Hospital CBRNE Preparedness – Are we Ready?

CBRNE Newsletter Terrorism

Volume 42, 2012

Cyber News

www.cbrne-terrorism-newsletter.com

NASA says it was hacked 13 times last year

Source: http://www.reuters.com/article/2012/03/02/us-nasa-cyberattack-idUSTRE8211G320120302

NASA said hackers broke into its computer systems 13 times last year, stealing employee credentials and gaining access to mission-critical projects in breaches that could compromise U.S. national security.

The National Aeronautics and Space Administration spends only $58 million of its $1.5 billion annual IT budget on cyber security, Paul Martin, the agency's inspector general, told a Congressional panel on NASA security earlier this week.

"Some NASA systems house sensitive information which, if lost or stolen, could result in significant financial loss, adversely affect national security, or significantly impair our nation's competitive technological advantage," Martin said in testimony before the U.S. House Committee on Science, Space and Technology, released on Wednesday.

He said the agency discovered in November that hackers working through a Chinese-based IP address broke into the network of NASA's Jet Propulsion Laboratory.

He said they gained full system access, which allowed them to modify, copy, or delete sensitive files, create user accounts for mission-critical JPL systems and upload hacking tools to steal user credentials and compromise other NASA systems. They were also able to modify system logs to conceal their actions, he said.

"Our review disclosed that the intruders had compromised the accounts of the most privileged JPL users, giving the intruders access to most of JPL's networks," he said.

In another attack last year, intruders stole credentials for accessing NASA systems from more than 150 employees.

Martin said the agency has moved too slowly to encrypt or scramble the data on its laptop computers to protect information from falling into the wrong hands.

Unencrypted notebook computers that have been lost or stolen include ones containing codes for controlling the International Space Station as well as sensitive data on NASA's Constellation and Orion programs and Social Security numbers, Martin said.

PERSPECTIVES ON TERRORISM
a journal of the Terrorism Research Initiative

Use of the Internet to Counter the Appeal of Extremist Violence.

Conference Summary & Follow-up/ Recommendations

by the United Nations Counterterrorism Implementation Task Force (CTITF), Working Group on Use of the Internet for Terrorist Purposes Riyadh, 24 - 26 January 2011.

Source: http://www.terrorismanalysts.com/pt/index.php/pot/article/view/CTITF-Use-of-Internet/html

Background

The Internet is a key way for violent extremists to encourage others to adopt their views. In their messaging to potential supporters and vulnerable audiences, extremists use simplistic analysis and offer violent solutions to problems that span a range of complex social, economic and political issues at both a local and global level.

Finding effective ways to counter such messages was at the heart of discussions at the Riyadh Conference on the "Use of the Internet to Counter the Appeal of Extremist Violence." Co-hosted by the United Nations Counterterrorism Implementation Task Force (CTITF) and the Naif Arab University for Security Sciences in Riyadh in partnership with the Center on Global Counterterrorism Cooperation, and supported by the Governments of Germany and Saudi Arabia, the Riyadh conference followed two previous meetings of the CTITF Internet Working Group, one on legal aspects of the use of the Internet for terrorist purposes, and the other on technical aspects.[1] The conference brought together around 150 policy-makers, experts and practitioners from the public sector, international organisations, industry, academia and the media. Several States participated at ministerial or ambassadorial level. The choice of Saudi Arabia as a venue reflected its considerable effort to identify effective counter-terrorism measures, including in combating terrorist use of the Internet and in constructing and delivering effective counter-narratives.

The conference focused on identifying good practices in using the Internet to undermine the appeal of terrorism, to expose its lack of legitimacy and its negative impact, and to undermine the credibility of its messengers. Key themes included the importance of identifying the target audience, crafting effective messages, identifying credible messengers, and using appropriate media to reach vulnerable communities. The Conference agreed that Governments might not always be best placed to lead this work and needed the cooperation of civil society, the private sector, academia, the media and victims of terrorism. Given the global nature of terrorist narratives and the need to counter them in the same space, there was a special role for the United Nations in facilitating discussion and action.

This report includes a list of possible follow-up projects, further recommendations, and a summary of the discussion.

Action Points/Possible Follow-on Projects:

1. Collect examples of extremist messages on the Internet and identify the strengths and weaknesses of both their content and delivery through web-stats analysis and user reactions so as to be able to undermine strengths and exploit weaknesses in constructing and delivering counter-narratives. Analyze themes and discussion threads on extremist websites.
2. Collect and analyze examples of counter-narratives on the Internet so as to build a picture of what works and what does not, both in terms of content and delivery.
3. Build a hub for deconstructing extremist narratives on the Internet, providing counter narratives and training workshops for practitioners, students, journalists, etc.
4. Identify the types/groups of users who access extremist messages so as to be able to reach them through the same portals with counter-narratives that play to their specific concerns and cultural influences.

5. Draw up a register of potential messengers both by category/geography and as individuals and create a platform for interaction. Messengers might include victims and former extremists.
6. Provide journalists with an easily accessible roster of experts on extremism and counter-extremism that they can turn to for substantive comment (i.e. by building on efforts such as the Global Expert Finder of the Alliance of Civilizations). Identify and draw up a list of media partners.
7. In consultation with the Organization of the Islamic Conference establish a project to offer analysis of radical messages and training for all interested stakeholders on the design and delivery of counter-narratives in order to avoid legitimizing extremist messaging and wherever possible expose its illegitimacy (in partnership with the Alliance of Civilizations).
8. Discuss with industry partners (incl. search-engine hosts) the technical possibilities of ensuring counter-narratives appear at or near the top of results pages for specific search criteria.

Recommendations:

1. Promote counter-narratives through all relevant media channels (online, print, TV/Radio).
2. Make available in the same space a counter-narrative whenever a new extremist message appears on Facebook, YouTube or similar outlets.
3. Offer rapid counter-narratives to political developments (e.g. highlight the absence of Al-Qaida and other extremist groups from popular protests).
4. Consider selective take-down of extremist narratives that have the elements of success.
5. Ensure that counter-narratives include messages of empathy/understanding of political and social conditions facing the target audience, rather than limiting the counter-narrative to lecturing or retribution.
6. Offer an opportunity for engagement in crafting and delivering counter-narratives to young people who mirror the 'Internet Brigade' members of Al-Qaida.
7. Support the establishment of civil society networks of interested groups, such as women against violent extremism, parents against suicide bombers or schools against extremism.

Summary:

Session I: Framing the Issue – The Spread of Violent Extremism through the Internet

The Internet, though a neutral medium, can play a key role in spreading violent extremist messages to individuals who might otherwise remain immune. The Internet empowers the shy and allows alienated people with extremist views to find others who agree with them. This can lead to mutual reinforcement of beliefs and validation of a world view that is otherwise hard to sustain. Forums that promote a radical philosophy however, often contain many different ideological strands. Audiences often approach forums in a state of confusion which then clarifies as they gravitate towards other members and harden their outlook. While it can and does happen, people do not always approach a forum with the intention of joining a terrorist group or even of becoming members of the ideological ghettos that exist on the Internet. The effectiveness of networks depends on their success on several levels: organizational (binding members together), narrative (strengthening self-definition); doctrinal (hardening beliefs and objectives); technological (improving capacity), and social (building trust and loyalty). Opportunities to break down networks also exist in all these categories.

The Internet has enabled the collection of extremist ideas and materials that may lead a vulnerable individual to recruit himself, sometimes unaided by any intermediary. Such self-recruited extremists can join a community of like-minded individuals which then develops its own ideology. These networks are resilient and adaptive, despite growing law enforcement efforts to take them down. Online extremist forums can play a key role in the radicalization process of an individual or a group. Often identified with religious symbolism and rituals, and a rejection of western cultures, these forums provide individuals that feel emotional outrage with a sense of identity and purpose which may lead them to consider it a personal duty to take action as soldiers in a war to protect their community. The problem of radicalization however is not limited to Al-Qaida-related terrorism. Extremism can grow out of the domestic conditions of any country, and the Internet can play a facilitating role in radicalizing any set of vulnerable individuals in the same way that it does for Al-Qaida-related extremists.

In this respect, participants cautioned against using misleading terminology, in particular as relates to deviations from Islam and the actions of violent Muslims; terms such as jihad or neo-jihad are unhelpful and counter-productive. There was complete agreement that Al-Qaida represents neither the Muslim community nor Islamic belief.

Session I: Framing the Issue II – the Terrorist Narrative (Objective and Success)

A speaker presented a comprehensive study of terrorist web forums and the ways they have been used to develop terrorist ideas and activities. These web forums provide relative anonymity; wide availability; resilient infrastructure; interactivity, and comprehensive pools of information, as well as links between armed extremists and their support bases and among themselves. It was noted that even though many Al-Qaida web forums are weakening and some have not recovered from take-down actions, they should not be underestimated, as at least three or four principal forums are fully active and in direct contact with the Al-Qaida leadership. Most Al-Qaida web forums are now password-protected, allowing access only to established members.

Another speaker examined the types of Internet content terrorists access, using the example of the Madrid bombers. The terrorists had used the Internet for communication within and beyond the terrorist network, to share information on current events, as a tool for indoctrination and to maintain ideological group cohesion, and to share operational knowledge on violent tactics and on targets. The computers recovered from the bombers contained propaganda and proselytizing texts and audio/video clips from key leaders as well as from unidentified preachers, all reinforcing the legitimacy of terrorism.

As much as the Internet is a complementary tool for individual radicalization, in many cases the key radicalization channel still remains face-to-face interaction. Often a surprisingly short time elapses between a person becoming interested in radical ideas on the Internet and meeting someone in real life who reinforces those ideas.

The main objectives of the terrorist message are to build a sense of community, instill a sense of responsibility to defend it and promote the idea that it is under attack from a specific enemy.

Session II. The Message: Crafting a Counter Narrative

Participants made the point that extremists often get things wrong and that the web allows an opportunity for an aggressive exploitation of their mistakes. One example was the intimidating messages sent to imams and others in Afghanistan which in fact exposed the violence and intolerance of the terrorist approach. A counter-narrative was likely to succeed better if it was aggressive rather than defensive. It was also useful to underline the lack of success enjoyed by terrorist groups, the counterproductive consequences for the communities that terrorists claim to defend and the lack of legitimacy for terrorist action. However, while terrorist argumentation often shows weaknesses in content and logic, the counter-narrative that points these out needs more substance to sustain itself. Counter narratives should contain facts and have a transparency that undermines any criticism of them as information operations.

Participants emphasized the importance of finding voices that resonate with the audiences that counter narratives aim to reach, for example those of former terrorists. It was important to highlight the arguments that had led them to denounce violence. Similarly, it was useful to examine the content of internal critiques that are known to have had an impact on extremist thought. In the case of Indonesia, messages by people still involved in the movement had more impact than arguments against bombings made by former militants, in part because they went beyond the usual point-counterpoint of most arguments. Their impact suggested that an effective Internet counter-narrative requires a thorough familiarity with ongoing debates. If extremist movements are constantly evolving, then counter-strategies aimed at an Internet audience will need to do the same, showing flexibility and an ability to adapt to changing events.

A successful counter narrative should not necessarily be limited to renouncing violence but also point out that violence does not achieve the desired outcomes, while showing understanding of the political and social conditions that face target audiences. The audience that a counter-narrative should aim to

persuade does not comprise foot-soldiers, but rather reasonably well-educated computer-literate members of religious discussion groups, the intellectuals who are or might become recruiters and trainers in terrorist circles, and university students who might be tempted to provide moral, logistical or financial support. An effective message should urge them to act in a different, more effective and positive capacity. An empathetic message that demonstrates understanding of the issues that may push an individual to extremism is likely to have greater effect than one that simply says he is wrong.

A discussant gave the example of Abu Muhammad al-Maqdisi's criticism of his former pupil, Abu Musab al-Zarqawi which was translated into Indonesian as *They are Mujahidin But They Made Mistakes (Mereka Mujahid Tapi Salah Langkah*). The success of such counter-narrative efforts is largely dependent on the timing of their release, especially in the immediate aftermath of incidents that have dealt major setbacks to the movement.

Participants also discussed the importance of exploiting terrorist groups' strategic and doctrinal vulnerabilities. According to a discussant, this would mean that counter narrative messages need to compete in a space where undecided young people are trying to decide what activity they should support. Therefore, deploying sustained messaging to key audiences is essential. In doing so, counter narrative messages can also highlight the collateral damage of terrorist acts (Al-Qaida is killing the Ummah), challenge Al-Qaida's doctrinal vulnerabilities, undermine the authority of the messenger ('Who made you the leader, anyway?') and attack the terrorist brand image ('This isn't what I signed up for!').

Similarly, counter-narrative efforts need to focus on deconstructing religious extremist propaganda in the media where images and videos provoke emotional outrage. It is necessary to deconstruct such content by analyzing the religious sources in their original context, demonstrate the terrorist intention and replace the terrorist interpretation with a mainstream moderate perspective.

An aspect that could also be exploited is the way that web forums allow for top-down authority, and so can shape the debate towards peaceful protest, albeit radical, rather than violent protest.

Session III. The Messengers and the Media: Delivering the Narrative

The importance of the role of the messenger was highlighted repeatedly, given that the messenger is as important as the message itself. Participants discussed the critical damage that may be done if a messenger communicates the wrong message or is not knowledgeable about the topic. Individuals who have been victims of terrorism form possibly the most powerful group of messengers as they can promote a counter-narrative through personal stories and so 'speak truth to terror'. A representative of a terrorism victims' network argued that instead of terrorists getting all the attention from the media, the victims of terrorism should be allowed the same platform to challenge the terrorist narrative.

Participants discussed the routes to radicalization, and whether conditions conducive to the spread of terrorism have less to do with ideology than with personal experience of social exclusion and marginalization. In radicalisation there was often a degree of accidental contact in an hour of need rather than a deliberate path. While there was no agreement as to the specifics of what "causes" terrorism, discussants agreed that effective counter-narratives had to focus in particular on vulnerable and marginalized communities, with an aim to empowering young people. Research from across different regions - including the Middle East, Europe, and South America - seemed to indicate that radical movements were often most successful in recruiting new followers when offering some form of identity/sense of belonging. In this context, one participant highlighted the similarities in the recruitment approach of terrorist groups and criminal gangs, pointing out that a common factor was the focus on young people. Comparing a group like Al-Qaida to a street gang could be part of an effective counter-narrative, but an effective strategy had to offer more than words or remote role models. It had to provide the emotional and physical support that individuals sought by joining terrorist or criminal gangs. It was further agreed that developing and implementing coherent youth programs was potentially one of the more effective ways to counter the extremist narrative.

Credible Messengers as Important as the Message

While it was important to craft effective messages focused on particular target audiences, participants agreed that having credible messengers deliver the message was as important as the message itself. One participant pointed out that the image presented by Usama bin Laden was extremely persuasive to devout Muslims, regardless of what he said and did, and the counter narrative should hesitate to attack such iconic figures head on. There was broad agreement about the significance of former extremists who generally have greater credibility within their communities than governments or international organizations. The problem, however, was that there was a high demand but low supply of such voices.

Furthermore, engaging with former extremists posed two significant challenges:

1) most are not part of any organized structure (i.e. NGOs/civil society organizations) so it is difficult to reach out to them; and 2) many of them often do not have the tools (facts, religious understanding, etc) to be effective in engaging other members of their communities susceptible to extremist ideologies. One way to address this was to build networks of credible voices, across terrorist groups, gangs, cults and other sectors of society (for example sports stars), and provide an institutional home such as a NGO which could coordinate their activities and provide them a platform.

Noteworthy Initiatives: The Power of Peace Network

Participants highlighted the important role technology can play in both crafting and delivering counter-narratives. One participant highlighted a UNESCO-led Initiative entitled the "Power of Peace Network" which strives to become a worldwide social networking community in pursuit of peace. The Network aims to engage and inspire young people by harnessing the power of media and information technology to support diverse social and cultural self-expression. In doing so, the initiative aims to self-generate effective counter-narratives as well as provide avenues for dissemination of those messages. It also aims to be a clearinghouse for audio-visual content for schools and universities as well as endorse university curricula.

Role of the Media

Participants also discussed the role of the media both in reporting on terrorism and in spreading counter-narratives. As with governments, mainstream media outlets could not easily disseminate counter-narratives. While mainstream media may generally cover terrorism objectively, it was unlikely that professional journalists would intentionally spread counter-narratives. Furthermore, language could sometimes be a barrier for foreign media. One participant highlighted several cases in which interesting repudiations of terrorism by repentant extremists, which could serve as highly effective counter-narratives if disseminated to a broader audience, simply did not get picked up by mainstream media due to a lack of language ability or a lack of appreciation of the source's credibility and impact. Some of these challenges could be offset by providing journalists with specific training or an online guide, or by linking them with a group of experts whom they can easily turn to for substantive knowledge and additional context, similar to the Global Expert Finder (GEF) program of the UN Alliance of Civilizations (see: < http://www.theglobalexperts.org/ >).

On the upside, participants pointed out that mainstream media did have significant reach, often also into vulnerable communities and relevant audiences. And while not being co-opted as propaganda instruments, professional journalists did have the responsibility to "dig deeper" – with solid reporting going beyond mere news coverage, and ideally focusing on uncovering the truth behind a story, including going beyond the terrorist narrative, discounting prevailing myths, and establishing transparency. One of the effective ways to leverage media reporting was to encourage and disseminate articles/stories about the debates and arguments inside terrorist organizations. Exposure of these fault lines – while being sound reporting – could also be used by credible messengers to pinpoint the weaknesses and illegitimacy of the terrorist narrative. Indeed, such topics could provide the strongest counter-narratives. One participant highlighted the current debate among Al-Qaida strategists on the justifications for killing Muslims. In this regard, studies had shown that Al-Qaida-related terror attacks had killed eight times more Muslims than non-Muslims. It was

agreed that mainstream media could and should report this type of information while preserving necessary objectivity and transparency and ensuring proper sourcing.

Session IV: What Has Been Done, What Should Be Done – National, Regional, Global Initiatives

Participants learnt about one country's efforts to harness the internet to spread counter-terrorist narratives as well as to limit/filter its content in order to prevent vulnerable groups from being exposed to radical websites and chatrooms. While internet filtering is not without debate, representatives of that government explained how the internet had become in that country the main source of motivation for people travelling to conflict zones. Terrorist websites had grown from about 15 in 1998 to several thousand in 2010, many of them, however, were not accessible from within that particular country. At the same time, positive messages, including images and videos, were effective tools in engaging vulnerable groups, especially the country's youth. Government initiatives included a cadre of about 200 volunteers who engaged participants in radical chatrooms to challenge the ideologies and extremist ideas spread through online discussions and websites. One of the key successes in countering the influence and ideology of terrorist groups was an independent campaign (supported by a Government Ministry) to counter online radicalization and recruitment. Focusing on a significant group of violent extremists, the campaign uses Islamic scholars to interact online with individuals looking for religious knowledge with the aim of steering them away from extremist sources, leading about 1500 out of 3250 participants to renounce their extremist beliefs. The government also promoted the role of the family in monitoring the use of the Internet in the home.

Many participants acknowledged that while governments had become relatively successful on the repressive side of counter-terrorism, it was imperative to focus more energy on the preventive side. The move of some governments from monitoring websites that incited to violence to shutting them down was noted as a countervailing current. However, while counter-terrorism policies should continue to evolve, there was also a danger in "securitizing" counter-terrorism-related policies (i.e. socio-economic development programs, integration policies, human rights campaigns, etc), which had a merit of their own. Governments needed to walk a fine line between utilizing such programs as part of an effective counter-narrative and tainting particular programs/institutions with a counter-terrorism label. Furthermore, effective counter-narratives – and effective counter-terrorism in general – needed to be grounded in the rule-of-law and in a respect for human rights. Similarly, the debate around monitoring terrorist websites vs. shutting them down needed to take into account privacy and freedom of expression concerns. Several participants called for increased international cooperation in this area where many felt too little had been achieved to date.

One key recommendation was for governments to increase their support for translation and dissemination of messages by repentant radicals. Those messages, while often very specific to a particular context, frequently contained very effective material for counter-narratives but were only available in one language. In order to reach local audiences more efficiently, the messages/stories needed to be translated and disseminated (though not necessarily by governments). It was noted that terrorist organizations had become very adept at spreading propaganda through the internet in numerous languages. Several participants stated that Al-Qaida's online/media activity had become as important to the group's global reach as its real-world activity.

Participants discussed how governments could more effectively counter the challenge of internet/media-savvy terrorist groups. One approach entailed working more closely with the private sector/industry, for example with regards to search engines, in order to ensure that radical content does not appear among the top search results. Furthermore, private sector companies can play a critical role in designing and disseminating effective counter-narratives as government efforts (online and offline) are often poorly designed and not very attractive to target audiences. Participants also recommended that the United Nations, through the Counter-Terrorism Implementation Task Force, could create both a library of effective counter-narratives and build a platform for credible messengers.

One of the challenges, according to some participants, was that Western

audiences often only learned about Islam through translated statements by extremists which caught the attention of the media. Instead, some argued, governments as well as NGOs and religious leaders should ensure that knowledge of mainstream Islam is enhanced in the Western world – also with a view to reaching vulnerable communities – to highlight how religion is being distorted by terrorist organizations such as Al-Qaida. This was as easily achieved through the general exposure of the population to the reality of other religions and cultures, for example through TV shows, as it was through a deliberate counter-narrative. A further problem was the lack of a coordinated plan to react to the exploitation of issues by radical extremists, such as the publication of cartoons disrespectful to Islam in Europe in 2005.

Session IV: Ideas for New Initiatives; the Role of the UN and other Mechanisms for Cooperation

Role of social media and search engines

Participants stated that one of the major challenges for countering radicalization online was to identify the right target audience, and then design the message in a way that resonated with it. News environments were becoming increasingly insular and balkanized and people had begun to gravitate toward news sources that simply validated their opinions, thus making it more difficult to challenge their views. Social-networking such as Facebook and Twitter was increasingly used by terrorist organizations without any sustained/credible counter-effort in those forums. One participant highlighted the need to increase positive messaging and "anti-Al-Qaida" information which was very hard to find on the internet, so as to drive out the bad with the good. When searching for statements about Al-Qaida or similar extremist groups, search results were more likely to turn up extremist content then counter-narratives – and with about 75% of users never going beyond the first page of search results, this presented a major challenge. Such search-engine-optimization should become a critical component of government dialogue with the private sector.

