1 Network)*
khiafah.net *(Datacenter: Peer 1 Network)*

### In Toronto, O.N.:

**Sites affiliated with the Al Aqsa martyrs brigade:**
fateh.org ----> INACTIVE
alwatanvoice.com *(Registrar: Tucows Inc.)*
kataebaqsa1.com *(Registrar: Tucows Inc..)*
palvoice.com *(Registrar: Tucows Inc., Service Provider: Tucows, Inc.)*

**Sites affiliated with Hamas:**
isocg.org *(Registrar: Tucows Inc.)*
alkotla.com *(Registrar: Tucows Inc..)*
aqsavoice.net ----> INACTIVE (previous 'access denied' message gone)
Islamso.org *(Registrar: Tucows Inc.)*

**Sites affiliated with Hizb-ut-Tahrir:**

khilafat.org ----> INACTIVE
hizb-ut-tahrir.info *(Registrar: Tucows Inc., Service Provider: Tucows, Inc.)*
albadil.edaama.org - DEACTIVATED

**Other Sites**:
alfirdaws.org ----> NEW SITE *(Registrar: Tucows Inc.)*
alhawali.com *(Datacentre: Almina Multimedia)*
islamicawakening.com *(Registrar: Tucows Inc.)*
alsakifah.org *(Registrar: Tucows Inc.)*
tasjeelat.net *(Registrar: Tucows Inc.)*
as-sahwah.com *(Registrar: Tucows Inc.)*
ikhwan.net – re-directs to www.hassanalbana.org *(Registrar: Tucows Inc.)*
jamaat-islamia.org -> mirror site for www.islamicawakening.com *(Registrar: Tucows Inc.)*
al-multaqa.net - redirects to www.hassanalbana.org (Registrar: Tucows Inc.)
d3wa.net (Service Provider: Canaca-com Inc.)

## In Vancouver, B.C.:

**Sites affiliated with Hizb-ut-Tahrir:**
Khilafah.com *(Datacentre: WebServe Canada, Webhost: WebServe Canada, Service Provider: Web Serve Canada)*

**Other sites:**
jihadunspun.com *(Datacentre: WebServe Canada, Webhost: WebServe Canada, Service Provider: Web Serve Canada)*

At this point, fateh.org, aqsavoice.net and khilafat.org remain inactive. At khilafat.org, the error message from the previous week has disappeared and the site is simply non-existent now. As well, one other site has gone offline - albadil.edaama.org, a hizb ut-tahrir site – has disappeared. This brings to four the number of sites rendered inactive since the start of this project, not a significant amount by any means.

ikhwan.net and al-multaqa.net continue to re-direct to www.hassanalbana.org
while jamaat-islamia.org remains a mirror site for www.islamicawakening.com.

Perhaps the most significant aspect of this week's findings – however – is the appearance of alfirdaws.org (found through another series of searches) registered under Tucows of Toronto and falling under the label of 'other sites'. This brings the total of sites in my study back up to 29. The fact that so many sites affiliated with extremist Islamist groups banned in Canada remain active raises questions as to whether or not ISPs like Tucows are aware of the existence of such sites on their servers. It also means that everything seems pretty static as far as these sites go – in other words, the majority of these sites are apparently not facing any sizable threats to their continued operation.

# Appendix F

This week, I have begun to see that a lot of my prior assumptions – expectations that sites would go up and down at random, major changes in format, the disappearance and re-appearance of different sites – are not really proving prophetic. This week saw the disappearance of a site, but the re-appearance of several others. The majority of sites in my study have remained with their respective registrars, servers and datacentres so far, and have not really gone anywhere.

I suspect that many Canadian ISP's don't really have an interest in shutting these sites down... Either that, or they're just handling too much of a load at one time and are not aware that they are providing services to extremist, Islamist websites. One wonders too about law enforcement here... If Canadian security organizations are aware of the existence of these sites, which they probably are, why are these sites not going down?

