NAVAL
POSTGRADUATE
SCHOOL

MONTEREY, CALIFORNIA

Cyber-Herding:

Exploiting Islamic Extremists Use of the Internet

by

David B. Moon, Capt, USAF
Joint Information Operations Student
Department of Defense Analysis

The views expressed in this paper are those of the author and do not necessarily reflect the official policy, position, or endorsement of the Naval Postgraduate School, the United States Special Operations Command, the Department of the Air Force, the Department of the Navy, the Department of Defense, or the United States Government.

Additionally, the author of this paper has no knowledge of any public or private agencies, organizations, groups, or individuals engaged in cyber-herding as described in this paper or any similar activities. It is entirely possible that some entity is engaged in cyber-herding or similar activities, but this author could not find any evidence in the public record to indicate anyone is practicing cyber-herding.

Introduction:

On November 28, 2006, the Al-Fajr Information Center released the first issue of the *Technical Mujahid Magazine.*[1] The purpose of the online magazine is to help prevent aggressive acts against Muslims in cyberspace and to assist the mujahid in their efforts.[2] A mujahid is a Muslim fighting in a war or involved in any other struggle.[3] 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 they say this is a golden opportunity for the mujahid. The internet provides Islamic extremists an excellent medium to spread their ideas to billions 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’ websites has grown from less than 30 to more

[1] http://memri.org/bin/latestnews.cgi?ID=SD137506

[2] Ibid

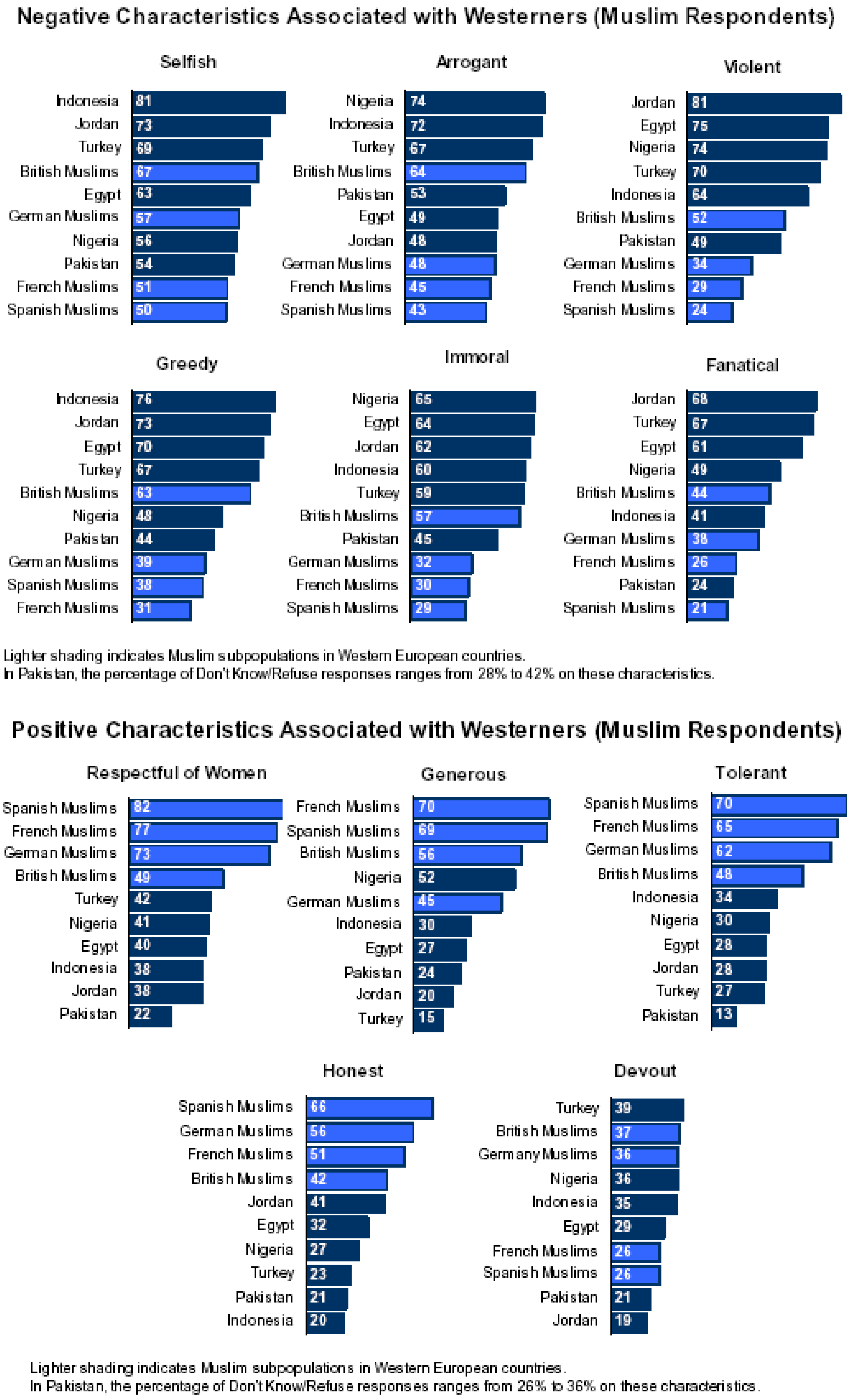
[3] http://en.wikipedia.org/wiki/Mujahideen

