NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CYBER-HERDING AND CYBER ACTIVISM:
COUNTERING QUTBISTS ON THE INTERNET

by

David B. Moon

December 2007

Thesis Co-Advisors: John Arquilla
Dorothy Denning

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE December 2007	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE Cyber-Herding and Cyber Activism: Countering Qutbists on the Internet	5. FUNDING NUMBERS
6. AUTHOR(S) David B. Moon	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

The Internet provides Islamic militants ("Qutbists") a golden opportunity to bypass normal media outlets and take their message directly to the people. This allows them to spread their ideas to an ever-growing audience. What should be done about these web sites has been the focus of an ongoing debate. Some advocate shutting down these web sites while others prefer to monitor them for information. Both views have merit, and both have problems. The purpose of this thesis is to propose and evaluate three strategies for countering Qutbists on the internet: a covert active strategy of cyber-herding, an overt passive strategy of cyber activism, and a combination of these two strategies.

14. SUBJECT TERMS Cyber Activism, Cyber-Herding, Cyber-War, Cyber Strategies, Herding, Information Operations, Internet, Qutbists, Terrorists, Terrorism	15. NUMBER OF PAGES 73
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

CYBER-HERDING AND CYBER ACTIVISM:
COUNTERING QUTBISTS ON THE INTERNET

David B. Moon
Captain, United States Air Force
B.S., Regents College, 2000

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
December 2007

Author: David B. Moon

Approved by: John J. Arquilla
Thesis Co-Advisor

Dorothy E. Denning
Thesis Co-Advisor

Gordon H. McCormick
Chairman, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Internet provides Islamic militants (“Qutbists”) a golden opportunity to bypass normal media outlets and take their message directly to the people. This allows them to spread their ideas to an ever-growing audience. What should be done about these web sites has been the focus of an ongoing debate. Some advocate shutting down these web sites while others prefer to monitor them for information. Both views have merit, and both have problems. The purpose of this thesis is to propose and evaluate three strategies for countering Qutbists on the internet: a covert active strategy of cyber-herding, an overt passive strategy of cyber activism, and a combination of these two strategies.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I am normally a man of few words so I will try to keep this short. I would first like to thank Professor John Arquilla, Professor Dorothy Denning, and Professor Robert O'Connell. They planted the first seeds that grew into the three strategies outlined in this thesis. I also want to express my gratitude to Professor Glenn Robinson, who encouraged me to put my ideas down on paper for the first time. I appreciate Colonel Brian Greenshields, Colonel Kenneth J. Alnwick USAF (Ret), and Ms. Lisa Chandler for their support and editorial skills. Furthermore, I want to thank the Special Operations Low Intensity Conflict Division of the National Defense Industrial Association for selecting my essay on cyber-herding as their essay contest winner. It was a huge honor being selected and it told me this idea had "legs." I also want to show appreciation to Major Philip Acquaro and Captain Timothy Marenic for being sounding boards for some of my crazy ideas. I also want to express my gratitude to Captain Daniel Vaniman for helping me develop my ideas on cyber activism. Lastly, I wish to express my love and thanks to Tanya, my beautiful wife and friend, and to Christian and Damian, our headstrong kids, for their support and love over this past year and a half. With them, I can accomplish anything. Without them, I am nothing.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. AUTHOR'S NOTE

Words have power and meaning, so it is important to choose them wisely. Unfortunately, when referring to Islamic terrorists, it has become all too common to refer to them as Islamic extremists, Islamofascists, Muslim terrorists, Jihadists, and other similar terms. This language is insulting to millions of Muslims who have nothing to do with terrorism. In addition, using the term "Jihadist" is counter productive. To many Muslims, jihad means to "struggle," notably to "struggle in the way of God" or "to struggle to improve one's self and/or society." Thus, when we refer to these terrorists as Jihadists, we are saying they are struggling in the name of God. This is not the message we want to send to the Muslim world.

In this light, this author will adopt a recommendation from the *Militant Ideology Atlas* that calls for labeling the entire Islamic terrorist movement as Qutbism (pronounced Kuh tahb' ism). The authors of the *Militant Ideology Atlas* suggest this nomenclature for three reasons. The first reason is in recognition that the majority of Islamic terrorists cite Sayyid Qutb more than any other modern author.[1] The second reason is that Muslim opponents of Islamic terrorists have used this term in reference to the terrorists.[2] The last reason is that the Islamic terrorists themselves would dislike being referred to as Qutbists

[1] William McCants, *Militant Ideology Atlas*, Combating Terrorism Center, November 2006; available from http://www.ctc.usma.edu/atlas/Atlas-ExecutiveReport.pdf (accessed 10 September 2007).

[2] Ibid.

because it implies they are followers of a man versus followers of Allah. Thus for this paper, this author will refer to the followers of Qutbism as Qutbist.

B. BACKGROUND

On November 28, 2006, the Al-Fajr Information Center released the first issue of the *Technical Mujahid Magazine.*[3] The magazine stated that its purpose is to help prevent aggressive acts against Muslims in cyberspace and to assist the mujahid in their efforts.[4] A mujahid is a Muslim fighting in a war or involved in any other struggle.[5] The magazine proclaims that the Internet provides a golden opportunity for the mujahid to break the Western media control over information. The magazine also recognizes that the internet could represent a vulnerability to the mujahid and suggests security measures for the mujahid to follow.

The magazine is correct when it says this is a golden opportunity for the mujahid. The internet provides Qutbists an excellent medium to spread their ideas to hundreds of millions of people, and over the years, the extremists have steadily made a greater presence on the information superhighway. As an example, Gabriel Weimann states that from 1998 to the present, "the number of terrorists' web sites has grown from less than 30 to more

---

[3] Special Dispatch Series, No. 1375, 1 December 2006; available from http://memri.org/bin/latestnews.cgi?id=sd137506 (accessed 3 December 2006).

[4] Ibid.

[5] Mujahideen, 17 November 2007; available from http://en.wikipedia.org/wiki/Mujahideen (accessed 17 November 2007).

than 4,300."[6] Qutbists have used these web sites for recruitment, fundraising, coordination, training, propaganda, and a whole host of different activities.

What should be done about these web sites has been the focus of an ongoing debate. Some advocate shutting them down while others prefer to monitor them for information. Both notions have merit, and both have problems. Shutting down a web site removes a source of propaganda from the internet, but the Qutbists can normally restore the web site in a matter of hours or days on a different server. To be effective, constant monitoring of the internet for existing and emerging Qutbists' web sites needs to take place. When found, the sites need to be systematically shut down. Monitoring the Qutbists' web sites provides a wealth of information, but it also leaves the site operational to influence and persuade others to join the Qutbist cause. This allows the Qutbists to expand their ranks and raise the level of homegrown terrorists.

C. PURPOSE

The purpose of this thesis is to propose and evaluate three strategies for countering Qutbists on the internet: 1) a covert strategy of cyber-herding; 2) an overt strategy of cyber activism; and 3) a combination of the two.

D. METHODOLOGY

This thesis will evaluate three strategies using a strategic assessment methodology. This methodology involves describing the strategies, identifying minimum requirements the strategies need to meet, identifying

[6] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Dulles, VA: Potomac Books, 2006), 15.

comparative criteria for the strategies, and assessing and scoring the strategies using the comparative criteria to identify the preferred strategy (see Figure 1).

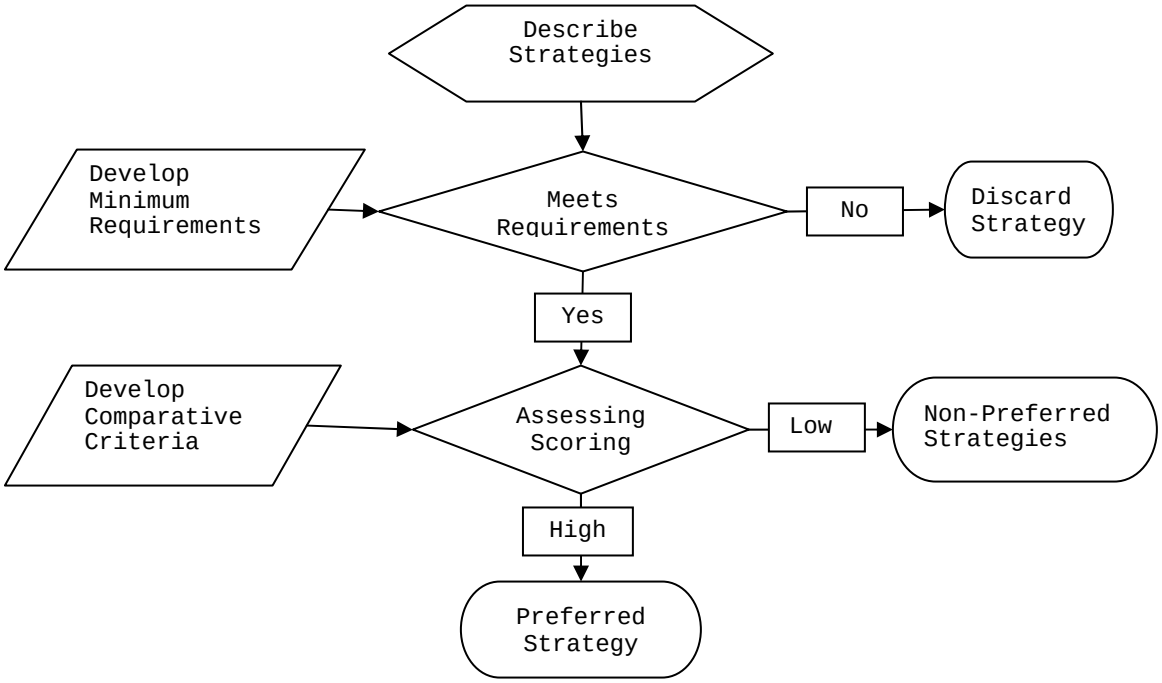


Figure 1. Strategic Assessment Methodology

II. DESCRIPTION OF CYBER STRATEGIES

A. CYBER-HERDING[7]

1. Defining Cyber-Herding

For thousands of years, mankind has used various methods to herd livestock. These methods include fear, incentive, barriers and imprinting. Using the fear method, the herder threatens the herd with pain. The herder does not have to inflict pain on the herd as long as the herd perceives that pain will come. The incentive method is based on providing the herd something that they want such as food, service, or shelter to get the herd to go where the herder wants them to go. The physical method incorporates natural or fabricated structures to guide the herd to the desired goal. The imprinting method involves making the herd believe that the herder is a member and the leader of the herd. Utilizing these methods, a herder can get the herd to do what the herder wants.