My results for week four are as follows:

30 sites in total active
1 site de-activated
2 sites re-activated

### In Edmonton, A.B.:

**Sites affiliated with Hizballah**:
aljarha.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
al-nour.net *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
alrassoul.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
alemdad.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
daralislamia.com *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
maahadalmahdi.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*

### In Kelowna, B.C:

**Sites affiliated with Hizballah:**
nasrollah.net *(Datacentre: Rackforce Hosting Inc.)*

### In Montreal, Q.C.:

**Sites affiliated with Hizb-ut-Tahrir:**
hilafet.org *(Datacenter: Peer 1 Network)*
al-waie.org *(Datacenter: Peer 1 Network)*
khiafah.net *(Datacenter: Peer 1 Network)*

### In Toronto, O.N.:

**Sites affiliated with Al Aqsa Martyrs Brigade:**
fateh.org ----> INACTIVE
alwatanvoice.com *(Registrar: Tucows Inc.)*
kataebaqsa1.com *(Registrar: Tucows Inc..)*
palvoice.com *(Registrar: Tucows Inc., Service Provider: Tucows, Inc.)*

**Sites affiliated with Hamas:**
isocg.org *(Registrar: Tucows Inc.)*
alkotla.com *(Registrar: Tucows Inc..)*
aqsavoice.net ----> INACTIVE
Islamso.org *(Registrar: Tucows Inc.)*

**Sites affiliated with Hizb ut-Tahrir:**
khilafat.org ----> REACTIVATED
hizb-ut-tahrir.info *(Registrar: Tucows Inc., Service Provider: Tucows, Inc.)*
albadil.edaama.org ----> REACTIVATED

**Other Sites:**
alfirdaws.org ----> DEACTIVATED
alhawali.com *(Datacentre: Almina Multimedia)*
islamicawakening.com *(Registrar: Tucows Inc.)*
alsakifah.org *(Registrar: Tucows Inc.)*
tasjeelat.net *(Registrar: Tucows Inc.)*
as-sahwah.com *(Registrar: Tucows Inc.)*
ikhwan.net – re-directs to www.hassanalbana.org *(Registrar: Tucows Inc.)*
jamaat-islamia.org -> mirror site for www.islamicawakening.com *(Registrar: Tucows Inc.)*
al-multaqa.net - redirects to www.hassanalbana.org (Registrar: Tucows Inc.)
d3wa.net (Service Provider: Canaca-com Inc.)

## In Vancouver:

**Sites affiliated with Hizb-ut-Tahrir:**
Khilafah.com *(Datacentre: WebServe Canada, Webhost: WebServe Canada, Service Provider: Web Serve Canada)*

**Other sites:**
jihadunspun.com *(Datacentre: WebServe Canada, Webhost: WebServe Canada, Service Provider: Web Serve Canada)*

In week four, aqsavoice.net and fateh.org remain inactive. Joining these sites on the inactive list is alfirdaws.org, which appeared only last week.

ikhwan.net and al-multaqa.net still re-direct to www.hassanalbana.org – jamaat-islamia.org remains a mirror site for www.islamicawakening.com.

The most significant aspect of week four is that khilafat.org and albadil.edaama.org have once again become active – both of these are sites hosted in Toronto and affiliated with Hizb ut-tahrir. This brings the total number of sites active - out of a total of 32 that I had initially been watching - back up to 30. I will continue to do searches throughout the coming weeks – I have a feeling that there are more extremist Islamist websites being hosted in Canadian webspace, and that there are a firm set of reasons behind the fact that they don't really seem to change position as often as one would assume.

# Appendix G

For the first week since the beginning of this study, there have been no significant changes. No sites have re-appeared or disappeared – neither have there been any new sites.

My results for week five are as follows:

29 sites in total active

3 sites inactive
2 sites re-directing
1 mirror site

### In Edmonton, A.B.:

**Sites affiliated with Hizballah**:
aljarha.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
al-nour.net *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
alrassoul.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
alemdad.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
daralislamia.com *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
maahadalmahdi.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*

### In Kelowna, B.C:

**Sites affiliated with Hizballah:**
nasrollah.net *(Datacentre: Rackforce Hosting Inc.)*

### In Montreal, Q.C.:

**Sites affiliated with Hizb ut-tahrir:**
hilafet.org *(Datacenter: Peer 1 Network)*
al-waie.org *(Datacenter: Peer 1 Network)*
khiafah.net *(Datacenter: Peer 1 Network)*

### In Toronto, O.N.:

**Sites affiliated with Al Aqsa Martyrs Brigade:**
fateh.org ----> INACTIVE
alwatanvoice.com *(Registrar: Tucows Inc.)*
kataebaqsa1.com *(Registrar: Tucows Inc..)*
palvoice.com *(Registrar: Tucows Inc., Service Provider: Tucows, Inc.)*

**Sites affiliated with Hamas:**
isocg.org *(Registrar: Tucows Inc.)*
alkotla.com *(Registrar: Tucows Inc..)*
aqsavoice.net ----> INACTIVE
Islamso.org *(Registrar: Tucows Inc.)*