A One-Stop-Shop for Counter-Narratives

Participants agreed that there was a need to develop a one-stop-shop for counter-narratives, for example by building an online library which could contain texts and other material arguing for moderation and non-violence, a CVE (countering violent extremism) news hub, victims' statements, and exposés of false statements made by terrorist organizations. Another idea was to promote citizen journalism, including videos made by youth groups and NGOs. Governments should encourage the private sector to do more on this front, such as through crowd sourcing. At the same time, governments themselves should engage more in positive messaging, particularly through social-networking forums. Participants acknowledged that there could be authenticity issues with some government-driven initiatives. Experience has shown, however, that target audiences will look at such messages if they are well designed. Furthermore, the internet can be leveraged to provide platforms and venues for people coming together to solve radicalization problems, to exchange experiences from different national contexts, and to discuss what worked and what did not. Some of these efforts could be led by the United Nations; others could be led by regional organizations or national governments. One national experience highlighted the recent institutionalization of a *Center for Strategic Counterterrorism Communications* which tried to leverage information technology in countering terrorist narratives.

The meeting agreed that there should be a baseline for a counter-narrative that was as simple as the terrorist message that the West was at war with Islam. This could centre on the actual consequences of terrorism. It was important to be able to react with a counter narrative to actions by terrorists as quickly as terrorists reacted to actions by States. Often terrorists were able to cover up or 'justify' their mistakes before States took any action. It was pointed out that even in the war paradigm there was a difference between fighting and killing.

Understanding the Target Audience & Encouraging Former Extremists

Other participants gave examples of how counter-narratives had become a major part of counterterrorism, even on the operational level, for example in defeating the Taliban in the Pakistani Swat valley, during which targeted messages on the internet (as well as through

traditional media) had played a major role. Yet nothing had been more powerful than a video of the Taliban flogging a young woman, or a recording of a Taliban leader claiming to be the only true Muslim, and every advantage should be taken of such self-inflicted setbacks. There was still an insufficient understanding of target audiences which could vary even within a particular country – here, too, former extremists could be the key to a more effective outreach, using their knowledge of local languages and local circumstances. It was thus important for governments to do a lot more to win over and encourage such ex-militants. The importance of political will to unite and sustain any effort to promote counter narratives on a regional or international basis was self-evident, but it often failed at the first hurdle because there was no clarity in many States as to who was in charge of such initiatives.

Many participants emphasized the importance of working with community leaders, including religious leaders and recognized figures from the sports and entertainment world. Counter-narrative work was a "slow-burn" activity and finding partners in communities, as well as seeing what messages resonate, took time. And while the terrorists were increasingly relying on the Internet to spread their ideology, several participants recalled that there was still limited access to the Internet in many parts of the world, particularly in communities governments would like to reach. This, in turn, meant that counter-narrative work could not be limited to new technologies but should encompass traditional media as well.

While extremists might exploit vulnerable people to recruit them to terrorism, most radicals were self-selecting and they needed to be able to access counter arguments to violence. It was unclear what role governments could play in this process, whether facilitation, initiation, inspiration or some other role. Civil society was clearly an essential force-multiplier that could promote positive messages about alternatives to terrorism that would have a more powerful impact than the negative messages distributed by violent extremists. The key was to operate in the same milieus as the extremists, for example within diaspora groups.

Conference Roundtable "The Path to Rejecting Violent Extremism"

The conference also featured a roundtable discussion between two former extremists who explained what had led them down the path of radicalization towards violent extremism. The discussants explained how different drivers had motivated them to join terrorist organizations, ranging from the Palestinian situation in the 1970s and 1980s and corrupt governments, to conflicting information they had received about the meaning of 'jihad'.

One discussant stated that while studying religion he was approached by people from his local community and began to form ideas about the situation of Muslims in Afghanistan under Soviet occupation. When beginning to shape his opinions about how to address these perceived or actual injustices, the discussant was approached by violent extremists trying to recruit anyone they felt was vulnerable enough to adopt their ideology and engage in their cause. The discussant recalled how he eventually rose through the ranks until he became the "emir" of Abu Musab Al-Zarqawi in Jordan, and how his role continued even for part of his sixteen year-long prison sentence. As emir, he became both a theorist propagating the terrorist organization's beliefs and a controller of its activities. He admitted to deliberately misleading his followers through radical explanations of religious texts, knowing that they were open to alternative interpretations. The discussant highlighted that the Al-Qaida leadership was convinced that young people could easily be manipulated and deceived in their search for recognition and a sense of belonging. The extremely lively audience participation tended to underline that the lack of ideological cohesion was an area of vulnerability for terrorist groups.

Session V: Follow-up Discussions and Recommendations on Crafting Narratives

Participants broke out in two separate sessions designed to discuss practical areas for follow-up and concrete proposals for future action.

The breakout-session on crafting the narrative discussed the need for different messages for different target audiences. Participants agreed on the need to do more research on why and how people became terrorists in the first place, and of indicators that an individual was about to cross the line. This would help in designing the counter-narrative. The language of the counter-narrative had to be clear and

easily understood, it needed to avoid using terms that had been hijacked by terrorist groups, and by ignoring them allow them to recover their proper meaning. The counter-narrative should show some sympathy for people who had been tempted towards extremism and an understanding of the reasons. Participants agreed that a counter-narrative should explain what terrorism is and expose the gap between what terrorists say and what they do. It should be fact-based and highlight the illegitimacy of terrorist behaviour and the lack of any policy solutions offered by terrorists to the grievances they exploit. The message should aim to promote a proactive narrative rather than a reactive counter-narrative. It should be personalised as well as targeted. Ridiculing terrorists is a useful tactic, as is exposing drug dealing or other anti-social activity as a source of terrorist income.

Participants agreed that the ownership of the counter narrative remained with the global community, not with governments or the United Nations. It should not reflect particular cultural values except where the audience shared those values. In relation to Al-Qaida-related groups, the counter-narrative should highlight in particular the significant Muslim contribution to the fight against terrorism in both words and deeds. The counter-narrative should emphasise the unattractiveness of terrorist groups and their failure to terrorize their intended victims. There should also be some conformity between macro and micro level initiatives. There was agreement on the need to identify, share and reinforce success and a suggestion that the United Nations should host a central repository of messages and examples that anyone could draw from in crafting a counter narrative.

The breakout-session on delivering the narrative focused its discussion on the audience, the best ways to reach it and the messengers. Participants agreed that the audience could potentially be segmented and different communications applied accordingly. The primary target audience was a broad section of youth, who had access to a range of technologies and media but had no common religious or cultural heritage. Social networking forums were one of the key areas where the vulnerable audience met, and could be reached. Participants agreed that messages were not just single verbal narratives but rather layered and diverse, and they underlined the importance of images. Participants also underlined the role of public diplomacy in correcting the misconceptions that play into the terrorist narrative and the capability of industry, including Internet, telecoms and cable firms, to reach out to the target audience, while avoiding branding their efforts as Counter Terrorism.

The Working Group was of the general view that the ideal carriers of counter-narrative messages should be part of the audience, which posed a great challenge for governments, not only in identifying the messengers but in managing the political risk when messengers had anti-government opinions. Participants agreed that a variety of messengers was desirable, such as victims, repentant extremists, or government officials. Civil society networks such as those of *Women against Violent Extremism*, *Parents against Suicide Bombers* or *Schools against Extremism* could reach out to a wide audience. Whilst not all networks might desire links to governments, governments could play an important role by supporting and institutionalizing such efforts.

There should be an attempt to close research gaps, especially on audience segmentation and mapping, as well as on available capacity-building resources and current initiatives. Participants also proposed creating a platform/task force for mobilizing counter messages and disseminating them widely and rapidly around key events.

Conclusion

The meeting showed that there was considerable interest in and support for action on using the Internet to counter the appeal of terrorism. The Working Group proposes to turn the recommendations and proposals that emerged from the meeting into practical projects for the consideration of Member States, subject to further financial support.

Note

[1] CTITF reports on legal and technical aspects of countering terrorist use of the internet are available at < www.un.org/terrorism/internet >.

Literature on Terrorism, Media, Propaganda & Cyber-Terrorism

Selected by **Eric Price**

NB: some of the items listed below are clickable and allow access to the full text; those with an asterix [*] only have a clickable table of contents.

Altheide, D. L. (2006) *Terrorism and the politics of fear* Lanham, MD.: AltaMira Press [*http://www.loc.gov/catdir/toc/ecip061/2005028887.html]
Altheide, D. L. (2009) *Terror post 9/11 and the media* New York: Peter Lang
Andersen, R. (2006) *A century of media, a century of war* New York: Peter Lang[*http://www.loc.gov/catdir/toc/ecip0616/2006019560.html]
Barton, P. A. (2002) *A history of racism and terrorism, rebellion and overcoming: the faith, power, and struggle of a people* Philadelphia: Xlibris
Catherwood, C. & DiVanna, J. (2008) *The merchants of fear: why they want us to be afraid* Guilford, Conn.: Lyons Press [*http://www.loc.gov/catdir/toc/ecip089/2008003680.html]
Centre of Excellence Defence Against Terrorism. North Atlantic Treaty Organization. (ed.) (2008) *Responses to cyber terrorism* Washington, DC.: IOS Press
Chang, M. (2005) *Brainwashed for war, programmed to kill* Batu Caves, Selangor Darul Ehsan, Malaysia: Thinker's Library
Colarik, A. M. (2006) *Cyber terrorism: political and economic implications* Hershey, PA.: Idea Group Pub. [*http://www.loc.gov/catdir/toc/ecip064/2005034831.html]
Dimaggio, A. R. (2004) *Mass media, mass propaganda: examining American news in the "War on Terror"* Lanham, MD.: Lexington Books [*http://www.loc.gov/catdir/toc/ecip0810/2008004452.html]
Dover, R. & Goodman, M. S. (eds.) (2009) *Spinning intelligence: why intelligence needs the media, why the media needs intelligence* New York: Columbia University Press
Ehrlich, R. (ed.) (2002) *Incitement and propaganda against Israel and Zionism in the educational system of the Palestinian Authority and the alternative Islamic educational system identified with Hamas* Tel Aviv: Intelligence and Terrorism Information Center at the Center for Special Studies
Fortner, R.S. & Fackler, P.M. (eds.) (2011) *The handbook of global communication and media ethics* Chichester, West Sussex, U.K.; Malden, MA.: Wiley-Blackwell [*http://www.loc.gov/catdir/enhancements/fy1114/2010043496-b.html]
Fandy, M. (2007) *(Un)civil war of words: media and politics in the Arab world* Westport, Conn.: Praeger Security International [* http://www.loc.gov/catdir/toc/ecip0710/2007003038.html]
Forest, J. J. F. (ed.) (2009) *Influence warfare: how terrorists and governments fight to shape perceptions in a war of ideas* Westport, Conn.: Praeger Security International
Fullerton, J. A. & Kendrick, A.G. (2006) *Advertising's war on terrorism: the story of the U.S. State Department's Shared Values Initiative* Spokane, Wash.: Marquette Books [*http://www.loc.gov/catdir/toc/ecip067/2006003231.html]
Gerdes, L.I. (2009) *Cyber crime* Detroit: Greenhaven Press [*http://www.loc.gov/catdir/toc/ecip0822/2008027519.html]
Janczewski, L. J. & Colarik, A. M. (eds.) (2008) *Cyber warfare and cyber terrorism* Hershey: Information Science Reference [*http://www.loc.gov/catdir/toc/ecip077/2006102336.html]
Gustin, J. F. (2004) *Cyber terrorism: a guide for facility managers* Lilburn, Ga.: Fairmont Press
Jalālzaʾī, M. K. (2010) *Britain's national security challenges: extremism, cyber terrorism, sectarianism and takfiri jihadism* London: Afghan Academy International
Janczewski, L.J. & Colarik, A.M. (2005) *Managerial guide for handling cyber-terrorism and information warfare* Hershey PA.: Idea Group Publishing [*http://www.loc.gov/catdir/toc/ecip052/2004023593.html]
Johnson, L. K. (ed.) (2007) *Strategic intelligence* Westport, Conn.: Praeger Security International [*http://www.loc.gov/catdir/toc/ecip071/2006031165.html]
Lebaron, W. D. (2007) *Five deadly arrows of terrorism: radiological dispersion devices, chemical weapons, biological weapons, nuclear weapons, cyber terrorism : a manual of information and practice* New York: Nova Science Pub. Inc.
Lee, T. F. (2005) *Battlebabble: selling war in America: a dictionary of deception* Monroe, Me.: Common Courage Press [*http://www.loc.gov/catdir/enhancements/fy0713/2007273831-d.html]

McLaren, P. (2005) *Capitalists and conquerors: a critical pedagogy against empire* Lanham, MD.: Rowman & Littlefield Publishers [*http://www.loc.gov/catdir/toc/ecip053/2004026498.html]
Mushrif, S. M. (2009) *Who killed Karkare? the real face of terrorism in India* New Delhi : Pharos Media & Pub.
Nacos, B. L. (2012) *Terrorism and counterterrorism* Boston: Pearson Longman
O'Shaughnessy, N. J. (2004) *Politics and propaganda: weapons of mass seduction* Ann Arbor: University of Michigan Press
Pak Institute for Peace Studies (PIPS) (2010) *Understanding the militants' media in Pakistan: outreach and impact* Islamabad: Pak Institute for Peace Studies
Palmer, M. & Palmer, P. (2004) *At the heart of terror: Islam, Jihadists, and America's war on terrorism* Lanham, MD.: Rowman & Littlefield Publishers
[*http://www.loc.gov/catdir/toc/ecip0417/2004009249.html]
Reilly, P. (2006). 'Civil Society, the Internet and Terrorism: Case Studies from Northern Ireland'. In: Oates S, Owen D and Gibson RK (eds) *The Internet and Politics: Citizens, Voters and Activists*. London: Routledge, pp. 118-135.
Ross, S. D. &Tehranian, M. (eds.) (2009) *Peace journalism in times of war* New Brunswick: Transaction Publishers
Sauter, M. A. & Carafano, J. J. (2005) *Homeland security: a complete guide to understanding, preventing, and surviving terrorism* New York: McGraw-Hill
[*http://www.loc.gov/catdir/toc/ecip055/2004030511.html]
Schmalleger, F. & Pittaro, M. (eds.) (2009) *Crimes of the Internet* Upper Saddle River, N.J.: Prentice Hall [*http://www.loc.gov/catdir/toc/ecip087/2007052871.html]
Shlaifer, R. (2011) *Perspectives of psychological operations (PSYOP) in contemporary conflicts : essays in winning hearts and minds* Brighton; Portland, Or.: Sussex Academic Press
Steuter, E. & Wills, D. (2008) *At war with metaphor: media, propaganda, and racism in the war on terror* Lanham: Lexington Books [http://www.loc.gov/catdir/toc/ecip0816/2008016776.html]
Taylor, P. M. (2003) *Munitions of the mind: a history of propaganda from the ancient world to the present era* Manchester; New York: Manchester University Press
[*http://www.loc.gov/catdir/enhancements/fy0623/2003059333-t.html]
Tischauser, J. (2010) *Anti-Arab and anti-Muslim bias in American newspapers: how they reported the 2006 Israeli-Hezbollah and Israeli-Hamas wars* Lewiston: The Edwin Mellen Press
Valantin, J.-M. (2005) *Hollywood, the Pentagon and Washington* London: Anthem Press
[*http://www.loc.gov/catdir/toc/fy0713/2007405656.html]
Van Der Veer, P & Munshi, S. (eds.) (2004) *Media, war, and terrorism: responses from the Middle East and Asia* London; New York: Routledge [*http://www.loc.gov/catdir/toc/ecip045/2003013627.html]
Verton, D. (2003) *Black ice: the invisible threat of cyber-terrorism* New York: McGraw-Hill/Osborne
[*http://www.loc.gov/catdir/toc/mh041/2004272545.html]
Webster, M. (2003) *Inside Israel's Mossad: the Institute for Intelligence and Special Tasks* New York: Rosen Pub. Group
Wright, M. I. (2004) *If you're not a terrorist-- then stop asking questions: remixed war propaganda* Philadelphia: Xlibris

Non-conventional Literature (incl. dissertations)

Berger, M. A. (2010) *How resisting democracies can defeat substate terrorism: formulating a theoretical framework for strategic coercion against nationalistic sub-state terrorist organizations* [thesis] University of St. Andrews
Boyd, C.D. (1994) *Terrorism as a psychological operation: a comparative analysis of the Zionist and the Palestinian Terrorist Campaigns* [thesis] Naval Postgraduate School: Monterey, California
[http://www.hsdl.org/?view&did=465052]
Briant, E. L. (2011) *Special relationships' : the negotiation of an Anglo-American propaganda 'War on Terror'* [thesis] University of Glasgow [http://theses.gla.ac.uk/2840/]
Brundin, P (2008) *Politics on the Net: NGO practices and experiences* [thesis] Orebro University [http://urn.kb.se/resolve?urn=urn:nbn:se:oru:diva-2121]

Buckle, C. (2011) *The 'War on Terror' metaframe in film and television* [thesis] University of Glasgow [http://theses.gla.ac.uk/3014/01/2011bucklephd.pdf]
Butler, J. O. (2010) *The power & politics of naming: literaryonomastics within dystopian fiction* [thesis] University of Glasgow [http://theses.gla.ac.uk/1706/01/2009butlerMPhil.pdf]
Commission of the European Communities (2007) *Impact Assessment* EU: Brussels [http://ec.europa.eu/governance/impact/ia_carried_out/docs/ia_2007/sec_2007_1424_en.pdf]
Coteanu, G. C. (2005) *Cyber consumer law: State of the art and perspectives* [thesis] Leiden University [http://hdl.handle.net/1887/4387]
Dumas, J. M. (2010) *The race for Muslim hearts and minds: a social movement analysis of the U.S. war on terror and popular support in the Muslim world* [thesis] University of St. Andrews
Elfwing, S. (2007) *Embodied Evolution of Learning Ability* [thesis] KTH, Sweden [http://kth.diva-portal.org/smash/record.jsf?pid=diva2:12636]

Jannepally, H. R. (2010) *The 2008 Mumbai Attack and Press Nationalism: A Content Analysis of Coverage in the New York Times, Times of London, Dawn, and the Hindu* [thesis] University of Ohio [http://etd.ohiolink.edu/view.cgi?acc_num=ohiou1283534128]
Lindquist, T. (2003) *A war of words, from Lod to Twin Towers: defining terrorism in Arab and Israeli newspapers 1972-1996 (2001), a study in propaganda, semantics and pragmatics* [thesis] Uppsala, Sweden: Uppsala Universitet
de Mesquita, E.B. & Dickson, E.S. (n.d.) *The Propaganda of the Deed:Terrorism, Counterterrorism, and Mobilization* [http://www.nyu.edu/gsas/dept/politics/faculty/dickson/dickson_propaganda.pdf]
Murphy, D.M. (et al.) (eds.) (2006) *Information as Power* United States Army War College [http://www.au.af.mil/au/awc/awcgate/army-usawc/info_as_power_v1.pdf]
Musgrove, L. (2008) *The social psychology of emotion in reactions to propaganda about the war on terror* [thesis] Australian National University
O'Regan, M. (2009) *Framing the Israeli-Palestinian conflict: a case-study analysis of the Irish national 'opinion leader' press - July 2000 to July 2004* [thesis] University of Sterling. [http://hdl.handle.net/1893/1921]
Ramos, R.T. (2007) *Legislating after Terrorism: September 11, the News Media and the Georgia Legislature* [thesis] Georgia State University [http://digitalarchive.gsu.edu/cgi/viewcontent.cgi?article=1033&context=communication_theses]
Rast, M. (2011) *Tactics, Politics, and Propaganda in the Irish War of Independence, 1917-1921* [thesis] Georgia State University [http://digitalarchive.gsu.edu/cgi/viewcontent.cgi?article=1045&context=history_theses]
Reilly, P. (2007) *Framing online communications of civil and uncivil groups in post-conflict Northern Ireland* [thesis] University of Glasgow [http://theses.gla.ac.uk/131/01/2007Reillyphd.pdf]
Skoczylis, J. (2009) *Media framing of terrorism post 7/7 bombings* [thesis] University of Oxford
Theohary, C.A. & Rollins, J. (2011) *Terrorist Use of the Internet* CRS Report [http://www.statewatch.org/news/2011/apr/us-crs-terr-internet.pdf]
Tikk, E. (2011) *Comprehensive legal approach to cyber security* [thesis] Tartu University [http://hdl.handle.net/10062/17914]
Transnational Terrorism, Security & the Rule of Law. (2008) *Terrorism and the Media* European Commission [http://www.transnationalterrorism.eu/tekst/publications/WP4%20Del%206.pdf]
Wagner, R.A. (2005) Terrorism and the Internet: Use and Abuse [in] Last, M. & Kande, A. *Fighting Terror in Cyberspace* World Scientific [http://www.worldscibooks.com/etextbook/5934/5934_chap1.pdf]

Prime Journal Articles & Book Chapters

Alexander, Y.: Terrorism and the Media *Terrorism: An International Journal* 2 (1-2) 1979 pp.1-147
Altheide, D.L.: Format and symbols in TV coverage of terrorism in the United States and Great Britain *International Studies Quarterly* 31 (2, June) 1987 pp.161-176
Altheide, D.L.: Terrorism and the politics of fear *Cultural Studies Critical Methodologies* 6 (4, November) 2006 pp.415-439
Altheide, D. L.: Terrorism Programming *Critical Studies on Terrorism* 2 (1) 2009 pp.65-80