than 4,300."[4] Islamic extremists have used these websites for recruitment, fundraising, coordination, training, propaganda, and a whole host of different activities.

While all of these activities service Islamic extremists' multiple interest, the spreading of their propaganda is perhaps the most dangerous. Over the years, these extremists have learned to shape their messages to appeal to Muslim audiences. Muslims receive messages from the extremists pointing out the unfair policies of the West against Muslim countries, how the West blindly supports Israel against the "poor" Palestinian people, and the West's' attempts to control the Muslim world. The recent wars in Afghanistan and Iraq have only added fuel to this message. The extremists have used these conflicts to reshape their messages by showing the West attacking and occupying two Muslim countries. There is fertile ground in the Muslim world for messages of this nature, as evidenced by the following selections from the Pew Global Attitudes Project's report on The Great Divide: How Westerners and Muslims View Each Other.[5]

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

[5] http://pewglobal.org/reports/display.php?PageID=831



Lighter shading indicates Muslim subpopulations in Western European countries.
In Pakistan, the percentage of Don't Know/Refuse responses ranges from 28% to 42% on these characteristics.

Lighter shading indicates Muslim subpopulations in Western European countries.
In Pakistan, the percentage of Don't Know/Refuse responses ranges from 26% to 36% on these characteristics.

Figure 1

The results from the Muslims interviewed reveal a very negative image of the West. Islamic extremists shape their messages to reinforce this negative view. What can be done to counter these messages? The first step is to understand the medium that the extremists are using.

The internet has many characteristics that support extremists’ information operations, such as being able to reach large audiences. Yet the internet also has inherent weaknesses that can be exploited. One of these weaknesses is the ambiguous nature of the net. You trust that when you go to a website that it is legitimate. If it looks professional, you tend to believe that the site is real. However, criminals or terrorists could just as easily be running that website. The same is true when you chat with someone online. They could be who they say they are, but they could just as easily be someone else pretending to be the person you want them to be. A group called “Perverted Justice,” as featured on Dateline NBC, has made great success in catching child predators by using the internet’s ambiguous nature.[6] Terrorist organizations also have an inherent weakness that can be exploited using the internet. This weakness is the decentralized nature of terrorist

[6] http://www.perverted-justice.com/

organizations. Many terrorist organizations that do not have state sponsorship organize and accomplish work utilizing social networks versus a hierarchy command structure. This only makes sense. Individuals engaged in criminal activities need to work with people they trust so they can accomplish their mission. In the physical world, social networks are very reliable. However, in the virtual world social networks can be exploited because personalities in the virtual world can be real or fictitious. In order to exploit these weaknesses, a cyber system that invisibly drives Islamic extremists from terrorist websites to covertly controlled websites can be developed. I will generically refer to this system as cyber-herding.[7]

Defining Cyber-herding:

Cyber-herding is the action by which an individual, group, or organization drives individuals, groups, or organizations to a desired location within the electronic realm. Why implement cyber-herding versus engaging in an all out war on extremist websites? The answer to that

[7] Author's note: While discussing this idea with Prof John Arquilla from the Naval Postgraduate School, he applied the term cyber-herding to this concept. The term stuck and this author has been applying it to this concept ever since. Cyber-herding can also be found on the internet in reference to cattle herding, which has nothing to do with the ideas in this paper.