**Sites affiliated with Hizb ut-Tahrir:**
khilafat.org
hizb-ut-tahrir.info *(Registrar: Tucows Inc., Service Provider: Tucows, Inc.)*
albadil.edaama.org

**Other Sites:**
alfirdaws.org ----> INACTIVE
alhawali.com *(Datacentre: Almina Multimedia)*
islamicawakening.com *(Registrar: Tucows Inc.)*
alsakifah.org *(Registrar: Tucows Inc.)*
tasjeelat.net *(Registrar: Tucows Inc.)*
as-sahwah.com *(Registrar: Tucows Inc.)*
ikhwan.net - re-directs to www.hassanalbana.org *(Registrar: Tucows Inc.)*
jamaat-islamia.org -> mirror site for www.islamicawakening.com *(Registrar: Tucows Inc.)*
al-multaqa.net - redirects to www.hassanalbana.org (Registrar: Tucows Inc.)
d3wa.net (Service Provider: Canaca-com Inc.)

## In Vancouver:

**Sites affiliated with Hizb ut-Tahrir:**
Khilafah.com *(Datacentre: WebServe Canada, Webhost: WebServe Canada, Service Provider: Web Serve Canada)*

**Other sites:**
jihadunspun.com *(Datacentre: WebServe Canada, Webhost: WebServe Canada, Service Provider: Web Serve Canada)*

Fateh.org, aqsavoice.net and alfirdaws.org remain inactive – noteworthy here – however – is a temporary splash page appearing in place of Fateh.org, indicating that "Our server is down for maintenance process, we will come back soon..." and on the bottom of the page, "If your website have website at our server it will come soon, don't worry." Obviously, someone is still in control of this domain name and intends to bring fateh.org back up at some point. The Hizballah site nasrollah.net is now also inactive.

The only other thing worth noting this week is the replacement of what was once the Hamas site aqsavoice.net with a general advertisement page for a range of adult elements, including "Free Girls Naked", "Sex Photo Personal Ads" and "Real Sex in Russia". I'm not sure who is responsible for putting up these ad pages in place of former extremist Islamist websites, but I have witnessed this before in visiting a few addresses of former extremist sites – hosted in the United States – which had been replaced with similar advertisement pages.

# Appendix H

In week six, I have again noticed movement and activity. A few interesting things have happened this week which I have not yet seen. A few sites which were previously re-directing to a certain site have again changed direction and are now pointing to a different site. As well, a few sites have again been de-activated, though surprisingly not at the Tucows server.

As I've said before, though, it really doesn't seem like a significant amount of sites are changing position at all.

My results for week 6 are as follows:

28 sites in total active
3 Sites inactive
2 sites de-activated
1 mirror site
1 site re-directing
1 site no longer re-directing

### In Edmonton, A.B.:

**Sites affiliated with Hizballah:**
aljarha.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
al-nour.net --> DEACTIVATED
alrassoul.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
alemdad.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
daralislamia.com *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
maahadalmahdi.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*

### In Kelowna, B.C:

**Sites affiliated with Hizballah:**
nasrollah.net --> DEACTIVATED

### In Montreal, Q.C.:

**Sites affiliated with Hizb ut-tahrir:**
hilafet.org *(Datacenter: Peer 1 Network)*
al-waie.org *(Datacenter: Peer 1 Network)*
khiafah.net *(Datacenter: Peer 1 Network)*

### In Toronto, O.N.:

**Sites affiliated with Al Aqsa Martyrs Brigade:**
fateh.org ----> INACTIVE
alwatanvoice.com *(Registrar: Tucows Inc.)*
kataebaqsa1.com *(Registrar: Tucows Inc..)*
palvoice.com *(Registrar: Tucows Inc., Service Provider: Tucows, Inc.)*

**Sites affiliated with Hamas:**
isocg.org *(Registrar: Tucows Inc.)*
alkotla.com *(Registrar: Tucows Inc..)*
aqsavoice.net ----> INACTIVE
Islamso.org *(Registrar: Tucows Inc.)*

**Sites affiliated with Hizb ut-Tahrir:**
khilafat.org *(Datacenter: Almina Multimedia)*
hizb-ut-tahrir.info *(Registrar: Tucows Inc., Service Provider: Tucows, Inc.)*
albadil.edaama.org *(Registrar: Tucows Inc.)*

**Other sites:**
alfirdaws.org ----> INACTIVE
alhawali.com *(Datacentre: Almina Multimedia)*
islamicawakening.com *(Registrar: Tucows Inc.)*
alsakifah.org *(Registrar: Tucows Inc.)*
tasjeelat.net *(Registrar: Tucows Inc.)*
as-sahwah.com *(Registrar: Tucows Inc.)*
ikhwan.net – no longer re-directs to www.hassanalbana.org *(Registrar: Tucows Inc.)* – goes to own address
jamaat-islamia.org -> mirror site for www.islamicawakening.com *(Registrar: Tucows Inc.)*
al-multaqa.net - no longer re-directs to www.hassanalbana.org – now redirects to www.ikhwan.net/vb/
d3wa.net (Service Provider: Canaca-com Inc.)