Anderson, J.: The Neo-Nazi Menace in Germany *Studies in Conflict & Terrorism* 18 (1) pp.39-46
Anon.: Psychological Warfare and How to Wage It *Current History and Forum* LI (1940) pp.52-53
Asher, T. R.: Uncomfortably numb *Index on Censorship* 32 (3) 2003 pp.105-111
Atkinson M. & Young K.: Terror Games: Media Treatment of Security Issues at the 2002 Winter Olympic Games *Olympika: The International Journal of Olympic Studies* 11 (2003) pp.53-78
Barry T. E. & Howard D. J.: A review and critique of the hierarchy of effects in advertising *International Journal of Advertising* 9 (2, March) 1990 p.121ff.
[http://fabriken.akestamholst.se/akestamholst/files/critique_of_the_hierarchy_of_effects.pdf]
Bergen, P. & Reynolds, A.: Blowback Revisited *Foreign Affairs* 84 (November/December) 2005
[http://www.foreignaffairs.com/articles/61190/peter-bergen-and-alec-reynolds/blowback-revisited]
Bennett W. L.: Toward a theory of press state relations in the United States *Journal of Communication* 40 (2, Spring) pp.103-117 [http://tombirkland.com/399/bennett1990.pdf]
Berinato S.: The truth about cyber-terrorism *CIO Magazine* 1 (June) 2003
[www.cio.com/archive/031502/truth.html]
Bowman-Grieve, L. & Conway, M. (in press). Considering the Content and Function of Dissident Irish Republican Online Discourses. *Media War & Conflict (Special Issue)*.
Bowman-Grieve, L. The Internet & Terrorism: Pathways toward terrorism & counter-terrorism. In: A. Silke (Ed.), *Psychology, Terrorism and Counterterrorism*. Oxon: Routledge, 2011.
Bowman-Grieve, L. (2010). 'Irish Republicanism and the Internet: Support for New Wave Dissidents', *Perspectives on Terrorism,* Vol. IV, Issue2, pp. 22-34.
Burnett, J. & Whyte D.: Embedded expertise and the new terrorism *Journal for Crime, Conflict and the Media* 1 (4) 2005 pp.1-18
Burris, V. (et al.): White supremacist networks on the Internet *Sociological Focus* 33 (2, May) 2000 pp.215-235 [http://darkwing.uoregon.edu/~vburris/whites.pdf]
Caiani, M. & Parenti, L.: The Dark Side of the Web: Italian Right-Wing Extremist Groups and the Internet *South European Society and Politics* 14 (3) 2009 pp.273-294
Caiani, M. & Wagemann, C.: Online networks of the Italian and German extreme-right: an explorative study with social network analysis *Information, Communication & Society* 12 (1) 2009 pp.66-109
Castells, M.: Toward a sociology of the network society *Contemporary Sociology* 29 (5, September) 2000 pp.693-699
Clem A. (et al.).: Health implications of cyber-terrorism *Pre-hospital and Disaster Medicine*
[http://pdm.medicine.wisc.edu/Volume_18/issue_3/clem.pdf]
Conway M.: What is Cyberterrorism? *Current History* 101 (659), December 2002, pp.436-442.
Conway M.: Terrorism and the Internet: New Media, New Threat? *Parliamentary Affairs* 59 (2, February) 2006, pp.283 - 298.
Conway, M.: 'Terrorist Web Sites: Their Contents, Functioning, and Effectiveness.' In: P. Seib (ed.) *Media and Conflict in the Twenty-First Century*. New York: Palgrave, 2005, pp. 185-215.
Cotter, J. M.: Sounds of Hate: White Power Rock and Roll and the Neo-Nazi Skinhead Subculture. *Terrorism and Political Violence,* Vol. 11, Issue 2, 1999 pp.111-140.
Cowen, T.: Terrorism as theater: Analysis and policy implications *Public Choice* 128 (2006) pp.233-244
[http://econfaculty.gmu.edu/bcaplan/pdfs/terrorism.pdf]
Crilley, K.: Information warfare: new battlefields Terrorists, propaganda and the Internet *Aslib Proceedings* 53 (7, July/August) 2001 pp.250-264
[http://202.41.82.144/data/HACKING_INFORMATION/PRINTED%20PAPERS/informan%20warfare%20new%20battlefields.pdf]
Ducol, B. (2012). 'Uncovering the French-Speaking Jihadisphere: An Exploratory Analysis', *Media, War & Conflict* 5(1*): [forthcoming - page numbers not yet available].*
Eastwood, M.: Lessons in hatred: the indoctrination and education of Germany's youth *The International Journal of Human Rights* 15 (8) 2011 pp.1291-1314
Elliot, P., Murdock G. & Schlesinger P.: Terrorism and the state: a case study of the discourses of television *Media, Culture and Society* 5 (2) 1983 pp.155-177
Ermlich, F.A.: Terrorism and the media: Strategy, coverage, and responses *Political Communications* 4 (2) 1987 pp.135-139
Foltz C. B.: Cyberterrorism, computer crime, and reality *Information Management & Computer Security* 12 (2) 2004 pp.154-166

Garrison, A.H.: Defining Terrorism: Philosophy of the Bomb, Propaganda by Deed and Change Through Fear and Violence *Criminal Justice Studies* 17 (3, September) 2004 pp.259-279 [http://cjc.delaware.gov/PDF/defining%20terrorism.pdf]
Gerstenfeld. P. B. (et al.): Hate online: a content analysis of extremist Internet sites *Analysis of Social Issues and Public Policy* 3 (1) 2003 pp.29-44 [http://www.asap-spssi.org/pdf/asap31-Gerstenfeld.pdf]
Glaser, J. (et al.) : Studying hate crime with the Internet: what makes racists advocate racial violence? *Journal of Social Issues* 58 (1) 2002 pp.177-193 [http://collections.lib.uwm.edu/cipr/image/286.pdf]
Gordon S. & Ford R.: Cyberterrorism? *Computers and Security* 21 (May) 2011 [http://www.symantec.com/avcenter/reference/cyberterrorism.pdf]
Guth, D. W.: Black, White, and Shades of Gray: The Sixty-Year Debate Over Propaganda versus Public Diplomacy *Journal of Promotion Management* 14 (33-4) 2009 pp.309-325
Heuston S.: Weapons of Mass Instruction: Terrorism, Propaganda Films, Politics, and Us: New Media, New Meanings *Studies in Popular Culture* 27 (3, April) 2005 pp.59-74 [http://pcasacas.org/SiPC/27.3/Weapons%20of%20Mass%20Instruction%20-%20Terrorism,%20Propoganda%20Film,%20Po.pdf]
Holton, G.: Reflections on Modern Terrorism. *Terrorism: An International Journal* 1 (3-4) 1978 pp.265-276.
Howard, P. (et al.): When Do States Disconnect Their Digital Networks? Regime Responses to the Political Uses of Social Media 14 (3) 2011 pp.216-232
Jacobson, M.: Terrorist financing and the Internet *Studies in Conflict & Terrorism* 33 (4) 2010 pp.353-363
Karim, K. H.: Cyber-utopia and the myth of paradise: using Jacques Ellul's work on propaganda to analyse information society rhetoric *Information, Communication & Society* 4 (1) 2001 pp.113-134
Kaufmann C.: Threat inflation and the failure of the marketplace of ideas: The selling of the Iraq war *International Security* 29 (1) 2004 pp.5-48 [http://belfercenter.ksg.harvard.edu/files/kaufmann.pdf]
Kellner, D.: September 11, the media, and war fever *Television and New Media* 3 (2, May) 2002 pp.143-151 http://ics.leeds.ac.uk/papers/pmt/exhibits/1865/Kellner2.pdf]
Kellner, D.: 9/11, spectacles of terror, and media manipulation *Critical Discourse Studies* 1 (1) 2004 pp.41-64
Kern, S.: Radical Islamic Television Arrives in Spain *Hudson New York* December 22, 2011 [http://www.hudson-ny.org/2692/islamic-television-spain]
Kingston, S.: Terrorism, the media, and the Northern Ireland conflict *Studies in Conflict & Terrorism* 18 (3) 1995 pp.203-231
Kitch, C.: 'Mourning in America': ritual, redemption, and recovery in news narrative after September 11 *Journalism Studies* 4 (2) 2003 pp.213-224
Klaehn J.: Behind the Invisible Curtain of Scholarly Criticism: Revisiting the Propaganda Model *Journalism Studies* 4 (2003) pp.359-369
Kohlmann E. F.: The real online terrorist threat *Foreign Affairs* 85 (September-October) 2006 [http://www.foreignaffairs.com/articles/61924/evan-f-kohlmann/the-real-online-terrorist-threat]
Lee, E. & Leets, L.: Persuasive storytelling by hate groups online: examining its effects on adolescents *American Behavioral Scientist* 45 (6, February) 2002 pp.927-957 [http://www9.georgetown.edu/faculty/lll27/files/leets8.pdf]
Livingston S. & Bennett W. L.: Gatekeeping, indexing, and live-event news: is technology altering the construction of news? *Political Communication* 20 (4, October) 2003 p..336-380 [http://ics.leeds.ac.uk/papers/pmt/exhibits/2012/livingstone&bennet.pdf]
Luskin B. J.: Toward an understanding of media psychology *T H E Journal* 23 (1996) [http://thejournal.com/articles/1996/02/01/toward-an-understanding-of-media-psychology.aspx]
Martin, L. J.: Disinformation: An instrumentality in the propaganda arsenal *Political Communication* 2 (1) 1982 pp.47-64
Martin, L. J.: The media's role in international terrorism *Terrorism* 8 (2) 1986 pp.127-146
Matusitz J.: Postmodernism and networks of cyberterrorists *Journal of Digital Forensic Practice* 2 (1, January) 2008 pp.17-26
Mendes, E.P.: Democracy, Human Rights and the New Information Technologies in the 21st Century--The Law and Justice of Proportionality and Consensual Alliances *National Journal of Constitutional Law* 10 (3) 1999 pp.351-372

Miller, B. H.: Terrorism and language: a text-based analysis of the German case *Terrorism* 9 (4) 1987 pp.373-407
Miller, D. & Mills, T.: The terror experts and the mainstream media: the expert nexus and its dominance in the news media *Critical Studies on Terrorism* 2 (3) 2009 pp.414-437
Minei, E. & Matusitz, J.: Cyberterrorist Messages and Their Effects on Targets: A Qualitative Analysis *Journal of Human Behavior in the Social Environment* 21 (8) 2011 pp.995-1019
Mockaitis, T.: Winning hearts and minds in the 'War on Terrorism' *Small Wars & Insurgencies* 14 (1) 2003 pp.21-38
Nalton, J., Ramsey, G. and Taylor, M. (2011). 'Radicalization and Internet Propaganda by Dissident Republican Groups in Northern Ireland Since 2008'. In: P. M. Currie and M. Taylor (eds) *Dissident Irish Republicanism*. New York: Continuum, pp. 119-141.
Narula, S.: Psychological operations (PSYOPs): A conceptual overview *Strategic Analysis* 28 (1) 2004 pp.177-192
Nemes, I.: Regulating Hate Speech in Cyberspace: Issues of Desirability and Efficacy *Information & Communications Technology Law* 11 (3) 2002 pp.193-200
Patrick, B. A. & Thrall, T. A.: Beyond Hegemony: Classical Propaganda Theory and Presidential Communication Strategy After the Invasion of Iraq *Mass Communication and Society* 10 (1) 2007 pp.95-118
Payne, K.: Winning the Battle of Ideas: Propaganda, Ideology, and Terror *Studies in Conflict & Terrorism* 32 (2) 2009 pp.109-128
Plaisance, P. L.: The Propaganda War on Terrorism: An Analysis of the United States' "Shared Values" Public-Diplomacy Campaign After September 11, 2001 J*ournal of Mass Media Ethics* 20 (4) 2005 pp.250-268
Padovani, C.: The extreme right and its media in Italy *International Journal of Communication* 2 (2008) pp.753-770 [http://ijoc.org/ojs/index.php/ijoc/article/view/314/191]
Qin, J. (et al.): Analysing terror campaigns on the Internet: TECHNICAL sophistication, content righness and web interactivity *International Journal of Human - Computer Studies* 65 (2007) pp.71-84 [http://ai.arizona.edu/intranet/papers/paper-Jialun-WebMetrics.pdf]
Ryan M.: Journalistic ethics, objectivity, existential journalism, standpoint epistemology, and public journalism *Journal of Mass Media Ethics* 16 (3) 2001 pp.3-22
Ryan M.: Mainstream news media, an objective approach, and the march to war in Iraq *Journal of Mass Media Ethics* 21 (4) 2006 pp.4-29
Ryan, M. & Switzer, L.: Propaganda and the subversion of objectivity: media coverage of the war on terrorism in Iraq *Critical Studies on Terrorism* 2 (1) 2009 pp.45-64
Schmid, A.P.: Terrorism as Psychological Warfare *Democracy and Security* 1 (2005) pp.137–146 [http://ics.leeds.ac.uk/papers/pmt/exhibits/2745/TasPW.pdf]
Schmid, A. P. : The Importance of Countering Al-Qaeda's 'Single Narrative'; in: E.J.A.M. Kessels (ed) *Countering Violent Extremist Narratives.* The Hague: National Coordinator for Counterterrorism, 2010, pp. 46-57.
Sarma, K.: Defensive Propaganda and IRA Political Control in Republican Communities *Studies in Conflict & Terrorism* 30 (12) 2007 pp.1073-1094
Schleifer, S. A.: Media and religion in the Arab/Islamic World *The Review of Faith & International Affairs* 7 (2) 2009 pp.61-68
Slone M.: Response to media coverage of terrorism *Political Communication Conflict Resolution* 44 (4, August) 2000 pp.508-522
Sorenson, J.: Constructing terrorists: propaganda about animal rights *Critical Studies on Terrorism* 2 (2, August) 2009 pp.237-256
[http://ethik.univie.ac.at/fileadmin/user_upload/inst_ethik_wiss_dialog/Sorenson__J._2009._Constructing_terrorists__propaganda_about_a_r.pdf]
Soriano, M. & Torres, R.: Spain as an Object of Jihadist Propaganda *Studies in Conflict & Terrorism* 32 (11) 2009 pp.933-952
Sproule J. M.: Progressive propaganda critics and the magic bullet myth *Critical Studies in Mass Communication* 6 (3, September) 1989 pp.225-246
Stenersen, A. (2008). The Internet: A Virtual Training Camp. *Terrorism & Political Violence,* Vol. 20, Issue 2, pp. 215-233.

Steuter, E.: Understanding the media/terrorism relationship: An analysis of ideology and the news in time magazine *Political Communication* 7 (4) 1990 pp.257-278
Streckfuss, R.: Objectivity in journalism: a search and a reassessment *Journalism Quarterly* 67 (4, Winter) 1990 pp.973-983
Taylor, P.M.: Strategic Communications and the Relationship between Governmental 'Information' Activities in the Post 9/11 World *Journal of Information Warfare* 5 (3) 2006 pp.1-26 [http://ics.leeds.ac.uk/papers/pmt/exhibits/2831/JIW5_3_final_draft.pdf]
Tilley, E.: Responding to terrorism using ethical means: the Propaganda Index *Communication Research Reports* 22 (1) 2005 pp.69-77
Toohey, K. & Taylor, .T: Here be Dragons, Here be Savages, Here be bad Plumbing Australian Media Representations of Sport and Terrorism *Sport in Society* 9 (1) 2006 pp.71-93
Torres S. M. R.: Spain as an object of jihadist propaganda *Studies in Conflict & Terrorism* 32 (11) 2009 pp. 933-952
Torres, M. R., Jordan, J. & Horsburgh, N.: Analysis and Evolution of the Global Jihadist Movement Propaganda *Terrorism and Political Violence* 18 (3) 2006 pp.399-421
Torres, S. & Manuel, R.: The Road to Media Jihad: The Propaganda Actions of Al Qaeda in the Islamic Maghreb *Terrorism and Political Violence* 23 (1) 2010 pp.72-88
Tugwell, M.: Politics and propaganda of the provisional IRA *Terrorism* 5 (1-2) 1981 pp.13-40
Tsfati Y. & Weimann G.: www.terror.com: Terror on the Internet *Studies in Conflict and Terrorism* 25 (2002) pp.317-332 [http://www.psci.unt.edu/jbooks/TerrorBib_files/Terrorism%20&%20the%20Media/Tsfati%20&%20Weimann-www.terrorism.com.pdf]
Weimann, G.: Conceptualizing the effects of massacre mediated terrorism *Political Communication* 4 (3) 1987 pp.213-216
Weimann, G.: Virtual disputes: the use of the internet for terrorist debates *Studies in Conflict and Terrorism* 29 (7, October-November) 2006 pp.623-639
Western, J.: The War over Iraq: Selling War to the American Public *Security Studies* 14 (1) 2005 pp.106-139
Wilkinson, P.: The media and terrorism: a reassessment *Terrorism and Political Violence* 9 (2) 1997 pp.51-64 [http://ics.leeds.ac.uk/papers/pmt/exhibits/755/The%2520Media%2520and%2520Terrorism.pdf]
Wilske S. & Schiller, T.: International Jurisdiction in Cyberspace: Which States May Regulate the Internet? *Federal Communications Law Journal* 50 (1997) pp.129-142
Wright, J. & Bryett, K.: Propaganda and justice administration in Northern Ireland *Terrorism and Political Violence* 3 (2) 1991 pp.25-4
Zhou, Y. (et al.): U.S. domestic extremist groups on the web: link and content analysis *IEEE Intelligent Systems* 20 (2006) pp-1-44 [http://ai.arizona.edu/intranet/papers/Zhou_Domestic_MainText.pdf]

See also resources on the Internet:

Cyber Terrorism Resource Centr [http://www.globaldisaster.org/cyberterrorrescen.shtml]
Internet / Network Security Resource guide on Cyber-terrorism [http://netsecurity.about.com/cs/cyberterrorism/]
IWS United Kingdom Website Listing [http://www.iwar.org.uk/cyberterror/index.htm]
National Cyber Security Alliance [http://www.staysafeonline.info/]
Terrorism Questions and Answers: Cyber-terrorism [http://www.terrorismanswers.com/terrorism/cyberterrorism.html]
Terrorism questions and answers: Cyber-terrorism Europe [http://www.terrorismanswers.com/coalition/europe.html]
U.S. Department of State: Country Reports on Terrorism [http://www.state.gov/s/ct/rls/crt/index.htm]

Eric Price *is a professional information specialist. He worked for many years with the International Atomic Energy Agency in Vienna (IAEA).*

The YouTube Jihadists: A Social Network Analysis of Al-Muhajiroun's Propaganda Campaign

By Jytte Klausen, Eliane Tschaen Barbieri, Aaron Reichlin-Melnick, and Aaron Y. Zelin

Source: http://www.terrorismanalysts.com/pt/index.php/pot/article/view/klausen-et-al-youtube-jihadists/html

Abstract

Producers of Al-Qaeda inspired propaganda have shifted their operations in recent years from closed membership online forums to mainstream social networking platforms. Using social network analysis, we show that behind the apparent proliferation of such sources, YouTube account holders associated with incarnations of the British al-Muhajiroun collude to post propaganda and violent content. European groups commonly use American platforms and domain names registered with American companies. Seeking shelter under speech rights granted by the First Amendment, they evade European laws against incitement and hate speech.

Introduction

The successes of the popular uprising of the Arab Spring have been credited, at least in part, to social networking media, and in particular to *Facebook*, *YouTube*, and *Twitter*. Relatively unnoticed, certainly uncelebrated, is the fact that closer to home the same mainstream social networking media platforms have been exploited by radical Islamists. They feature again and again in a series of recent terrorism indictments involving jihadists.

After following a number of recent cases in which material broadcast on *YouTube* inspired violence, we noticed that many accounts appeared to be incarnations of the same online entity. Is this the result of deliberate coordination, even a virtual representation of a political organization? Or are like-minded people simply finding one another by chance on the Internet?

Over a three-month period in early 2011, we identified 41 *YouTube* accounts –technically known as "channels"—that posted jihadist content and carried brand names with a family resemblance to incarnations of the British-based banned organization, *al-Muhajiroun*. Twenty-one used some version of the *Shariah4* label, playing on the name of Islam4UK, a banned organization in the *al-Muhajiroun* clan.

A remarkable feature of these channels is that although they are generally authored in Europe they are legally based in the US, and therefore enjoy protection under the First Amendment. In an earlier attempt to steer clear of law enforcement, jihadist groups migrated from open online forums to invitation-only sites. The strategy was unsatisfactory, because invitation-only sites limited access to potential recruits. In contrast, the social networking sites reach an unrestricted audience. Anyone can link up at the click of the mouse and dissemination is easily amplified by means of automatic reposting. Operators can also hide potentially illegal material in the mass of online postings on the sites.

The legal shield given to mainstream platforms compels law enforcement and service providers to close down sites and remove extremist videos on an ad hoc basis, one by one. First Amendment considerations make this a delicate matter if sites are registered in the US. In 2008, *Dynadot*, an American domain name registrar and webhost, faced pressures over its hosting of *Wikileaks* following a complaint from a Swiss bank. Judge Jeffrey S. White of the Federal District Court in San Francisco temporarily ordered the company to cease hosting the *Wikileaks* website. A coalition of free speech groups filed a court brief protesting the restraining order on First Amendment grounds.[1] The judge later reversed the decision, commenting that his judgment had raised "serious questions of prior restraint (on speech) and possible violations of the First Amendment."[2] *Dynadot* retains the right in its customer agreements to terminate accounts associated with "morally objectionable activities."[3] The company is one of the webhosts frequently used by jihadists.

Taking Online Jihadism onto Social Networking Platforms

The new internet-based technologies lower the bar for participation in the

global jihadist movement. On the web, one can proselytize for the jihad all day and night with friends from around the world by posting and cross-posting content on social networking platforms linked to a website with a domain name that allows the projection of an online brand.

Domain names are hostnames that are identified with a specific location on the Internet known as an Internet Protocol (IP) address. The right to use a particular online domain name, such as *RevolutionMuslim.com*, can be obtained from hosting service providers for a fee. The companies also act as web hosts by providing bandwidth on the Internet and remote storage space for subscribers on servers they own or lease.