question lies in the realm of intelligence gathering and in the freedom of the internet. While the threat from Islamic extremists' use of the internet is high, intelligence agencies have successfully harvested information from these sites. Thus, an all-out denial-of service attack on extremists' websites would limit intelligence agencies capability to gather information. Indeed, some extremists' websites have been actively targeted and shut down. However, the problem that emerges from this tactic is the freedom of the internet allows extremists to restore or relocate their websites in a matter of hours to days. Thus, these attacks could embolden the extremists by reinforcing the fact that they can set up a new site within a short period. Simply stated, the attacks and subsequent re-emergence could provide them with a simple affirmation: *The powerful United States tries to keep us off the internet but they cannot!* On the other hand, cyber-herding has the potential to covertly neutralize undesirable websites, mine data from controlled websites, map virtual social networks, manipulate extremist messages, and modify the extremists' story. To implement a cyber-herding program effectively, a minimum of four nodes are required.

Objectives of the Cyber-herding Nodes:

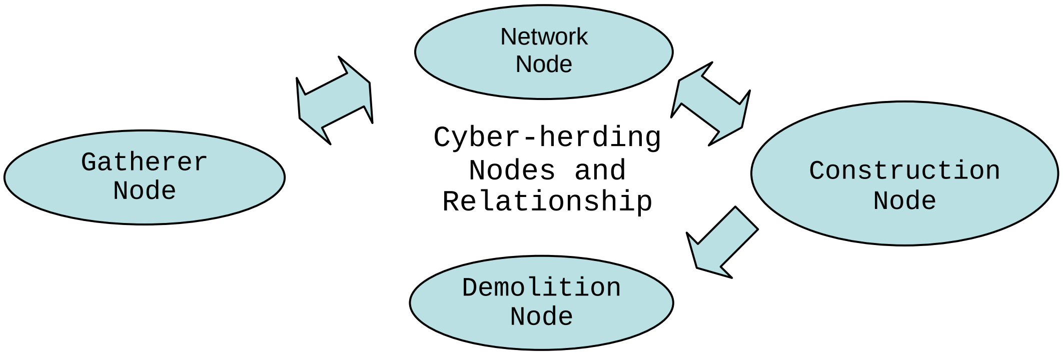


Figure 2

The Gatherer Node:

The gatherer node’s objective is to compile and maintain an up to date list for all extremists related uses of the internet.

The Network Node:

The members of the network node have two objectives. The first objective is to insert themselves into the extremists’ virtual social network. The second objective is to identify major “hubs” and “links” within the extremists’ virtual social network.

The Construction Node:

The members of the construction node have two objectives. The first objective is to create realistic doppelganger extremists websites and chat rooms. A doppelganger refers to a ghostly double or a look alike. In some traditions, it is an omen of death to see your own doppelganger. The second objective is to create several content rich Darknet environments that offer e-mail, file sharing, chat, instant messenger, and streaming video services. A Darknet is a private virtual network where users connect only to people they trust.[8]

The Demolition Node:

The demolition node's objective is to remotely destroy or disable all extremists' websites, chat rooms, Darknets, etc.

The Cyber-herding Process:

Phase One:

The gatherer node begins the cyber-herding process by tracking down extremists' websites and chat rooms. To facilitate this process, the node seeks public help by placing web-based advertisements asking people to submit Uniform Resource Locators (URL) for any suspected extremist website.[9] The node seeks out help from private groups such as the Rand Corporation, the Search for International Terrorist (SITE) Institute, and the Middle East Media Research Institute (MEMRI) and academic terrorism research

[8] http://en.wikipedia.org/wiki/Darknet
[9] http://en.wikipedia.org/wiki/URL

groups.[10,11,12] The node compiles a list of extremist website URLs. This list becomes a living document that the node constantly updates with identified extremists' 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 begin phase two.

