

INTERNET-SAVVY U.S. AND MIDDLE EASTERN EXTREMIST GROUPS

Edna Reid and Hsinchen Chen[†]

Using an interdisciplinary perspective, this study provides a hyperlink and content analysis of 44 U.S. domestic and 40 Middle Eastern extremist groups' websites to analyze their use of computer-mediated communication (CMC) to support collective identity and mobilization. The findings contrast Middle Eastern extremist groups' use of the Internet to develop virtual communities and support their virtual command/control operations with the U.S. domestic groups' focus on communication and ideological indoctrination. Finally, the results suggest that the usages of CMC are underpinned by the geographical reach of extremist groups' campaign as well as their strategic goals, ideologies, needs, and political legitimacy, driving the various groups to use CMC in a distinctive manner.

The last decade has seen the rise of extremist social movement groups' use of the Internet as a social space and tool for communication, psychological warfare, fundraising, and global expansion (Diani 1999). Because of environmental challenges (i.e., technical, legal, and political), research about the groups' cyber activities is only in the infancy stage. Technical challenges include problems in identifying and locating the groups' web artifacts (e.g., web sites, discussion forums, videos, etc.), the sheer volume of artifacts, the diversity of languages used, the dynamic nature of some websites, and the limited methods available for analyzing the groups' multilingual and multimedia artifacts.

Information scientists, primarily concerned with the collection, classification, and dissemination of information, have designed methods, tools, and research studies that focus on overcoming the challenges. Since social scientists might be interested in, yet unaware of, the work done by information scientists, this article presents methods and data that can be used to analyze extremist groups' Internet activities. We compare U.S. domestic and international extremist groups' use of computer-mediated communication (CMC) to support their respective campaigns. CMC involves people shaping media for a variety of purposes (December 1997). Internet-based CMC tools, such as websites, discussion forums, blogs, and chat sessions, have been used by social movement groups to support public and private communications (Diani 1999; Burris, Smith, and Strahm 2000; Gerstenfeld, Grant, and Chiang 2003).

INTERNET-SAVVY EXTREMIST GROUPS

Before we turn to our research questions, we begin with a discussion of trends in extremist groups' use of the Internet. Researchers and commentators agree that during the 1990s the world experienced a new phase of terrorism that is characterized by shifts in organization structures, ideologies, tactics, and communication strategies (Bergesen and Han 2005; Jenkins 2004). These include a shift in form, from hierarchical toward network organization structures with members from various nationalities, geographical locations, and virtual networks; an ideological shift from political to more religious motives; a tactical shift from convenient targets

[†] Send all correspondence to Edna Reid, Department of Library Science, Clarion University, 840 Wood Street, Clarion, PA 16214.

toward a global dispersion of targets; a organizational shift from centralized command and control toward virtual command and control; and, finally, a shift in communication strategies from reliance on media outlets toward Internet-savvy groups that create their own “terrorist news networks” (Bergesen and Han 2005; Jenkins 2004).

The Internet-savvy extremist groups can be viewed as learning organizations that are able to draw on their awareness of the global situation to adapt their behavior in innovative ways based upon lessons learned (Forest 2006). For example, Lia and Heggerhammer show how jihadi strategic documents were used to issue virtual commands to disrupt the 2004 Spanish elections. These groups use websites, private discussion boards, and blogs in which they create their own news, provide real-time interpretations of the popular press, and speak directly to millions of people (e.g., members, supporters, enemies, media) via their computers (Jenkins 2004). The Internet allows the groups to bypass the traditional communication channels and gatekeepers of information.

According to estimates, the U.S. domestic extremist groups (e.g., Knights of the Ku Klux Klan, National Alliance) have created hundreds of websites, listservs, chat sessions, and discussion forums that range in size from a few pages to vast collections of reports, multimedia, and e-commerce merchandise (Chaudhry 2000; Levin 2002; SPLC 2004). However, the extensive media coverage of Middle Eastern groups’ Internet usage highlights the explosive growth in their websites and increased sophistication (Coll and Glasser 2005; Kelley 2002; Lipton and Lichtblau 2004). Estimates for the number of Middle Eastern extremist groups’ websites and discussion forums place these artifacts in the thousands (Weimann 2004; 2006). They range from simple, text-based pages with a few paragraphs to sophisticated sites with multimedia, discussion forums, chat rooms, tutorials, and extensive digital libraries (ISTS 2003; Reid, Zhou, Lai, Sageman, Weiman, and Chen 2005; Thomas 2003; Tsfaty and Weimann 2002). Some web pages are posted in multiple languages to appeal to different audiences: members, current and potential supporters, international publics, and enemy publics (e.g., citizens of the states targeted by these movements) (Bunt 2004; Chen, Qin, Reid, Chung, Zhou, Zi, Lai, Bonillas, and Sageman 2004; Weimann 2004; Corman and Schiefelbein 2006). The abundance of primary materials available from the groups’ websites, videos, discussion forums are underutilized by the research communities and policy makers (International Crisis 2006). Because these materials shed light on the groups’ operations, levels of coordination, and shifts in tactics and operations, they can be used in content, discourse, social network, and frame analysis to answer fundamental questions.

The first question should respond to the call by social scientists for more systematic studies that apply theoretical and methodological approaches (e.g., hyperlink, social network analysis) to explore groups’ utilization of the web to form virtual online communities (Burris, Smith, and Strahm 2000; Tateo 2005). For instance, how have extremist groups used the web and CMC to form online communities? The Burris et al. (2000) study used social network analysis and found that web hyperlink structure appear to provide a reasonably accurate representation of the white supremacy groups’ interorganizational structures (Tateo 2005; Zhou, Reid, Quin, Chen, and Lai 2005). They also found that Internet usage helped to create an international virtual community of extremists. Although the analysis of U.S. domestic groups’ use of the Internet has been an area of concern for social scientists (see the review of studies in Zhou et al. 2005), researchers seldom investigate web usage patterns comparing U.S. domestic and international groups.

METHOD AND DATA

We used an integrated quantitative and qualitative methodology to address the following questions: (a) How have extremist groups’ used the web infrastructure and CMC to form web communities?; (b) How do U.S. domestic and Middle Eastern groups use CMC to support

their campaigns?; and (c) What are the differences in the CMC usage between the U.S. domestic and Middle Eastern groups?

We used web mining methodology in tandem with hyperlink and content analysis to analyze the U.S. domestic and Middle Eastern extremist groups' websites. The Middle Eastern extremist groups were chosen because their use of the web has become so potent and important not only for achieving their aims but also for networking their sympathizers. Web mining is the extraction and discovery of potentially useful patterns and implicit information from web artifacts, e.g., websites, discussion forums, and blogs (Galeas n.d.).