## In Vancouver, B.C.:

**Sites affiliated with Hizb ut-Tahrir:**
Khilafah.com *(Datacentre: WebServe Canada, Webhost: WebServe Canada, Service Provider: Web Serve Canada)*

**Other sites:**
jihadunspun.com *(Datacentre: WebServe Canada, Webhost: WebServe Canada, Service Provider: Web Serve Canada)*

In this week, fateh.org, aqsavoice.net and alfirdaws.org remain inactive. As well, Al-Nour.net and nasrollah.net have become deactivated – both of these are Hizballah affiliated sites.

Again, jamaat-islamia.org remains a mirror site for www.islamicawakening.com. However, ikhwan.net and al-multaqa.net no longer re-direct to www.hassanalbana.org – instead, al-multaqa.net and hassanalbana.org re-direct to ikhwan.net. This is an interesting turns of events, one that I can't really explain.

# Appendix I

I am nearing the end of my two month study (only one week left) and am not feeling like my study has yielded the results I expected. The results which I have seen - a few sites up and down here and there – have been less than dramatic. I did not expect the rapid fluctuation of sites up and down on a daily basis, although neither did I expect that the majority of sites which I've been monitoring would stay up so long.

My results for week seven are as follows:

29 sites in total active
5 sites inactive
1 new site active
1 site no longer hosted by Canadian company
(still registered by Canadian company)

### In Edmonton, A.B.:

**Sites affiliated with Hizballah:**
aljarha.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
al-nour.net --> INACTIVE
alrassoul.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
alemdad.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
daralislamia.com *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
maahadalmahdi.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
almadiscouts.org --- > NEW SITE *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*

### In Kelowna, B.C:

**Sites affiliated with Hizballah:**
nasrollah.net ----→ INACTIVE

### In Montreal, Q.C.:

**Sites affiliated with Hizb ut-Tahrir:**
hilafet.org *(Datacenter: Peer 1 Network)*
al-waie.org *(Datacenter: Peer 1 Network)*
khiafah.net *(Datacenter: Peer 1 Network)*

### In Toronto, O.N.:

**Sites affiliated with Al Aqsa Martyrs Brigade:**
fateh.org ----> INACTIVE
alwatanvoice.com *(Registrar: Tucows Inc.)*
kataebaqsa1.com *(Registrar: Tucows Inc..)*
palvoice.com *(Registrar: Tucows Inc., Service Provider: Tucows, Inc.)*

**Sites affiliated with Hamas:**
isocg.org *(Registrar: Tucows Inc.)*
alkotla.com *(Registrar: Tucows Inc..)*
aqsavoice.net ----> INACTIVE
Islamso.org *(Registrar: Tucows Inc.)*

**Sites affiliated with Hizb ut-Tahrir:**
khilafat.org *(Datacenter: Almina Multimedia)*

hizb-ut-tahrir.info -→ no longer hosted by Canadian company *(Registrar: Tucows Inc..)*
albadil.edaama.org *(Registrar: Tucows Inc.)*

**Other sites:**
alfirdaws.org ----> INACTIVE
alhawali.com *(Datacentre: Almina Multimedia)*
islamicawakening.com *(Registrar: Tucows Inc.)*
alsakifah.org *(Registrar: Tucows Inc.)*
tasjeelat.net *(Registrar: Tucows Inc.)*
as-sahwah.com *(Registrar: Tucows Inc.)*
ikhwan.net – *(Registrar: Tucows Inc.)*
jamaat-islamia.org -> mirror site for www.islamicawakening.com *(Registrar: Tucows Inc.)*
al-multaqa.net – site to redirects to www.ikhwan.net/vb/
d3wa.net (Service Provider: Canaca-com Inc.)

## In Vancouver, B.C.:

**Sites affiliated with Hizb ut-Tahrir:**
Khilafah.com *(Datacentre: WebServe Canada, Webhost: WebServe Canada, Service Provider: Web Serve Canada)*

**Other sites:**
jihadunspun.com *(Datacentre: WebServe Canada, Webhost: WebServe Canada, Service Provider: Web Serve Canada)*

In week 7, al-nour.net, nasrollah.net, fateh.org, aqsavoice.net and alfirdaws.org remain inactive. Fateh.org still has the same splash page representing it as seen in week five – it appears that 'maintenance' is taking longer than expected on the site.