While most people think of sheep and cattle when you refer to herding, these methods are also used on humans. All of us are herded, whether at sporting events, rallies, shopping, schools, prisons, or just queuing up at your favorite fast food restaurant. This form of human herding is normally referred to as crowd control, but it is also found in marketing to get customers to attend a sale or buy a product. The next evolution in herding is in the electronic realm – cyber-herding. This cyber-herding is

[7] The section on cyber-herding is a modified version of this author's paper published by the Joint Special Operations University. See David Moon, "Cyber-Herding: Exploiting Islamic Extremists Use of the Internet," JSOU and NDIA SO/LIC Division Essays, (JSOU, Hurlburt Field, Florida, April 2007).

the action by which an individual, group, or organization drives, guides, or attracts other individuals, groups, or organizations to a desired location within the electronic realm. Spammers have been cyber-herding for years to get people to go to a web site or provide them personal information. It is highly likely that you have been a target of their herding attempts. They use e-mails crafted to utilize herding methods: Your credit is in trouble click here (fear), you just won $10,000 click here (incentive), a friend asked you to visit a great web site (imprinting). These herding methods can also be used against Qutbists and potential Qutbists on the internet. The physical method can be used to covertly create doppelganger web sites and neutralizes Qutbists' web sites. As the number of real Qutbists' web sites shrink, the more likely the herd will be driven to the doppelganger web sites. The fear method can be used to drive people away from real Qutbists' web sites by posting that a site is being monitored or is a fake. The imprinting method can be used by having people posing as Qutbists recommend the doppelganger web sites. The incentive method can be used by offering Qutbists and potential Qutbists content rich web sites. On these doppelganger web sites, data can be mined, virtual social networks can be mapped, the Qutbists' messages can be manipulated, and their story modified.

2. Implementing Cyber-Herding

A cyber-herding program consists of seven phases and four nodes. At its core, a cyber-herding program is a deception and psychological campaign. The deception element begins in Phase 2 with Node members trying to insert themselves into existing Qutbists' web sites. The

deception continues in Phase 3 with the introduction of web sites owned by the cyber herding program and later on with the introduction of Darknets. The psychological element begins in Phase 5 as the node attempts to influence the Qutbists' message and ideology.

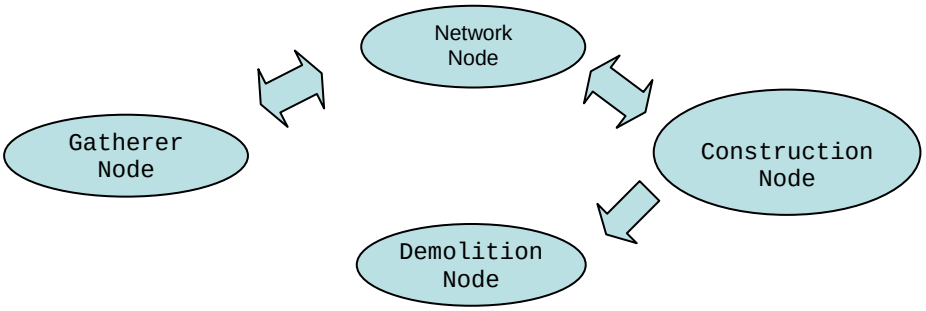


Figure 2. Cyber-Herding Nodes and Relationships

Node	Objective
Gatherer	Compile and maintain an up-to-date list for all Qutbists' related uses of the Internet.
Network	Insert themselves into the Qutbists' virtual social network. Identify major "nodes" and "links" within the Qutbists' virtual social network.
Construction	Create realistic *doppelganger*—ghostly doubles or look-alike Qutbist Web sites and chat rooms. (In some traditions, it is an omen of death to see your own doppelganger.) Create several content-rich *Darknet* environments—a private virtual network where users connect only to people they trust[8]—that offer e-mail, file sharing, chat, instant messenger, and streaming video services.
Demolition	Remotely destroy or disable all Qutbists' Web activities (e.g., sites, chat rooms, and Darknets).

Table 1. Cyber-Herding Nodes

[8] Darknet, 9 December 2006; available from http://en.wikipedia.org/wiki/darknet (accessed 12 December 2006).

a. Phase 1, Gather

The Gatherer node begins the cyber-herding process by tracking down Qutbists' Web sites and chat rooms. To facilitate this phase, the node seeks public help by placing web-based advertisements asking people to submit Uniform Resource Locators (URL) for any suspected Qutbist Web site.[9] The node seeks out help from private groups such as the RAND Corporation, the Search for International Terrorist Entities (SITE) Institute, the Middle East Media Research Institute (MEMRI), and academic terrorism research groups.[10] The node compiles a list of Qutbist Web site URLs. This list becomes a living document that the node constantly updates with identified Qutbists' sites. In addition, a program constantly checks identified URLs to verify the sites are still active and automatically deletes dead sites. During this process, the Network node makes a copy of the list and begins Phase 2.

b. Phase 2, Network

Upon accessing a site on the list, the members of the Network node pose as Qutbist sympathizers and/or supporters and begin interacting with members of the site. In chat rooms, the node members start or join conversations supporting Qutbists' themes. The objective is to develop trust relationships with Qutbists. Node members contact Qutbists' web sites to see what they can do to support the

[9] Uniform Resource Locator, 9 December 2006; available from http://en.wikipedia.org/wiki/url (accessed 10 December 2006).

[10] See www.rand.org/about, www.siteinstitute.org/index.html, and www.memri.org (accessed 10 December 2006).

cause. If needed to help build trust, the Network node would have the authority to make donations to Qutbists' web sites.

During this phase, the Network node maps the Qutbists' chat rooms. Mapping a chat room involves creating a sociogram, a social network diagram, of who is talking to whom. The members of the Network node are looking for "nodes," people using the sites, who have more connections then anyone else. In his book *The Tipping Point*, Malcolm Gladwell refers to these people as "connectors."[11]

The members of the Network node develop virtual fictitious identities. They keep detailed records of their conversations for each identity. This way any member of the Network node can be that virtual person. All they have to do is pick a character and research his or her history before chatting.

If the Network node discovers any web sites not identified on the Phase 1 master list, they add the new URLs to the list and forward these sites to the Gatherer node. The members of the Network node mark the list to identify sites they are currently working; this practice ensures that the Demolition node does not destroy those sites. Subsequently, the Network node forwards the list to the Construction node.

c. Phase 3, Construct

After the members of the Construction node receive the list from the Network node, they start

[11] Malcolm Gladwell, *The Tipping Point: How Little Things Can Make a Big Difference, (*Boston, MA: Little, Brown, 2002).

accessing the sites. They copy the content, format, graphics, files, and links of each site. Using this information, the Construction node builds doppelganger Qutbist web sites, which are independent—that is, having only passing similarities with other existing sites. The Construction node should not hijack existing Qutbists' web sites because this could cause distrust in the target audience.[12] However, if the Qutbists start setting up the same web site on multiple ISPs as a countermeasure, then hijacking one of these sites or setting an identical site becomes feasible.

The Construction node forwards all created sites to the Network node, which then endorses them with their contacts. The members of the Construction node remove all Web sites that the Network node marked and any sites they created from the list. Then the Construction node forwards the list to the Demolition node.

d. Phase 4, Demolish

After receiving the list from the Construction node, the Demolition node systematically begins a process of attacking every site on the list. These attacks can be simple, such as contacting the site's service provider to try to get the site removed. They can also use more sophisticated attacks such as denial of service attacks, hijacking a web site, Structured Query Language (SQL) injections, Cross Site Scripting attacks, JavaScript

[12] Page hijacking, 8 December 2006; available from http://en.wikipedia.org/wiki/page_hijacking (accessed 10 December 2006).

injections, and other hacking methods.[13] Depending on where the host server is located, it may not be politically feasible to attack some sites directly. In these cases, the Demolition node might post the Qutbists' URLs on Internet chat rooms and blogs in the hope that private citizens, such as Mr. Aaron Weisburd who runs a web site called Internet Haganah dedicated to finding and shutting down threatening web sites, and/or groups, such as MEMRI, can bring down the sites.[14]

The appendix to this thesis is a mathematical model of terrorist and doppelganger web sites. All of the numbers in this paper that relate to this model should be considered hypothetical and subject to change. The model uses Gabriel Weimann's few available numbers on terrorists' web sites to determine the growth rate.[15] The result is that at least 854 terrorists' web sites are created each year. At this rate, the estimated number of terrorists' web sites in 2006 was about 6,850. Weimann's numbers included all terrorists groups, but here they are applied to just Qutbists.

Using this data, the Demolition node would need to take down at least 2.34 web sites a day if the objective is just to maintain the status quo. The estimate for

---

[13] Lori Eldridge, Stop 302 Redirects Hijacking Web Page PR (Page Rank) and Stop Scrapers from Using Your Content, 17 November 2004; available from www.loriswebs.com/hijacking_web_pages.html . Also EthernetSecuritydb.org, The Web site Attack Guide, no date; available from www.milw0rm.com/papers/111 (accessed 11 December 2006).

[14]. Online vigilantes answer call of anti-terrorist defender, *The Washington Post*, April 2006, available from http://www.smh.com.au/news/World/Online-vigilantes/2005/04/25/1114281505819.html (accessed on 17 November 2007).

[15] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Dulles, VA: Potomac Books, 2006), 15.

parity is 711 days if the Demolition node can take down an average of 9 web sites a day and the Construction node can build web sites at an average of 2.34 a day as illustrated in Figure 3. The purpose of reaching parity is to give Phase 5 the best chance of succeeding. Phase 5 is all about changing the Qutbists' message. If the message is changed too soon, then the doppelganger web sites may not succeed in attracting an audience to influence. On the other hand, if the message is changed at the end of the cyber-herding process, then valuable time will be wasted that could be used to influence impressionable Muslims who are interested in the Qutbists' cause.