The methodology includes three components: constructing a testbed of U.S. domestic and Middle Eastern extremist groups' websites; conducting web hyperlink mining (henceforth referred to as hyperlink analysis) to visualize the groups' web communities; and conducting web content mining (henceforth referred to as content analysis) to discover and compare the group's CMC usages. The testbed construction approach is described in studies by Zhou et al. (2005) and Reid et al. (2005). Several automated processes were applied to both the U.S. domestic and Middle Eastern extremist groups. In several ways, the identification of seed Universal Resource Locator (URL) procedure is similar to Gerstenfeld, Grant, and Chiang's (2003) content analysis of 157 U.S. domestic extremist groups' websites, where they used several nonprofit watchdog organizations and Yahoo's categories, "white pride and racialism."

Testbed of Websites

For the U.S. domestic collection, seed URLs were identified in December 2003 from the Southern Poverty Law Center (SPLC) and Anti-Defamation League (ADL) websites and the Google directory. SPLC is one of the leading watchdog organizations in tracking white supremacist activity (Sharpe 2000: 605). A total of 97 URL addresses were deemed relevant for the U.S. domestic groups. We downloaded all the web documents from the identified websites. We selected the largest websites to form a subset of 44 websites, representative of the U.S. domestic extremist groups. table 1 provides a summary of the U.S. domestic extremist groups' sample. In table 1, the first column identifies the group's category, which is based on our schematic diagram of U.S. domestic groups' movements and ideologies on the Internet. We also identified 40 URLs that are organized by categories based on our schematic diagram of ideologies and movements associated with Middle Eastern extremist groups. Table 1 also provides a summary of the Middle Eastern groups sample. For example, the Sunni¹ branch of Islam has several ideologies, such as the Salafi² that is supported by movements including the Afghan fighters, and extremist groups (e.g., al Qaeda and Islamic Jihad).

Table 1. Sample of U.S. Domestic and Middle Eastern Extremist Groups

<i>U.S. Domestic Groups</i>	<i>No. of Websites</i>	<i>Examples of Group</i>
Black Separatist	2	Nation of Islam
Christian Identity (CI)	13	Kinsman Redeemer Ministries
Ecoterrorism/Animal Rights	1	Earth Liberation Front (ELF)
Militia	8	Michigan Milita
Neoconfederate	4	Texas League of the South
Neo-Nazi	9	American Nazi Party
White Supremacy	7	Ku Klux Klan (KKK)
<i>Total</i>	44	
<i>Middle Eastern Groups</i>	<i>No. of Websites</i>	<i>Examples of Group</i>
Sunni	19	Al Qaeda
Shi'a	5	Hizbollah
Secular	16	Al-Aqsa Martyr's Brigades
<i>Total</i>	40	

Hyperlink Analysis

The second methodological component is hyperlink analysis. The goal here is to visualize and analyze the groups' Web communities and interorganizational relationships. Hyperlinks between websites are a promising new type of data that can be mined to identify hidden communities and important cues for estimating the content similarities of any website in a collection (Park and Thelwall 2001). We employed these cues to confirm our initial manual website classification according to ideological categories. This involves calculating a similarity measure between all pairs of websites in our collection. In addition, a hyperlink is weighted proportionally to how deep it appears in the website hierarchy. We validated the results using a procedure described in Tateo's (2005) analysis of Italian rightwing extremist websites.

Content Analysis

Content analysis is the third component of our method. Using the resource mobilization theory (Langman and Morris 2002; Diani 1999), we developed a coding scheme for analyzing the content of websites and identifying groups' CMC usages to support resource mobilization. Table 2 provides a summary of the ways that extremist groups use CMC to support their resource mobilization tasks such as enhancing communication and increasing funding.

The content analysis scheme uses CMC usage processes (e.g., communications) to identify the types of resources needed for mobilization (Gustavson and Sherkat 2004; Weimann 2004) and recommended by domain experts. Each process is composed of resources that are assigned weights based on the richness of media. For example, communication is a process

Table 2. How CMC Supports Extremist Groups

<i>Processes</i>	<i>Web Features (Preece 2000)</i>	<i>CMC Supports</i>
Enhance communication (Becker 2005; Crisis 2006; Weimann 2004, 2006)	<ul style="list-style-type: none"> ▪ Synchronous (chat, video conference, multiuser dungeons/MUDs) ▪ Asynchronous (email, bulletin board, listserv, newsgroup) 	<ul style="list-style-type: none"> ▪ One-to-one, one-to-many communications ▪ Composing, sending and receiving messages ▪ Searches for messages, information, people ▪ Maintaining anonymity ▪ Maintaining virtual communities
Increase fundraising (ISTS 2003; Weimann 2004, 2006)	<ul style="list-style-type: none"> ▪ Hyperlinks to other resources ▪ Payment instruction ▪ E-commerce application 	<ul style="list-style-type: none"> ▪ Publicizing need for funds ▪ Providing traditional & online payment options ▪ Expanding funding and money laundering operations globally
Share ideology and propaganda (Gustavson and Sherkat 2004; Weimann 2004, 2006)	<ul style="list-style-type: none"> ▪ Accessible ▪ Directory for documents ▪ Hyperlinks ▪ Navigation support ▪ Search, browsable index 	<ul style="list-style-type: none"> ▪ Posting resources in multiple languages ▪ Providing links to forums, videos and other resources ▪ Using websites as online clearinghouse for groups
Provide for recruitment and training opportunities (ISTS 2003; Weimann 2004, 2006)	<ul style="list-style-type: none"> ▪ FAQ, alerts ▪ Interactive services (e.g., cartoons, games, animated maps, e-commerce) ▪ Multimedia (videos, audios) ▪ Online registration process 	<ul style="list-style-type: none"> ▪ Building massive and dynamic online libraries ▪ Hosting martyrs stories, speeches, recruitment resources ▪ Using flashy logos, banners, cartoons to appeal to different audiences
Overcome environmental challenges from law enforcement and military (Coll and Glasser 2005; Kelley 2001)	<ul style="list-style-type: none"> ▪ Anonymous email accounts ▪ Downloadable encryption software ▪ Email security ▪ Password protected or encrypted services ▪ Virus spreading ▪ Stenography 	<ul style="list-style-type: none"> ▪ Moving websites to different servers (server hopping to protect the site and make it difficult to find and shut down) ▪ Sending encrypted messages via email, forums, or posting on websites ▪ Attach viruses to files to set booby traps

that is composed of resources such as email, telephone, online feedback forum, and multimedia (e.g., video, audio). The appendix summarizes the coding scheme that includes eight CMC processes. The processes are categorized into two groups: (a) common CMC usages (e.g., communications) that are frequently cited in studies (Burris et al. 2000; Whine 1997; Conway 2005; Weimann 2004; 2006); and (b) other, more elaborated, usages. The common usages by Middle Eastern extremist groups are information provision, financing, networking, recruitment, and information gathering (Conway 2005). Other usages such as virtual community and virtual command and control indicate that extremist groups have expanded their requirement for CMC (ISTS 2004; SITE 2004; Weimann 2004). Virtual command and control refers to the trans-mission of ideas, suggestions, or instructions through public and private CMC channels to persons or organizations who, in turn, may be encouraged to act on those ideas and sugges-tions independently (Dishman 2005). Examples include messages by Osama bin Laden that are broadcasted in the media, political reports on potential targets circulated on the web, videos by al Zaraqawi posted on websites, and instructions distributed via discussion forums (SITE 2004).