Other than this, one new site has come into being – this is a Hizballah site, almadiscouts.org.

# Appendix J

This the final week of my study. To put it lightly, I have seen a few - but no dramatic – changes in the two month observation period I have undertaken. I suspect there was a lot more going on in this study than I know about hopefully the literature will help to solve some of the ambiguities I've seen in this project.

My results for week eight are as follows:

27 sites in total active
5 sites inactive
2 site(s) deactivated

### In Edmonton, A.B.:

**Sites affiliated with Hizballah:**
aljarha.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
al-nour.net --> INACTIVE
alrassoul.org --> DE-ACTIVATED
alemdad.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
daralislamia.com *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
maahadalmahdi.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*
almadiscouts.org *(Datcentre: Tera-byte.com, Host: Tera-byte.com, Service Provider: Tera-byte.com)*

### In Kelowna, B.C.:

**Sites affiliated with Hizballah:**
nasrollah.net --> INACTIVE

### In Montreal, Q.C.:

**Sites affiliated with Hizb ut-Tahrir:**
hilafet.org *(Datacenter: Peer 1 Network)*
al-waie.org *(Datacenter: Peer 1 Network)*
khiafah.net *(Datacenter: Peer 1 Network)*

### In Toronto, O.N.:

**Sites affiliated with Al Aqsa Martyrs Brigade:**
fateh.org ----> INACTIVE
alwatanvoice.com *(Registrar: Tucows Inc.)*
kataebaqsa1.com *(Registrar: Tucows Inc..)*
palvoice.com *(Registrar: Tucows Inc., Service Provider: Tucows, Inc.)*

**Sites affiliated with Hamas:**
isocg.org *(Registrar: Tucows Inc.)*
alkotla.com *(Registrar: Tucows Inc..)*
aqsavoice.net ----> INACTIVE
Islamso.org *(Registrar: Tucows Inc.)*

**Sites affiliated with Hizb ut-Tahrir:**
khilafat.org *(Datacenter: Almina Multimedia)*
hizb-ut-tahrir.info *(Registrar: Tucows Inc..)*
albadil.edaama.org *(Registrar: Tucows Inc.)*

**Other sites:**

alfirdaws.org ----> INACTIVE
alhawali.com *(Datacentre: Almina Multimedia)*
islamicawakening.com *(Registrar: Tucows Inc.)*
alsakifah.org *(Registrar: Tucows Inc.)*
tasjeelat.net *(Registrar: Tucows Inc.)*
as-sahwah.com *(Registrar: Tucows Inc.)*
ikhwan.net – *(Registrar: Tucows Inc.)*
jamaat-islamia.org -> DE-ACTIVATED
al-multaqa.net – site to redirects to www.ikhwan.net/vb/
d3wa.net (Service Provider: Canaca-com Inc.)

**In Vancouver, B.C.:**

**Sites affiliated with Hizb ut-Tahrir:**
Khilafah.com *(Datacentre: WebServe Canada, Webhost: WebServe Canada, Service Provider: Web Serve Canada)*

**Other sites:**
jihadunspun.com *(Datacentre: WebServe Canada, Webhost: WebServe Canada, Service Provider: Web Serve Canada)*

In this final week, it appears that 27 total sites are still active out of an original total of 32 sites. This is not really what I had envisioned the end result of my project being when I had first started. I had expected – at the outset of my project – to see large fluctuations – I had assumed in the first place that I would find more sites to begin with.

The last week in this observation period is thus only really notable for the amount of sites that still active. Perhaps as a combination of the fact that running an extremist website is not illegal per-se in Canada, and the fact that most Canadian service providers seem to have a high tolerance for extremist websites such as the ones I've observed in my study, nothing there was no significant decrease in the amount of sites I observed in my study.

At the end of this week, al-nour.net, nasrollah.net, fateh.org, aqsavoice.net and alfirdaws.org remain inactive. Alrassoul.org and Jamaat-islamia.org are also inactive as of this week.

I feel at this point that – despite the unspectacular results of my research, something can be said about the fact that so many sites belonging to groups banned in Canada continue to operate. It may – in fact – have to do with the security situation in Canada. Perhaps it is more beneficial to leave these sites online then to take them down – not solely for the fact that potential site visitors can be monitored (by law enforcement) by doing so, but even more so that – if Canadian law enforcement and intelligence agencies leave such sites up – they may in fact be fomenting a relationship in which Canadian service providers work at the behest of Canada's law enforcement community. This theory definitely merits more investigation.