The Internet Corporation for Assigned Names and Numbers (ICANN) delegates the registration of domain names to hosting companies. The companies are responsible for keeping a registry of the name and number systems of Internet domains. Registrants must submit personal contact information to the hosting companies. This is posted on the searchable WHOIS database. (We used it to determine the hosting companies and domain holder identities of websites linked to the *YouTube* channels.)

YouTube is an Internet portal specialized in video sharing. It was launched in 2005 but usage did not catch on until spring 2006. Anyone can watch posted videos, but only registered users can upload videos. To increase traffic, *YouTube* account holders often place links to their uploaded videos on a personal webpage or on their *Facebook* profile. Google acquired *YouTube* in 2006, and the portal has recently been adapted to other languages, including Arabic. Known as "localization," the foreign-language platforms provide user access in local languages but do not affect the engineering or hosting. *YouTube*'s hosting server is located in Mountain View, California. The portal has become the chosen vehicle for the posting of jihadist videos and other content for the obvious reason that the multi-lingual and audio-visual format suits the purpose.

Facebook is also an Internet portal. Launched in 2004, it has an estimated 800 million users worldwide. The United States leads the way with more than 150 million users, which means that close to 50% of the American population has a *Facebook* profile.[4] The United Kingdom ranks fourth with about 30 million users. (Second and third are much more populous Indonesia and India.) Users register to set up their own profile on the portal and add other users as "friends" to allow content to cross-post.

Twitter, the most recent and the smallest of the three platforms, was created in 2006. It is designed as a phone-based application and limits users to text-based postings of messages composed of a maximum of 140 characters, the standard length of a SMS. Celebrities use it to broadcast their doings and thoughts to followers. The *emirs* associated with the *Al-Qaeda*-inspired *YouTube* accounts analyzed in this article started "tweeting" in March and April 2011. *Twitter* is used to post instant observations on current affairs (e.g. "The rise of Muslims in Syria will be the end of Israel […]") and redirecting adherents to new postings on other platforms (e.g. "The US constitution & its laws are not even worthy for the US President to abide by & to respect www.Shariah4America.com has some solutions").[5]

American hosting servers are a popular choice for practical and legal reasons. A domain name can be registered for as little as $11.99 per year. Hosting services with global bandwidths can be rented for four dollars and less per month from companies like GoDaddy.com and *Dynadot*.com. The *Dynadot* server, located in San Mateo, California, offers a privacy service, which allows registrants to mask their identity by listing addresses as "care of" the company, a convenience that has made it particularly popular with jihadists and Internet activists hoping to elude the authorities.

Much of the content of the jihadist sites would be deemed illegal in Europe. The passage of two laws in the UK (Racial and Religious Hatred Act 2006 (c. 1) and Serious Crime Act 2007 (c. 27) target hate speech or incitement to violence.[6] The German Penal Code (Section 13) prohibits hate speech and "utterances capable of instigating violence, hatred, or discrimination." The shift to American host servers exploits the First Amendment protection allowed to US-based Internet providers.

This is not a new development, nor is it limited to media-savvy European jihadists. The main *Al-Qaeda* forum, *Shmukh al-Islam,* was hosted in the United States through Domains by

Proxy, Inc., but moved to an Indonesian server. The domain name is registered in the US. *Salafi Media* is hosted by HostMonster. *Authentic Tawheed* was hosted by an American server but is now hosted by a Syrian server, while *The Tawheed Movement* was previously hosted by Bytehost but recently moved to *Dynadot*.

Al-Muhajiroun's Online Media Productions

Based upon the similarities in content and design, we suspected that many of the *YouTube* channels that feature *Al-Qaeda*-inspired proselytizing are incarnations of the same organization, albeit designed to appear independent. They are calculated to be resilient to disruption, so that if one is taken down the others are able to continue to post the same material, or new ones can be easily created to replicate them.

We found that indeed there was a single production entity behind most of the propaganda: *Al-Muhajiroun*.

Al-Muhajiroun (the Emigrants) was created in 1986 by Omar Bakri Muhammad as a shell organization for Hizb ut-Tahrir (HuT), a pan-Islamic extremist organization created in the 1950s. When Bakri Muhammad left HuT in 1996, he declared it independent and the organization functioned as his vehicle until 2004 when he disbanded it to forestall proscription. Bakri Muhammad was exiled from the United Kingdom in 2005 when the UK Home Secretary, Charles Clarke, revoked his residency permit. Some of Britain's most notorious jihadists have been *al-Muhajiroun* members. Britain's first suicide bomber, Bilal Ahmed, who blew himself up in Kashmir in December 2000, allegedly was a member. Asif Hanif and Omar Khan Sharif, who carried out suicide actions at a bar in Tel Aviv in 2003, and Omar Khyam, the ring-leader of the so-called "fertilizer plot" who was convicted in 2006 on charges of wanting to blow up Parliament and targets in London, were also members.

Bakri Muhammad allegedly formed over eighty front organizations in at least six countries. He continues to play a role, logging on from Lebanon, where he now lives. He was sentenced to life in prison in Lebanon in November 2010 for training *Al-Qaeda* operatives at a camp in northern Lebanon. Lebanese authorities arrested Bakri Muhammad shortly afterwards, but he is at present free on bail pending a retrial.

In 2009, one of Bakri Muhammad's disciples, Anjem Choudary, re-formed *al-Muhajiroun* in the UK. *Al-Muhajiorun* and several aliases of the group have been banned. Most recently, another incarnation reconstituted under the banner of *Islam4UK* was banned in January 2010. The names and aliases have acquired a second life as online domains. Today what remains of the group has shrunk to less than a hundred members. It now operates primarily under the alias of *Muslims Against Crusades* (MAC).

Choudary's boundary-pushing stunts have created an outcry in the United Kingdom. He received much publicity in 2009 after he declared that Buckingham Palace should be turned into the seat for the new Caliph.[7] The reaction encouraged Choudary. His subsequent releases targeting the American media market included mock-up photos indicating a jihadist take-over attached to articles on "The White Masjid," which is an allusion to the White House. The Islamic Demolition of the Statue of Liberty is dramatized by draping a *burqa* over the monument. Another posting announces the creation of the International Sharia Court of Justice to replace the United Nations in New York City. One photo shows Choudary in front of the White House with a black flag of Islam.

The content of the *YouTube* channels is strikingly similar. Over images of Muslims suffering at the hands of Western military forces, the sound track broadcasts *anasheed* (a vocal musical genre favored by jihadists) and texts from the Koran, or a voice-over explaining the righteous path. Anjem Choudary, Omar Bakri Muhammad, and Abu Hamza al-Masri are the most frequently used speakers. Videos featuring Osama Bin Laden and Anwar al-Awlaki are also popular. Programs addressed specifically to particular national audiences feature local celebrity emirs and activists. Choudary officially endorsed one of the channels, *Sharia4Belgium*, in March 2010: "We support our brothers in Belgium under the banner of *Sharia4Belgium* and we are ready, whatever they need to send more people to support them in their activities, in their duty, and fulfilling their responsibility."[8]

The *YouTube* channels in the *Shariah4* network also cross-post many of the same videos. Some *Shariah4* channels are created, with content uploaded, and then rarely updated.

The most active channels include *Sharia4Belgium* (and its successor channels), *Shariah4Holland, Shariah4Australia* (and its successor channel), *Shariah4Poland, Shariah4Pakistan, and Shariah4AlAndalus*. The recent uprisings in the Arab world produced a proliferation of new channels with similarly themed content: *Shariah4Tunisia, Sharia4Egypt,* and *Sharia4Yemen.*

The *Shariah4Tunisia* channel, for instance, highlights four videos of demonstrations in which members of *al-Muhajiroun* call for an Islamic state in Tunisia. Two of the videos show a British Tunisian. The other two videos feature Anjem Choudary. Choudary also makes an appearance in a video titled "Shariah 4 Libya" that was uploaded to *YouTube* by *londondawah*, another channel of British jihadists that is loosely affiliated with *al-Muhajiroun*. The *Sharia4Egypt* and *Sharia4Yemen* channels had only one video each. Both videos have *anasheed* in the background with pictures from the protests and text of the Koran in Arabic and English calling for the establishment of Shariah.

Recent Incidents Involving YouTube Channels Linked to Al-Muhajiroun Affiliates

These *YouTube*-based jihadist channels promote violent acts, broadcast threats, and announce and direct events and demonstrations. Counter-terrorism strategies are geared to pick up cues from surveillance of radical environments. Online extremism has moved the radicalization process into suburban living rooms, and made it possible for *Al-Qaeda* agents to recruit "homegrown" terrorists over the Internet.[9]

Violent Acts

We identified three violent acts involving the same network of *YouTube* and *Facebook* contacts, including channels from the *al-Muhajiroun YouTube* network that we analyze here. In each case law enforcement was taken by surprise. Cues indicating a need to put these individuals on watch list were either missed or non-existent.

Taimour Abdulwahab al-Abdaly, a 30-year old Iraqi-born Swedish citizen who had lived in Luton, England since 2001, set off two bombs in downtown Stockholm on December 11, 2010. One was a car bomb and the other a pipe bomb that went off in his backpack, possibly prematurely. Al-Abdaly was killed and two bystanders injured. A Glasgow man was arrested three months later in connection with the attack, but little is known of his role. Al-Abdaly was an avid user of *Facebook* and *YouTube*. He sent an email to newspapers just before he blew himself up and may have been trying to film and broadcast his martyrdom. Al-Abdaly's *Facebook* profile and *YouTube* viewing habits were captured by *Internet Haganah*, an online investigative project. One video al-Abdaly watched shortly before his violent act was uploaded by *videomuslim*, a subscriber account to *Shariah4Holland*, one of the main *al-Muhajiroun* channels in this study. We identified six account holders in the second wave of subscriber channels in our sample of *al-Muhajiroun* related channels, which were also on al-Abdaly's viewing list.[10]

On March 2, 2011, Arid Uka, a 21-year old Kosovo Albanian who grew up in Germany, fatally shot two U.S. soldiers who were boarding a bus at Frankfurt airport. Uka told prosecutors that he had been motivated by a video of U.S. soldiers raping a Muslim woman. The video—in fact a scene from Brian De Palma's fictional anti-Iraq War movie *Redacted* [11]—was uploaded on at least two *Shariah4* channels days before the shooting.[12] Uka, whose *Facebook* name was "Abu Rayyan", added the German Jihadist group *Dawa FFM* as a friend on February 25.[13] Uka was not a known member of local jihadist networks and was not under surveillance prior to his attack, although he was deeply enmeshed in online jihadist social networking. Uka was a *Facebook* "friend" of several well-known jihadists who also were on the Stockholm bomber's list of *Facebook* friends.[14]

On June 22, 2011, authorities arrested two men in Seattle, USA, on charges of planning an attack on an Army recruiting center. The leader, Abu Khalid Abdul-Latif, an African-American convert, also known as Joseph Anthony Davis, was an active online propagandist. He has said that he wanted jihad in America to be "physical" and not merely "media jihad."[15] A second man, Walli Mujahidh (a.k.a. Frederick Domingue Jr.), also a black convert, was arrested after he traveled to Seattle on a bus from Los Angeles. It was apparently the first time the men had met in person. Abdul-Latif's *YouTube* account (*akabdullatif*) included videos of himself preaching and giving advice on Islam. His account had only

a couple of thousand views, but a search of his *Facebook* and *YouTube* accounts turned up first-degree connections to a dozen sites related to Anwar al-Awlaki's Western-based supporters and the *al-Muhajiroun YouTube* proselytizing network.[16] A third man who agreed to become an informer alerted the police to the conspiracy. The investigation was initiated on June 2, 2011, only twenty days prior to the arrests.

We caution that it is premature to conclude that online self-radicalization was involved in those cases. Radicalization involves a prolonged and gradual descent into an alternative world. Terrorist action rarely occurs without some personal contact with extremist facilitators. A perpetrator may say "the video made me do it" when in fact it was no more than a catalyst for actions for which the person was primed by others. Neighbors, prison radicalization, and family members may be powerful influences. Nonetheless, it is becoming apparent that the expansion of online proselytizing means that much of that process occurs through virtual communities outside the reach of traditional counter-terrorism prevention strategies.

The Communication of Threats

Jihadists are quick to describe their propaganda and barely veiled (or unveiled) incitement to violence as a free speech right. The First Amendment does not protect speech acts involving imminent threats but preventive removal of online content rarely meets the legal standard for "imminent." The key question is often whether the speech act under consideration, however offensive it might be, is criminal. An ongoing instance is a prosecution in connection with online threats against an episode of *South Park*, a cartoon show on Comedy Central. On May 13, 2011, the U.S. government filed an indictment against Jesse Curtis Morton (a.k.a. Younus Abdullah Mohammad) on charges of communicating threats. Morton was arrested in Morocco.

Morton's indictment followed the prosecution of Zachary Adam Chesser (a.k.a. Abu Talhah al-Amrikee), who pleaded guilty in October 2010 to posting threats and to providing material support to al-Shabaab, an *Al-Qaeda* affiliate in Somalia. The threats were posted on *RevolutionMuslim.com* and a number of other websites including the *al-Qimmah Forum*, which is the official forum of al-Shabaab.[17]

Morton created *RevolutionMuslim.com* in collaboration with Joseph Cohen (a.k.a. Yousef al-Khattab) in late 2007 after splitting from an older group, The Islamic Thinkers Society. The latter was created in Queens, New York, in 1998 as a branch of the British *al-Muhajiroun*. It still exists and mainly carries out proselytizing from *dawah* (mission) stalls in Times Square. When Cohen split from the group in late 2009, Morton and Chesser started to run the *Revolution Muslim* website together. They allegedly met in person only once.[18] The Morton indictment alleges that Chesser expressed hope that his campaign against *South Park* would mobilize Muslims in the US the same way the *fatwa* (ruling on a matter of Islamic religious law) against Salman Rushdie in retribution for his book, *Satanic Verses,* had galvanized British Muslims.[19]

After Chesser was arrested in July 2010, and after Morton disappeared, Britons took over the management of *RevolutionMuslim.com*. On November 3, a *fatwa* with a "hit list" of UK parliamentary members who voted for the war in Iraq was posted on the website. [20] The posting cites a *hadith* stating: "Whoever dies and has not fought or intended to fight [Jihad in the path of God] has died on a branch of hypocrisy," and called on the faithful to "raise the knife of jihad" against the MPs. The locations and hours of constituency open-house of the parliamentarians were listed together with a picture of a large knife and a link telling readers where to obtain one. The website was taken down following requests from the British authorities.[21]

Bilal Zaheer Ahmad, a 23-years old man from Wolverhampton in the United Kingdom who posted the hit list, was arrested and pleaded guilty to soliciting murder.[22] Ahmad is also held responsible for an Internet posting from May 2010, which was cited as an inspiration by Roshonara Choudhry, a 21-year old Briton who stabbed and nearly killed a Member of Parliament, Stephen Timms. Choudhry also cited as her inspiration videos featuring Anwar al-Awlaki that circulated on *YouTube* channels linked to *al-Muhajiroun*. The videos have now been removed. The incident bounced back and forth in the online echo chamber created by the jihadist proselytizing sites. After the attack, Choudhry was praised as a heroine on *RevolutionMuslim.com* and hailed as a victim of government suppression after she was convicted.

In January 2011, another self-styled *fatwa* targeted the UK Home Secretary, Theresa May. It was also printed as mocked-up "Wanted" posters plastered up overnight in Tooting, South London.[23] There was little doubt about the paternity of the May *fatwa*. In an interview given just days earlier, Anjem Choudary, the leader of the present incarnation of *al-Muhajiroun*, anticipated the message to come: "I can envisage people issuing *fatwas* against people like Theresa May and David Cameron."[24]

Online Recruitment and the Broadcasting of Extremist Propaganda

The *Shariah4* online network generated a string of national spinoffs in the past year, most of which use domains that are hosted by American companies, and which offer IP addresses outside the jurisdiction of the European authorities. It started organizing events through social networking platforms. More often than not, demonstrations have been announced and then canceled in the last minute. Anjem Choudary took his *Shariah4* brand to the United States, under the banner of *Shariah4America*, and announced a demonstration in front of the White House to take place on March 3, 2011 (the anniversary of the abolition of the Caliphate in 1924). No demonstration was held but Choudary was invited onto both CNN and Fox News as a result of his American campaign.[25] On March 29, *Muslims Against Crusaders* posted a new *fatwa* entitled "Muslims to Disrupt Royal Wedding." The post threatened a "nightmare" on the April 29, 2011, the day of the royal wedding of Prince William should the British military not withdraw from Muslim lands. It featured a live countdown of days, minutes, and seconds to the wedding day. The police did not permit the demonstration.

In April 2011, a new French offshoot called *Jamaat Tawheed* posted an online invitation in halting French to Choudary and two other leaders in the *al-Muhajiroun*-inspired network to attend a demonstration in Paris against the French ban on the public wearing of the *niqab* (face veil). The two other *emirs* invited were Abu Izzadeen (Trevor Brooks), a Briton, and Abu Imran (Fouad Belkacem), the leader of the Choudary-linked Belgian group *Shariah4Belgium*.[26] In this case the plans for a demonstration went ahead but Belkacem was arrested by the French police on a warrant from the Moroccan authorities. He was returned to Belgium where he is awaiting trial on charges of communicating threats. Choudary was turned back and permanently banned from French territory. The Belgian prosecutor has also charged Choudary, along with Belkacem, with hate speech.[27]

RevolutionMuslim.com was originally registered in December 2007 with GoDaddy, an American hosting service, and later made the rounds of other hosting companies. The Theresa May fatwa was posted on an American-based website (theresamayfatwa.com) registered with *Dynadot*.com. The *Shariah4* website domains are often also registered with *Dynadot*.com. The same server has hosted the *Muslim Against Crusades* website.[28] *Jamaat Tawheed's* website, where a call was posted to join the *niqab* ban protests in France, was also hosted by *Dynadot*. AnjemChoudary.com was previously hosted by *Dynadot*.com but is today hosted by a Canadian server and has an IP address in Montreal. Another channel, German Dawa FFM, which has numerous online aliases, has an IP address listed in Orem, Utah.[29]

Methodology and Findings

Our thesis is that *YouTube* proselytizing accounts linked to the jihadist-inspired online groups constitute an integrated and centrally directed network. Although the *Shariah4* channels and the other channels in the jihadist media network are presented as independent set-ups, created by like-minded but unaffiliated administrators, we suspect that they are part of the same operation, and are designed to make removals by the *YouTube* administrators or government officials ineffective.

To test our hypotheses we subjected the channels and their subscribers to social network analysis. A chief advantage of this methodology is that information about communication points can be coded in a formalized manner and subjected to statistical analysis. We created two datasets, one consisting of jihadist channels, and a second dataset made up of *YouTube* channels linked to the Texas *Tea Party* movement. To avoid biasing our results, the channels were selected based upon name resemblances to the aliases used by *al-Muhajiroun* and the group's leaders. The *Tea Party* data serves

as a case-control. By comparing the channels propagandizing jihadism to the online activism of another political movement, we are able to test the null-hypothesis that the jihadist-inspired network is *not* centrally managed. The Texas *Tea Party* nodes were selected as a comparison because the postings represent political online activism and in this regard have a superficial resemblance to the online jihadists. We can reasonably assume that their postings are not centrally directed, and the channel owners have no reason to evade anti-terrorism laws.

All but seven of the 41 channels we identified as *Al-Qaeda*-inspired account holders with some name resemblance to the know aliases of the *al-Muhajiroun* clan were created between September 2010 and March 2011, when we finished compiling the data (listed in Table 1). Of these, twenty-one were created between December 2010 and March 2011. Three were taken down, all in February 2011, after complaints were made about the content to the hosting service. The rest was still active when we stopped collecting information. The two oldest channels are vehicles for Anjem Choudary and *Izharudeen,* a website created by Omar Bakri Muhammad. Four of the channels selected had no available subscriber information, either because they did not have any subscribers or because they did not disclose the information, and were therefore not used in the analysis.