To ensure the coding scheme's reliability, four research students coded randomly selected U.S. domestic extremist groups' websites in our testbed collection. The average Cronbach's alpha reliability score of 0.807 was obtained and reported in an earlier study (Zhou et al. 2005: 48). In 2005, two students translated and coded Middle Eastern extremist groups' (Arabic language) websites in our testbed collections. They also found high reliability scores for the Middle Eastern sites (Cronbach's alpha = 0.83).

The differences of mean values of CMC processes between the U.S. and Middle Eastern groups were obtained using t-tests. Finally, a classification system was constructed by mapping the different extremist groups' clusters onto a two-dimensional system based on the cluster's CMC usages and geographic reach. This integrative visual tool could be helpful for understanding of the strategic intent, collective capabilities, and environmental constraints that drive the groups in the clusters to use CMC in a distinctive manner.

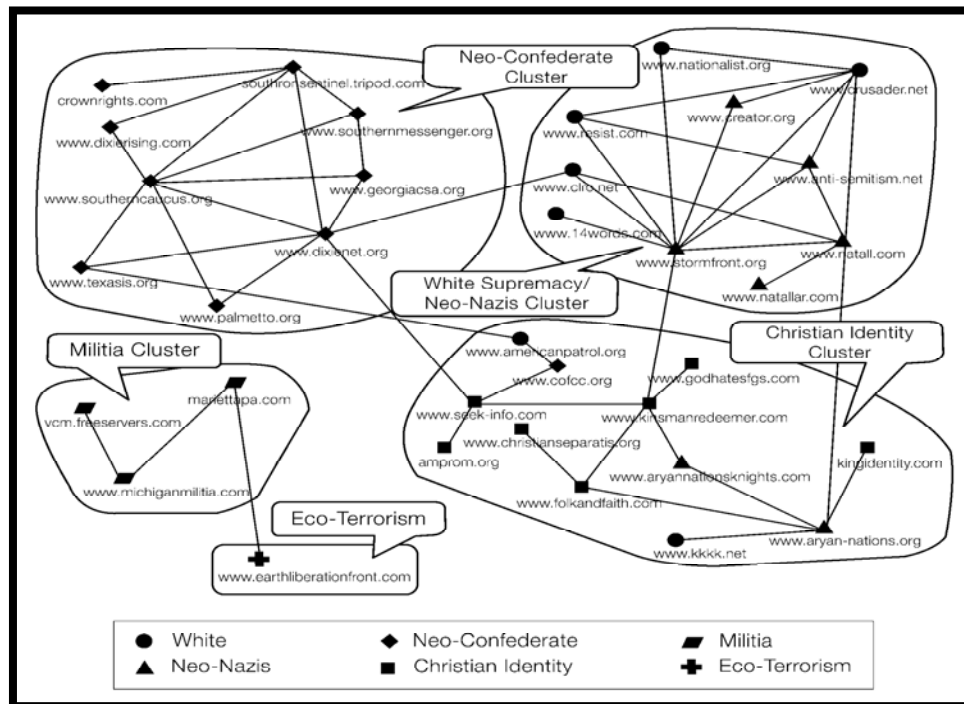
RESULTS

The findings indicate that the hyperlink and content analysis of 44 U.S. domestic and 40 Middle Eastern (Arabic language) extremist groups' websites supported the identification and analysis of the groups' web communities and their CMC usage patterns. The sample websites range from basic U.S. domestic groups' websites to sophisticated Middle Eastern groups' multilingual sites with extensive digital libraries, multimedia collections, and password protected discussion forums embedded in some websites.

Online Hyperlinked Communities of U.S. Domestic Groups

In addressing the first research question about how groups used the Web to form online communities, we used hyperlink analysis to look at the extremist groups' interorganizational relationships. Figure 1 displays the hyperlinked networked clusters for five communities (neo-confederate, white supremacy/neo-Nazi, Christian identity (CI), militia, and ecoterrorism clusters) identified from the U.S. domestic extremist groups.³

In figure 1, the neoconfederate cluster in the top left corner consists mainly of sites espousing a separatist ideology to establish an independent state in the southern U.S. The cluster shares white supremacist ideas with other racist organizations such as the Ku Klux Klan (KKK). The white supremacy/neo-Nazi cluster in the network's top right corner includes the Stormfront and the White Aryan Resistance, and the National Alliance, as an overt neo-Nazi site. The bottom right corner identifies a cluster of primarily Christian identity

Figure 1. Web Hyperlinked Communities of U.S. Domestic Extremist Groups

(CI) websites. The CI cluster includes some neo-Nazi and white supremacist sites. It was difficult to make a clear distinction between Christian identity and white supremacy/neo-Nazi groups, which is consistent with earlier research findings (Burris et al. 2000; Gerstenfeld et al. 2003; Gustavson and Sherkat 2004). The clusters espouse white nationalism and separatism.

In figure 1, there are only a few hyperlinks connecting the neoconfederate, the Christian identity, and the white supremacy/neo-Nazi clusters. Prominent websites linked the three clusters together. For example, the Klan is represented by Stormfront (www.stormfront.org) in the white supremacy/neo-Nazi cluster, and the Christian Identity cluster is represented by the Aryan Nations (www.aryan-nations.org, used as the ego in Gustavson and Sherkat's, 2003 network study). The neoconfederate cluster contains the Dixie Net (www.dixienet.org) website, a popular site for discussions of separation of races (Burris et al. 2000), which is the node that links both the white supremacy and Christian identity clusters.

Stormfront.org is an online information hub that hosts discussion forums and web pages from a variety of groups. As a central node of the white supremacist networks, Stormfront.org maintains ties to other network members, may indirectly controls resource distribution for the movements, and serves as a crucial intermediary between otherwise unlinked sites (Burris et al. 2000). Other researchers say that sites, such as Stormfront.org, support the "lone wolf" or leaderless resistance⁴ strategy that encourages individuals to go out and act on their own (Chaudhry 2000; Damphouse 2004; Levin 2002). The Internet is important in the leaderless resistance strategy because it allows individuals to keep abreast of events and remain a part of a larger movement, even though such individuals do not attend meetings or put their names on membership lists (Levin 2002).

Figure 1 also shows two isolated communities in the network's bottom left corner: the Militia and ecoterrorism clusters. These communities have distinct interests and ideologies. This result agrees with Burris et al. (2000) who found no bridges between the white supremacist movements and the militia. To validate the clustering, the local density of each cluster

was calculated and compared to the overall density of the network. In hyperlink analysis, density indicates the overall level of network integration and reflects how the websites are connected to each other in an overall network (Park and Thelwall 2003). The local densities, such as 0.42 for the white supremacy/neo-Nazi and 0.41 for the neoconfederate clusters, are sufficiently higher than the overall network density (0.08) to indicate valid clustering.