All in all, a worthwhile study despite the unspectacular results.

## WORKS CITED


Abbey, A.D. (2004). Virtual Jihad. *Jerusalem Post, May 7, 24.*

Ariza, L.M. (2006). Virtual Jihad. *Scientific American, 294, 18-21.*

Arquilla, J., Ronfeldt, D. & Zanini, M. (2000). Information Age Terrorism. *Current History, 99, 179-185.*

Australian Free Press (2006). US Net Lead Slips. *The Australian, 152, 32.*

Becher, K. (n.d.). IISS/CEPS European Security Forum. *Retrieved July 2, 2006 from http://www.eusec.org/heisbourg1a.htm.*

Bell, S. (2005). *Cold terror : How Canada nurtures and exports terrorism around the world.* Toronto: Wiley.

Booth K. & Dunne, T. (2002). *Worlds in collision: Terror and the future of global order.* New York: Palgrave MacMillan.

Brisard, J.C. (2005). *Zarqawi: The new face of Al-Qaeda.* New York: Other Press.

Bunt, G. (2000). *Virtually Islamic: Computer-mediated communication and cyber Islamic environments.*

Bunt, G. (2003). *Islam in the digital age: E-Jihad, online fatwas and cyber Islamic environments.* London: Pluto Press.

Burnett, R. & Marshall, D. (2003). *Web theory: An introduction.* London: Routledge
Cleaver, H. (1997). The Zapatista Effect: The Internet and the Rise of an Alternative Political Fabric. *Journal of International Affairs, 51, 621-641.*

Center for Strategic and International Studies (1998). *Cybercrime, cyberterrorism-cyberwarfare: Averting an electronic Waterloo.* Washington: CSIS Press.

Casciani, D. & Sakr, S. (2006). The battle for the mosque. *Retrieved July 8, 2006 from* http://news.bbc.co.uk/1/hi/uk/4639074.stm.

Claburn, T. (2006). Ready for you Close-up? Google Goes Hi-Res. *Information Week, 1094, 18.*

Clark, C. (2005). Canadians Want Strict Security: Poll. *Globe and Mail, August 11, c7.*

Clarke, D. (2004). *Technology and Terrorism.* Brunswick, N.J., U.S.A.: Transaction.

Coll, S. & Glasser, B. (2005). Terrorists Turn to the Web as a Base of Operations. *Retrieved June 20, 2006 from http://www.washingtonpost.com/wp-dyn/content/article/2005/08/05/AR 2005080501138.html*

Conway, M. (2002). Reality Bytes: Cyberterrorism and the Terrorist 'Use' of the Internet. *Retrieved June 7, 2006 from www.firstmonday.org/issue7_11/conway/index.html*

Daniels, R.J., Macklem, P., & Roach, K. (2001). *The security of freedom: Essays on Canada's anti-terrorism Bill.* Toronto: University of Toronto Press.

Dartnell, M.Y. (2006). *Insurgency online: Web activism and global conflict.* Toronto: University of Toronto Press.

Denning, D.E. (2000). Cyberterrorism - Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives. *Retrieved June 14, 2006 from* http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.

Di Justo, P. (2002). How Al-Qaida Site was Hacked. *Retrieved August 4, 2006 from www.wired.com/news/culture/0,1284,54455,00.html*

Ehrlich, R. & Dworzecka, M. (1998). On the Road to Damascus: Technology, Fear and Fear of Technology. *Journal of College Science Teaching, 27, 179-182.*

Elchoubaki, Amr (2006). The New Face of Terror. *Retrieved September 15, 2006 from http://weekly.ahram.org.eg/2006/794/op33.htm* .

Ellsmore, N. (2002). Cyber-Terrorism in Australia: The Risk to Business and a Plan to Prepare. *Sift Pty Ltd, Dec 9, 1-25.*

Embar-Seddon, A. (2002). Cyberterrorism: Are we Under Siege? *American Behavioural Scientist, 45, 1033-1043.*

Filkins, D., Jehl, D., Lichtblau, E., & Hulse, C. (2004). The Struggle for Iraq: Revenge Killing. *New York Times, May 12, a. 11.*

Galloway, A. (2004). *Protocol: How control exists after decentralization.* Cambridge, M.A., U.S.A.: MIT Press.