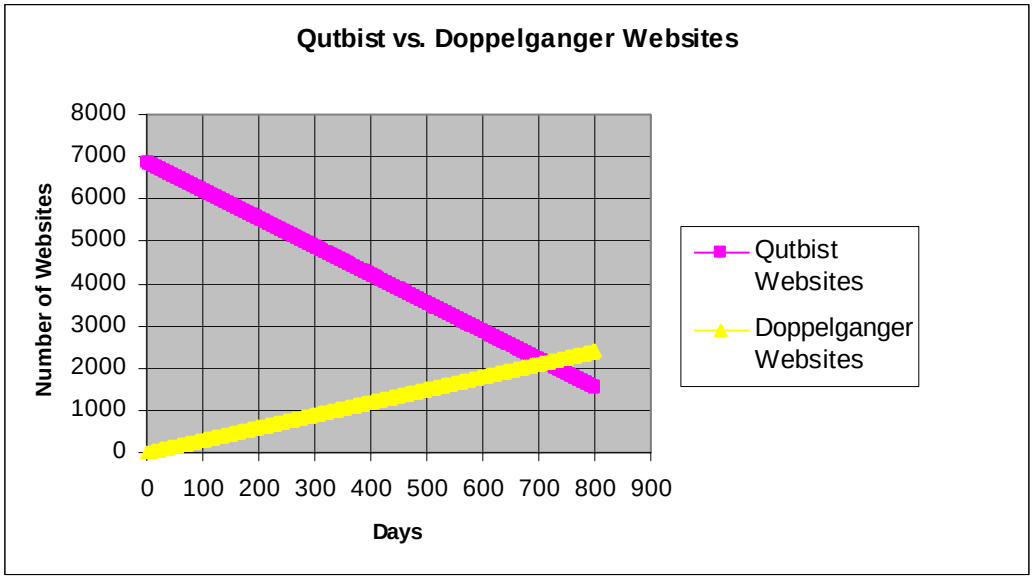


Figure 3. Qutbist vs. Doppelganger Web Sites

Phases 1 through 4 cover the basic mechanics of the cyber-herding process. The next three phases involve changing the Qutbist messages, concentrating Web sites, and developing Darknets. A visual illustration of the entire process follows the description of Phase 7.

e. Phase 5, Change Message

Qutbists are essentially salesmen; they sell their ideology to the world. As good salesmen, they highlight the positive qualities of their movement and suppress the negative aspects. Qutbists suppress two main items: a) the violence they commit against Muslims and b) their harsh version of an Islamic state they wish to impose upon people, states, and nations. Virtually all Qutbists expound on the need for an Islamic state or Caliphate. For them, this state would solve all of the world's problems. However, none of them actually describes what an Islamic state would look like or how it would function.

Qutbists' violence and desire for an Islamic state are weaknesses that Phase 5 exploits. During this phase, the Construction node makes subtle changes to the web sites under their control to highlight violent acts committed by Qutbists. The overwhelming majority of Muslims view Islam as the religion of peace. To them, the association of violence and Islam is a contradiction. By focusing on the violent acts committed by Qutbists in the name of Allah, support for the Qutbists should wane within the Muslim community.

In this phase, the Construction node also starts to describe what an Islamic state will look like and how it will function. However, each site has a different version of what an Islamic state will look like. Some sites focus on installing an Islamic Caliphate, while others focus on national Islamic states.[16] The *Caliphate* is an Islamic federal government that represents both political

[16] Caliphate, 12 December 2006; available from http://en.wikipedia..org/wiki/caliphate#reestablishment_of_a_modern_caliphate (accessed 12 December 2006).

leadership and unities of the Muslim world applying Islamic rule known as Shariah law.[17] Because no set Shariah law exists—that is, as recognized by all Muslims—each site has its own version of Shariah law that will be enforced under the Islamic state.[18]

The sites also highlight the role of women in an Islamic state, rights of non-Muslims, and punishments for violating Shariah law. The ultimate purpose is to let potential supporters of the sites know what they are getting into. An Islamic state may sound like a good idea to many Muslims. However, once they understand the details, they may start questioning whether the idea is good or not. In addition, attaching different versions of an Islamic state to different Qutbist groups should foster hostilities between them and thereby help keep the different factions from uniting to achieve their goals.

f. Phase 6, Concentrate Web Sites

Using the math model, by day 1,032 virtually all of the Qutbists' web sites could potentially be eliminated. However, the math model deals with absolutes while the real world changes as the situation changes. Most likely, the Qutbists will counter the attack on their web sites by increasing the production of web sites. The only way to counter this is to recalibrate the attack rate until equilibrium is achieved between creation and destruction. At this time, the Construction node stops making new web sites. The Demolition node continues to attack any

[17] Caliphate, 12 December 2006; available from http://en.wikipedia..org/wiki/caliphate#reestablishment_of_a_modern_caliphate (accessed 12 December 2006).

[18] Sharia, 13 December 2006; available from http://en.wikipedia.org/wiki/shariah (accessed 13 December 2006).

identified Qutbists' sites and starts to shut down Construction node sites at the same rate they are attacking the Qutbists' web sites. At this pace, all web sites would be eliminated by day 1375. However, on day 1369, the Demolition node stops shutting down sites created by the Construction node to leave about 50 sites in operation for monitoring and message control (as illustrated in the Figure 4). The Demolition node continues to attack any Qutbist's web site that makes it on the list.

During these constant attacks, it is likely that the Qutbists will dive deeper into the internet by creating more Darknet environments and moving to them. There is little to counter this measure, but it does provide an opportunity for members of the Network node to try to follow the Qutbists down their rabbit hole and infiltrate these new Darknets. In addition, as the Qutbists dive deeper into the internet, their ability to communicate with the mass public Muslim audience and influence potential Qutbists will be severely reduced.

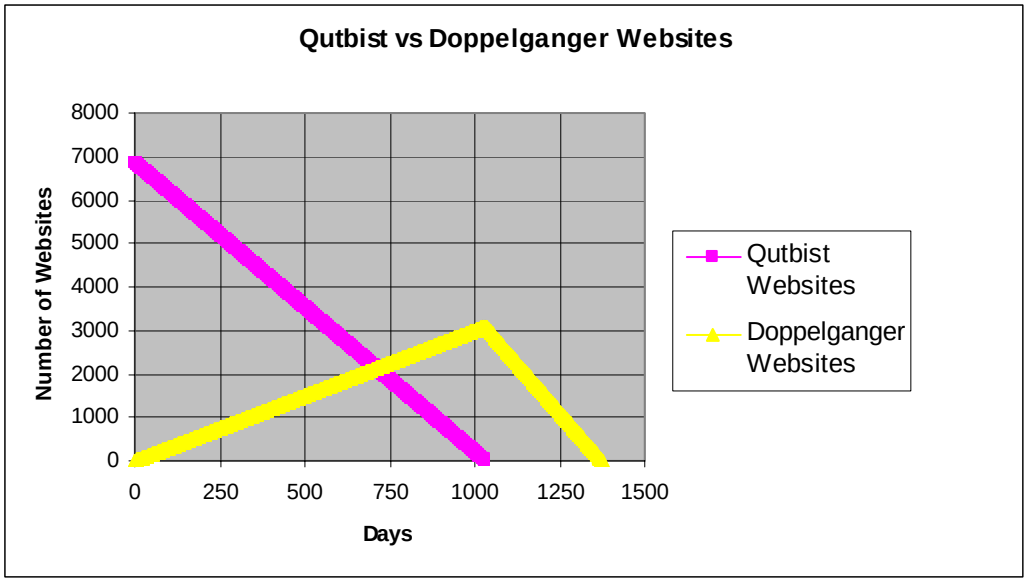


Figure 4. Qutbist vs. Doppelganger Web Sites

g. Phase 7, Develop Darknet

During this phase, the Construction node develops content-rich Darknet environments. This phase could be started in conjunction with Phase 5. As stated earlier, a Darknet is a password-protected virtual private network where users connect only to people they trust.[19] These Darknet environments offer e-mail, file sharing, chat, instant messenger, and streaming video services. Once a Darknet is created, the Construction node sends the URL to the Network node.

The Network node picks a connector with whom they have developed a strong trust relationship and invites him or her to become a member of the Darknet. This invitation comes in the form of three e-mails to give the URL of the site, temporary user name, and temporary password, respectively. Many terrorist and criminal groups are already using password-protected web sites to further their operations, so this concept should be familiar to many Qutbists on the internet. When the connecter clicks on the URL, a web page opens.

The only thing on this page is a form for a user name and password, with a submit button. When the connector completes the fields and clicks the button, a prompt appears requesting the user to establish a new user name and password. When that task is complete, a welcome message appears similar to the following:

[19] Darknet, 9 December 2006; available from http://en.wikipedia.org/wiki/darknet (accessed 12 December 2006).

a. You are entering a secure web site developed to promote the Jihadists' causes and were chosen for access because of your faith and dedication.

b. You can invite up to 10 people to join the Web site, but only invite those you trust 100 percent.

A message of this nature makes the user feel special and secure. If the connector likes the Web site, he may choose to invite others. On the other hand, if he does not like the Web site, the Network node will have to start over with a new connector. Anyone invited to join the network will go through the same process as the connector. Using small-world theory, the Network node can have Qutbists build a detailed map of their virtual social network.[20] In his 1967 study, psychologist Stanley Milgram illustrates this theory by showing that no more than six people separate people from each other.[21] As people join the Darknet, a computer program constructs a social network map showing the connections between the individuals and people that invited them to join the network. The program also performs these tasks:

a. Updates the map whenever users send e-mails from their Darknet accounts and chat with other Darknet users.

b. Runs Internet Protocol (IP) and e-mail tracking software against all users. This software provides estimated geographical locations for each user's IP address and Darknet e-mail account.

c. Provides contact information for the person who owns the IP address and for the person's host service provider.

---

[20] Small World Phenomenon, 12 December 2006; available from http://en.wikipedia.org/wiki/small_world_phenomenon (accessed 14 December 2006).

[21] Ibid.

The social network map incorporates all of this information. The map can be used to identify geographical clusters within the network, links between clusters, and vital network hubs that can be targeted for human intelligence surveillance. If multiple users are accessing the Darknet using the same computer, a possible headquarters for a Qutbist group may emerge that can be targeted for human intelligence. Another benefit of the Darknet is the ability to mine data from Darknet e-mail accounts, file sharing, and chat room conversations.