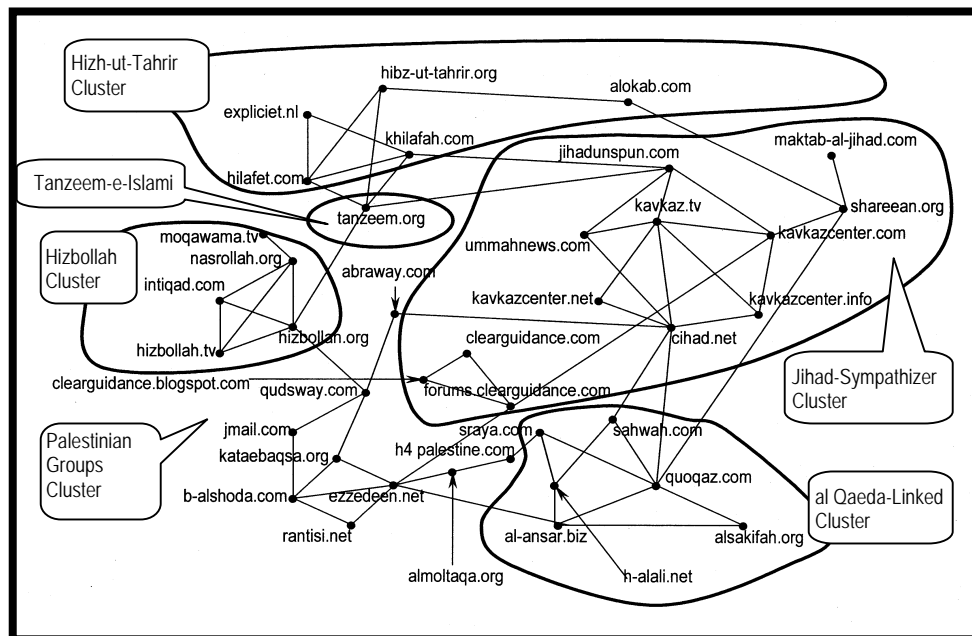
Online Hyperlinked Communities of Middle Eastern Groups

Although a clear distinction among most of the U.S. domestic clusters was difficult to establish, the distinctiveness of Middle Eastern extremist groups' online communities is more easily discerned. Figure 2 identifies six extremist group clusters: Hizbollah, Tanzeem-e-Islami (one site only), Hizb-ut-Tahrir, Jihad sympathizers, al Qaeda-linked, and Palestinian groups, which include Hamas and Palestinian Islamic Jihad, among others. The Palestinian cluster is at the bottom-left of figure 2 but for reasons of presentation the sites are not outlined.

At the bottom right corner of figure 2, one can see that two sites in the al Qaeda-linked cluster (www.al-ansar.biz and www.sraya.com) have links to two websites of the Palestinian group Hamas. The website [Al-ansar.biz](http://www.al-ansar.biz) is sponsored by the Saudi Salafi-Jihad that gathers and distributes information in support of the al Qaeda movement. However, the reverse is not true. Official Palestinian websites do not provide hyperlinks to al Qaeda linked websites.

Examples of official Palestinian websites include the Hamas' Qassam Brigades (www.ezzedeen.net); Palestinian Islamic Jihad (PIJ) site (www.qudsway.com) containing notices, archival material about its activities, and PIJ-sponsored books and articles; and the Al-Aqsa Martyrs Brigades (www.kataebaqsa.org). Al-Aqsa Martyrs Brigades is the military wing of Fateh, a secular group. Hamas, PIJ, and Al-Aqsa Martyrs Brigades are national (or regional) movements, unlike al Qaeda which is a transnational movement. This is reflected in the hyperlink structures in figure 2. Hamas and PIJ tend to disassociate themselves from al Qaeda on occasions and are both supported by Shiite-dominated Islamic Republic of Iran.

Figure 2. Web Hyperlinked Communities of Middle Eastern Extremist Groups



The cluster densities, such as 0.70 for the Hizbollah and 0.53 for the al Qaeda linked clusters, provide a validation of the clusters indicating that local densities are again higher than the overall density of the network (0.099). The online communities for both the U.S. domestic and Middle Eastern groups reflect or mirror their real world relationships.

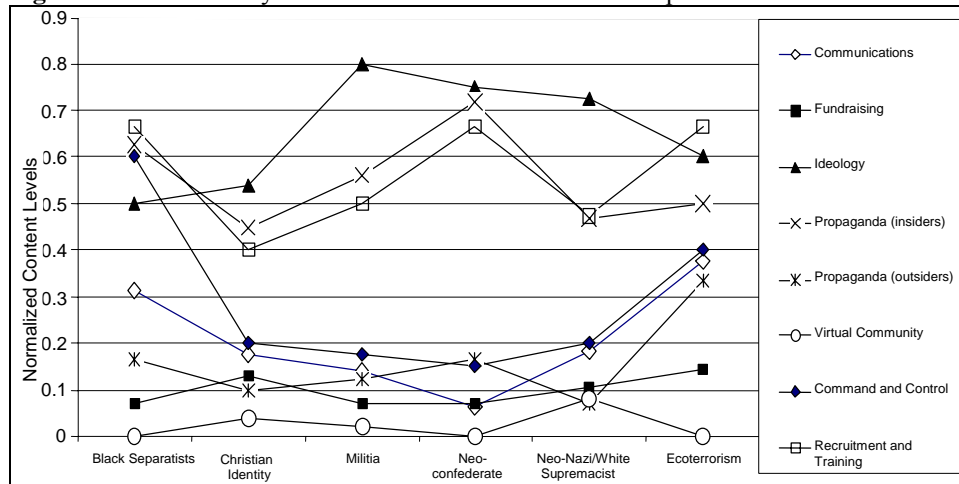
CMC Usage: U.S. Domestic Groups

To answer the next research question of how U.S. domestic and Middle Eastern groups use CMC to support their campaigns, we aggregated the content analysis data from all websites belonging to a cluster and calculated the normalized content levels into several dimensions. The content analysis data provide insight on how they are using the Internet. Figure 3 shows the content levels for six U.S. domestic extremist group clusters (black separatists, CI, militia, neoconfederates, white supremacy/neo-Nazi, and ecoterrorism) with a range of CMC usages from common (e.g., communications) to other (e.g., virtual community). The common CMC processes with the highest frequency of occurrence in U.S. domestic extremist groups' websites are sharing ideology, propaganda to insiders, and recruitment and training.

The sharing ideology process encapsulates all communication media devoted to portraying the goals of the group, presenting its ideologies, and defining its strategies. Overall the websites used a diversity of resources (e.g., National Alliance Nazi symbols, the Turner Diaries) to propagate ideologies, build ideological commitments, enhance ideological understandings, and justify the selective use of violence. With the exception of the Black Separatist groups and the ecoterrorism cluster, the results indicate that the other U.S. domestic groups' clusters take advantages of the common usages of CMC (e.g., sharing ideology, propaganda directed to insiders). Except for the ecoterrorism cluster, there is a low level of content concerning the propaganda directed towards outsiders. This may be because ecoterrorism groups have a much wider audience than groups such as the black separatists and the white supremacists who address primarily racial issues.