Phase Two:

Upon accessing a site on the list, the members of the network node pose as Islamic extremist sympathizers and/or supporters and begin interacting with members of the site. In chat rooms, the node members start or join conversations supporting extremists themes. The objective is to develop trust relationships with Islamic extremists. Node members contact extremists' websites to see what they can do to support the cause. If needed, the network node would have the authority to make small donations to extremists websites to help build trust. During this phase, the network node maps the extremists' chat rooms. Mapping a chat room involves creating a social network diagram of who is talking to whom within the chat room. The members of the network node are looking for "hubs"

[10] http://www.rand.org/about/
[11] http://www.siteinstitute.org/index.html
[12] http://www.memri.org/

using the sites. These hubs are people who have more connections then anyone else. Malcolm Gladwell in his book, *“The Tipping Point,”* refers to these people as “connectors.”[13]

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 read up on his or her history before chatting.

If the network node discovers any websites not identified on the list, they will update the master list with the new URLs and forward these sites to the gatherer node. The members of network node mark the list to identify sites they are currently working, this ensures the demolition node does not destroy a site the network node is currently operating in. Subsequently, the network node forwards the list to the construction node.

Phase Three:

After the members of construction node receive the list from the network node, they start accessing the sites.

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

They copy the websites content, format, graphics, files, and links. Using this information, the construction node builds doppelganger extremists’ websites. All website created should be independent sites, with only passing similarities with other existing websites. At no time will the construction node hijack an existing extremist website as this could cause distrust in the target audience.[14] The construction node forwarded all created sites to the network node. The members of the network node endorse these new websites with their contacts. The members of construction node remove all websites the network node marked and any sites they created from the list. Afterwards, the construction node forwards the list to the demolition node.

Phase Four:

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 sites service provider to protest the site to try to get the site removed. They can also use more sophisticated attacks such as denial of service attacks, hijacking a website, Structured Query Language (SQL) injections, Cross Site Scripting cookie

[14] http://en.wikipedia.org/wiki/Page_hijacking

stealing, JavaScript injections, and other hacking methods.[15,16] 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 could post the extremists' URLs on internet chat rooms and blogs in the hope that private citizens and/or groups can bring down the sites.

Using the sparse numbers on extremists' websites in Gabriel Weimann's book, *Terror on the Internet,* I have created a mathematic model; see attachment 1, to determine the growth rate of extremists' websites.[17] Utilizing math modeling, I estimated the rate of growth for extremists' websites on the internet is, at least, 2.33 websites a day. At this rate of growth, I have estimated that the total number of extremists' websites ending in 2006 is approximately 6,850 websites. Using this knowledge, the construction node needs to take down at least 2.33 websites a day just to maintain the status quo. But, maintaining the status quo is not the objective.

Going back to math modeling, I estimated parity is achievable in 711 days if the demolition node can take down

[15] http://www.loriswebs.com/hijacking_web_pages.html

[16] http://72.14.203.104/search?q=cache:uXBMKQ2TURkJ:milw0rm.com/papers/111+attacking+websites +methods&hl=en&gl=us&ct=clnk&cd=9

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

an average of nine websites a day and the construction node can build websites at an average of 2.33 websites a day. This is illustrated in figure 3 below. Once parity is achieved, phase five begins.

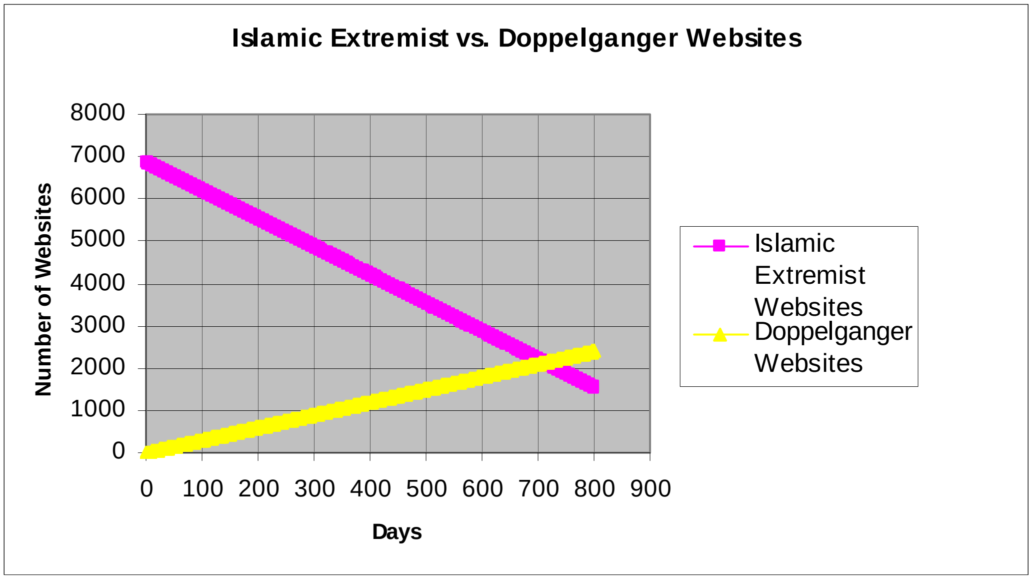


Figure 3

Phase Five:

The purpose of phase five is to change the message. Think of the Islamic extremists’ as salesmen. They are selling their ideology to the world. As good salesmen, they highlight the positive qualities of their movement, and suppress negative qualities of their movement. The two main items Islamic extremists suppress is the violence they commit, and their desire to impose their harsh version of an Islamic state upon people, states, and nations. Virtually all internet Islamic extremists expound about the need for an Islamic state. For them, an Islamic 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. Extremists’ violence and desire for an Islamic state are weaknesses that phase five exploits. During phase five, the construction node will make subtle changes to the websites under their control to highlight violent acts committed by extremists. In the view of most Muslims, Islam is the religion of peace. To them, the association of violence and Islam is a contradiction. By focusing on the violent acts committed by Islamic extremists in the name of Allah, support for the extremists should wane within the Muslim community. The construction node will also start to describe what an Islamic state will look like and how it will function. However, each site will have a different version of what an Islamic state will look like. Some sites will focus on installing an Islamic Caliphate, while others will focus on national Islamic states.[18] The Caliphate is an Islamic federal government that represents both political leadership and unities of the Muslim world applying Islamic

[18] http://en.wikipedia.org/wiki/Caliphate#Reestablishment_of_a_modern_Caliphate

law know as Shariah law.[19] As there is no set Shariah law recognized by all Muslims, each site would have its own version of Shariah law that will be enforced under the Islamic state.[20] The sites will also highlight the role of women in an Islamic state, rights of non-Muslims, and punishments for violating Shariah law. The purpose of all of this 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 these Muslims come to understand the details of an Islamic state, they may start questioning if it really is a good idea after all. In addition, by attaching different versions of an Islamic state to different extremist groups should foster hostilities between these groups. This should help keep the different factions from uniting to achieve their goals.

Phase Six:

Going back to math modeling, by day 1,032 virtually all of the extremists' websites could potentially be eliminated. At this time, the construction node would stop making new websites. The demolition node will continue to attack any identified Islamic extremists' sites.

[19] Ibid

[20] http://en.wikipedia.org/wiki/Shariah

Additionally, the demolition node will start to shut down construction node sites at the same rate they were attacking the extremists websites. At this pace, all websites will be eliminated by day 1375. I recommend that on day 1369, the demolition node stop shutting down sites created by the construction node. This will leave approximately 50 sites in operation for monitoring, and message control. This is illustrated in figure 4 below. The demolition node will continue to attack any extremists' website that makes it on the list.