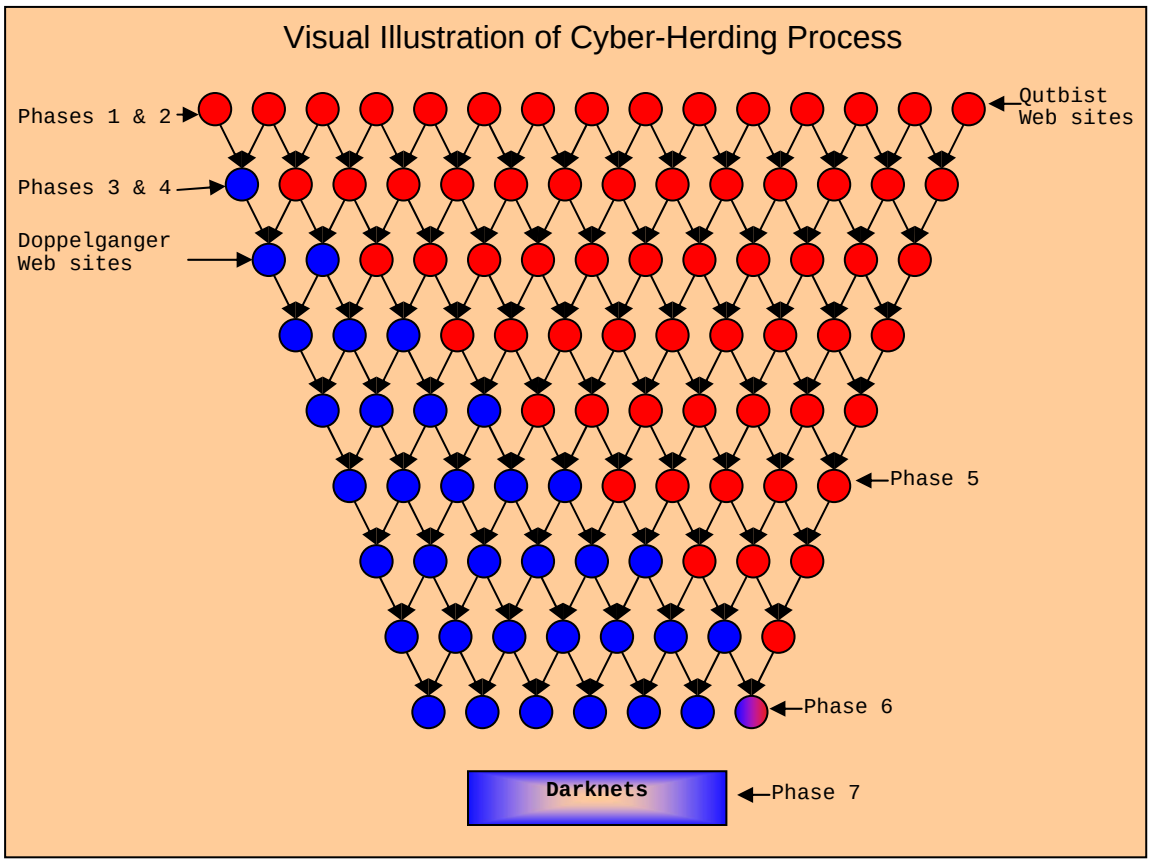


Figure 5. Visual Illustration of Cyber-Herding Process

B. CYBER ACTIVISM

1. Defining Cyber Activism

The strategy of cyber activism is derived from mass social movements. According to social movement expert Manuel Castells, social movements are "purposive collective actions whose outcome, in victory as in defeat, transforms the values and institutions of society."[22] With this in mind, cyber activism could be used to galvanize the global population around a counter-Qutbist ideology.

The first step is to establish a one-stop internet web site for combating Qutbist ideologies. Aaron Kreider, an online activist, highlighted a conceptual framework used to establish support for a cause: the development of a strategy, training, allies, sharing, and technical savvy community.[23] All of these components would be included through an international consortium in order to educate the masses on Qutbist rhetoric and to discredit their messages; mobilize groups of like-minded individuals at the grassroots level; and provide guidance and suggestions for taking action.

2. Format of Web Site

a. International

Many people throughout the world do not trust the United States. For Muslims this is especially true.[24] To

---

[22] Manuel Castells, *The Power of Identity* Vol. 2, *Economy, Society & Culture*, (Oxford: Blackwell, 1997), 3.

[23] Aaron Kreider, "Online Activism 2.0: Movement Building," ZNet, available from http://www.zmag.org/content/showarticle.cfm?ItemID=11802 (accessed 5 September 2007).

maximize the potential for the Cyber Activism (CyAct) web site to succeed it should have an international face. A good beginning would be to invite participants of the United Nations Security Council Counter-Terrorism Committee to join the CyAct web site in accordance with resolution 1373 and follow this up with invitations to all countries currently fighting Qutbists.[25]

b. Multilingual

If the CyAct web site is international, then it only makes sense that the CyAct web site will also need to be multilingual. Not everyone speaks English. Even people who speak English as a second language would be more likely to use the CyAct web site if it were offered in their native tongue. Offering the CyAct web site in multiple languages will increase the number of users on the CyAct web site and the usability of the CyAct web site to those users.

c. User-Run

Similar to many wiki sites, such as Wikipedia, the CyAct web site will utilize the worldwide cyber community to assist in running and maintaining the site's content. By implementing a user-run site, the CyAct web site can harness the free labor on the internet, thus reducing the overall staffing and funding needed for the CyAct web site. To avoid abuse and to maintain accuracy of

[24] The Great Divide: How Westerners and Muslims View Each Other, Europe's Muslims More Moderate, 22 June 2006; available from http://pewglobal.org/reports/display.php?pageid=831 (accessed 4 December 2006).

[25] UN Security Council CT Committee, "List of International, Regional and Subregional Organizations," available from http://www.un.org/sc/ctc/pdf/iros-nairobi2007.pdf (accessed 10 September 2007).

the CyAct web site, all inputs will go through an approval process similar to Scholarpedia. Scholarpedia requires all inputs to go through an anonymous peer review followed by approval or disapproval from a curator.[26] The CyAct web site will use this two-person concept to approve or disapprove user inputs. When a user submits material to the CyAct web site, two random users will be selected to review the input and approve or disapprove the data. If approved, the CyAct web site is updated with the user's input. If disapproved, the user is notified. In addition, just like Wikipedia and Scholarpedia, all users will be able to modify content on the CyAct web site. Of course, any modifications will also have to go through the same approval process.

While this two-person concept is intended to limit abuse, it should be assumed that some Qutbists will join the CyAct web site with the intent of sabotaging this process. To counter this, user actions, such as input, approvals, and disapprovals, should be monitored for pro-Qutbists' leanings and perhaps even tested by sending a known Qutbist's web site to a user to see if the user approves or disapproves the web site. If a user is identified as a possible saboteur, then the user's account is flagged. A flagged user will no longer receive other users' inputs for review.

d. Mirrored

If the CyAct site is successful, then it will most likely come under distributed denial-of-service (DDoS) attacks. To limit the impact of these DDoS attacks, the

[26] Eugene M. Izhikevich (2006) Main Page. Scholarpedia, p. 1286 available from http://www.scholarpedia.org (accessed 9 November 2007).

CyAct web site will have multiple geographically separated mirrors. A mirror site is an exact copy of another Internet site. In this way, if a site comes under attack, then users can still access the site through a mirror. Also, when the attack is over, then the site that was down can update itself from the other sites.

3. Education

Over one hundred sixty years ago, Alexis De Tocqueville wrote in *Democracy in America* that "the American system contains a great number of truths so evident that men, if they are only educated, cannot fail to see them."[27] This is just as true today. The truth is a powerful weapon. When confronted with it, people must either accept the truth or close their mind to reality. Those that close their minds to the truth are lost to us. However, for those open-minded people, the truth will find fertile ground to take root. Education is the key to spreading the truth. The CyAct web site will provide an excellent platform to educate users on the Qutbists' ideology and counter ideology. It will also provide interactive sections so the users can contribute and become a part of the education.

a. Qutbists' Ideology

The first step in educating users is to explain the Qutbist's ideology and what the Qutbists want. This can be a difficult task as oftentimes Qutbist rhetoric and actions do not go hand in hand. However at the core of the

[27] Alexis DeTocqueville, *Democracy in America*, 1899, Henry Reeve Translation, revised and corrected, available from http://xroads.virginia.edu/~HYPER/DETOC/ch2_08.htm (accessed 10 September 2007).

Qutbist ideology is a desire to strike at the West (especially the United States) as well as what Qutbists perceive as infidel regimes within Muslim lands. The grounds Qutbists proclaim their attacks upon are that these non-Muslim elements have tainted their lands and religion and that the only way to eliminate these obstacles towards a purely Muslim society ruled by Islamic law is to engage in jihad ("resistance against aggression, especially against non-believers who are aggressive and oppressive of Muslims"[28]). According to these radicals, the absence of Shariah law is what has led to many of the problems within society like poverty, injustice, and corruption.[29] Once the non-Muslim elements have been removed and Shariah law imposed, the radicals believe they will live in a much better society in the eyes of Allah.

b. Discredit Qutbists' Ideology

Qutbists lose credibility among mainstream Muslims when they attack women, children, and the elderly; damage the sources of a nation's wealth (such as tourism and oil); kill other Muslims; and declare other Muslims apostates.[30] Per Albert Bandura, terrorists use mechanisms of moral disengagement to justify these attacks.[31] The most

---

[28] Lisa Katz, "Radical Islamic Ideology Legitimizes Terrorism," About.com, available from http://judaism.about.com/library/1_terrorism/bl_terrorismisrael_d.htm (accessed 10 September 2007).

[29] Kim Cragin, "Understanding Terrorist Ideology," Rand Corporation, 12 June 2007, available from http://www.rand.org/pubs/testimonies/2007/RAND_CT283.pdf (accessed 11 September 2007).

[30] William McCants, *Militant Ideology Atlas*, Combating Terrorism Center, November 2006, available from) http://www.ctc.usma.edu/atlas/Atlas-ExecutiveReport.pdf (accessed 10 September 2007).