For most U.S. domestic extremist groups, there was limited content (e.g., listservs, chat sessions, message boards, blogs) directed to the virtual community process. For U.S. domestic groups, discussion forums were often not embedded within their websites. Because the freedom of movement and speech are constitutionally guaranteed in the U.S., domestic extremist groups do not seem to depend on exploiting virtual communities for resources. They have wider latitude for conducting routine operations, e.g., meetings, trainings, fundraising, which are protected by the First Amendment of the U.S. Constitution.

Figure 3. Content Analysis of U.S. Domestic Extremist Groups' Websites



CMC Usage: Middle Eastern Groups

For the Middle Eastern extremist groups, figure 4 identifies the content levels for five extremist clusters:⁵ Hizb-ut-Tahrir, Hizbollah, al Qaeda linked, Jihad Sympathizers, and Palestinian groups. The recruitment and training, and the sharing ideology processes have the highest frequency. Another process is virtual community, which is considerably higher for some clusters. Due to the clandestine nature of al Qaeda and its associates (e.g., al Qaeda in Iraq), virtual community is seen as an important mechanism for bringing together supporters, sympathizers, and other like-minded persons. In contrast, nationalistic groups like Hizbollah usually enjoy a much wider margin of freedom, freely holding meetings, and hence exhibit limited need for virtual communities.

Of all the groups, the virtual community process is the lowest for Hizbollah and the highest for Hizb-ut-Tahrir (see figure 4). Since Hizb-ut-Tahrir is a political party, the recruitment, training, and command and control activities are the lowest among all clusters. Their main focus is on ideological propagation as opposed to planning and conducting attacks.

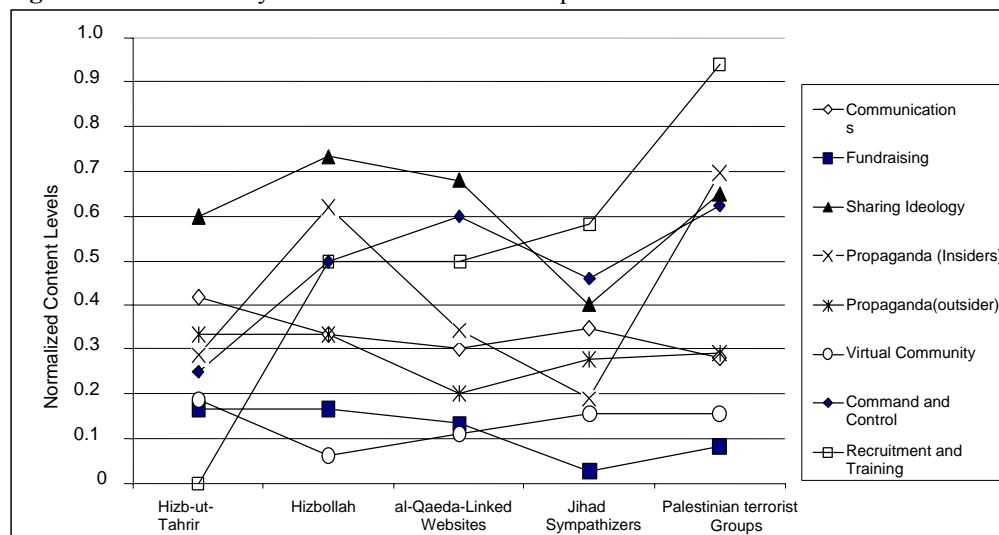
The Palestinian and Hizbollah clusters tend to use the web for propaganda (insiders)—in other words, disseminating their ideas within their communities (see figure 4). Al Qaeda linked groups tend to emphasize propaganda towards outsiders. Their messages, ideological icons, and multimedia presentations target multiple audiences such as members, current and potential supporters, media, and enemies. They are also produced in various languages such as English, French, and Bahasa (a language used in Malaysia and Indonesia).

This supports findings from other studies which report that some Middle Eastern groups are engaged in a virtual war using propaganda messages for various audiences (Weimann 2004; Corman and Schiefelbein 2006). These patterns emerged because of the limited freedom of expression as well as environmental constraints, e.g., political, legal, and security, on al Qaeda-affiliated groups.

Differences in CMC Usage

For the last research question of differences in the CMC usages between the U.S. domestic and Middle Eastern groups, we found that some Middle Eastern groups frequently resort to the use of other CMC processes (e.g., virtual command and control, virtual community) because

Figure 4. Content Analysis of Middle Eastern Groups' Websites



of there being several operational environment constraints. Table 3 shows that the means for U.S. domestic and Middle Eastern groups are statistically and significantly different. In table 3, the U.S. domestic groups ($n = 44$) scored higher in common CMC processes such as fundraising ($p < 0.10$) and sharing ideology ($p < 0.05$). The U.S. domestic extremist groups exploit the web for purposes of fundraising, sharing ideology, publicizing propaganda to their local, national, and transnational branches as well as for supporting recruitment and training.

On the other hand, as indicated in table 3, the Middle Eastern groups ($n = 40$) fared better in only one common CMC usage: communications ($p < 0.01$). They exploit the web to support sophisticated communication strategies. Groups such as al Qaeda linked and Jihad sympathizers have developed sophisticated communication and media approaches. They not only use the Web to legitimize their movements' social and religious agenda to propagate messages to sympathetic global audiences, but also to intimidate their antagonists through issuance of threatening fatwas online and disseminating video clips of actual and violent attacks (Bunt 2003; Corman and Schiefelbein 2006).

They also fared better in other CMC usages, namely: propaganda to outsiders ($p < 0.01$); virtual community ($p < 0.01$); and virtual command and control ($p < 0.05$). These results indicate that Middle Eastern groups exploit the web for massive dissemination of their ideologies and ideas, the development and expansion of global online communities, and for sharing instructional videos on packaging low-tech, homemade explosives and suicide bombing, and persistent informal calls for sympathetic actions that encourage others to act independently on behalf of the movement(s).

As summarized in table 4, Middle Eastern groups have five clusters each that are mapped to the CMC usage patterns. Four U.S. domestic (e.g., Christian identity, neoconfederate) and three Middle Eastern clusters (Hizbollah, Hizb-ut-Tahrir, and Palestinian groups) use CMC more as a mechanism to support common usages such as communications, fundraising, and propaganda (insiders) activities. Furthermore, in accord with the categories of our coding scheme,

Table 3. Group Comparisons

<i>CMC Processes</i>	<i>Origin</i>	<i>Mean</i>	<i>SD</i>
1. Communications ^{***}	Domestic	1.39	0.92
	Middle Eastern	2.33	0.89
2. Fundraising [*]	Domestic	0.70	0.67
	Middle Eastern	0.43	0.64
3. Ideology ^{**}	Domestic	3.36	0.75
	Middle Eastern	2.95	1.06
4. Propaganda (insiders) ^{***}	Domestic	3.98	1.36
	Middle Eastern	2.73	1.99
5. Propaganda (outsiders) ^{***}	Domestic	0.32	0.47
	Middle Eastern	0.78	0.53
6. Virtual Communities ^{***}	Domestic	0.61	1.02
	Middle Eastern	1.25	1.13
7. Command and Control ^{**}	Domestic	1.07	1.15
	Middle Eastern	1.75	1.32
8. Recruitment and Training ^{***}	Domestic	1.45	0.70
	Middle Eastern	1.00	0.82