Table 1. Jihadist *YouTube* Channels Used in Network Analysis

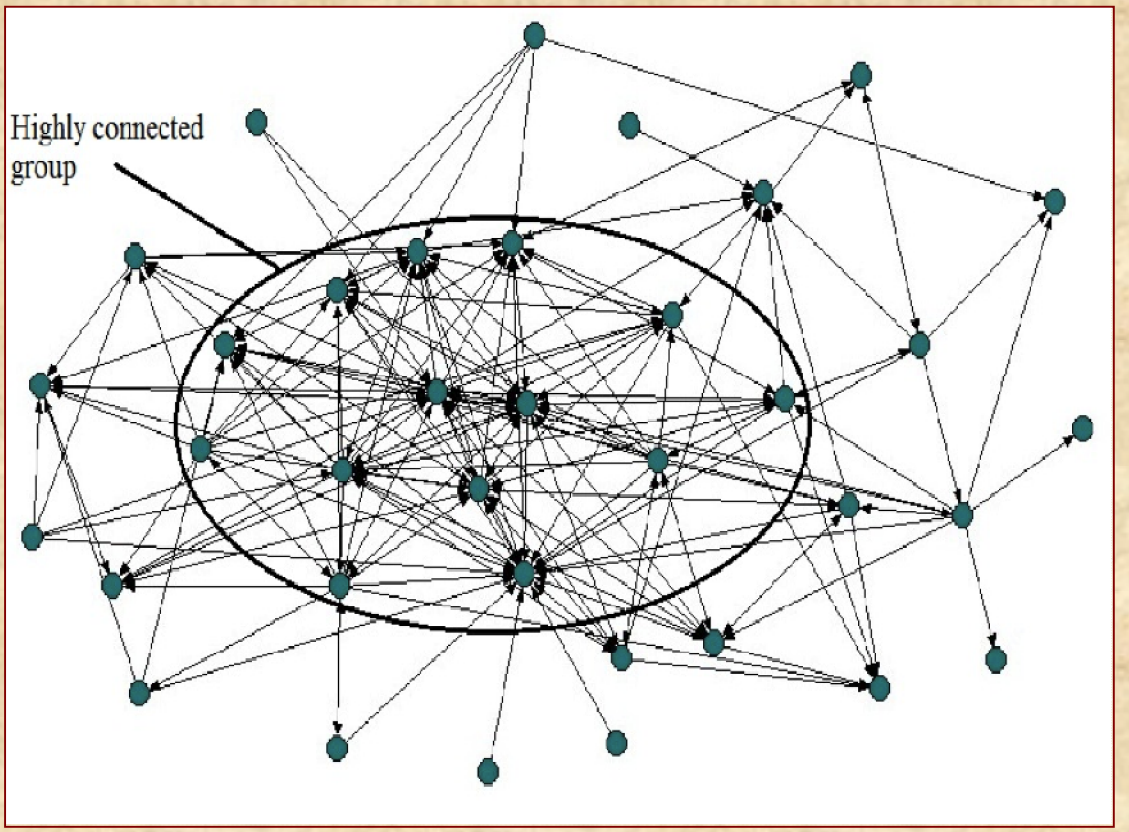
Account	Creation	Terminated	Date Data Compiled
Sharia4Belgium	2/9/10	2/9/11	11/22/2010; 2/9/11
ShariahMedia	2/4/11	Active	3/14/11
ShariahforBelgium	2/13/11	Active	3/14/11
ShariahChannel	2/10/11	2/25/11	2/11/11
ShariahTube	2/22/11	Active	3/14/11
Sharia4Yemen*	2/3/11	Active	3/14/11
GlobalSharia	3/9/10	Active	3/14/11
ShariahForEarth	1/8/10	Active	3/14/11
GlobalShariahGroups*	1/4/11	Active	3/14/11
Sharia4Egypt	2/1/11	Active	3/14/11
Sharia4NewMexico	2/3/11	Active	3/14/11
Sharia4America	10/28/10	Active	3/14/11
Sharia4Nebraska	1/4/11	Active	3/14/11
Sharia4WVirginia	1/5/11	Active	3/14/11
ShariaForKentucky	1/2/11	Active	3/14/11
Shariah4Holland	12/13/10	Active	3/14/11
Shariah4Australia	10/19/10	2/9/11	1/25/11
Sharia4Australia	2/13/11	Active	3/14/11
Shariah4Poland	12/19/10	Active	3/14/11
Sharia4Indonesia	9/12/10	Active	3/14/11
Shariah4Pakistan	12/1/10	Active	3/14/11
Shariah4UK	1/26/11	Active	3/14/11
Sharia4AlAndalus	2/16/11	Active	3/14/11
Shariah4Tunisia	1/22/11	Active	3/14/11
Shariah4TheVatican	1/18/11	Active	3/14/11
Shariah4Bangladesh	11/8/10	Active	3/14/11
Izharudeen	1/29/08	Active	3/15/11
Izzharudeen	N/A	N/A	3/15/11
Izhrudeen*	9/10/08	Active	3/15/11
Islam4UK*	5/11/08	Active	3/15/11
Islam4USA	N/A	N/A	3/15/11
MuslimsAgnstCrusades	N/A	N/A	3/15/11
MuslimsVsCrusades	1/18/11	Active	3/15/11
MuslimsAgstCrusaders	11/16/10	Active	3/15/11
IslamPolicy	1/5/11	Active	3/15/11
AlMuhajiroun	8/31/09	Active	3/15/11
SheikhOmarBakri	5/15/10	Active	3/15/11
AnjemChoudary	10/30/08	Active	3/15/11
Islamicthinkers	2/28/09	Active	3/15/11
IbrahimSiddiqConlon	10/26/10	Active	3/15/11
Londondawah	8/26/07	Active	3/15/11

* Channels with no subscriber information

The data on subscribers - other *YouTube* channels that sign up to follow a particular channel - is best suited to an analysis of the interconnections between related channels. This is because a subscriber actively seeks a connection with the channels it follows, and hence presupposes a willingness to interact. *YouTube* channels can also have "friends", but unlike subscribers, account holders need not approve "friends." A third category is subscriptions—the other channels an account holder has signed up to—but privacy settings allow channel administrators to keep such information offline. Our analysis is restricted to the relationships between the *Shariah4* channels and their channel subscribers. Including "friends" in the study might have reinforced our conclusions but proved unmanageable in terms of size.

Using a "snowball" method, we coded a first wave of subscribers to the original "starter" channels and then a second wave of subscribers' subscribers. For the purpose of social network analysis, the channels and accounts are "nodes" and subscriber links between them are "edges". The sampling method produced a jihadist-inspired dataset of over 41,000 accounts and 76,000 subscriptions. The set was too large for effective social network analysis. The solution was to remove all the subscribers with just one connection to the network, which produced 37 starting nodes with a total of 9,331 nodes and 43,576 edges (links). Chart 1 shows the subscriber links between the starting nodes in the jihadist *YouTube* dataset. Arrows indicate the direction of information flowing from "uploader" channels to subscribers downloading material.

Chart 1. Diagram of Subscriber Links between the Starting Nodes in the Jihadist



***YouTube* Dataset**

For the *Tea Party* network, our control dataset, we also removed all subscribers with just one connection. This left six starting nodes (listed in table 2) and a total of 6,480 nodes with 16,159 edges.

Table 2. Texas *Tea Party* Channels Used as Control Case in Network Analysis

Account	Creation	Terminated	Date Compiled
sateaparty	3/25/09	Active	3/23/11
hlteaparty	9/5/09	Active	3/23/11
WacoTeaParty	4/5/09	Active	3/23/11
rgvtpweb	8/29/09	Active	3/23/11
lonestarteaparty1	4/16/10	Active	3/23/11
dallasteaparty	4/15/09	Active	3/23/11

Using likenesses of known *al-Muhajiroun* incarnations as a selection criterion netted channels that perhaps did not belong in the clan. One account holder noted on his profile, in capital lettering, "Attention: this is not RevolutionMuslim's site (a prominent member of the *al-Muhajiroun* clan), [..] so spamming my channel will not help you get at them." The branding is not always transparent, and we probably missed channels in the empire in our first wave sampling. Our intuitive selection did not detect some of the most prolific *YouTube* channels in the network, which entered the study in the second-wave of data sampling of subscribers. This is a good thing, methodologically speaking. We did not inadvertently bias the study by sampling "on the dependent variable"; starting by selecting the channels most likely to support our argument. The second wave subscriber accounts also included some with no jihadist content. We identified a number of bot channels ("zombies") presumably designed to function as "listening" devices, one of which was our own, as well as channels that we guessed belonged to non-adherents, e.g. an account belonging to *TheKuffarKid*.[30]

The number of subscribers to the starting nodes ranged from only three (*Sharia4Egypt*) to 525 at the high end (*Izharudeen*). The average was 93.22 subscribers per starting node. The top-viewed videos were watched between thirty and forty thousand times, but as viewers can watch the same video many times the statistic does not tell us anything about the number of unique viewers. Overall, these are not impressive numbers for *YouTube*

videos. A sermon about why Michael Jackson should become a Muslim by a South African preacher whom we identified as one of the second-wave subscribers had over eighty thousand viewings.

Different algorithms are used to measure various properties of networks: the probability that by chance a particular pattern of subscribers relations would occur, the hierarchy (or lack thereof), density, and structural duplication or redundancy. Hierarchy indicates the difference, at the extremes, between a network clustering around a central "celebrity" channel (e.g. Lady Gaga telling her fans how fabulous she is but uninterested in the non-fabulousness of her fans) and one that is "flat" because channels repost content through mutual subscriptions. Density is a measure of integration and an indication of coordination. Structural duplication suggests the existence of a planned architecture.

a. Probability:

In the case of channel subscribers, a subscription by channel B to channel A is an outward directed edge from A to B, representing the flow of information from A to B. We tested our assumption that the *Shariah4* channels and the other *Al-Qaeda*-inspired channels have many mutual subscriptions in order to make them resilient against disruption. This was accomplished by comparing the actual number of out-degree edges within the starting node group to the number of edges we would find by chance by taking a random sample of the same size from the entire network. In fact, the nodes in the jihadist network have indeed far more outward-directed relationships amongst each other (an average of 212) than one would statistically expect by chance (8.74). It is highly unlikely that this large number of cross-subscriptions could be obtained by chance (>.0000). In contrast, the starting channels in *Tea Party* network do not subscribe to each other at all. This outcome was less than what one might expect by chance, that half of the channels would subscribe to another channel.

b. Hierarchy:

Degree centrality is a count of the number of edges connecting a node to another node. It measures popularity by rank-ordering nodes in term of the number of subscribers. The single most popular channel was *Izharudeen*, a vehicle for Omar Bakri Muhammad and *Muslims Against Crusades*. No single node stands out as controlling the network but each of them has a medium-high number of connections. None of the jihadist starter channels were on the top ten list of nodes based upon popularity. The most popular channel in the relatively flat landscape of the jihadist network was *ShiismRevealed*, which entered our study as a second-wave channel subscriber to the *al-Muhajiroun* channels. In contrast, a celebrity "uploader" channel (*DontBeObamaZombies*) dominated the *Tea Party* network with 3.5 times the number of subscribers of the second most popular channel in the network.

Betweenness centrality measures the number of nodes that a particular node is connecting through indirect links. It is a so-called "shortest path" analysis, which identifies the gatekeepers in a network. Rather than rank-ordering nodes by the number of links, it is a measure of the degree to which a starting node controls the dissemination of content through strategic placement in the network. The higher the betweenness centrality the greater the number of unique "shortest paths" pass through the node. If our thesis that the jihadist-inspired starting nodes are duplicates is correct, we would expect the key nodes to have relatively low betweenness centrality scores compared to the *Tea Party*. The normalized (weighted) network scores were relatively similar -- .00139 for the *Tea Party* network and .00126 for the jihadist-inspired network. However, the normalized betweenness score for the starting nodes in the *Tea Party* network was on average more than two and a half times higher (.06544) than that of the jihadist-inspired network (.02499). The controlling nodes in the *Tea Party* network are individually more important to the flow of information through the network.

The finding that the betweenness centrality values are relatively low for the starting nodes in the jihadist-inspired network and the concomitant findings that multiple medium-sized channels form a core in the network and a consistent pattern of redundant reposting by means of mutual subscriptions are consistent with our expectation that the network is designed to be resistant to disruption by turning the nodes into redundant bullhorns for proselytizing. This suggests that the *Al-Qaeda*-inspired

channels' owners have a high degree of coordination, which is consistent with the hypothesis that they form a single organization.

c. Density:

A *k-core* is a sub-network (cluster) in a network where all of the nodes are connected to k number other nodes within the cluster. The letter *k* here indicates the unknown value. This enables us to compare groups within the network with respect to density and the degree of integration. We can measure how many nodes in a network belong to a cluster and by how many threads. *K*-core values measure how many connections a member has to other nodes in the sub-network and enables us to compare groups with respect to density and degree of integration. A 5-core group, for example, is a cluster where all the members have ties to at least five other members. Relaxing the criteria to 4 ties (4 core) adds more members but also makes the cluster less dense. If the hypothesis is correct we expect the starting nodes in the jihadism-inspired network to be in high *k*-value core clusters indicative of an anticipated need to resist disruption.

We found that 18 of the starting nodes in the jihadist-inspired network belonged to highly integrated sub-networks where each node had 20 or more subscriber ties to other members. Most of the network had at least two or three ties to other nodes. 4,033 (out of over 9,000) had at least two links to other subscribers (2-core). 2/3 of the network had at least double or triple subscriptions. Only 7 of the starting nodes in the jihadism-inspired network belonged to sub-networks with a *k*-value below 10.

In contrast, the *Tea Party* network had two sub-networks of over 2,000 people comprising the majority of the network but with low *k*-values. Only two of the starting nodes were members of a core with a *k*-value equal to or above 10. The clear difference supports our hypothesis that the jihadist-inspired network is pooled and highly interlinked. The *Tea Party* network in contrast is hierarchical, a pattern consistent with a lack of collusion or little concern over the consequences of a starting node being taking down.

d. Redundancy:

Structural equivalence is a measure of how similar the nodes in a network are to each other. If two nodes are structurally the same they are likely to fulfill similar roles in the network so the measure can be used to test for channel redundancy in the network. Strictly, two nodes should have identical lists of subscribers to be structurally similar, but a more relaxed definition compares nodes based upon their patterns of connections. We found that only 9 of the 37 jihadist starting nodes did not share a structurally similar cluster with at least one other starting node in our initial sample of channels. 13 of the 17 clusters in the jihadist-inspired network of more than 9.000 nodes were "fed" by one of the 37 starting nodes. This means that the majority of the *Al-Qaeda*-inspired channels could be replaced by at least one other node in the network. In contrast, the *Tea Party* starting nodes did not have a single cluster of structurally similar node configurations.

A real-life test of our thesis that the architecture of the jihadist *YouTube* network is designed to resist occurred in mid-September 2011 when hackers took down one of the channels (*westlondondawah*) run by the *al-Muhajiroun* media production outfit, SalafiMedia. (The channels were included in this study as part of the second-wave data collection.) The content was immediately uploaded on a previous idle *YouTube* channel (*salafimediaHD*). Over ten hours, 34 videos were re-uploaded to the reserve channel. In quick time, the entire archive from the hacked channel was transferred. In less than a month thousands of hours of videos were uploaded; two-thirds of the content transferred during the first ten days after the *westlondondawah* channel was hacked.[31]

Conclusion

Our findings are consistent with the hypothesis that *al-Muhajiroun* is the single organizing entity behind a network of related *YouTube* media channels. Redundancy is one of the critical features of the network and indicative of a coordinated effort to build an online proselytizing network resistant to disruption. The reliance on US-based hosting companies adds a legal barrier to British counter-terrorism efforts against the group.

Initial enthusiasm for using social network analysis (SNA) to detect patterns of clandestine coordination between *Al-Qaeda*-inspired groups gave way in recent years to disappointment for a

number of reasons.[32] Open source information with sufficient detail about relationships in large-scale networks is rarely available. When information is available, statistical testing may not be possible for lack of random sampling or an appropriate control sample. In consequence, studies using social network analysis are either highly theoretical or use the methodology for heuristic purposes.

Our study illustrates the utility of network analysis as a diagnostic tool when dealing with proselytizing for terrorism on social media platforms. SNA can be used to map communication structures and provide an intuitive understanding of different types of communication network. Quantitative analysis can be used to back up analysis. The SNA metrics also proved efficient in our study for the purpose of differentiating between *al-Muhajiroun*-related channels and seemingly similar jihadist propaganda channels, which nonetheless proved to be stand-alone platforms with a partly overlapping audience. Among the downsides are that data collection can be time-consuming. The Boolean logic of network analysis is demanding of the software. It proved impossible, for example, to analyze "friends" who ideally should have been included to obtain a full picture of the communication structures of the networks studied.

The study highlights the dilemmas faced by enforcement agencies hoping to stem the tide of terrorist propaganda online. The massive number of sites threatens to overload investigators. Removing illegal or offensive material can be like hacking kudzu weeds. A video with a sermon by Anwar al-Awlaki, "The Dust Will Never Settle", is still easily found by surfing the channels included in this study despite having been a target for removal by the British and U.S. governments and *YouTube* administrators. On the other hand, the public platforms offer advantages. Users often assume that social media platforms enable them to obscure their identity and circumvent restrictions on permissible speech but this is only partially true. Material posted on social media sites is not private and not subject to privacy protections, and therefore the identity of the author (or authors) public information. Moreover, while postings by Britons and other foreigners on US-owned sites are protected under US law, the speakers are subject to sanctions in their country of residence. Jurisdiction-shopping will in such cases protect the speech but not the speaker.

Postscript November 2011

British Home Secretary Theresa May ordered a ban on *Muslims Against Crusades* (or MAC), starting midnight November 11, 2011. The primary website, *www.muslimsagainstcrusades.com*, is no longer available. A *Twitter* account by the same name was also taken offline. At the time of this writing, aliases of the now banned incarnation of *al-Muhajiroun* nonetheless continue to operate on *YouTube*, including *MuslimsAgstCrusaders* and *MuslimsvsCrusades*. The Home Office ban was a response to the group's announcement of demonstrations in connection with Armistice Day celebrations in London but provided nonetheless a real-life test of our conclusions regarding the resilience of the social media propaganda networks against disruption. Barely three weeks after the ban, Anjem Choudary began redirecting followers to a new website and an interlinked network of *YouTube* channels using variants of *OneUmmah* and *UnitedUmmah*. In the meantime, MAC's foreign affiliates filled the gap left by the banned sites.

In separate developments, on November 20, 2011, an indictment was filed in Manhattan criminal court against Jose Pimentel, who is accused of producing pipe bombs and seeking to blow up targets in New York City. Pimentel maintained a website named *trueislam1.com* and a *YouTube* channel under the name of *mujahidfisibillilah1*. When Pimentel's online aliases were made public we identified him as a subscriber to nine of the starting nodes in the *al-Muhajiroun*-related data set used in this study; *Sharia4Nebraska, ShariaTube, Shariah4Earth, SheikhOmarBakri, Shariah4Bangladesh, ShariahMedia, Shariah4Pakistan, IslamicThinkers* and *GlobalShariah.* In addition, Pimentel was "friends" with five of the starting nodes in the study; *SheikhOmarBakri, Shariah4Nebraska, Shariah4Earth, ShariahMedia,* and *Shariah4Pakistan*. His channel showed up a whopping 1,030 times in the snowball analysis.

The growth of cyber jihadism does not mean that the risk of attacks has similarly increased. The types of actions and the sources of recruitment to terrorist actions may change but it is too early to say with certainty. Only two

conclusions can safely be made; first, Internet-based technologies have become an important activity for the contemporary Western-based *Al-Qaeda*-inspired movement and, second, would-be terrorists who are active on the Internet stand a good chance of getting arrested or have their plans disrupted.

Notes:

[1] Amici Curiae filed in the United States District Court for the Northern District of California, San Francisco Division, Case no. CV08-0824 JSW February 29, 2008, available at the website of The Reporters Committee for Freedom of the Press, http://www.rcfp.org/news/documents/20080229-amicusbrie.pdf, last accessed July 2, 2011.

[2] Egan Orion, "Judge reverses Wikileaks injunction." *The Inquirer,* March 2 2008, available at http://www.theinquirer.net/inquirer/news/1039527/judge-rethinks-wikileaks#ixzz1Pjh06B2b, last accessed July 2, 2011.

[3] Dynadot Service Agreement, Version 3.5.15, Effective May 31, 2011. Available at http://www.Dynadot.com/registration_agreement.html, last accessed July 2, 2011.

[4] Statistics available at http://www.checkfacebook.com/, last accessed November 29, 2011.

[5] The quotes are from AnjemChoudary: https://twitter.com/#!/anjemchoudary.

[6] The Racial and Religious Hatred Act of 2006 amended the Public Order Act of 1986 by adding Part 3A, which prohibits "a person who uses threatening words or behavior, or displays any written material which is threatening, is guilty of an offence if he intends thereby to stir up religious hatred." A year and a half later, the Serious Crime Act of 2007 legislation passed, replacing the British common law crime of incitement with a statutory offense of encouraging or assisting crime.

[7] Brian Flynn, "Mall Qaeda." *The Sun*, Oct 30 2009, available at http://www.thesun.co.uk/sol/homepage/news/2705919/Preacher-demands-Buckingham-Palace-be-turned-into-a-mosque.html, last accessed July 2 2011.

[8] This video first appeared on Anjem Choudary's website, http://www.anjemchoudary.com/, on March 28, 2010 and uploaded to the *Shariah4*Belgium YouTube page on September 1, 2010. For more in the video see: *Sharia4*belgium, "A message supporting brothers of *Shariah4*Belgium from UK," *YouTube,* September 1, 2010.

[9] "Americans Self-Radicalized, recruited," UPI.com, May 25, 2011, available at http://www.upi.com/Top_News/US/2011/05/25/Americans-self-radicalized-recruited/UPI-19961306368303/, last accessed July 2, 2011.

[10] Internet Haganah (13 December 2010), available at http://internet-haganah.com/harchives/007103.html, last accessed July 2, 2011; Sofir Blog (18 December, 2010), available at http://www.sofir.org/sofir/blog.php, last accessed July 2, 2011.

[11] Souad Mekhennet, "Frankfurt Attack Mystifies Suspect's Family," *The New York Times,* March 8, 2011, available at http://www.nytimes.com/2011/03/09/world/europe/09frankfurt.html, last accessed July 2, 2011; "Flughafenattentat: Angebliches Vergewaltigungsvideo war Filmszene," *Themen Portal*, March 9, 2011, available at http://www.themenportal.de/nachrichten/flughafenattentat-angebliches-vergewaltigungsvideo-war-filmszene-87983, last accessed July 2, 2011; Rusty Shackleford, "Confirmed: German Jihadi Motivated by "Redacted" Movie Clip on YouTube Being Passed Around by Islamists as "Documentary" Evidence of US War Crimes," Jawa Report, March 11, 2011, available at http://mypetjawa.mu.nu/archives/206757.php, last accessed July 2, 2011.

[12] *Shariah4Andalus* uploaded the "American Soldiers Rape our Sisters! Awakwe oh Ummah!" on February 25 and *Shariah4Holland* uploaded it on February 25 and 26. The last upload was still available on March 11 when we found it. The video is no longer available on YouTube.

[13] Matthias Bartsch and Holger Stark, "Islamism and the Like Button: Can Radicalization Via Facebook Be Stopped?", *Der Spiegel,* March 15, 2011, available at: http://www.spiegel.de/international/germany/0,1518,750912,00.html, last accessed July 2, 2011.

[14] Samir Khan, an American Internet jihadist who was web master for the Yemen-based *Al-Qaeda*-affiliated Anwar al-Awlaki, was *Facebook* friend with both Uka and al-Abdaly, see *Internet Haganah*, December 13, 2010, available at http://internet-haganah.com/harchives/007103.html, last accessed July 2, 2011. Khan was killed in a drone attack in Yemen on September 30, 2011.