[31] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Dulles, VA: Potomac Books, 2006), 55.

popular mechanism is the displacement of responsibility, which consists of blaming the authorities, the circumstances, or even the victims themselves.[32] This mechanism is often used in conjunction with the mechanism of diffusion of responsibility, which minimizes personnel responsibility by distributing responsibilities so no individual task is too terrible.[33]

The CyAct web site will attempt to counter these tactics and others by providing videos of Qutbists violence against women, children, the elderly, and fellow Muslims. Other videos will show the Qutbists using civilians as human shields, Qutbists fighting from religious buildings, and Qutbist videos declaring other Muslims apostates. Using this visual medium, will firmly place the responsibility back with the Qutbists.

Additional measures to discredit the Qutbists' ideology would be to implement the following measures addressed in the *Militant Ideology Atlas:*[34]

1. Highlight statements by influential Salafi clerics denouncing terrorism.
2. Convince Jihadi intellectuals who are truly influential in the movement to renounce certain targets and tactics. Al-Tartusi, for example, shocked his Jihadi colleagues when he renounced suicide attacks after the London bombings; the same happened after al-Maqdisi criticized some of Zarqawi's tactics.

---

[32] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Dulles, VA: Potomac Books, 2006), 55, 56.

[33] Ibid., 55.

[34] William McCants, *Militant Ideology Atlas*, Combating Terrorism Center, November 2006, available from http://www.ctc.usma.edu/atlas/Atlas-ExecutiveReport.pdf (accessed 10 September 2007).

3. Focus on the divisive issues described above as part of broader efforts to delegitimize violence against non-combatants and to impugn the methods of Jihadis as ineffective and counterproductive means for social change.

4. Counter the recurring themes found in Jihadi literature (detailed above) with the following messages:

   — Jihadis want a totalitarian system of government in which people are not allowed to think for themselves. Not even the Saudi government is strict enough. Anyone who does not share their understanding of Islam will be declared an apostate and executed. If you want to know what a Jihadi state will look like, contemplate the Taliban—the only state in recent memory that Jihadis consider to have been legitimately Islamic.

   — The Jihadi message is so weak and unappealing that they have to use violence to persuade people. They claim to be saving Islam, but they are giving it a bad reputation. They are hurting their own people and national resources.

5. Remind people of what happens when Jihadis come to power. This could be done with commercials and documentaries focusing on the atrocities committed by the Taliban or by al-Qa`ida in Falluja, or perhaps a video game or movie in which the setting is a Middle East governed by the Jihadi caliphate.

Convincing Jihadi intellectuals to renounce certain targets and tactics would most likely produce the greatest results in countering the Qutbists' ideology. Unfortunately, this measure would also be the most difficult to implement. While many Muslim scholars have spoken out against Qutbists' actions, there are a couple of

reasons for them not being as vocal as they could be. One reason is that it is fairly common for prominent critics of Qutbists to receive death threats against themselves and their families. This serves as a deterrent to others that would speak out. Another reason many prominent Muslims may refrain from being vocal is to avoid fitna. Fitna has many definitions in Arabic, but it basically means conflict or disunity within the Muslim Ummah (the community of all Muslims). In the Muslim culture, fitna is to be avoided at all costs.

For these reasons, the cyber activism process should try to seek out these influential Muslims, but should put the main focus on implementing the other measures. The one measure that could produce results and could be implemented fairly easily is reminding people what happens when Qutbists come to power. This can be accomplished using a combination of web and television commercials directed toward the host and world populations. The other measures can also be incorporated into these adverts.

c. Counter Ideology

The Bush administration has proposed a counter strategy of promoting effective democracies.[35] This strategy is based on the Democratic Peace Theory that proposes that democracies never or almost never go to war with each other.[36] Yet, the United States has never been

[35] National Security Council, *National Strategy for Combating Terrorism,* September 2006, available from http://www.whitehouse.gov/nsc/nsct/2006/nsct2006.pdf (accessed 10 September 2007).

[36] Democratic peace theory, 13 November 2007, available from http://en.wikipedia.org/wiki/Democratic_peace_theory, (accessed 9 November 2007).

consistent in promoting democracies throughout the world. When it is in the United States self interest, it has developed and maintained working relationships with dictators, monarchs, and communist governments throughout its history. This inconsistency causes many people throughout the world to question the United States promotion of democracy.

Additionally, the ability to reach out to Muslim populations will require trusted experts and professionals from within the Muslim religion and culture. To counter the Qutbists' ideology, the CyAct web site will seek out Muslim individuals and groups that can help argue against the Qutbists ideology and at the same time understand the cultural and religious sensitivities to the various target audiences. One such group is the Religious Rehabilitation Group (RRG). The RRG is a voluntary group formed by Islamic scholars and teachers focused on countering Qutbist ideology.37 On their web site, they provide a response and a counter to the Qutbists' ideology. While this counter ideology is focused on the Singapore group of Jemaah Islamiyah, it can be used as a basis of developing counter arguments to other groups as well.

d. Interactive Map

The interactive map is an up to date map of the world showing Qutbists incidents and deaths caused by Qutbists' attacks. To populate the map's database, the CyAct site should seek collaboration with organizations like the Memorial Institute for the Prevention of Terrorism

37 Religious Rehabilitation Group, "RRG – An Introduction", available from http://www.rrg.sg/subindex.asp?id=A033_07 (accessed 10 September 2007).

(MIPT) in order to share data, including their Terrorism Knowledge Base (TKB). The MIPT TKB is a comprehensive database of global terrorist activities. In addition, users will be encouraged to submit inputs to keep the interactive map up to date.

e. Bulletin Board

The CyAct web site's bulletin board provides users a forum to discuss the CyAct web site, Qutbists' ideology, the counter ideology, and methods of action. Users can ask questions and post comments.

4. Taking Action

The purpose of education is to motivate the cyber community to get involved and decide to take action. The CyAct web site will harness this potential in the cyber community and direct it by providing users with multiple paths to direct their energy.

a. Database

In July 2007, the Middle East Media Research Institute (MEMRI) suggested that an effective measure against the Qutbists' online activities would be to establish a database - governmental or non-governmental -, which would regularly publish information about Islamist/Jihadi sites, and/or provide it to ISPs upon request.[38] The CyAct web site will take this idea a step forward. The CyAct web site's database will provide an up

[38] Gary Ackerman & Mike Pence, "The Enemy Within: Where Are the Islamist/Jihadist Web sites Hosted, and What Can Be Done About It?," Middle East Media Research Institute, *Inquiry and Analysis Series - No. 374*, 19 July 2007, available from http://memri.org/bin/articles.cgi?Page=subjects& Area=jihad&ID=IA37407 (accessed 10 September 2007).

to date list containing each Qutbists' web site's address, internet protocol address, contact information for the web site's internet service provide/host, and a comments section. The database will do a systematic search of the web sites on the list to verify the site is available. If the site is down, then that site will automatically be removed from the database.

b. Contacting ISPs

The CyAct web site advocates that users contact the ISPs about the web sites on the list and ask the ISPs to remove those sites. The ISPs have a legal authority to remove sites that violate the law or web sites that abuse their own regulations as laid down by the ISPs.[39] Thus, with information on Qutbists' sites at their disposal, the ISPs should have both the ability and the obligation to remove such sites from their servers.[40] If the ISP does not take action against a Qutbists' web site, then the next step would be for the user to contact the appropriate legal authority for the ISP and report the ISP for hosting a Qutbist's web site. In addition, the user can access the Qutbist's web site and try to disrupt it from within by posting comments and content counter to the site's content.

c. Finding/Submitting Web Sites

The CyAct web site will also explain to users how to locate Qutbists' web sites on the internet and ask them

---

[39] Gary Ackerman & Mike Pence, "The Enemy Within: Where Are the Islamist/Jihadist Web sites Hosted, and What Can Be Done About It?," Middle East Media Research Institute, *Inquiry and Analysis Series - No. 374*, 19 July 2007, available from http://memri.org/bin/articles.cgi?Page=subjects& Area=jihad&ID=IA37407 (accessed 10 September 2007).

[40] Ibid.

to submit these web sites to the database. To find Qutbists' Arabic web sites, a user might first use Google Translate to convert word combinations from English to Arabic, and then do a Google search on the translated words. These word combinations need to be creative. Just doing a search on Osama bin Laden will provide thousands of results mostly from legitimate sources making the identification of an actual Qutbist's web site unlikely. In addition, doing a search on terms such as terrorist, Islamic extremist, radical Islam, etc., would most likely lead nowhere as the Qutbists do not see themselves in these terms. The best approach would be to review Qutbist literature and use terms and phrases that they favor. This will still produce hundreds of web sites, but the potential that a Qutbist's web site is now in the users search has gone up. At this point, the user should consider developing a group of users to assist in analysis the results from the search.

To help analyze a web site, the user could click on the translate webpage option that Google provides. If a user believes they have found a Qutbist's web site, they can then collect information on the web site by going to sites such as www.allwhois.com, www.whois.net, http://godaddy.com, www.apnic.net, www.arin.net, and www.ripe.net.

Some of these sites require the actual IP address for the site. An easy way to get the actual IP address is to open up a command prompt, type in ping followed by the web site's name, and then click enter. This will provide the user the actual IP address for the site. Once the user has collected all of the necessary information, they can

submit the web site to the database. To help craft the criteria to determine if a site is a Qutbist's web site, the CyAct web site managers should contact MEMRI, Internet Haganah, and the Search for International Terrorist Entities (SITE) Institute to see if they would be willing to share the criteria they use. In addition, the CyAct web site managers should ask these organizations their methods of tracking down web sites so these methods could be shared with the sites' users.

d. Report Information

This section of the CyAct web site provides a Qutbist wiki that users can browse to obtain information, to include photos, on Qutbist individuals and groups. Users can also submit updates to the wiki. In addition, the CyAct site will request users to submit specific information concerning Qutbists' locations, activities, and possible operations. The message for users is that through their actions, they can save an innocent life or lives. When users submit information, they will be given an access code for a reward program. If the information leads to the capture or death of a wanted Qutbist or the uncovering of a Qutbists operation, then a reward for the access code is activated.

When the user visits the CyAct web site and types in the access code, the CyAct site will inform the user that the user qualified for a reward. The CyAct site will request the user to select a payment method, either directly by mail or an online bank account or indirectly through a third party. By setting up the reward program in

this way, it should prompt more people to provide usable information, because they do not have to interact with anyone.