*** $p < 0.01$, ** $p < 0.05$, * $p < 0.10$

Table 4. Summary of CMC Usages Among U.S. Domestic and Middle Eastern Clusters

<i>Terrorist Groups</i>	<i>Common CMC Usages by Cluster^a</i>	<i>Advanced CMC Usages^b</i>
<i>U.S. Domestic</i>	Christian identity cluster	Ecoterrorism cluster
44 groups	Neoconfederate cluster	
5 clusters	Militia cluster	
	White supremacist/neo-Nazi cluster	
<i>Middle Eastern</i>	Hizbollah cluster	al Qaeda-linked cluster
40 groups	Hizb-ut-Tahrir cluster	Jihad sympathizers cluster
5 clusters	Palestinian groups cluster	

Notes: ^a Common CMC usages are communications, fundraising, and propaganda to insiders.
^b Advanced CMC usages are giving support to virtual communities, and propaganda to outsiders.

we find that one U.S. domestic cluster (ecoterrorism) and two Middle Eastern clusters (al Qaeda-linked, and Jihad sympathizer) have expanded their use of CMC to employ advanced usages meant to support virtual communities, and provide propaganda to outsiders. According to the FBI, groups in these clusters represent some of the most violent extremists that have transnational goals and thus pose major challenges to law enforcement communities (FBI 2004).⁶ Their usages of the CMC have been adapted to support the trajectory of their life cycle (planning, growth, development, and transformation) and are important for organizational learning and survival. For instance, the al Qaeda-linked cluster maintains hyperlinked digital libraries of codified knowledge (e.g., manuals, speeches, strategy documents) in diverse formats (e.g., audio, video, print, animated images) at different web locations. The resources can be used to support virtual communities, who may or may not share similar ideologies, and provide virtual command and control for leaderless resistance strategies (summarized in table 4).

The www.h-alali.net Arabic language website in the al Qaeda-linked cluster provides a digital library of resources (e.g., speeches, training materials, multimedia). Figure 5 is one of its web pages that focuses on ideologies about the dangers of cultural globalization, goals of the Western presence in the Gulf region, and the role of ulama (clerics) in resisting this presence.

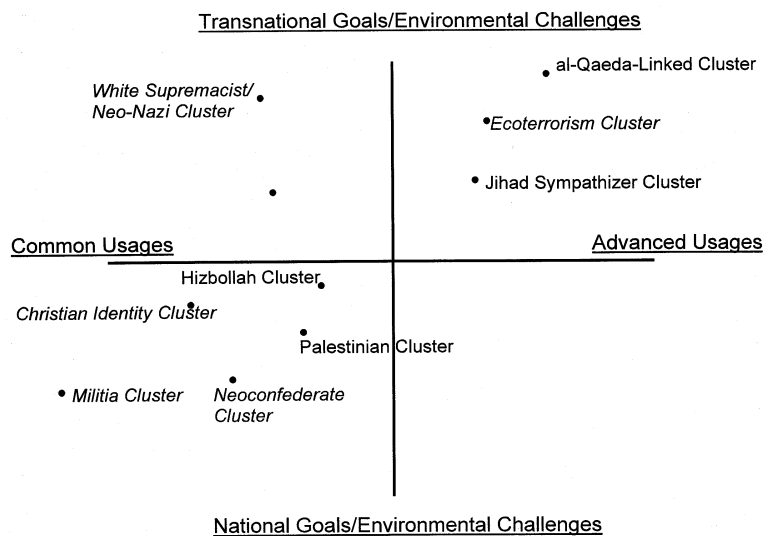
Figure 5. Example of Sharing Ideology (www.h-alali.net)

[illegible]

The foregoing results can be synthesized by mapping the various clusters onto a proposed classification system. The system combines the two dimensions of CMC usage (i.e. from common to other) as the horizontal axis and geographic reach (i.e., from national/local to transnational/global) as the vertical axis. The latter is approximated on the basis of the groups' ideological perspectives, strategic goals, and contextual challenges. Figure 6 shows how each of the clusters fit into the four quadrants engendered by the two dimensions.

For example, the neoconfederate cluster, made up of white nationalist focused groups whose operations are politically and legally constrained in the U.S., use CMC for traditional purposes. Thus, the neoconfederate cluster is situated in the lower left quadrant because its CMC usage does not substantially impact the other groups within this cluster. However, the ecoterrorism and al Qaeda-linked clusters, which have transnational goals, radical ideologies, and environmental challenges (i.e., limited freedom to operate legally), have designed and experimented with innovative CMC processes to support their needs for public- and private-mediated communications, according to our analysis. And because they are heavily dependent on CMC, they are placed in the top right quadrant. Situated in the bottom left quadrant is the Hizbollah cluster by virtue of the groups' regional and nationalist goals which they can easily advance using common CMC processes (e.g., propagation of ideologies and fundraising). The groups in this cluster do not heavily depend on CMC because they can openly utilize other forms of mass media. One such example is Hizbollah's television network (before the August 2006 attacks). The proposed classification system in figure 6 provides an integrated framework for analyzing groups' usage of CMC to mitigate the constraints posed by the socio-political and legal environments in which they operate and thus reach their intended audiences. For these groups, CMC has become a flexibly constructed environment that can be adapted to support their groups' goals, ideologies, environmental challenges, and life-cycle development.

Figure 6. Classification of Clusters of U.S. Domestic^a and Middle Eastern Extremist Groups by CMC Usage Patterns.^b



Notes: ^a U.S. domestic groups in italics.

^b Common CMC usages are communications, fundraising, and propaganda to insiders. Advanced CMC usages are giving support to virtual communities, and propaganda to outsiders.

CONCLUSION

This study afforded us the opportunity to systematically employ hyperlink and content analysis methodology for analyzing extremist groups' websites. Our results indicate that both U.S. domestic and Middle Eastern extremist groups have networked web clusters that appear to be organized based on ideologies and contain prominent websites (e.g., www.stormfront.org for Ku Klux Klan and www.al-ansar.biz for the Middle East) acting as nodes that link different clusters. The nodes provide access and control a pool of resources (e.g., publications, multimedia, symbols, and discussion forums) that are available to members, sympathizers, and interested organizations.

CMC provides an interactive environment and anonymity that other mediated forms of communication lack. Despite the lack of warmth and the intensity of direct, face-to-face communication (Diani 1999), the extensive use of multimedia, such as animated images, videos, and audios of speeches, enable extremist groups to provide emotional support, community connections, and shared experiences. The message content piped through such channels encourages people, generates mutual binding, supports calls to action, and provides training—features that augur well for leaderless resistance strategies.