[15] Levi Pulkkinen and Scott Gutierrez, "Seattle man implicated in plot to blow up military recruiting station," *SeattlePI*, June 23, 2011, available at http://www.seattlepi.com/local/article/Seattle-man-implicated-in-plot-to-blow-up-1437405.php#ixzz1QVccLSxR, last accessed July 2, 2011; United States v. Abdul-Latif, et al., Criminal Complaint, available at http://www.atf.gov/press/releases/2011/06/062311-abdul-latif-complaint.pdf, last accessed July 5, 2011.

[16] *Internet Haganah*, (25 June, 2011), available at: http://Internet-haganah.com/harchives/007379.html, last accessed July 2, 2011.

[17] Author interview with Zachary Adam Chesser on June 29, 2010, available at http://azelin.files.wordpress.com/2010/07/interview-with-abu-tale1b8a5ah-al-amriki.pdf; last accessed July 2, 2011.

[18] United States of America v. Zachary Adam Chesser in the United States District Court for the Eastern District of Virginia. Statement of Fact filed October 20, 2010, available at http://s88179113.onlinehome.us/2010-10-27/USA_v_Chesser-Statement_of_Facts.pdf, last accessed July 2, 2011
[19] United States of America v. Jesse Curtis Morton in the United States District Court for the Eastern District of Virginia. Affidavit filed May 13, 2011, available at:
http://www.investigativeproject.org/documents/case_docs/1561.pdf, last accessed July 2, 2011.
[20] Bilal, "MPs That Voted for War on Iraq," *Revolution Muslim*, November 3, 2010, no longer available at http://www.revolutionmuslim.com/2010/11/mps-that-voted-for-war-on-iraq.html, (copy may be obtained from the authors); Aaron Y. Zelin, "Revolution Muslim: Downfall or Respite?" *CTC Sentinel*, 3:11/12, (2010).
[21] "Extremist Website Urges Muslims to Track Down MPs," *The Times* (U.K.), November 5, 2010, available at http://www.thetimes.co.uk/tto/news/politics/article2795909.ece; last accessed July 2, 2011.
[22] Edward Chadwick, "Wolverhampton man called on Muslims to attack MPs who voted for war in Iraq," *The Birmingham Mail,* June 11, 2011, available at http://www.birminghammail.net/news/top-stories/2011/06/11/wolverhampton-man-called-on-muslims-to-attack-mps-who-voted-for-war-in-iraq-97319-28859646/, last accessed July 2, 2011.
[23] The website is: http://theresamayfatwa.com; Gavin Allen, "Fatwa against Theresa May: Scotland Yard investigates Islamic poster campaign targeting Home Secretary," *The Daily Mail,* January 27, 2011, http://www.dailymail.co.uk/news/article-1350993/Fatwa-Theresa-May-Islamic-poster-campaign-launched-Home-Secretary.html, last accessed July 2, 2011.
[24] "Fatwa issued against Home Secretary Teresa May," Demotix, January 26, 2011, available at http://www.demotix.com/news/569014/fatwa-issued-against-home-secretary-teresa-may, last accessed July 2, 2011.
[25] Choudary was on Eliot Spitzer's show on CNN on October 30, 2010, before he launched his US publicity, and again on the Sean Hannity show on FOX on February 2, 2011, after the White House hoax.
[26] The invitation is available here: http://www.jamaat-tawheed.com/INVITATION_OFFICIELLE.pdf; last accessed July 5, 2011.
[27] "Sharia-Prozess in Antwerpen vertagt," *Belgischer Rundfunk,* June 17, 2011, available at http://brf.be/nachrichten/national/226832/, last accessed July 2, 2011.
[28] See http://www.muslimsagainstcrusades.com/.
[29] DawaFFM.de has an IP address listed in Orem, UT, USA.
[30] "Bots" are also known as spiders or crawlers. They are software commands designed to automatically search and retrieve documents and files, and then record the information and links found on the pages.
[31] The new channel carries a message to hackers: "THIS IS AN ARCHIVE WEBSITE - SHOULD SALAFIMEDIA.COM GO DOWN YOU MAY DOWNLOAD ALL OUR MATERIAL FROM HERE- THE TRUTH WILL NEVER DIE AND WE WILL DEPEND ON ALLAH ALONE TO CARRY THESE WORDS SHOULD THEY EVER TRY TO SILENCE US."
[32] Mette Eilstrup-Sangiovanni and Calvert Jones, "Assessing the Dangers of Illicit Networks: Why al-Qaida May be Less Threatening Than Many Think." *International Security* v. 33, no. 2 (Fall) 2008: 7-44.

Jytte Klausen *is the Lawrence A. Wien Professor of International Cooperation at Brandeis University and an Affiliate at the Center for European Studies at Harvard University. She is a Carnegie Scholar. Her most recent book is "The Cartoons That Shook the World" (Yale University Press 2009) about the Danish cartoons of the Prophet Muhammad and the worldwide protests that followed their publication. She is the Principal Investigator of the Western Jihadism Research Project.*
Eliane Tschaen Barbieri *is a Postdoctoral Fellow on the Western Jihadism Research Project. She received her PhD in political science from Brandeis University in 2010. In addition to her research in counterterrorism, she is currently writing a book manuscript on the emergence of hegemons.*
Aaron Reichlin-Melnick*has a B.A. from Brandeis University and has been a research analyst on the Western Jihadism Research Project since 2009.*
Aaron Y. Zelin *has a M.A. in Islamic and Middle Eastern Studies from Brandeis University and is a Research Assistant on the Western Jihadism Research Project. He also maintains the website Jihadology.net, which tracks jihadist primary source material.*

Electromagnetic pulse and American security

By Eric Hannis

Source: http://www.afpc.org/files/february2012.pdf

One of our nation's most glaring national security "Achilles Heels," the threat of an electromagnetic pulse (EMP) incident, has received new attention of late in the popular media as well as the Republican presidential debates. This focus is certainly welcome, but it is far from typical; beyond a small circle of think tanks and policy wonks inside the Washington Beltway, few people even know that this threat exists.

So what is an electromagnetic pulse? An EMP is a burst of electromagnetic radiation that is usually caused by either a very high yield explosion—such as a nuclear detonation – or by a natural solar eruption that periodically emanates from our sun. If the explosion or solar burst is strong enough, the resulting high energy electromagnetic fields can produce electrical voltages so intense that they can destroy electrical components used in everyday items, such as computers and communications equipment, as well as large infrastructure equipment and transformers used in our electric grid.

New salience

The EMP threat has been known for some time. During the Cold War, we were aware that the Soviets maintained an EMP attack plan in their portfolio of nuclear options. Our primary deterrent to such a Soviet EMP attack was the same as for other scenarios at the time: simple nuclear retaliation. We knew

that were this attack to be used, it would likely be only one adversary launching it. It was an effective and logical deterrent.

But in the intervening decades, we have become ever more dependent on our information technologies (IT) and computer-based infrastructure systems, thus making us an even more appealing and likely target for an EMP attack. In addition, since nuclear and missile technologies have spread to even more unpredictable and "rogue" nation states, relying solely on a strategy of nuclear deterrence is increasingly insufficient.

The stakes are grave indeed. One successful high altitude EMP detonation has the capability to disable electronic systems that could result in our population plunging back into the 18th century overnight. While immediate and direct deaths from an EMP detonation would be minimal, associated long term mortality would be very high. Multiple successful detonations above the continental United States could potentially result in the entire nation becoming completely incapable of utilizing any technologies dependent on electricity. Very quickly, our just-in-time and highly efficient infrastructure systems that supply food, energy, and transportation would be rendered inoperable. Hospitals and emergency services could be incapacitated. Water would not flow, vehicles would not run, and food would spoil and go undelivered. The result would be starvation, disease, and lawlessness on a scale not experienced in modern times.

The capability to deliver an EMP attack, moreover, is expanding. Whereas decades ago only a handful of states possessed the capability to create an electromagnetic pulse event, today the associated knowledge has become more diffuse – and the ability to do so more widespread.

Two of the three nations that were named by the Bush administration as members of the "Axis of Evil," North Korea and Iran, are known to be developing capabilities to launch EMP attacks. North Korea is developing several technologies that could allow it to launch an EMP attack.

These include long-range nuclear-capable missile technologies, according to recent testimony to Congress by the Defense Intelligence Agency. Moreover, according to South Korean military officials, North Korea is in the process of finishing the development of a "Super-EMP" nuclear warhead. Although it lacks an ICBM capability, Iran too could cause devastating harm to the U.S. through a ship-launched

EMP attack. The Iranian regime is known to have conducted missile launches off surface vessels in the Caspian Sea – tests that bear a striking resemblance to EMP launch exercises.

But EMP attacks need not be launched directly by an adversary nation-state. Iran, or another rogue state, could use a proxy organization to launch a missile from a freighter in the Atlantic.

Moreover, we also have known for some time that non-state terrorist organizations like al-Qaeda have been urgently trying to acquire nuclear weapons.

However, an attack is not the only way that an EMP event could happen. Many scientists believe there is a strong chance that impending solar eruptions, called "coronal mass ejections" (CME), have the potential to cause the same effects as an EMP detonation on terrestrial systems. In fact, many scientists believe the question is not "if" such storms will occur, but "when." Solar storms of strong magnitude erupt in 11-year cycles, and our sun's solar storm activity is expected to peak in 2013. One of the biggest threats from a CME event is the potential damage it could cause to our electric grid. Power surges caused by solar particles can destroy giant transformers. The costs from the loss of power to our most vulnerable east coast cities for even weeks or months could easily reach the billions of dollars. And even if the CMEs that occur between now and next year do not cause massive disruptions or damage to our electric infrastructures, our continued and increasing reliance on electronic systems means that we will be even more vulnerable during the next 11-year cycle of solar storms.

A lagging response

While we clearly are aware of these current EMP threats, both natural and man-made, what have we done to prepare our nation? The answer, unfortunately, is very little.

The United States first began to seriously address the current EMP threat through the establishment of a formal commission (known as the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack) back in 2001. Following years of study, this blue-ribbon panel produced a thorough analysis of the potential effect of EMP attacks, and provided the government with concrete steps needed to safeguard our nation.

Yet to date, very few of the Commission's recommendations actually have been implemented. In its recommendations, the Commission focused its attention on a quartet of basic steps necessary to prepare for and deter an EMP incident. These include:

Infrastructure hardening

Hardening our infrastructure systems and post-incident planning will allow our most important systems to function after an EMP incident. It will also make us a less appealing target, signaling to hostile nations that they would only be able to hamper us temporarily – and then only at potentially catastrophic retaliatory cost Unfortunately, however, the federal agencies charged with post-incident planning and hardening of our electric grid have failed to move beyond the theory and discussion phase. The Department of Energy (DoE), likewise, has done little to prepare for an EMP incident. While hardening our entire electric grid is unrealistic, DoE could do much to mitigate the effects of an EMP incident by establishing plans, in coordination with industry, on how to most efficiently restore electric power after an EMP incident. Yet it has failed to do much of anything in this regard. This is true even though experts estimate that it would cost in the hundreds of millions of dollars to protect our 300 largest transformers, and less that $1 billion to harden an additional 3,000 smaller transformers – a comparatively small price to pay in order to stem the potential loss of life and destruction of our infrastructure and economy that would result from an EMP attack.

Communicating during an EMP event

The responsibility for developing civilian protocols for command and control in the event of an EMP attack largely falls on the Department of Homeland Security (DHS).

Since its inception in 2001, the EMP Commission has provided many actionable recommendations to DHS in regard to planning and incident response. DHS, however, shows no indication of working to develop solutions to the shortfalls specified in the recommendations. In fact, an EMP threat scenario has not even been included in the DHS's "National Planning Scenarios," its list of the nation's most critical threat scenarios, despite the potentially catastrophic nature of such an event.

Hardening of defense and space systems

Unlike DHS and DoE, the Department of Defense (DoD) has begun to undertake many of the steps recommended by the EMP Commission, particularly the hardening of electronic components used in critical weapon systems. In particular, DoD has been making investments in hardening our strategic weapons systems, such as the nation's nuclear forces.

In addition, it has started to invest in enhancements that provide for electronic hardening during upgrades of existing conventional weapon systems such as bombers and fighter aircraft.
However, these steps are still early ones; much of our conventional force still remains vulnerable to an EMP attack. And the military's increasing use of commercial electronic technologies, which have no hardening characteristics, make vulnerability to EMP an escalating problem.

Defending against EMP and EMP-capable attack

A key component to our EMP defenses is the ability to intercept incoming ballistic missiles. The Commission correctly asserts that a viable missile defense system is our nation's best deterrent to an EMP attack. While neither the Bush nor Obama administrations did enough to harden our infrastructure, the differences on missile defense are starker. During the Bush administration, our Ballistic Missile Defense (BMD) capabilities advanced through several programs with the capability to protect the homeland from an EMP attack (including the Aegis Ballistic Missile Defense System and the Airborne Laser). The Obama administration, by contrast, has done considerably less. Despite unveiling a new four-phase missile defense plan in September 2009, it began to make large cuts to the missile defense budget beginning in FY2010. In addition, the Obama administration has cancelled or delayed the fielding of systems that held much potential to defend against EMP attacks. The DoD's *Ballistic Missile Defense Review Report*, released in early 2010, indicates that the Obama administration is retreating on the fielding of the ground-based midcourse defense (GMD) systems to defend the U.S. and Europe against potential ballistic missile attacks. While the Bush administration planned to field 44 ballistic missile interceptor systems in the U.S. and 10 in Europe, the Obama administration is planning to field just 30 systems in the U.S. and none in Europe.
In addition, the ABL program was cancelled by the Obama Administration back in 2009. Lastly, the Obama administration, via the New START Treaty, has limited our future missile defense options as part of its attempted "reset" of relations with Russia.

Steps toward a solution

Over the last few years, responding to these deficiencies, Congress has fielded several legislative initiatives to address our shortfalls in EMP incident preparation and infrastructure hardening. As of yet, however, no EMP-focused bill has yet been sent to the President for signature.
The so-called SHIELD Act (Secure High-voltage Infrastructure for Electricity from Lethal Damage Act) is one of the better plans currently under consideration. It would amend the Federal Power Act by encouraging cooperation between industry and government to mitigate vulnerabilities in the electric grid and develop solutions to current shortcomings associated with a major EMP event. The SHIELD Act, sponsored by Rep. Trent Franks (R-AZ), calls for the establishment of protection standards and hardware fixes (such as the hardening of large transformers and other key elements of the nation's power infrastructure). Another attribute of the SHIELD Act is that it does not rely solely on government for a solution, but rather depends on a partnership of government and industry to achieve its goals of protecting American electric infrastructure.
If passed, the legislation would eliminate many of our vulnerabilities to an EMP event, whether caused by an attack or by nature. Moreover, the SHIELD Act's bipartisan list of supporters shows that threat of an EMP attack is one of very few issues that unites both Republicans and Democrats in this highly-polarized Congress.

Time to act

Our federal government, through the EMP Commission, has now studied the threat posed by EMP for over a decade. Policymakers in Washington now need to move beyond theory, and into practice.
This means expending the appropriate resources to harden our military and civilian infrastructures. It also requires building the redundancies and communication capabilities that would make it possible for America to weather an EMP event more or less intact. The proposals outlined in the SHIELD Act provide a blueprint for doing so. We now need our federal government and agencies to at long last take the EMP threat seriously, and begin to protect against it. ●

Eric Hannis is Executive Director at Etherton and Associates, a defense consulting firm, as well as a Lt Col in the Air Force reserve. Previously, he was the Military Legislative Assistant to Rep. Randy Forbes, Chairman of the House Armed Services Committee's Readiness Subcommittee.

NATO commander target of persistent Facebook cyberattacks

Source: http://www.homelandsecuritynewswire.com/dr20120313-nato-commander-target-of-persistent-facebook-cyberattacks

The senior commander of NATO has been the target of repeated Facebook-based cyberattacks that are believed to have originated from China.

The Observer reports that Admiral James Stavridis is the subject of a campaign to gain information about him and his colleagues, friends, and family. Hackers have repeatedly tried to dupe those close to Stavridis by setting up fake Facebook accounts in his name in the hope that his acquaintances will make contact and answer private messages, potentially divulging sensitive information about the commander or themselves.

This tactic is known as "social engineering" and is an increasingly common form of cyberattack.

NATO officials are unclear one exactly who is behind the attacks, but believe that China is the likely source.

Attributing cyberattacks with absolute clarity is impossibly difficult, but "the belief is that China is behind this," an anonymous NATO official told the *Observer*.

According to intelligence analysts, the sophistication and determination of the hackers behind these "advanced persistent threat" attacks suggests they are state-sponsored.

In Operation Night Dragon, hackers in China were accused of conducting a similar campaign where they impersonated executives from companies in the United States, Taiwan, and Greece to steal trade secrets.

Stavridis is an active user of social media and maintains a personal account. The commander of NATO as well as all American forces in Europe frequently uses social media to keep the public informed. Most notably, last year he used Facebook to declare the end of the military campaign in Libya.

NATO has been working with Facebook to remove fake pages as soon as they are detected. According to the *Observer*, dummy accounts are usually removed within one to two days of discovery.

An unnamed NATO official said over the last two years "there have been several fake SACUER [Supreme Allied Commander Europe] pages. Facebook has cooperated in taking them down… the most important thing is for Facebook to get rid of them."

NATO has warned its senior officials about the dangers of social engineering online and to defend against this threat it has awarded a $62 million contract to a defense giant to bolster cybersecurity.

New Interest in Hacking as Threat to Security

Source:http://www.nytimes.com/2012/03/14/us/new-interest-in-hacking-as-threat-to-us-security.html?_r=1

During the five-month period between October and February, there were 86 reported attacks on computer systems in the United States that control critical infrastructure, factories and databases, according to the Department of Homeland Security, compared with 11 over the same period a year ago.

None of the attacks caused significant damage, but they were part of a spike in hacking attacks on networks and computers of all kinds over the same period. The department recorded more than 50,000 incidents since October, about 10,000 more than in the same period a year earlier, with an incident defined as any intrusion or attempted intrusion on a computer network.

The increase has prompted a new interest in cybersecurity on Capitol Hill, where lawmakers are being prodded by the Obama administration to advance legislation that could require new standards at facilities where a breach could cause significant casualties or economic damage.

It is not clear whether the higher numbers were due to increased reporting amid a wave of high-profile hacking, including the arrest last week of several members of the group Anonymous, or an actual increase in attacks.

James A. Lewis, a senior fellow and a specialist in computer security issues at the Center for Strategic and International Studies, a policy group in Washington, said that as hacking awareness had increased, attacks had become more common. He said that the attacks on the nation's infrastructure were particularly jarring.

"Some of this is heightened awareness because everyone is babbling about it," he said of the reported rise in computer attacks. "But much of it is because the technology has improved and the hackers have gotten better and people and countries are probing around more like the Russians and Chinese have."

He added: "We hit rock bottom on this in 2010. Then we hit rock bottom in 2011. And we are still at rock bottom. We were vulnerable before and now we're just more vulnerable. You can destroy physical infrastructure with a cyberattack just like you could with a bomb."

The legislation the administration is pressing Congress to pass would give the federal government greater authority to regulate the security used by companies that run the nation's infrastructure. It would give the Homeland Security Department the authority to enforce minimum standards on companies whose service or product would lead to mass casualties, evacuations or major economic damage if crippled by hackers.

The bill the administration backs is sponsored by Senators Joseph I. Lieberman, independent of Connecticut, and Susan Collins, Republican of Maine. It has bipartisan support, and its prospects appear good. Senator John McCain, Republican of Arizona, is sponsoring a more business-friendly bill that emphasizes the sharing of information and has fewer requirements for companies.

Last week on Capitol Hill, Janet Napolitano, the secretary of Homeland Security; Robert S. Mueller III, the director of the Federal Bureau of Investigation; and Gen. Martin E. Dempsey, the chairman of the Joint Chiefs of Staff, made their pitch to roughly four dozen senators about why they should pass the Lieberman-Collins bill.

At a closed-door briefing, the senators were shown how a power company employee could derail the New York City electrical grid by clicking on an e-mail attachment sent by a hacker, and how an attack during a heat wave could have a cascading impact that would lead to deaths and cost the nation billions of dollars.

"I think General Dempsey said it best when he said that prior to 9/11, there were all kinds of information out there that a catastrophic attack was looming," Ms. Napolitano said in an interview. "The information on a cyberattack is at that same frequency and intensity and is bubbling at the same level, and we should not wait for an attack in order to do something."

General Dempsey told the senators that he had skipped a meeting of the National Security Council on Iran to attend the briefing because he was so concerned about a cyberattack, according to a person who had been told details of the meeting. A spokesman for General Dempsey said the chairman had "sent his vice chairman to the meeting on Iran so that he could attend the Senate meeting and emphasize his concern about cybersecurity."

"His point was about his presence at the cyber exercise rather than a value judgment on the 'threat,' " the spokesman, Col. David Lapan, said.

Experts say one of the biggest problems is that no part of the government has complete authority over the issue. The Central Intelligence Agency and the National Security Agency give the government intelligence on potential attacks, and the F.B.I. prosecutes hackers who break the law. The Department of Homeland Security receives reports about security breaches but has no authority to compel business to improve their security.

"Nobody does critical infrastructure of the dot-com space where America now relies on faith healing and snake oil for protection," Mr. Lewis said. "The administration wants it to be the Department of Homeland Security, but the department needs additional authorities to be effective."

Utah's $1.5 billion cyber-security center under way

By Steve Fidel

Source: http://www.deseretnews.com/article/705363940/Utahs-15-billion-cyber-security-center-under-way.html

Thursday's groundbreaking for a $1.5 billion National Security Agency data center is being billed as important in the short term for construction jobs and important in the long term for Utah's reputation as a technology center.

"This will bring 5,000 to 10,000 new jobs during its construction and development phase," Sen. Orrin Hatch, R-Utah, said on Wednesday. "Once completed, it will support 100 to 200 permanent high-paid employees."