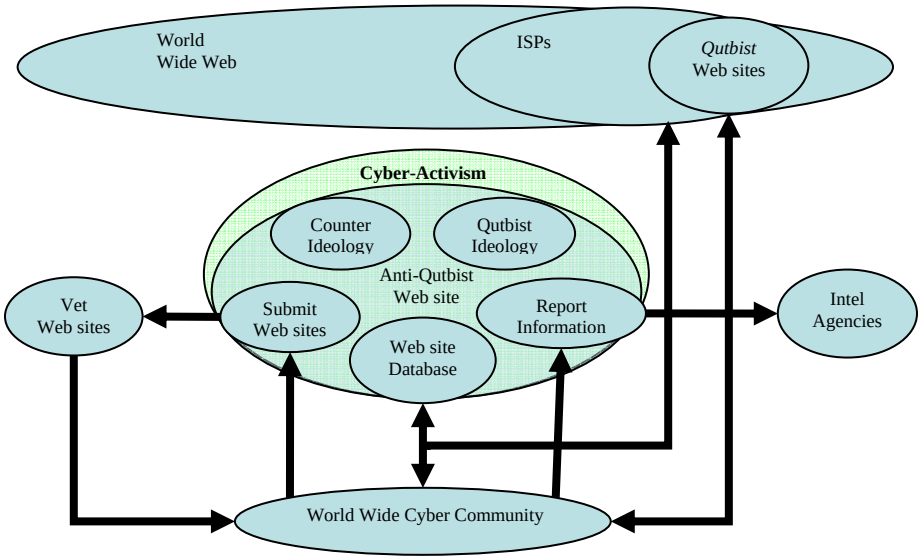


Diagram of Cyber Activism

Figure 6. Diagram of Cyber Activism

5. Mobilization

For the CyAct web site to succeed it needs people to access, join, and participate. Three methods to get people to visit the CyAct web site are an active ad campaign, adding links to existing web sites, and a grassroots campaign.

a. Ad Campaign

The first step in getting the word out about the CyAct web site will be to engage in a massive ad campaign. The CyAct web site would purchase ad spots with ISPs. The ads need to be crafted to maximum hits to the CyAct web site. A possible slogan for the ad could be “Terrorism -

Join the Fight." This slogan is cryptic enough to get people from different sides of the Qutbists' battle to click on it and go to the CyAct web site.

b. Links

Most people who use a search engine only look at the first couple of pages returned by the search engine. If you want your web site visited, you want your web site as high as possible on those first couple of pages. The most popular search engine on the internet is Google.[41] To rank web pages, Google uses a method based on PageRank. PageRank relies on the uniquely democratic nature of the web by using its vast link structure as an indicator of an individual page's value. In essence, Google interprets a link from page A to page B as a vote, by page A, for page B.[42] All votes are not equal. Popular web sites' votes count more than less popular web sites. To maximize the CyAct web site's page rank, all state, federal, and partner countries web sites should be asked to link to it on their web sites.

c. Grassroots

It has been said that the best form of advertizing is word of month. People are more likely to try or buy a product if a friend or a family member recommends it. The mixed strategy takes advantage of this marketing technique by requesting users that visit the

---

[41] Danny Sullivan, "Nielsen NetRatings Search Engine Ratings," The Click Z Network, 22 August 2006, available from http://searchenginewatch.com/showPage.html?page=2156451 (accessed 11 September 2007).

[42] Google Advertising Programs, "Reach in-market customers at every step of the buying cycle," Google.com, available from http://www.google.com/forms/ads7.html (accessed 10 September 2007).

CyAct web site to invite their friends and family to the CyAct site. By incorporating the social networks of a small number of people in the beginning, the message should spread rapidly to other networks around the world.

C. MIXED STRATEGY

The mixed strategy consists of cyber activism combined with some elements of cyber-herding. In this strategy, cyber-herding is reduced to a "cyber-herding lite" that consists of a Construction node and the Network node.

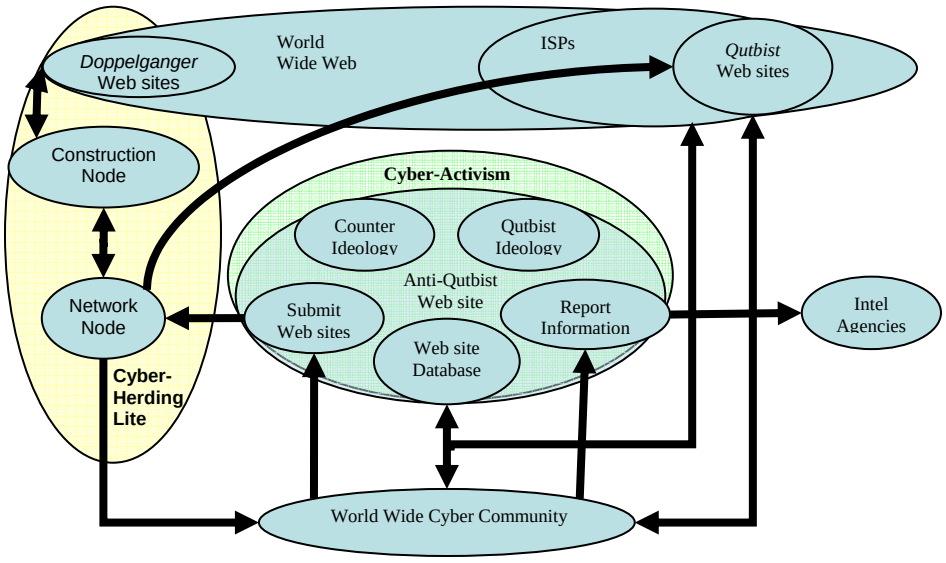


Figure 7. Diagram of Cyber Activism with Cyber-Herding Lite

Cyber activism replaces the Gatherer Node and the Demolition Node. This strategy has a few differences from the other two strategies.

The first difference involves submitting suspected web sites to the cyber activism web site. Instead of going straight to a voting process, the IP address is sent to the Network node of the cyber-herding lite program. The

Network node reviews the web site to determine if it is rich in users, documents, videos, graphics, messages, or other content. If the Network node determines the site is not worth infiltrating, then the site is forwarded to the normal user review process of cyber activism. On the other hand, if the Network node determines the site is worth infiltrating, then it shares the IP address with the Construction node and puts a limited hold, such as 10 to 14 days, on forwarding the web site to the user review process.

During this hold period, the Network node mines the site for usernames, email address, conversations, etc. The Network node also starts to insert their own virtual fictitious identities into the Qutbist's web site to try to develop social ties in the Qutbists' network. In addition, during this period the Construction node accesses the Qutbist's site to mine documents, videos, messages, graphics, etc. for the creation of doppelganger web sites.

The second difference from cyber-herding is in the number of doppelganger web sites created by the cyber-herding lite operation. The Construction node will only create a manageable number of doppelganger web sites, instead of trying to create hundreds of doppelganger web sites to reach parity with Qutbists' web sites.

THIS PAGE INTENTIONALLY LEFT BLANK

III. STRATEGIC ASSESSMENT METHODOLOGY

A. EVALUATION

1. Minimum Requirements

The strategies must meet the following minimum requirements:

a. Identify Qutbists' Web Sites

Cyber-herding meets this requirement because it actively seeks out Qutbists' web sites. While cyber activism and the mixed strategy do not actively seek out Qutbists' web sites, these strategies do provide a platform for internet users to seek out Qutbists' web sites. It can be assumed that a percentage of the internet population is interested in finding Qutbists' web sites. If they decide to utilize the web site, then cyber activism and the mixed strategies meet this requirement.

b. Shut Down Qutbists' Web Sites

Cyber-herding meets this requirement because it actively tries to shut down Qutbists' web sites. While cyber activism and the mixed strategy do not actively shut down Qutbists' web sites, these strategies do provide a platform for internet users to help shut down Qutbists' web sites. It can be assumed that a percentage of the internet population is interested in shutting down Qutbists' web sites. If they decide to utilize the web site, then cyber activism and the mixed strategies meet this requirement.

c. Counter Qutbists' Ideology

Cyber-herding meets this requirement as it subtly changes the Qutbists' message and ideology over a period of time. Cyber activism meets this requirement because it directly counters the Qutbists' ideology. The mixed strategy meets the requirement by directly challenging the Qutbists' ideology and covertly changing the Qutbists' message and ideology.

d. Legal

There are two issues that could have legal ramifications: shutting down web sites and copyright infringement. Shutting down a Qutbist's web site is not in itself an illegal act, but it must be done in accordance with the host country's laws and regulations. As long as the Demolition node of cyber-herding follows its host country's laws and regulation, then it should meet the legal requirement. This may mean that the Demolition node will have to have a judge or a legal panel review and approve web sites before the node can shut the sites down. Cyber activism and the mixed strategy also meet the legal requirement because these strategies do not directly shut down any web sites. Instead, these strategies rely on ISPs, at user or law enforcement request, to shut down the Qutbists' web sites. Of course, some "hackers" may go beyond the web sites recommendations, but this does not reflect negatively against the strategies as the strategies only advocate legal methods of shutting down or disrupting web sites.

Each of these strategies involve using material that could possible fall under copyright law, more so for cyber-herding and the mixed strategy than the cyber activism strategy. While some of the material would fall under the provisions of the fair use doctrine, all of these strategies should have a legal review of material to determine status before it is copied. As long as these strategies do this, then these strategies would meet the legal requirement.

2. Comparative Criteria

In *Toward an Understanding of Military Strategy*, Arthur F. Lykke, Jr. developed an equation to explain what makes up a strategy.[43] His equation states that strategy equals the ends (objectives of the strategy) plus the ways (courses of action) plus the means (resources). While this equation does not explain how to choose a strategy, it does provide a good framework to start with. The courses of action (ways) you choose are based on achieving the objectives of the strategy (ends) and the resources available (means). It is logical to assume that you want to choose a course of action that maximizes your potential to achieve objectives while minimizing the use of resources or costs. But, this is still incomplete because it does not factor in the time to implement the course of action. Nor does it factor in the will to implement the course of action. Thus, deciding on a strategy is based on choosing the best course of action that you are willing to implement, that has the greatest potential to achieve the

[43] Arthur Lykke, **"**Toward An Understanding of Military Strategy", in *U.S. Army War College Guide Strategy*, Joseph R. Cerami and James F. Holcomb, Jr., eds., (Carlisle Barracks, PA: Strategic Studies Institute, 2001), 179.

objectives of the strategy, at the least cost, and within a timely manner. This forms the basis for the comparative criteria that follows:

a. Objectives

There are three objectives to compare: identify and shut down Qutbists' web sites, counter Qutbists' ideology, and collect information on Qutbists.

b. Cost

There are three costs to compare: manpower, hardware and software, and real estate

c. Time

The comparative criteria for time category is the time it takes to implement the course of action.

d. Will

The acceptability of the strategy to the government and decision makers, and the populations of the host country and the world influence "Will", so these areas will be compared.