Less extreme groups, such as the Michigan Militia, have used common CMC modalities as a mechanism to communicate and propagate their ideologies. For the more violent extremist groups, such as the Chechen extremists affiliated with al Qaeda (Jihad Sympathizers cluster), CMC usage has evolved into mission-critical processes that are key in supporting their communication strategies as well as realizing their strategic transnational goals. For them, the CMC-enabled environment nurtures virtual command and control, virtual communities, and virtual extensions that are vitally important for sustaining organizational learning, leveraging the state-of-the-art technologies, and survival.

Our results support the assertions from previous hyperlink studies of U.S. domestic extremist groups (e.g., Burris et al. 2000; Gerstenfeld et al. 2002), that distinctions between most white supremacist groups are blurry. In this study, however, we found that Middle Eastern extremist groups' online communities have distinctive characteristics. For both the U.S. domestic and Middle Eastern groups, their web communities mirror their real world relationships.

The results of this research have been useful for our work in that it provided systematic methodologies for capturing, classifying, and analyzing U.S. domestic and Middle Eastern (Arabic) extremist groups' websites. Because this study was limited to a sample of 84 websites (English and Arabic), future studies of this kind should endeavor to enlarge the sample and verify our general findings. Crucial, however, to the success of our study is the presence in our team of native analysts who, in addition to being proficient in translating the texts in Arabic language to English, are able to put the content within the sociopolitical and cultural environmental context. The absence of this latter skill would have created serious gaps which could have derailed our content analysis.

We envisage expanding our research in several directions. We plan to enhance the content analysis process by implementing automated feature extraction procedures. Lastly, we would like to conduct similar analysis on other international extremist groups and compare their web usage patterns with those of U.S. domestic counterparts.

NOTES

¹ Sunni branch of Islam is based on specific provisions of the Qur'an in which Muslim people are to be governed by consensus through an elected head of state, the khalifa (Bassiouni 1999).

² The Salafi ideology responds to the political, cultural, and military challenges of the West and seeks the "purification" of Islam by returning to the uncorrupted form that Salafists believe was practiced in the time of the prophet Muhammad and his companions (Rabasa et al. 2004; Brachman and McCants 2006).

³ Since none of the websites, in our collection, had links to the Black Separatist's websites then the Black Separatist was not displayed in figure 1.

⁴ Leadership resistance has been commonly called an unstructured violence strategy that is thought to be a new tactics that emerged among extremist/terrorist groups (Disham 2005; Damphouse and Smith 2004).

⁵ Since the Tanzeem-e-Islam cluster only had one website it was not included in the content analysis results.

⁶ It should be clarified, of course, that the members of al Qaeda and those persons involved in radical eco-protest have entirely different goals. Moreover, the number of persons are incidentally injured by those cells or groups of persons who are making pro-environmental messages—even in the context of alleged criminal disobedience—is nowhere near the death count intentionally caused by al Qaeda agents whose purpose is to maim and kill.

APPENDIX: CODING SCHEME FOR CMC USAGES

<i>Common CMC Usages</i>	<i>Examples of Resources Needed for Collective Action</i>
Communications	Communications, private and public. Email, telephone, online feedback form, multimedia (Conway 2005; Diani 1999; Gustavson and Sherkart 2004; ISTS 2003; Thomas 2003; Tsafiti and Weimann 2002)
Fundraising	Eternal aid mentioned, fund transfer, donation, charity, support groups, bank account (Burris et al. 2000; Conway 2005; Gerstenfeld et al. 2003; SITE 2004; Tsafiti and Weimann 2002)
Sharing Ideology	Ideological resources, mission, doctrine, justification, enemies. (Diani 1999; Gerstenfeld et al. 2003; ISTS 2004; Weimann 2004)
Propaganda (insiders)	Leaders, martyrs, narratives of operations and events, slogans, banners, etc. to stimulate loyalty, understanding, support, commitment to action. (Burris et al. 2000; Diani 1999; Gustavson and Sherkat 2004; Weimann 2004)
Recruitment and training	Invitation/appeal for recruits, foot soldiers, skilled activists, knowledgeable authorities, skill development. (Conway 2005 :12; Gerstenfeld, et al. 2003; SITE 2004; Thomas 2003; Weimann 2004)
<i>Other CMC Usages</i>	
Propaganda (outsiders)	Analytical interpretation of news, events, ideology, etc., media contacts, support and recognition. (Gustavson and Sherkat 2004; Lia and Heggerhammer 2004; Weimann 2004)
Virtual community	Listserv, text chat, message board, blogs, web ring, e-conference, interactive group-CMC (Conway 2005; Diani 1999; Jones 1997; Lia and Heggerhammer 2004; SITE 2004)
Virtual command and control	Multimedia (video, audio) presentation from senior members, vision, documentation of previous operation, creativity, games, animated pictures, leadership meetings, tactical instructions, strategic plans, supplies, tacit and explicit knowledge. (Gustavson and Sherkat 2004; Lia and Heggerhammer 2004; SITE 2004; Weimann 2004)

REFERENCES

- Bassiouni, M. C. 1999. *Introduction to Islam*. Washington, DC: Middle East Institute.
- Bergesen, A.J., and Y. Han (2005). "New Directions for Terrorism Research." 46(1-2):133-151.
- Brachman, J.R. and W.F. McCants. 2006. *Stealing al Qaida's Playbook*. West Point, NY: Combating Terrorism Center at West Point, U.S. Military Academy (<http://www.ctc.usma.edu>).
- Bunt, G. R. (2003). *Islam in the Digital Age: E-jihad, Online Fatwas and Cyber Islamic Environments*. Sterling, Pluto Press.
- Burris, V., Emory Smith, and Ann Strahm. 2000. "White Supremacist Networks on the Internet." *Sociological Focus* 33(3): 215-235.
- Chaudhry, L. 2000. *Hate Sites Bad Recruiting Tools*. Educational CyberPlayground, Wired Digital Inc.
- Chen, H., J. Qin, E. Reid, W. Chung, Y. Zhou, W. Zi, G. Lai, A. Bonillas, and M. Sageman. 2004. "Dark Web Portal: Collecting and Analyzing the Presence of Domestic and International Terrorist Groups