Officially named the Utah Data Center, the facility's role in aggregating and verifying dizzying volumes of data for the intelligence community has already earned it the nickname "Spy Center." Its really long moniker is the Community Comprehensive National Cyber-security Initiative Data Center — the first in the nation's intelligence community.

A White House document identifies the Comprehensive National Cyber-security Initiative as addressing "one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter." The document details a number of technology-related countermeasures to the security threat.

Hatch said Utah was chosen for the project over 37 other locations. He characterized the

cyber-security center as the "largest military construction project in recent memory."

Hatch said he promoted Utah's favorable energy costs, Internet infrastructure, thriving software industry and proximity to the Salt Lake City International Airport in the bid process that ended up with Camp Williams earning the data center.

The Army Corps of Engineers is overseeing the project that is under contract to a joint venture between Big-D Construction in Salt Lake City, U.K.-based Balfour Beatty Construction and DPR Construction out of California.

"This project is going to give an opportunity for an awful lot of Utahns" who have seen construction jobs in Utah drop from 100,000 in 2008 to about 66,000 today, said Rob Moore, president and COO of Big-D and chairman of the Associated General Contractors in Utah.

"My subcontractors, suppliers and vendors are very appreciative of the work that will be available on this project."

Grading work is already under way for the complex, which is scheduled to include 100,000 square feet for the data center and 900,000 square feet for technical support and administrative space. The center is designed to be capable of generating all of its own power through backup electrical generators and will have both fuel and water storage. Construction is designed to achieve environmentally significant LEED Silver certification.

"It is so unique and so intensive," Hatch said. "This will establish our state as one of the leading states for technology."

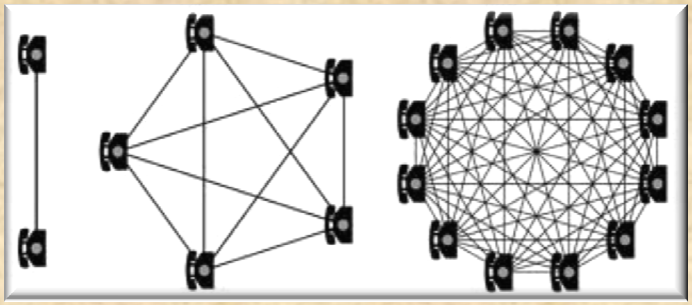
Steve Fidel *is a staff reporter for KSL and the Deseret News and is a former editor of deseretnews.com. He was a news photographer at the Sun Advocate in Price, Utah, and worked as a contributing photographer and reporter for The Associated Press.*

Using people with cell phones as surveillance nodes

Source:http://www.homelandsecuritynewswire.com/dr20120318-using-people-with-cell-phones-as-surveillance-nodes

Eighty-eight percent of Americans now own a cell phone, forming a massive network that offers scientists a wealth of information and an infinite number of new applications. With the help of these phone users — and their devices' cameras, audio recorders, and other features — researchers envision endless possibilities for gathering huge amounts of data, from services that collect user data to monitor noise pollution and air quality to applications that build maps from people's cell phone snapshots.

A Northwestern University release reports that today, user data provides some opportunities; for example, researchers can use Flickr photos to compile 3-D virtual representations of various landmarks. Even opportunities like these have limits, however, as researchers are limited to using only photos that people choose to take and share. This creates a significant imbalance: Some geographic areas and landmarks have thousands of Flickr photos, while others have none.



"Take the Lincoln Memorial, for example," said Fabian Bustamante, associate professor of electrical engineering and computer science at the McCormick School of Engineering. "Flickr has thousands of photos of the front of the Lincoln Memorial. But who takes a picture of the back? Very few people."

This has led researchers to ask the questions: How can we get mobile users to break out of their patterns, visit less frequented areas, and collect the data we need?

Researchers cannot force mobile users to behave in a certain way, but researchers at Northwestern University have found that they may be able to nudge users in the right direction by using incentives that are already part of their regular mobile routine.

"We can rely on good luck to get the data that we need, or we can 'soft control' users with gaming or social network incentives to drive them where we want them," Bustamante said.

In the paper, "Crowd Soft Control: Moving beyond the Opportunistic," Bustamante and his group designed a way to "soft control" people's movements by tapping into games or social networking applications. For example, a game might offer extra points if a player visits a certain location in the real world, or it might send a player to a certain location in a virtual scavenger hunt.

To test crowd soft control, the researchers created Android games, including one called Ghost Hunter in which a player chases ghosts around his neighborhood and "zaps" them through an augmented reality display on his phone. In actuality, the player's zapping motion snaps a photo of the spot where the ghost is supposedly located.

Unlike a regular "augmented reality game," where the ghosts might be placed randomly, in Ghost Hunter the researchers are able to manipulate where the ghosts are placed; while some are placed in frequently traveled areas, others are located in out-of-the-way, rarely photographed locations.

The game was tested on Northwestern students, who were told only that they were testing a new game. They were not informed which ghosts were placed randomly and which were placed for research purposes.

"We wanted to know if we could get the players to go out of their way to get points in the Ghost Hunter game," Bustamante said. "Every time they zapped a ghost, they were taking a photograph of Northwestern's campus. We wanted to see if we could get more varied photographs by 'soft controlling' the players' movements."

The participants were willing to travel well out of their regular paths to capture the ghosts, the researchers found. For example, researchers were able to collect photos of Northwestern's Charles Deering Library from numerous angles and directions — a far broader range of

data than the random sampling found on Flickr, where photographs overwhelmingly capture the front of the library.

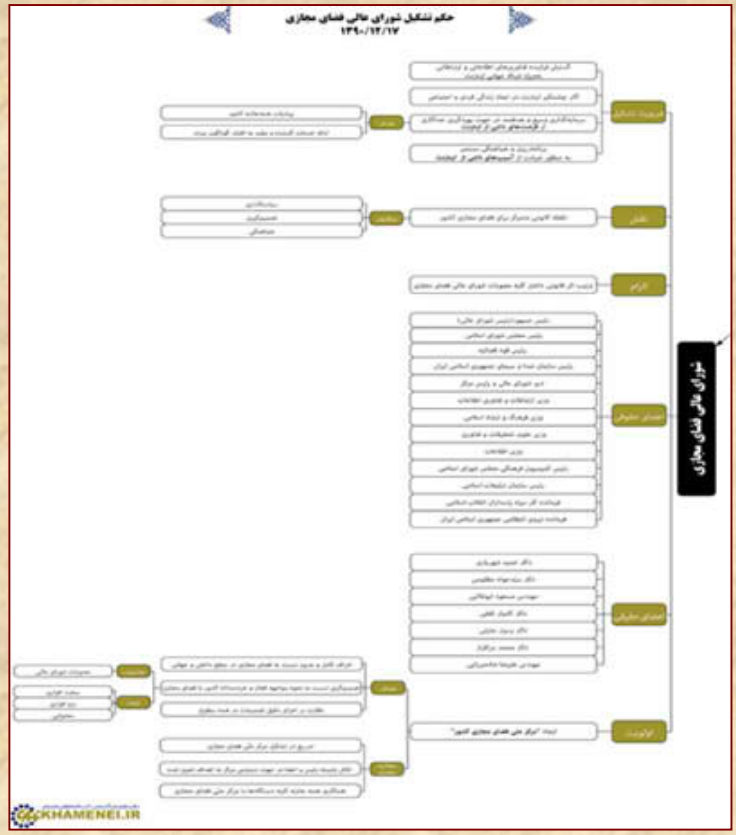
"Playing the game seemed to be a good enough vehicle to get people to go to these places," said John P. Rula, a McCormick graduate student and the lead author of the paper.

If this technology were implemented on a larger scale, users would need to be notified that their data was being collected for research purposes, Bustamante said.

"Obviously users need to know where their data is going," he said, "and we take every measure to protect user privacy."

Cyberspace comes under increasing control: Supreme Leader orders establishment of "Supreme Cyber Council"

Source: http://www.terrorism-info.org.il/malam_multimedia/English/eng_n/html/iran_e161.htm



The Supreme Leader's directive on the establishment of the Supreme Cyber Council, as it appeared on his official website

Last Wednesday, March 7, Supreme Leader Ayatollah Ali Khamenei issued a new directive on the establishment of a "Supreme Cyber Council". The directive says that the decision to establish the council was made in response to the growth of information and telecommunications technology, particularly the global internet network, and its impact on individual and social life. Other factors behind the establishment of the council are the need to facilitate the most effective possible use of the opportunities inherent in technological progress for the advancement of public services, and the need to step up planning and integration of efforts to prevent damage that can be caused by the growing use of cyberspace.

Headed by the president, the council members will include the Majles chairman, the chief of the judiciary, the head of Iran Broadcasting, the ministers of telecommunications, Islamic guidance, intelligence, and science, the chairman of the Majles Culture Committee, the chairman of the Islamic Propagation Organization, the chief of the Revolutionary Guards, the commander of the internal security forces, as well as seven experts on internet and information technology.

The new council has been instructed to promptly establish a "National Cyber Center" to be in charge of all cyber activities in Iran and elsewhere, which includes issues of software, hardware, and internet content. The center will also supervise the implementation of decisions made with regard to these issues. The Supreme Leader instructed all government institutions to cooperate with the new center.

Seyyed Mehdi Khamoushi, chairman of the Islamic Propagation Organization, discussed the need for the establishment of the new council. In an article published on the Supreme Leader's official website, Khamoushi said that Iran's enemies consider the "soft war" and the cultural attack on Iran to be the most important struggle intended to undermine the Islamic revolution. Iran needs to protect its philosophical, religious, and cultural borders, and take advantage of cyberspace to send out its message

to the world and fight against the messages sent by its enemies.

Iran is facing a "tsunami of information", which is why it needs a concerted effort to deliver its messages and deal with the efforts made by its enemies in this field. Iran is also facing a technological progress that can be harnessed to provide more effective social and government services and improve the relationship between the administration and the public.

The chairman of the Islamic Propagation Organization noted that, in recent years, experts, culture figures, clerics, and scientists have communicated their concerns about cyberspace to the Supreme Leader, and that the new council will be tasked with formulating ideas and plans in fields pertaining to the internet and information technology. These ideas will then be presented to the Supreme Leader (www.khamenei.ir, March 8).

Dr. Kamyar Saqafi, who has been appointed to the council, said that cyberspace cannot be the responsibility of just one government ministry, and that it requires coordination between many different bodies. Different models used so far to formulate policies on information technology were insufficient, as the field requires a broader outlook. Saqafi said that the composition of the council shows how important this issue is for the Supreme Leader (Mehr, March 10).

The establishment of the Supreme Cyber Council was widely covered by Iranian media and was even addressed by Ayatollah Ahmad Jannati, the Friday prayer leader in Tehran. Jannati, who serves as chairman of the Guardian Council, said that the establishment of the council is an indication of the attention given by the Supreme Leader to issues others tend to dismiss. Jannati noted that cyberspace makes it possible for secrets to be stolen, and that the internet poses a considerable threat to world nations and is intended to create insecurity in the world (Fars, March 10).

On the margins of the extensive media coverage about the council's establishment, the composition of the council was criticized by an Iranian blogger. In a post made by Ali Pour-Tabataba'i on his personal blog, the blogger said that while in principle he does support the establishment of the council, he has several reservations about its activity and composition, which may, in his view, weaken its ability to solve the severe problems that exist in Iranian cyberspace.

The blogger expressed his concern that the establishment of the council will undermine the Majles' authority and its ability to pass new laws pertaining to cyberspace. He noted that similar councils established in the past, such as the Supreme Council of the Cultural Revolution, saw themselves above all other branches of government and as having powers not subject to any kind of control. For instance, laws passed on the initiative of the Supreme Council of the Cultural Revolution could not be changed even by the Guardian Council or the Expediency Discernment Council.

In addition, the blogger said that the composition of the council will not allow it to be in charge of both content issues and technology issues involving cyberspace. He noted that most council members are engineers or technical experts. The council has no experts on social sciences or humanities, and no senior representative from the religious seminaries who could speak for top clerics and religion students.

The presence of representatives from the Revolutionary Guards, the Ministry of Intelligence, and the internal security forces is similarly problematic, Pour-Tabataba'i said, since it can prompt the council to adopt a "security-oriented approach". Such an approach considers every online activity a conspiracy that has to be combated. If this approach is adopted by the new council, the result may be an escalation of the struggle already waged on "cyberspace activists". This struggle has already provoked dissatisfaction from cyber activists who support the Islamic republic, according to Pour-Tabataba'i.

Finally, the blogger warned that the establishment of the new council will make it even more difficult to solve currently existing problems with cyberspace. Instead of scaling back the agencies involved in the field, the council may become a new bloated and inefficient government center that will provide no solution to the demands brought up by the Supreme Leader (http://www.kheyzaranonline.ir/1390/12/18/supreme-council-of-cyberspace-affect-all-irans-cyber-space).

As the authorities tighten their control of the internet, this week Telecommunications Minister Reza Taqipour once again addressed the threats posed by the network, and the intent to create a national intranet. In an interview given

to ISNA News Agency, the minister said that the intranet will operate separately from the global internet network and will make it possible to transfer information securely, which is currently impossible with the global network. He added that the creation of the national information network requires the cooperation of the public and private sectors (ISNA, March 10).

At a meeting with his Iraqi counterpart, Taqipour said that Western countries, particularly the United States, use the internet for spying and spreading corruption, but that Iran has launched activities designed to manage the use of the internet and limit its abuse. The internet should serve all countries in the world, not just the West, which uses it for its economic needs and for harming other countries, the minister said (Fars, March 10).

Meanwhile, this week the Iranian Center for Statistics published information on internet penetration and web surfing habits in Iran for 2010-2011. According to the information, during the period in question, the internet penetration rate reached 18.9 percent in urban areas and 4 percent in rural areas. A total of 11 million Iranians accessed the internet.

According to the data, 83.8 percent of all web surfers in Iran still use a dial-up connection, 13 percent use ADSL, and 0.9 percent have wi-fi.

- About 4.3 million of the 20.3 million families in Iran (21.4 percent) have an internet connection at home: 94 percent of families living in urban areas and only 6 percent of families living in rural areas. Among urban families 91.5 percent have a personal computer at home, compared to 12 percent of families in rural towns and villages.
- 6.4 million (58.1 percent) of Iran's web users are men and 4.6 million (41.9 percent) are women. 16.6 percent of Iran's male population use the internet, compared to 7.12 percent of the female population.
- 0.4 percent of internet users are less than 10 years old, 26 percent are 10-19, 43.2 percent are 20-29, 21 percent are 30-44, 8.7 percent are 45-64, and 0.5 percent are over 65.
- 75.2 of internet users surf the web at home, 22.4 percent use internet cafés, 14.4 percent surf at work, 13.4 percent surf at school, 4.3 percent use cellular telephones, 3.9 percent surf at other people's houses, and 1.4 percent surf in libraries.
- 26.1 percent of internet users access the web at least once a day, 33.1 percent at least once a week but not every day, 26.6 percent at least once a month but not every week, and 14.1 percent access the web less than once a month (Alef, March 11).

The Global Cyber Warfare Market 2011-2021

Source:https://www.asdreports.com/shopexd.asp?id=25802&desc=The+Global+Cyber+Warfare+Market+2011%2D2021&utm_source=SMI&utm_medium=email3rd&utm_campaign=cyber_defence

This report offers detailed analysis of the global Cyber Warfare market over the next ten years, and provides extensive market size forecasts by country and sub sector. It covers the key technological and market trends in the Cyber Warfare market. It further lays out an analysis of the factors influencing the demand for Cyber Warfare solutions, and the challenges faced by industry participants.

In particular, it provides an in-depth analysis of the following:

- Global Cyber Warfare market size and drivers: comprehensive analysis of the global Cyber Warfare market through 2011-2021, including highlights of the demand drivers and growth stimulators for Cyber Warfare solutions. It also provides an insight on the spending pattern and

modernization pattern in different regions around the world.
- Recent development and industry challenges: insights into technological developments in the global Cyber Warfare market, and an extensive analysis of the changing preferences of armed forces around the world. It also provides the current consolidation trends in the industry and the challenges faced by industry participants.
- SWOT analysis of the global Cyber Warfare market: exhaustive analysis of industry characteristics, determining the strengths, weaknesses, opportunities and threats faced by the Cyber Warfare market.
- Global Cyber Warfare market-country analysis: analysis of the key markets in each region, providing an analysis of the top segments of Cyber Warfare expected to be in demand.
- Major programs: details of the major programs in each segment expected to be executed during the forecast period.
- Competitive landscape and strategic insights: detailed analysis of competitive landscape of the global Cyber Warfare industry. It provides an overview of key Cyber Warfare solutions providers catering to the global Cyber Warfare sector, together with insights such as key alliances, strategic initiatives and a brief financial analysis.

Key Highlights

The global spending on cyber warfare systems is expected to remain robust over the forecast period due primarily to the increased importance of such systems in modern warfare. The formation of the US Cyber Command or USCybercom by the highest defense spender globally, highlights the importance of cyber warfare in today's world. Furthermore, the cyber attacks in South Korea, the US, Estonia and Georgia in 2011, add credence to the growing expenditure on global cyber warfare systems. Wars include a mix of physical, mental and tactical elements with information and communication technologies (ICT) playing a major role in the capabilities of mobile forces armed with real-time information devices. ICTs can be used to attack these battlefield systems directly, to capture sensitive data from defense contractors and governments or disrupt national infrastructure. Equally, defense systems must be built to detect and counter these attacks, making cyber warfare systems essential tools for maintaining an advantage in modern conflicts.

Scope

- Analysis of the global Cyber Warfare market size from 2011 through 2021
- Analysis of defense budget spending pattern by region
- Insights on the region wise defense modernization initiatives
- Sub-sector analysis of the Cyber Warfare market
- Analysis of key global Cyber Warfare market by country
- Key competitor profiling specifically focusing on the global Cyber Warfare market

In the Age of the Internet Russia Races Several Strains of Radical Islam

Source: http://www.jamestown.org/

There has recently been a spate of news stories in Russia about the Hizb ut-Tahrir al-Islami organization (Party of Liberation). This organization is on the Russian Supreme Court's official list of terrorist organizations and thus its activities in the country are banned (www.rg.ru/2006/07/28/terror-organizacii.html). An international pan-Islamic Sunni organization, Hizb ut-Tahrir is outlawed in Egypt and Germany and all of the Central Asia states. One wonders what this organization has to do with the North Caucasus.

Still, Ingushetia's law enforcement agencies have found followers of Hizb ut-Tahrir in the republic (www.magastimes.com/news/press-reliz-mvd-rf-po-ri). The accountant of the rights organization Mashr, Murad Yandiev, was one of four suspected adherents of this Islamic organization who were arrested. In the house where the arrests took place, police found

literature of the banned extremist "party." The head of Mashr stated that nobody in Ingushetia had heard of Hizb ut-Tahrir before (www.georgiatimes.info/articles/72867-1.html).

However, as soon as the name Hizb ut-Tahrir was heard in Russia, some experts, such as Ahmed Yarlykapov and Roman Silantyev, hastily declared that the group was advancing its interests in the North Caucasus, challenging Salafism.

This conclusion is hardly accurate. Salafism and the ideology of Hizb ut-Tahrir al-Islami are not opposed to each other. On the contrary, they are both parts of the same platform of radical Islam. Thus, making rash statements founded only on two or three Russian-language books that are distributed in Moscow and elsewhere in the country with the authorities' consent is not justified, because there are no signs of major ideological changes inside Russian Muslim society. The fact that the Salafis are making use of Hizb ut-Tahrir's literature confirms that the two Islamic movements have much in common, starting from their aims and ending with their methods of capturing power in various countries. To consider them rivals competing to control territories has little to do with the actual reality.

Still, Russian authorities are haunted by the image of Hizb ut-Tahrir not just in the North Caucasus, but throughout the country. Initially, the authorities started to take notice of this organization at the time arrests of Muslims started in Tatarstan. Groups of Muslims appeared there that did not recognize the authority of the official Islamic clergy, and this immediately caught the attention of the Russian security services. A preacher from Tashkent, Alisher Usmanov, was one of the founders of the branch of the party in Tatarstan. In 2005, Usmanov was convicted of participating in an extremist organization and possession of explosives (www.intertat.ru/ru/criminal/item/2892-halifat-strogogo-rezhima.html). Trials of members of Hizb ut-Tahrir are not infrequent in Tatarstan. The same trend can be seen in neighboring Bashkortostan. On February 23, 2012, a local court in Bashkortostan's Davlekanovsky district convicted four local residents of being members of an extremist cell of Hizb ut-Tahrir. Prior to that, other people suspected of participation in Islamic organizations also were put on trial (www.vz.ru/news/2012/2/23/563484.html).

The authorities also reported they had arrested members of Hizb ut-Tahrir in Moscow itself (www.rosbalt.ru/moscow/2011/09/14/889741.html), so these events should be interpreted as links in a chain, and the groups should not be viewed as different organizations competing with each other for influence in Russia's Muslim community.

Several dozen people are serving prison terms in Russia under Article 282-2 of Russia's Criminal Code for participating in various extremist Muslim organizations (http://lenta2012.ru/pulsblog/263580_zakluchennie-ekstremisti.aspx). It should be noted that Hizb ut-Tahrir al-Islami's leaders in Russia are normally people originating from Uzbekistan, Tajikistan and other Central Asian states. Leaders of the armed North Caucasian resistance and their supporters normally come from the North Caucasus. North Caucasian jamaats can be encountered across Russia and include not only natives of the Caucasus, but also ethnic Russians who converted to Islam.

An example of this was the case of 11 members of a jamaat in Novosibirsk who were arrested earlier this month (http://news.ngs.ru/more/378917/). The jamaat members were accused of plotting attacks and of financing the North Caucasian armed resistance. Similar jamaats operate in other parts of the country – from Kaliningrad to Vladivostok. For the time being, these jamaats act as missionary-educational groups and are not militarized. However, when the authorities decide that they have become too dangerous because they are starting to influence young people, the jamaats are declared accomplices of the North Caucasian militarized jamaats. This has happened to jamaat groups in Nizhnekamsk and Naberezhnye Chelny, in Tatarstan; and in Nizhnevartovsk, in the Khanty-Mansisk autonomous district (http://news.rin.ru/news/150375/).