B. ASSESSMENT

This section will assess each of the strategies and rank the strategies from best to worst in each area.

1. Objectives

a. Identify and Shut Down Qutbists' Web Sites

The cyber activism strategy relies on the internet community to identify and shut down Qutbists' web sites. The mixed strategy uses cyber activism, but it also

has individuals working in the Network node that may come across Qutbists' web sites. Thus, the mixed strategy is better than the cyber activism strategy. The cyber-herding strategy has individuals in two nodes with the sole job of finding and shutting down Qutbists' web sites. If the cyber activism and mixed strategies attract enough users, then they have the potential of outperforming the cyber-herding strategy. However, attracting users is an unknown. On the other hand, the cyber-herding strategy has the known quality of hiring people to perform these functions. Thus, even though the cyber activism and the mixed strategies have a greater potential than cyber-herding, this author has to rate the cyber-herding strategy as the best in this area due to the unknown nature of the other two strategies.

b. Counter Qutbists' Ideology

Cyber activism provides a direct counter to the Qutbists' ideology, but it still needs people to access the site to get the message. Cyber-herding is a little better because it actively employs individuals to make subtle changes to the Qutbists' message. The mixed strategy would be the best strategy in this area as it deploys both methods.

c. Collect Information on Qutbists

Cyber activism requests users provide information on Qutbists, but it still needs people to access the site and provide the information. Cyber-herding is better because it actively employees individuals in the Network node to collect information on the Qutbists. The mixed strategy would be the best strategy in this area as it deploys both methods.

2. Cost

a. Manpower

The cyber activism strategy is the most cost effective in manpower because it would only require a small workforce or it could use a virtual workforce of existing personnel. The mixed strategy would be next because it would require a smaller workforce than cyber-herding.

b. "Real Estate" (Space Requirements)

The cyber activism strategy is the most cost effective in real estate because it would only require a few offices or it could use virtual offices with existing personnel working from their primary jobs. The mixed strategy would be next because it would require less office space than cyber-herding.

c. Hardware and Software

Much of the automated social network software advocated for cyber-herding currently does not exist and will have to be developed. In the interim, cyber-herding will have to utilize manual social network software such as UCINET, Pajek, Netdraw, etc. The developmental costs plus the purchase of existing software will make cyber-herding the most costly of the three strategies. The mixed strategy requires the same software as cyber-herding yet will not have to support a Gatherer and Destruction nodes so its hardware and software costs will be slightly less than cyber-herding. The hardware and software requirements for the cyber activism strategy already exist and can be purchased off the shelf so it is the most cost effective.

3. Time to Implement

The cyber activism strategy could be implemented in the shortest period of time and the cyber-herding strategy would take the longest time to implement.

4. Will

a. Host and World Population Acceptability

The cyber activism strategy is an overt strategy so it would most likely be the most acceptable to the populations of the host county and the world. The cyber-herding strategy is a covert deception and psychological operation. Many people fear operations of this nature, because they feel that the government has either been lying to them or shaping their perceptions or both. Thus, if the cyber-herding strategy became known to the general public, it would most likely be less acceptable to both populations than the cyber activism strategy. The mixed strategy uses an overt strategy in conjunction with a covert strategy. If this becomes known to the general public, it raises all of the concerns that people would have against cyber-herding, but it also has the additional risks of alienating the general public and users of the CyAct web site who may feel that they have been deceived. Thus, the mixed strategy would be the least acceptable to both populations if it became known.

b. Government and Decision Makers Acceptability

All of the comparative criteria listed in this chapter would influence government and decision makers' acceptability of a strategy. In addition, government and decision makers would also be influenced by the strategy's

potential for blowback or unintended consequences. Blowback could occur from the press reporting that the government is running and supporting terrorists' web sites or that the government is spying on people who are just engaging in free speech. Some unintended consequences could be further radicalizing the Qutbists by influencing their messages, increasing recruitment, or alienating the Muslim community because of the appearance the strategy is targeting Islamic web sites.

C. SCORING

In this section, values of one to three are assigned to each of the areas based on the assessment in the previous section. One represents the best strategy, two represents the next best strategy, and three represents the least best strategy. These values are inputted in a decision matrix software call DECMAT.[44] DECMAT allows multiple strategies to be compared using various comparative criteria. Of course, not all comparative criteria are worth the same, so DECMAT also allows the user to weigh each of the comparative criteria against each other.

To help reduce subjectivity in weighing, DECMAT uses a technique of Pairwise Comparison. The first step is to rank the criteria in general importance. Then, you evaluate each criterion against each of the other criteria by assigning it a numerical importance factor. An input of one means that the criteria are equal, a two means that one criterion is slightly favored over the other, a three means that one criterion is favored over the other, and a four

[44] DECMAT Program for Windows Ver. 2.2, CPT Richard B. Stikkers, no copyright.

means that one criterion is strongly favored over the other. Table 2 shows the inputs used for the comparative criteria developed in this thesis.

Pairwise Comparison	Counter Ideology	Collect Information	Time	Manpower	Real Estate	Hardware & Software	Govt & Decision Makers	Host Country	World Population	Legend of Importance Factors 1 - Equal 2 - Slightly Favored 3 - Favored 4 - Strongly Favored
Identify and Shutdown	1	2	2	3	3	3	1	4	4	The importance factor of each horizontal evaluation criteria compared to each vertical evaluation criteria
Counter Ideology		2	2	3	3	3	1	4	4	
Collect Information			2	3	3	3	1	4	4	
Time				2	2	2	1	4	4	
Manpower					1	1	1	4	4	
Real Estate						1	1	4	4	
Hardware &Software							1	4	4	
Govt & Decision Makers								2	2	
Host Country									1	

Table 2. Pairwise Comparison

When values are selected and sent, DECMAT automatically assigns a mathematical weight for each criterion. The next step is to enter the courses of actions. Then input how the courses of actions rate against each other for each criterion. The DECMAT program automatically assigns a total value for each course of action.

D. RESULTS

The results of the DECMAT software place the mixed strategy as the best strategy to implement. It is followed by the cyber activism strategy and then by the strategy of cyber-herding. See Table 3 for the details of the results.

DECISION MATRIX

Weight	6.95	6.95	5.62	4.06	2.66	2.66	2.66	4.67	1.17	1.00	Total
Criteria / COA	Identifv and Shutdown	Counter Ideology	Collect Information	Time	Manpower	Real Estate	Hardware/ Software	Govt/Decisi on Makers	Host Country	World Population	
Cyber-Herding	1	2	2	3	3	3	3	2	2	2	81.882
Cyber Activism	3	3	3	1	1	1	1	1	1	1	77.457
Mixed	2	1	1	2	2	2	2	3	3	3	71.067

Relative Values Matrix
Less is better
Consistency Ratio = 95.96

Table 3. Decision Matrix

IV. RECOMMENDED COURSE OF ACTION

A. IMPLEMENTATION

The DECMAT software shows the mixed strategy is best, but the mixed strategy has one major flaw. The mixed strategy is based on cyber activism. If the CyAct web site is not successful, then the mixed strategy will not be successful. Because these two strategies are directly tied together, cyber-herding is the fall back strategy. Cyber-herding is a time intensive strategy and valuable time would be lost if the other strategies fail. The solution to this is to implement the mixed strategy in conjunction with a small Gatherer node and Demolition node. These nodes can act as seeds for the CyAct web site by supplying the web site with identified and shut down Qutbists' web sites. In addition, members of these nodes can start to develop methods and procedures from their nodes and can act as trainers to members joining the CyAct web site.

The next step will be to determine if the CyAct web site is successful. This is accomplished through testing. One way of testing would be to use dominant indicators to determine if it is successful or not.[45] Major indicators would include the number of web sites submitted, the number of web sites shut down, and the amount of valid actionable information submitted to the cyber activism web site. Minor indicators would include the number of users joining the web site, the number of hits on the web site, and the amount of user inputs to the web site.

[45] Scott Gartner, *Strategic Assessment of War, (*Yale University Press, New Haven, Connecticut, 1999).

If the CyAct web site proves to be successful using these indicators, then the next step would be to phase out the small Gatherer and Demolition nodes. On the other hand, if the indicators signify that the CyAct web site is unsuccessful, then the full cyber-herding strategy should be implemented by increasing the existing Gatherer and Demolition nodes. While the full cyber-herding strategy is ongoing, the CyAct web site should remain up and periodically tested using the dominant indicators. If the indicators ever start to show the CyAct web site succeeding, then the cyber-herding Gatherer and Destruction nodes should be phased out to create the mixed strategy.

B. COUNTERING QUITBISTS' DEFENSES

Throughout this process, the Qutbists will deploy measures to counter these strategies. Such measures will include attacks against the CyAct web site and increased production of Qutbists' web sites. While the mirrored CyAct sites should protect against most DDoS attacks, a determined hacker can cause a great deal of damage so additional measures may have to be implemented. Countering an increase in production will require an escalation of identification and shutting down Qutbists' web sites. This may be easier for the cyber-herding strategy because it has individuals dedicated to finding and shutting down Qutbists' web sites. If the mixed strategy is in place, then it will have to be constantly monitored to verify it is keeping up with the escalation. If it cannot keep up with the increase, then the small Gatherer and Destruction nodes may have to be temporarily established to handle the

increase. Either way, at some point an equilibrium point should be achieved between the creation and shutting down of Qutbists' web sites.

Due to the constant pressure on the Qutbists, this will most likely drive them deeper into the web by moving from open web sites to secure password protected Darknets. This could potentially have a negative impact on intelligence gathering, but it could also be an opportunity to increase intelligence gathering. If Qutbists join Darknets created by the Creation node, then valuable information could be collected from them. Also, if the Network node has succeeded in infiltrating the Qutbists' online networks, then this could also lead them to Darknets created by the Qutbists.