- on the Web." Proceedings of the 7th International Conference on IEEE Intelligent Transportation Systems (ITSC), October 3-6, Washington, DC.
- Coll, S. and S.B. Glasser. 2005. "Terrorists Turn to the Web as Base of Operations." Washingtonpost.com.
- Conway, M. 2005. Terrorist Use of the Internet and Fighting Back: Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities. Paper presented at the Oxford Internet Institute Conference, September 8-10, 2005, Oxford, Oxford University.
- Corman, S.R. and J.S. Schiefelbein. 2006. Communication and Media Strategy in the Jihadi War of Ideas. Consortium for Strategic Communication, Arizona State University. Retrieved from http://www.asu.edu/clas/communication/about/terrorism/publications/jihad_comm_media.pdf
- Damphouse, K.R. and B.L. Smith. 2004. "Terrorism and Empirical Testing: Using Indictment Data to Assess Changes in Terrorist Conduct." Pp. 75-92 in *Terrorism and Counterterrorism: Criminological Perspectives*, edited by M. Deflem. London: Elsevier.
- December, J. (1997). "Notes on Definition of Computer-Mediated Communication." CMC Magazine. Retrieved from <http://www.december.com/cmc/mag/1997/jan/december.html>
- Demchak, C., C. Friis, and T.M. LaPorte. 2001. Webbing Governance: National Differences in Constructing the Face of Public Organizations. Handbook of Public Information Systems. G. D. Garson. New York: Marcel Dekker.
- Diani, M. 1999. "Social Movement Networks Virtual and Real. A New Politics?" CCSS, University of Birmingham Conference. Retrieved from <http://www.nd.edu/~dmyers/cbsm/vol2/bgham99.pdf>.
- Dishman, C. 2005. "Leaderless Nexus: When Crime and Terror Converge." *Studies in Conflict and Terrorism* 28(3): 237-52.
- FBI. 2004. Congressional Testimony. Statement of John E. Lewis, Deputy Assistant Director, Counterterrorism Division, FBI. Washington, D.C.
- Forest, J.F. 2006. *Teaching Terror: Strategic and Tactical Learning in the Terrorist World*. Lanham, MD: Rowman and Littlefield.
- Galeas, P. N.d. *Web Mining*. Retrieved November 22, 2006 (<http://www.galeas.de/webmining.html>).
- Gerstenfeld, P., D. Grant, and C. Chiang. 2003. "Hate Online: a Content Analysis of Extremist Internet Sites." *Analysis of Social Issues and Public Policy* 3(1): 29-44.
- Glasser, S. B. 2005. *Martyrs in Iraq Mostly Saudis: Web Sites Track Suicide Bombing*. Washington Post: A1, A25.
- Gustavson, T.E., and D.E. Sherkat. 2004. "Elucidating the Web of Hate: the Ideological Structuring of Network Ties Among Right Wing Hate Groups on the Internet." Paper presented at the annual meeting of the American Sociological Association.
- International Crisis Group. 2006. *In Their Own Words: Reading the Iraqi Insurgency*. International Crisis Group, Middle East Report #50.
- ISTS. 2003. *Examining the Cyber Capabilities of Islamic Terrorist Groups*. Hanover, Institute for Security Technology Studies (ISTS), Dartmouth College. 2004.
- Jenkins, B. 2004. "World Becomes the Hostage of Media-Savvy Terrorists." *USA Today*.
- Jones, C. W. 2005. "Online Impression Management: Case Studies of Activist Web Sites and their Credibility Enhancing Tactics during the Kosovo Conflict." University of California, Berkeley. Retrieved from the Oxford Internet Institute, <http://www.oii.ox.ac.uk>.
- Kelley, J. 2002. *Militants Wire Web With Links to Jihad*. USA Today.
- Knight, A., and K. Ubayasiri. 2002. Report On Line: the Internet and Terrorism. On Line Opinion: Australia's e-journal of Social and Political Debate. August 2005.
- Langman, L., and D. Morris. 2002. "Internet Mediation: A Theory of Alternative Globalization Movements." Paper presented at the proceedings of the 1st International Workshop on Community Informatics. October 8, 2002. Montreal, Canada.
- Levin, B. 2002. "Cyberhate: a Legal and Historical Analysis of Extremists' Use of Computer Networks in America." *American Behavioral Scientist* 45(6): 958-88.
- Lia, B., and T. Heggerhammer. 2004. "Jihad Strategic Studies." *Studies in Conflict and Terrorism* 27: 355-75.
- Lipton, E., and E. Lichtblau. 2004. "Even Near Home, a New Front Is Opening in the Terror Battle." *New York Times on the Web*.
- McCaughey, M., and M. D. Ayers. 2003. "Introduction." Pp. 1-21 in *Cyberactivism: Online Activism in Theory and Practice*, edited by M. McCaughy and M. D. Ayers. New York: Routledge.

- Park, H. W., and M. Thelwall. 2003. "Hyperlink Analyses of the World Wide Web: a Review." *Journal of Computer-Mediated Communication* 8(4). Retrieved from <http://jcmc.indiana.edu/vol8/issue4/park.html>
- Preece, J. 2000. *Online Communities: Designing Usability, Supporting Sociability*. Chichester, UK: John Wiley & Sons.
- Rabasa, A., C. Benard, P. Chalk, C.C. Fair, T.W. Karasil, R. Lai, I.O. Lesser, and D.E. Thaler. 2004. *Muslim World After 9/11*. Santa Monica, CA: RAND.
- Reid, E., J. Qin, Y. Zhou, G. Lai, M. Sageman, G. Weimann, and H. Chen. 2005. "Collecting and Analyzing the Presence of Terrorists on the Web: a Case Study of Jihad Websites." Paper presented at Intelligence and Security Informatics: IEEE International Conference on Intelligence and Security Informatics, ISI 2005 held May 2005, Atlanta, Georgia: Springer.
- Sharpe, T. T. 2000. "Identity Christian Movement: Ideology of Domestic Terrorism." *Journal of Black Studies* 30(4): 604-23.
- SITE (2004). "Background on Terrorist Groups." SITE (Search for International Terrorist Entities) Institute, Washington, D.C. Retrieved from <http://www.siteinstitute.org/index.html>.
- SPLC. 2004. "Active U.S. Hate Groups in 2004." Southern Poverty Law Center (SPLC) Intelligence Project. Montgomery, SPLC. Retrieved from <http://www.splcenter.org>
- Tateo, L. 2005. "Italian Extreme Right On-line Network: An Exploratory Study Using an Integrated Social Network Analysis and Content Analysis Approach." *Journal of Computer-Mediated Communication* 10(2).
- Thelwall, M., L. Vaughan, et al. (2004). "Webometrics." *Annual Review of Information Science and Technology*. B. Cronin.
- Thomas, T. L. 2003. "Al Qaeda and the Internet the Danger of Cyberplanning." *Parameters* 33: 112-23.
- Thomas, M. J. 2004. "Counteracting Terror: Group Design and Response Modalities." Pp. 91-110 in *Terrorism and Counterterrorism: Criminological Perspectives*, edited by M. Deflem. London, Elsevier.
- Tsfati, Y., and G. Weimann. 2002. "www.terrorism.com: Terror on the Internet." *Studies in Conflict and Terrorism* 25: 317-22.
- Weimann, G. 2004. "www.terror.net: How Modern Terrorists Use the Internet." Washington, DC: U.S. Institute of Peace.
- Weimann, G. 2006. "Terror on the Internet: the New Arena, the New Challenges." Washington, DC: U.S. Institute of Peace.
- Whine, M. 1997. "Far Right on the Internet." Pp. 209-27 in *The Governance of Cyberspace*, edited by B.D. Loader. London: Routledge.
- Xu, J., and H. Chen. 2005. "CrimeNet Explorer: a Framework for Criminal Network Knowledge Discovery" *ACM Transactions on Information Systems* 23(2): 201-26.
- Zhou, Y., E. Reid, J. Qin, H. Chen, and G. Lai. 2005. "U.S. Domestic Extremist Groups on the Web: Link and Content Analysis." *IEEE Intelligent Systems* 20(5): 44-51.