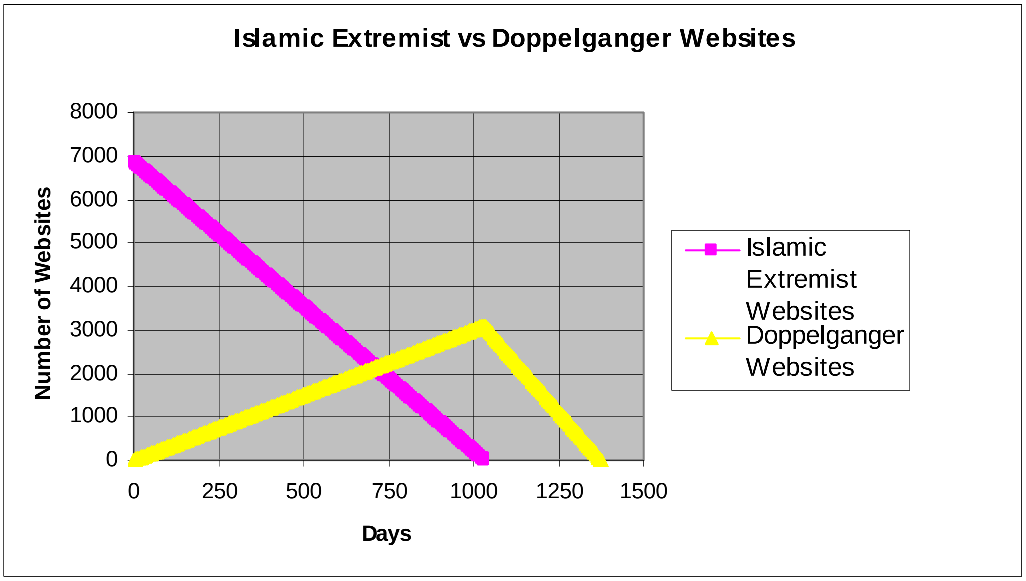


Figure 4

Phase Seven:

During this phase, the construction node will develop content rich Darknet environments. As stated earlier, a Darknet is a virtual private network where users connect only to people they trust.[21] These Darknet environments will offers e-mail, file sharing, chat, instant messenger, and streaming video services. Once a Darknet is created, the construction node will send the URL to the network node.

The members of network node will pick a connector with which they have developed a strong trust relationship, and invite that connector to become a member of the Darknet. This invitation will come in the form of three emails: one containing the URL of the site, one containing a temporary username, and one containing a temporary password. When the connecter clicks on the URL, a website will open. The only thing on this website is two fields for a username and a password and a submit button. When the connector fills in the fields and clicks the submit button, a prompt will appear requesting the user to establish a new username and password. Once the connector establishes a new username and password, a welcome message will appear. The welcome message informs the user that he is entering a secure website developed to promote the Islamic extremists' causes, and he was chosen to have access to the site because of his faith and dedication. The message will also tell the connector that he can invite

[21] http://en.wikipedia.org/wiki/Darknet

up to 10 people to join the website, but he must only invite people he trusts 100 percent. The purpose of this message is to make the subject feel special for being chosen, and to make the subject feel secure.

If the connector likes the website, then he may chose to invite others. On the other hand, if he does not like the website, then 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 extremists build a detailed map of their virtual social network.[22] Psychologist Stanley Milgram illustrates this theory in his 1967 study in which he showed that no less than six people separate people from each other.[23] The Six degrees of Kevin Bacon game also illustrates this theory, in which the game's objective is to connect any Hollywood actor with Kevin Bacon within six associations.[24]

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 updates the map whenever users send e-mails from their Darknet e-mail

[22] http://en.wikipedia.org/wiki/Small_world_phenomenon
[23] Ibid
[24] http://en.wikipedia.org/wiki/Six_Degrees_of_Kevin_Bacon

account, and chat with other Darknet users. Additionally, the Darknet runs IP and e-mail tracking software against all users. This software provides geographical locations for the users IP addresses and e-mail. In addition, the software provides contact information on the person that owns the IP address, and contact information on the person’s host service provider. 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, this may show a possible headquarters for extremists groups 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.[25]