Reducing Qutbists' web sites and driving the Qutbists deeper into the web has the main benefit of taking away a great propaganda tool from the Qutbists. In addition, when the Qutbists go dark, their ability to reach their target audiences in the Muslim world and in the West is severely diminished. This will reduce the Qutbists' ability to influence people to join their cause. And ultimately, this is the main goal of all of these strategies.

THIS PAGE INTENTIONALLY LEFT BLANK

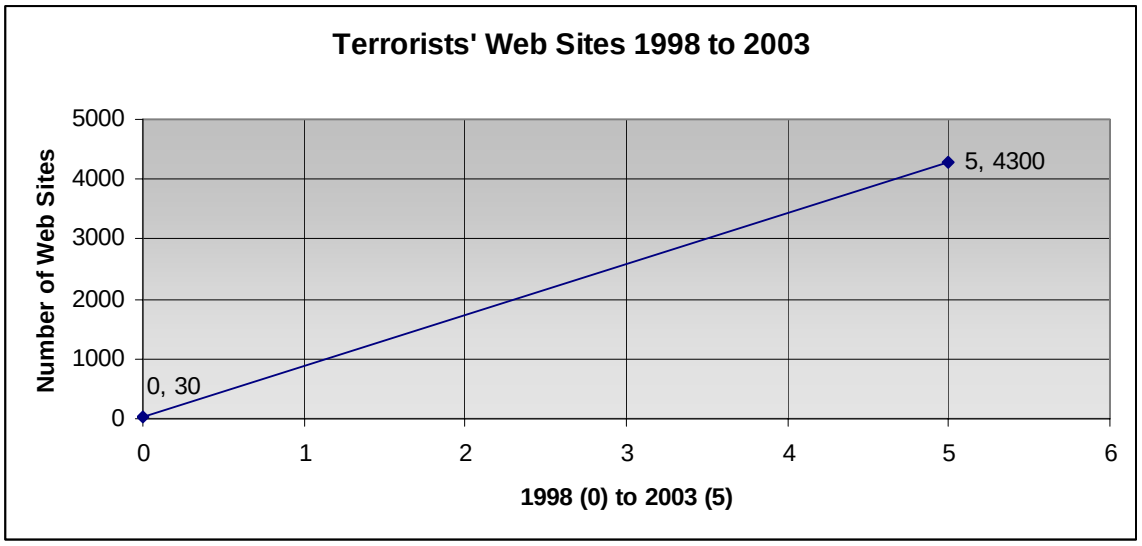
APPENDIX MOON'S MATH MODEL FOR TERRORIST AND DOPPELGANGER WEB SITES

1. Information on terrorist Web sites is very sparse; the only numbers available are as follows: 1998, 30 sites and 2003, 4,300 sites.

2. To determine the growth rate of terrorists' web sites, first plot a straight line using these sparse numbers.

For the x axis, 1998 equals zero and 2003 equals five.

For the y axis, use 30 and 4300.



3. The curve of the line is y = a*x + b. Solve for a and b to determine the growth rate of the web sites.

30=a*0 + b

30=b

4300=a*5 + b

4300=a*5 + 30

4270=a*5

854=a

The result is 854 web sites created a year.

4. Add 854 for each year after 2003 to get an estimate for total web sites for 2006. Total equals 6862.

5. Divide the number of web sites created yearly by 365 days to get the daily growth rate of terrorist web sites, the result being 2.34 web sites a day.

6. The following model is for the cyber-herding strategy. It demonstrates the theoretical decline in terrorist web sites and the growth and then decline of doppelganger web sites.

Terrorist Web sites (TW)

T(t+1) = T1 + daily growth rate - demolition rate

Doppelganger Web sites (DW)

D(t+1) = D1 + daily growth rate

Demolition Rate is 9.

When TW equals zero, model for DW changes to D(t+1) = D1 + daily growth rate - demolition rate.

Days	***TW Sites***	***DW Sites***	***Days***	***TW Sites***	***DW Sites***
1	6862	2	1029	15	3086
2	6855	5	1030	8	3089
3	6849	8	1031	2	3092
710	2140	2129	1367	0	68
711	2133	2132	1368	0	59
712	2126	2135	1369	0	50

Note: All numbers rounded to the nearest natural number.

LIST OF REFERENCES

Ackerman, Gary & Pence, Mike “The Enemy Within: Where Are the Islamist/Jihadist Web sites Hosted, and What Can Be Done About It?,” Middle East Media Research Institute, *Inquiry and Analysis Series - No. 374*, 19 Jul 2007, available from http://memri.org/bin/articles.cgi?Page=subjects& Area=jihad&ID=IA37407 (accessed 10 September 2007).

Caliphate, 12 December 2006; available from http://en.wikipedia..org/wiki/caliphate#reestablishment_of_a_modern_caliphate (accessed 12 December 2006).

Castells, Manuel *The Power of Identity* Vol. 2, *Economy, Society & Culture*, (Oxford: Blackwell, 1997), 3.

Cragin, Kim “Understanding Terrorist Ideology,” Rand Corporation, 12 Jun 2007, available from http://www.rand.org/pubs/testimonies/2007/RAND_CT283.pdf (accessed 11 September 2007).

Darknet, 9 December 2006; available from http://en.wikipedia.org/wiki/darknet (accessed 12 December 2006).

DECMAT Program for Windows Ver. 2.2, CPT Richard B. Stikkers, no copyright.

Democratic Peace Theory, 13 November 2007, available from http://en.wikipedia.org/wiki/Democratic_peace_theory, (accessed on 9 November 2007).

DeTocqueville, Alexis *Democracy in America*, 1899, Henry Reeve Translation, revised and corrected, available from http://xroads.virginia.edu/~HYPER/DETOC/ch2_08.htm (accessed 10 September 2007).

Eldridge, Lori Stop 302 Redirects Hijacking Web Page PR (Page Rank) and Stop Scrapers from Using Your Content, 17 November 2004; available from www.loriswebs.com/hijacking_web_pages.html . Also EthernetSecuritydb.org, The Web site Attack Guide, no date; available from www.milw0rm.com/papers/111 (accessed 11 December 2006).

Gartner, Scott *Strategic Assessment of War, (*Yale University Press, New Haven, Connecticut, 1999).

Gladwell, Malcolm *The Tipping Point: How Little Things Can Make a Big Difference, (*Boston, MA: Little, Brown, 2002).

Google Advertising Programs, "Reach in-market customers at every step of the buying cycle," Google.com, available from http://www.google.com/forms/ads7.html (accessed 10 September 2007).

Izhikevich, Eugene M. (2006) Main Page. Scholarpedia, available from http://www.scholarpedia.org (accessed 9 November 2007).

Katz, Lisa "Radical Islamic Ideology Legitimizes Terrorism," About.com, available from http://judaism.about.com/library/1_terrorism/bl_terrorismisrael_d.htm (accessed 10 Septebmer 2007).

Kreider, Aaron "Online Activism 2.0: Movement Building," ZNet, available from http://www.zmag.org/content/showarticle.cfm?ItemID=11802 (accessed 05 September 2007).

Lykke, Arthur **"**Toward An Understanding of Military Strategy", in *U.S. Army War College Guide Strategy*, Joseph R. Cerami and James F. Holcomb, Jr., eds., (Carlisle Barracks, PA: Strategic Studies Institute, 2001).

McCants, William *Militant Ideology Atlas*, Combating Terrorism Center, November 2006; available from http://www.ctc.usma.edu/atlas/Atlas-ExecutiveReport.pdf (accessed 10 September 2007).

Moon, David "Cyber-Herding: Exploiting Islamic Extremists Use of the Internet," JSOU and NDIA SO/LIC Division Essays, (JSOU, Hurlburt Field, Florida, April 2007).

Mujahideen, 17 November 2007; available from http://en.wikipedia.org/wiki/Mujahideen (accessed 17 November 2007).

National Security Council, *National Strategy for Combating Terrorism,* September 2006, available from http://www.whitehouse.gov/nsc/nsct/2006/nsct2006.pdf (accessed 10 September 2007).

Online vigilantes answer call of anti-terrorist defender, *The Washington Post*, April 2006, available from http://www.smh.com.au/news/World/Online-vigilantes/2005/04/25/1114281505819.html (accessed on 17 November 2007).

Page hijacking, 8 December 2006; available from http://en.wikipedia.org/wiki/page_hijacking (accessed 10 December 2006).

Religious Rehabilitation Group, "RRG – An Introduction", available from http://www.rrg.sg/subindex.asp?id=A033_07 (accessed 10 September 2007).

Sharia, 13 December 2006; available from http://en.wikipedia.org/wiki/shariah (accessed 13 December 2006).

Small World Phenomenon, 12 December 2006; available from http://en.wikipedia.org/wiki/small_world_phenomenon (accessed 14 December 2006).

Special Dispatch Series, No. 1375, 1 December 2006; available from http://memri.org/bin/latestnews.cgi?id=sd137506 (accessed 3 December 2006).

Sullivan, Danny "Nielsen NetRatings Search Engine Ratings," The Click Z Network, 22 Aug 2006, available from http://searchenginewatch.com/showPage.html?page=2156451 (accessed 11 September 2007).

The Great Divide: How Westerners and Muslims View Each Other, Europe's Muslims More Moderate, 22 June 2006; available from http://pewglobal.org/reports/display.php?pageid=831 (accessed 4 December 2006).

UN Security Council CT Committee, "List of International, Regional and Subregional Organizations," available from http://www.un.org/sc/ctc/pdf/iros-nairobi2007.pdf (accessed 10 September 2007).

Uniform Resource Locator, 9 December 2006; available from http://en.wikipedia.org/wiki/url (accessed 10 December 2006).

Weimann, Gabriel *Terror on the Internet: The New Arena, the New Challenges* (Dulles, VA: Potomac Books, 2006).

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Joint Special Operations University
   Hurlburt Field AFB, Florida

4. United States Special Operations Command J-7
   MacDill AFB, Florida

5. Brigadier General Jon M. Davis, USMC
   Deputy Commander
   USSTRATCOM/JFCC-NW
   Fort Meade, Maryland

6. Mrs. Mary Margaret Graham
   Deputy Director
   National Intelligence for Collection
   Office of the Director of National Intelligence
   Washington, DC

7. Assistant Secretary of Defense - Special Operations
   and Low Intensity Conflicts
   Washington, DC

8. United States Special Operations Command Library
   MacDill AFB, Florida