Gomes L. (2002). Digital Pearl Harbor Is More Marketing Ploy Than a Real Threat. *Wall Street Journal, December 16, b. 1.*

Green, J. (2002). The Myth of Cyberterrorism. *Washington Monthly, November, 8-13.*

Gunaratna, R. (2003). *Terrorism in the Asia Pacific: Threat and response.* Singapore: Eastern Universities Press.

Hannemyr, G. (2003). The Internet as Hyperbole: A Critical Examination of Adoption Rates. *The Information Society, 19, 111-121.*

Hartman, A. (2002). The Politicization of Terror: September 11 and American Historical Selectivity. *Retrieved June 7, 2006 from http://www.zmag.org/ZMag/articles/dec01hartman.htm.*

Herman, E.S. & Chomsky, N. (1988). *Manufacturing consent: The political economy of the mass media.* New York: Pantheon.

Hoffmann, B. (2004). Redefining Counterterrorism: The Terrorist Leader as CEO. *Rand Review, 40, 8-20.*

Hoffman, D.L., Novak, T.P. & Venkatesh, A. (2004). Has the Internet Become Indispensable? *Communications of the ACM, 47, 37-42.*

Hoffman, L. (1999). U.S. Opened Cyber-War During Kosovo Flight. *Washington Times, October 24, C1.*

House of Commons of Canada. (2005). *Bill C-74: An act regulating the telecommunications facilities to facilitate the lawful interception of information transmitted by means of those facilities and respecting the provision of telecommunications subscriber information.* Retrieved June 17, 2006 from http://parl.gc.ca/pdf/38/1/parlbus/chambus/house/bills/government/c-74_1.pdf.

Huey, L. & Rosenberg, R.S. (2004). Watching the Web: Thoughts on Expanding Police Surveillance Opportunities under the Cybercrime Convention. *Canadian Journal of Criminology and Criminal Justice, 46, 597-606.*

Hyland, S. (2005). *Community building in the twenty-first century.* Washington: School of American Research.

Internet Statistics. (1998). *Retrieved June 4th, 2006 from www.dns.net/andras/stats.html*

Jones A. (2005). Cyber Terrorism: Fact or Fiction. *Computer Fraud and Security 8, 4-7.*

Jones, D.M. (2004). *Globalization and the new terror: The Asia Pacific Dimension.* Northampton, M.A., U.S.A: Edward Elgar.

Kirkland, M. (2000). Major Attack on U.S. System may be Inevitable. *United Press International, October 19, n.p.*

Klotz, R.J. (2004). *The politics of internet communication.* Toronto: Rowman and Littlefield.

Kristof, N.D. (2005). Terrorists in Cyberspace. *New York Times, December 20th, A31.*

Lal, V. (2003). Terror and its networks: Dissapearing trails in cyberspace. *Retrieved September 6th, 2006 from http://www.nautilus.org/archives/virtual-diasporas/paper/Lal.html.*

Laquer, W. (1977). *Terrorism.* London: Weidenfeld & Nicholson.

Last, M. (2005). *Fighting terror in cyberspace.* Hackensack, NJ, U.S.A: World Scientific.

Leistyna, P. (2005). *Cultural studies: From theory to action.* Malden, M.A., U.S.A: Blackwell.

Lezner, R. & Vardi, N. (2004). The Next Threat. *Forbes, 174, 70-76.*

Lia, B. (2005). *Globalization and the future of terrorism.* New York: Routledge.

Mogull, R. (2002). Cyberattacks and Cyberterrorism: What Private Business Must Know. *Retrieved May 17, 2006 from http://www.gartnerg2.com/qa/qa-0902-0091.asp*

Morgan, D. (2006). U.S. seen balking at challenge by Islamist Web. *Retrieved September 7th, 2006 from http://news.yahoo.com/s/nm/20061028/wr_nm/security_internet_islamists_dc*

Mullins, W.C. (1997). *A sourcebook on domestic and international terrorism : An analysis of issues, organizations, tactics, and responses.* Springfield, Ill., U.S.A: C.C. Thomas.

M.J. (1996). Making the Internet Buckle Up. *Western Report 23, 32-33.*

N.A. (2004). Al-Qaida offers do-it-yourself terror training. *Retrieved June 28, 2006 from http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=36459.*

N.A. (2004). Attack on London 'inevitable'. *Retrieved July 2, 2006 from* http://www.theage.com.au/articles/2004/04/19/1082326119414.html?from=storyrhs &oneclick=true.