[25] http://en.wikipedia.org/wiki/Data_mining

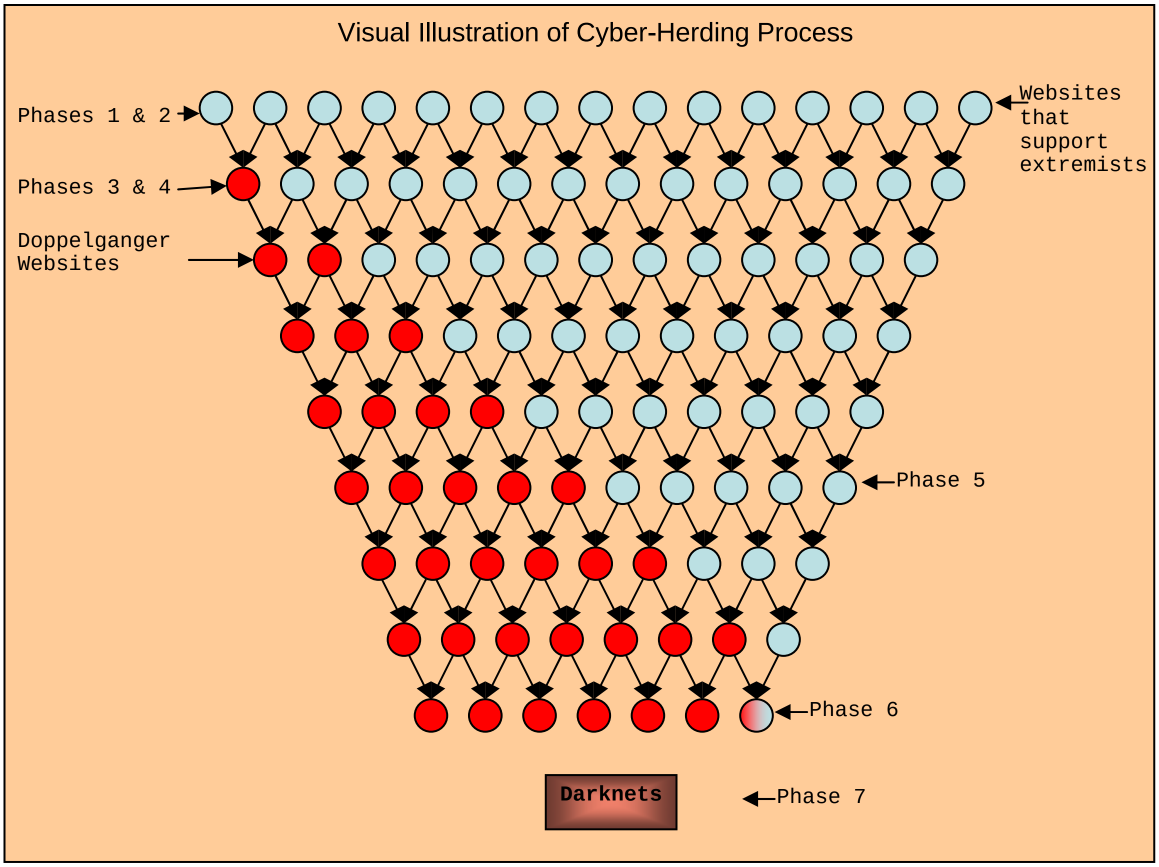

Visual Illustration of Cyber-Herding Process
Phases 1 & 2
Websites that support extremists
Phases 3 & 4
Doppelganger Websites
Phase 5
Phase 6
Darknets
Phase 7

Figure 5

Limits of Cyber-Herding:

The major limitation of cyber-herding is language fluency. Every node involved in this process will need to be multilingual, with a focus on Arabic. Before the process can begin, an investment must be made into recruiting people fluent in Arabic and training people in the Arabic language. The other limitation is time. Cyber-herding is not a quick easy fix. It will take time to develop trust relationships and attack offensive websites. The last limitation is in changing the message. The construction node can make subtle changes to the extremists message by highlighting weakness in Islamic extremists themes, however cyber-herding cannot be used to try to change people’s beliefs about America or the West. Any attempt to go down that path will lead to failure.

Conclusion:

The internet provides Islamic extremists 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. Utilizing the cyber-herding process, extremists’ information operations can be taken over and their messages and ideas can be modified to make them less appealing to their target audiences. Cyber-herding also increases monitoring and data collection of Islamic extremist information operations. Those willing to make cyber-herding a reality can seize the golden opportunity away from the Islamic extremists and make it their own.

References

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

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

http://en.wikipedia.org/wiki/Caliphate#Reestablishment_of_a_modern_Caliphate

http://en.wikipedia.org/wiki/Darknet

http://en.wikipedia.org/wiki/Data_mining

http://en.wikipedia.org/wiki/Mujahideen

http://en.wikipedia.org/wiki/Page_hijacking

http://en.wikipedia.org/wiki/Shariah

http://en.wikipedia.org/wiki/Six_Degrees_of_Kevin_Bacon

http://en.wikipedia.org/wiki/Small_world_phenomenon

http://en.wikipedia.org/wiki/URL

http://www.memri.org/

http://memri.org/bin/latestnews.cgi?ID=SD137506

http://pewglobal.org/reports/display.php?PageID=831

http://www.rand.org/about/

http://www.siteinstitute.org/index.html

http://www.loriswebs.com/hijacking_web_pages.html

http://www.perverted-justice.com/

http://72.14.203.104/search?q=cache:uXBMKQ2TURkJ:milw0rm.com/papers/111+attacking+websitesmethods&hl=en&gl=us&ct=clnk&cd=9