N.A. (2004). Canadian Security Intelligence Service Act. *Retrieved June 4, 2006, from http://www.csis.gc.ca/en/publications/act/csisact.asp.*

N.A. (2004). Combating Terrorism Through Technology. *Retrieved June 20, 2006 from http://www.nato.int/docu/review/2004/issue3/english/military.html.*

N.A. (2000). Cyber Attack: The National Protection Plan and its Privacy Implications. *Retrieved June 26, 2006 from www.gwu.edu/~dhs/congress/feb1_00.html.*

N.A. (2002). Report No. 2001/11: Information Operations. *Retrieved June 20. 2006 from http://www.csis.gc.ca/en/publications/perspectives/200111.asp.*

N.A. (2001). Royal Assent of Bill C-36, The Anti-Terrorism Act. *Retrieved June 20, 2006 from http://www.canada.justice.gc.ca/en/news/nr/2001/doc_28217.html.*

N.A. (2004). Testimony of Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI, Before the Senate Judiciary Subcommittee on Terrorism, Technology and Homeland Security, February 24, 2004. *Retrieved June 20, 2006 from http://www.fbi.gov/congress/congress04/lourdeau022404.htm.*

N.A. (N.D.) Tucows Over 4 Million Domain Names Registered. *Retrieved July 10, 2006 from http://www.thehostingnews.com/printout192.html*

Nacos, B. (2006). *Terrorism and counterterrorism: Understanding threats and responses in the post 9/11 world.* New York: Pearson.

Nassar, J.R. (2004). *Globalization and terrorism: The migration of dreams and nightmares.* Toronto: Rowman and Littlefield.

National Research Council, U.S. (1991). *Computers at risk : safe computing in the information age.* Washington: National Academy Press.

Naughton, J. (N.D.) Contested Space: The Internet and Society. *21st Century Trust, 1-27.*

O'day, A. (2004). *Cyberterrorism.* London: Ashgate.Olivero, A. (1998). *The state of terror.* Albany: State University of New York Press.

Perry, A. & Sindayen, N. (2001, June). Getting out the message. *Time Europe, 157, 84-87.*

Poulsen, K. (2001). Cyber Terror in the Air. *Retrieved June 28, 2006, from http://www.securityfocus.com/columnists/6.*

Preston, G. (2004). *How the internet works.* Indianapolis, Ind., U.S.A: Que.

Reynalds, J. (2006). *War of the web: Fighting the online Jihad.* Torrance, C.A., U.S.A.: World Ahead Publishing.

Sageman, M. (2004). *Understanding Terror Networks.* Philadephia: University of Pennsylvania Press.

Schwartau, W. (1991). *Terminal compromise.* New York: Interpact.

Shane, S. (2003). The Web as al-Qaida's safety net. *Retreieved September 6th, 2006, from http://www.marylandweather.com/news/weather/site/bal-te.journal28mar28,0,89984.column.*

Shephard, M. (2006). How Internet monitoring sparked a CSIS probe. *Retrieved June 17, 2006 from* http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_PrintFriendly&c=Article&cid=1149285034044&call_pageid=976163513378.

Swartz, J. (2005). Terrorists use of Internet Spreads. *USA Today, Feb 21, 03b.*

Thackrah, J.R. (1987). *Encyclopaedia of terrorism and political violence.* London: Routledge and Kegan Paul Ltd.

Tremayne, S. (2006). Not all Muslims are Luddites. *Anthropology Today, 22, 1-2.*

Tuman, J.S. (2003). *Communicating terror : The rhetorical dimensions of terrorism.* Thousand Oaks, C.A., U.S.A.: Sage.

Van de Donk, W., Loader, B.D., Nixon, P.G. & Rucht, D. (2004). *Cyberprotest: New media, citizens and social movements.* London: Routledge.

Van Rijn, N. (2006). Plot began in chat room. *Retrieved July 2, 2006, from* http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_PrintFriendly&c=Article&cid=1149460818073&call_pageid=968332188492.

Vegh, S. (2002). Hacktivists of Cyberterrorists? The Changing Media Discourse on Hacking. *Retrieved July 2, 2006 from http://www.firstmonday.org/issues/issue7_10/vegh/.*

Wallace, B. (2001). Cyber terrorism expected to emerge as new threat: Computers could turn into battlegrounds. *San Antonio Express-News, November 16, p. 3A.*

Walters, P. (2005). Laws Look to 21st Century. *The Australian, July 23, 11.*

Weimann, G. (2006). *Terror on the internet: The new arena, the new challenges.* Washington, United States Institute of Peace.

Weinberg, L. (2005). *Global terrorism: A beginners guide.* Oxford: One World.

Yagil, L. (2002). *Terroristes et internet : La cyberguerre.* Montreal: Trait D'union.