The two brands of radical Islam in Russia differ in some respects. Hizb ut-Tahrir puts an emphasis on attracting the maximum possible number of Muslims into its ranks to change the map of a region. The jamaats try to create structures in Russia that would contribute to the victory of the armed resistance in the North Caucasus. The supportive structures either turn into insurgent groups or financial support groups. At the same time, one should not clearly

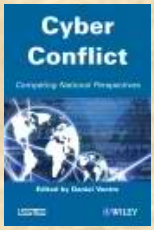
delineate these groups, inasmuch as they are not exact replicas of their maternal organizations in the North Caucasus and in the Middle East, respectively. The two brands of radicalism are still at the formative stage in Russia and the dividing lines between them are shadowy.

It is not surprising that Russia tries to point to Hizb ut-Tahrir's presence in the country as evidence confirming the official propaganda that all the tension and problems in the Muslim part of Russian society is connected to external influences. This was tried out in Chechnya, when the Russian government recast the members of the armed resistance as a branch of al-Qaeda in the North Caucasus. In fact, it was hard to agree with this conclusion, since al-Qaeda ignored the North Caucasus for a long time, discounting it as a region where it had no vested interest.

Thus, Islamic life in Russia is becoming more diverse than government authorities would like to admit. Stopping this process of integration of Russian Muslims into the world system of Muslim organizations in the age of the Internet is practically impossible now. While the Soviet Union managed to shut its borders and shield itself from external influences, this will not happen in today's Russia. The Russians, however, have not yet come to grasp the amount of Muslim influence on the country that will be exerted in the near future. The impact will not be a purely Russian phenomenon, but rather part of a worldwide trend.

Cyber Conflict

Competing National Perspectives



Edited by Daniel Ventre, CNRS, France
ISBN: 9781848213500
Publication Date: March 2012
Hardback 352 pp.
145.00 USD

Today, cyber security, cyber defense, information warfare and cyber warfare issues are among the most relevant topics both at the national and international level. All the major states of the world are facing cyber threats and trying to understand how cyberspace could be used to increase power.

Through an empirical, conceptual and theoretical approach, Cyber Conflict has been written by researchers and experts in the fields of cyber security, cyber defense and information warfare. It aims to analyze the processes of information warfare and cyber warfare through historical, operational and strategic perspectives of cyber attack. It is original in its delivery because of its multidisciplinary approach within an international framework, with studies dedicated to different states – Canada, Cuba, France, Greece, Italy, Japan, Singapore, Slovenia and South Africa – describing the state's application of information warfare principles both in terms of global development and "local" usage and examples.

Contents

9. A South African Perspective on Information Warfare and Cyber Warfare, Brett van Niekerk and Manoj Maharaj.
10. Conclusion, Daniel Ventre.

Table of Contents - PDF File - 89 Kb

Military and Strategic Affairs

Focus in cyberwarfare
Source: http://www.inss.org.il

NOTE: You can download full issue from the Newsletter's website – "CBRNE-CT Papers" link.

Passwords contribute to online insecurity

Source:http://www.homelandsecuritynewswire.com/dr20120404-passwords-contribute-to-online-insecurity

Online passwords are so insecure that 1 percent can be cracked within ten guesses, according to the largest ever sample analysis.

The research was carried out by Gates Cambridge scholar Joseph Bonneau and will be presented at a security conference held under the auspices of the Institute of Electrical and Electronics Engineers in May.

A University of Cambridge release reports that Bonneau was given access to seventy million anonymous passwords through Yahoo! — the biggest sample to date — and, using statistical guessing metrics, trawled them for information, including demographic information and site usage characteristics.

He found that for all demographic groups password security was low, even where people had to register to pay by a debit or credit card. Proactive measures to prompt people to consider more secure passwords did not make any significant difference.

There was some variation, however. Older users tended to have stronger online passwords than their younger counterparts. German and Korean speakers also had passwords which were more difficult to crack, while Indonesian-speaking users' passwords were the least secure.

Even people who had had their accounts hacked did not opt for passwords which were significantly more secure.

The release notes that the main finding, however, was that passwords in general only contain between ten and twenty bits of security against an online or offline attack.

Bonneau, whose research was featured in the *Economist*, concludes that there is no evidence that people, however motivated, will choose passwords that a capable attacker cannot crack. "This may indicate an underlying problem with passwords that users aren't willing or able to manage how difficult their passwords are to guess," he says.

How China Steals Our Secrets

By Richard A. Clarke

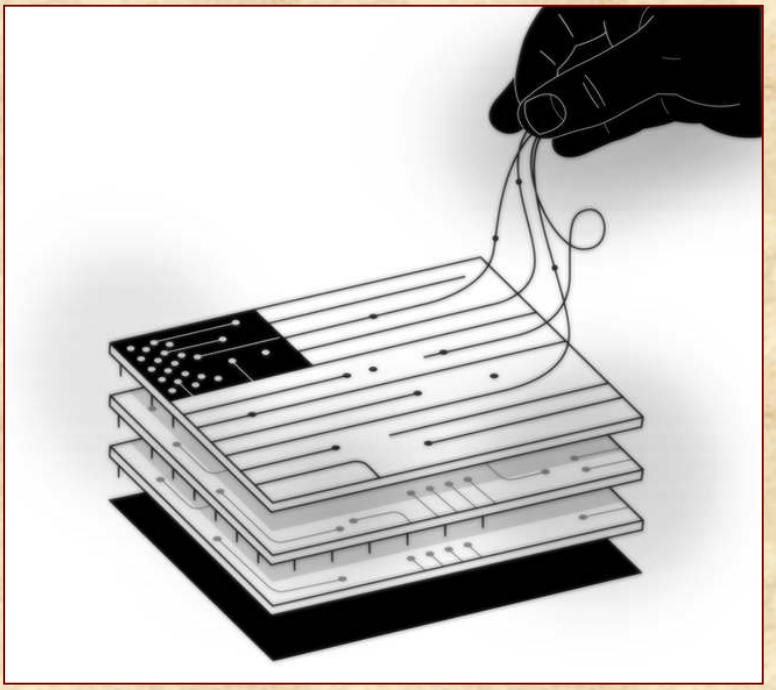
Source:http://www.nytimes.com/2012/04/03/opinion/how-china-steals-our-secrets.html?_r=1&ref=opinion

For the last two months, senior government officials and private-sector experts have paraded before Congress and described in alarming terms a silent threat: cyberattacks carried out by foreign governments. Robert S. Mueller III, the director of the F.B.I., said cyberattacks would soon replace terrorism as the agency's No. 1 concern as foreign hackers, particularly from China, penetrate American firms' computers and steal huge amounts of valuable data and intellectual property.

It's not hard to imagine what happens when an American company pays for research and a Chinese firm gets the results free; it destroys our competitive edge. Shawn Henry, who retired last Friday as the executive assistant director of the F.B.I. (and its lead agent on cybercrime), told Congress last week of an American company that had all of its data from a 10-year, $1 billion research program copied by hackers in one night. Gen. Keith B. Alexander,

head of the military's Cyber Command, called the continuing, rampant cybertheft "the greatest transfer of wealth in history."

Yet the same Congress that has heard all of this disturbing testimony is mired in disagreements about a proposed cybersecurity bill that does little to address the problem of Chinese cyberespionage. The bill, which would establish noncompulsory industry cybersecurity standards, is bogged down in ideological disputes. Senator John McCain, who dismissed it as a form of unnecessary regulation, has proposed an alternative bill that fails to address the inadequate cyberdefenses of companies running the nation's critical infrastructure. Since Congress appears unable and unwilling to address the threat, the executive branch must do something to stop it.



In the past, F.B.I. agents parked outside banks they thought were likely to be robbed and then grabbed the robbers and the loot as they left. Catching the robbers in cyberspace is not as easy, but snatching the loot is possible.

General Alexander testified last week that his organization saw an inbound attack that aimed to steal sensitive files from an American arms manufacturer. The Pentagon warned the company, which had to act on its own. The government did not directly intervene to stop the attack because no federal agency believes it currently has the authority or mission to do so.

If given the proper authorization, the United States government could stop files in the process of being stolen from getting to the Chinese hackers. If government agencies were authorized to create a major program to grab stolen data leaving the country, they could drastically reduce today's wholesale theft of American corporate secrets.

Many companies do not even know when they have been hacked. According to Congressional testimony last week, 94 percent of companies served by the computer-security firm Mandiant were unaware that they had been victimized. And although the Securities and Exchange Commission has urged companies to reveal when they have been victims of cyberespionage, most do not. Some, including Sony, Citibank, Lockheed, Booz Allen, Google, EMC and the Nasdaq have admitted to being victims. The government-owned National Laboratories and federally funded research centers have also been penetrated.

Because it is fearful that government monitoring would be seen as a cover for illegal snooping and a violation of citizens' privacy, the Obama administration has not even attempted to develop a proposal for spotting and stopping vast industrial espionage. It fears a negative reaction from privacy-rights and Internet-freedom advocates who do not want the government scanning Internet traffic. Others in the administration fear further damaging relations with China. Some officials also fear that standing up to China might trigger disruptive attacks on America's vulnerable computer-controlled infrastructure.

But by failing to act, Washington is effectively fulfilling China's research requirements while helping to put Americans out of work. Mr. Obama must confront the cyberthreat, and he does not even need any new authority from Congress to do so.

Under Customs authority, the Department of Homeland Security could inspect what enters and exits the United States in cyberspace. Customs already looks online for child pornography crossing our virtual borders. And under the Intelligence Act, the president could issue a

finding that would authorize agencies to scan Internet traffic outside the United States and seize sensitive files stolen from within our borders.
And this does not have to endanger citizens' privacy rights. Indeed, Mr. Obama could build in protections like appointing an empowered privacy advocate who could stop abuses or any activity that went beyond halting the theft of important files.
If Congress will not act to protect America's companies from Chinese cyberthreats, President Obama must.

***Richard A. Clarke**, the special adviser to the president for cybersecurity from 2001 to 2003, is the author of "Cyber War: The Next Threat to National Security and What to Do About It."*

Cyberweapon blowback

Source: http://www.homelandsecuritynewswire.com/dr20120403-cyberweapon-blowback

In the fall of 2010 the Iranian nuclear effort was brought to a temporary halt when sophisticated malware was introduced into Iran's uranium enrichment program. The malicious code, known as Stuxnet, was a highly specific virus targeting only Siemens supervisory control and data acquisition (SCADA) systems. In the world of cyberwarfare, it was a nuclear weapon.
On 2 July 2011, *The Hacker News* announced that the Stuxnet code was available for download, providing a link to obtain the code. The weapon was now available to anyone. On 1 September 2011, a worm subsequently named Duqu was discovered, and thought to be related to Stuxnet (experts have since concluded that Duqu was designed by the same people who designed Stuxnet).
In the security sector, there is an active debate as to whether or not these cyberweapons can be converted and used against the United States and its allies.
There are few known strands in this debate. One is that the worm itself is nothing special, in that it spreads indiscriminately once introduced into a system, a fundamental feature of this virus form. What is unique about Stuxnet is that it contains a malicious payload targeting specific

```
#include <windows.h>
#include <defs.h>


//-------------------------------------------------------------------------
// Data declarations

extern int dword_10001CD0[8]; // weak
extern char *off_10001CF2; // weak
extern char byte_10001CF9[3]; // weak
extern char byte_10001DC7; // weak
extern int dword_1000215A; // weak
extern int dword_10002162; // weak
extern int dword_10002166; // weak
extern int dword_1000216A; // weak
extern int dword_1000216E; // weak
extern int dword_10002172; // weak
extern int (__stdcall *dword_10002176)(_DWORD); // weak
extern int dword_1000217A; // weak
extern int dword_1000217E; // weak
extern int dword_10002182; // weak
extern int (__stdcall *dword_10002186)(_DWORD, _DWORD, _DWORD, _DW
extern int (__stdcall *dword_1000218A)(_DWORD, _DWORD, _DWORD, _DW
weak
extern int dword_1000218E; // weak
extern int dword_10002192; // weak
extern int dword_10002196; // weak
extern int (__stdcall *dword_1000219A)(_DWORD); // weak
extern _UNKNOWN unk_10003068; // weak
```

Siemens industrial control systems. Given that the Iranian systems attacked were isolated from the Internet, some analysts believe that it was introduced into the facilities network via a flash drive device.
Coupling this information with the fact that the specific systems attacked were known and included in the virus leads to the conclusion that espionage was involved in gathering the system information needed, and introducing the worm into the Iranian facilities' network.

The 1983 movie "War-games" depicted a dystopian vision of a computer-controlled Armageddon. Today, cyber-war is very much a reality. (United Artists)

This has led to the belief that Stuxnet could only have been created with nation-state support, and speculated that the United States or Israel, singly or in partnership, had created and released the worm.

Liam O Murchu, a manager of operations at Symantec Security Response, told Foxnews.com that it would be very difficult rework the Stuxnet and use it in an attack without having the source code. "So from that point of view, it's not so dangerous to have Stuxnet out in the wild right now. Even if you get your hands on it, you don't have the source code to refashion it to do something else."

The real danger is not that the code can be reused, but that its existence provides a pathway to the methodology. Code reuse is common practice, and certainly is applicable here. Tweaking the code itself, however, is not the major concern.
The real concern is that Stuxnet's existence demonstrates what is achievable.
Security analysts are confident that they can stop anything that is a variant of Stuxnet, but the real challenge is stopping something in the style of Stuxnet. This is where the confidence ends.

2012 Top Cyber-Threats

Source: http://info.publicintelligence.net/USAF-CyberThreat2012.pdf

Every year as technology grows and advances thus do the threats that surround it. Predicting what new cyber threats to look for may not always be an easy task. By keeping up with the past trends and ever changing current environment, may help to give us a good handle on how to prepare for what may be to come.

Last year we saw great changes in Hacktivism, mobile threats, social-media exploitation, clientside exploitation, and targeted attacks. As many of these will only continue to evolve as we step in to 2012, there are many more to be added to the list and not ignored.
According to McAfee, the top ten threats for 2012 are:

1. Attacking Mobile Devices – Over the last two years mobile devices and smartphones have experienced a huge increase in attacks with 2011 showing the largest levels in mobile malware history. As they did on PCs, rootkits and botnets deliver ads and make money off of their mobile victims the same way. The installation of software or spyware, ad clicks or premium-rate text messages, as well as a shift toward mobile banking attacks is just a few threats facing mobile device users. As more users handle their finances on mobile devices, techniques previously dedicated for online banking will now focus on mobile banking users, bypassing PCs and going straight for mobile banking apps.

2. Embedded Hardware – GPS, routers, network bridges, and recently many consumer electronic devices use embedded functions and designs. Malware that attacks at the hardware layer will be required for exploiting embedded systems. Attackers will often try to "root" a system at its lowest level. If code can be inserted that alters the boot order or loading order of the operating system, greater control is gained and can maintain long-term access to the system and its data. The consequence of this trend is that other systems that use embedded hardware, for example, automotive systems, medical systems, or utility systems will become susceptible to these types of attacks. These proofs-of-concept code are expected to become even more effective in 2012.

3. "Legalized" Spam – Since the drop in global spamming volumes from the peak in 2009 and the increased black market cost of sending spam through botnets, "legitimate" advertising agencies. The United States' CAN-SPAM Act was watered down so much that advertisers are not required to receive consent for sending advertising. "Legal" spams, and the technique known as "snowshoe spamming," are expected to continue to grow at a faster rate than illegal phishing and confidence scams.

4. Industrial Attacks – Gaining more attention every day, the cyber threat potential is one of few that pose real loss of property and life. Water, electricity, oil and gas are essential to people's everyday lives, Many industrial systems are not prepared for cyber attacks, yet many such as water, electricity, oil and gas are essential to everyday living. As with recent incidents directed at water utilities in the U.S., attackers will continue to leverage this lack of preparedness.

5. Hacktivism – One thing is certain, when a target was identified, hacktivists are a credible force. The problem in 2011 was the undefined structure, differentiating between rogue script kiddies and a politically motivated campaign was a task. McAfee Labs predicts that in 2012, either the "true" Anonymous group will re-invent itself, or die out. The other piece to look for in 2012, digital and physical demonstrations becoming more engaged and targeting public figures more than ever before.

6. Virtual Currency – Also commonly referred to as cyber-currency, a popular means to exchange money online which is not backed by tangible assets or legal tender laws. Many use services such as Bitcoin, which allows users to make transactions through a decentralized, peer-to-peer network using an online wallet to receive "coins" and make direct online payments. Users need a wallet address to be able to send and receive coins, the wallets however are not encrypted and the transactions are public. This boosts opportunity for cybercriminals, not to mention Trojan malware.

7. Rogue Certificates – We often tend to trust digitally-signed certificates without a second thought believing the digital signature or certificate authority they came from to be legit. Recent threats such as Stuxnet and Duqu used rogue certificates to evade detection and investigations have shown that as many as 531 fraudulent certificates were issued from DigiNotar, a troubled Dutch authority that recently declared bankruptcy. Increased targeting of certificate authorities and the broader use of fraudulent digital certificates will only increase, giving attackers an even greater advantage.

8. Cyber War – As more and more countries are realizing the harmful outcomes cyber attacks pose, industrial attacks for example, that carry crippling potential, the need for defense is more apparent than ever. McAfee Labs expects to see countries demonstrate their cyber war

capabilities in 2012, in order to send a message.

9. Domain Name System Security Extensions – A technology to protect name-resolution services from spoofing and cache poisoning by using a "web of trust" based on public-key cryptography; meant to protect a client computer from inadvertently communicating with a host as a result of a "man-in-the-middle" attack. Unfortunately it would also protect from spoofing and redirection of any attempts by authorities who seek to reroute Internet traffic destined to websites that are trafficking in illegal software or images. With governing bodies around the globe taking a greater interest in establishing "rules of the road" for Internet traffic, McAfee Labs expects to see more and more instances in which future solutions are hampered by legislative issues.

10. Advances in Operating Systems – Recent versions of Windows have included dataexecution protection as well as address-space layout randomization. These security methods make it harder for attackers to compromise a victim's machine. Encryption technologies have also boosted OS protection in recent years. As with most internal OS security measures, attackers very quickly found ways to evade them. Advances by the information security industry and operating system will continue to advance, but will that push malware writers to focus on directly attacking hardware? McAfee Labs expects to see more effort put into hardware and firmware exploits and their related real-world attacks through 2012.

Who is Waging Cyberwar Against the Jihadi Networks?

Source: http://www.time.com/time/world/article/0,8599,2111293,00.html#ixzz1rHCpz7VN

"The enemies of Allah who boast of their freedoms have not spared any effort to eradicate our blessed media." After two weeks of silence, the jihadist forum Shamukh al Islam came back online yesterday with a gloat: an apparent cyberattack against Shamukh and four similar sites had failed to shut it down permanently. But terrorism analysts see the event in a different light. As they investigate the mystery of who caused the outage and why, most can't help but see in

the blackout one more piece of evidence that al-Qaeda is in disarray.

Websites like Shamukh al Islam perform a critical function in jihadist circles. Loaded with videos that depict alleged Western atrocities against Muslims, they recruit supporters, while their chatrooms and forums allow jihadists around the globe to communicate with one another and to exchange information, including instructions on bomb construction and chemical warfare.

So when Shamukh al Islam, perhaps the most prominent of jihadist forums, suddenly fell silent on March 22 or 23, terrorism analysts took notice. That interest only grew over the next few days as four other sites went down and, with one exception, stayed that way. "For four of these sites to be offline for two weeks is unprecedented," says Aaron Zelin, a researcher at Brandeis University. "We've seen other cyberattacks on these sites before, but they've never managed to keep them down for that long."

However significant the outage may be, no one is quite sure of who caused it, or why.

Because Shamukh went down right after French authorities cornered and killed Mohammed Merah, the 23-year-old jihadist who shot seven people in Toulouse, some analysts have suggested a connection. "Our first suspicion was that the blackout was somehow connected to Merah, just based on the timing," says Evan Kohlmann, terrorism analyst at Flashpoint Partners, a consulting agency. "The presumption here is that someone is intent on thwarting, or at least complicating, al-Qaeda's efforts to release a particular piece of media" — perhaps the same Merah video that was sent to Al Jazeera but never aired.

Yet a French connection is not the only possibility. On March 27, Spanish authorities arrested Muhrad Hussein Almalki in the coastal city of Valencia. Known as "The Librarian" for his work administering and archiving jihadist websites, Almalki supervised one of the downed sites, and posted frequently under various aliases on at least two others. In a 2011 post to Shamukh, he answered a call for "enemy names" with a list of targets that included the two George Bushes, Bill Clinton and Tony Blair.

For Manuel Torres, terrorism expert at Seville's Pablo de Olavide University, Almalki's arrest suggests that the sites' operators may have taken down the forums themselves. "Almalki was an administrator, and that means his arrest posed a significant danger — in both this case and a similar one in 2010, police found a list of passwords," says Torres. "They might have taken down the sites themselves for protection."

When sites have voluntarily gone dark in the past however,, their administrators have usually posted messages to that effect — something that did not happen in the Shamukh case until April 2. But if the evidence does indeed point to a cyberattack, who was behind it?

On April 4, Pelayo Barro, a journalist for the Spanish digital newspaper *El Confidencial*, reported that the U.S. government had something to do with it. "My source, who works as an outside consultant for Spain's National Intelligence Center, told me that U.S. intelligence agents got in touch with their Spanish counterparts in late March," Barro told TIME. "They told them that, a few days earlier, a team of 10 hackers working for the Obama government had broken the passwords of several of the principal Islamist forums. They said it was the biggest cyberattack yet against these sites." According to Barro, information gleaned from this attack enabled Spanish authorities to locate and arrest "The Librarian," a figure they had been interested in for over a year.

Kohlmann, however, questions U.S. involvement. "Generally speaking, the U.S. government does not shut down jihadi websites," he says. "Most of the people that I know in U.S. law enforcement and intelligence agencies believe it is more fruitful to leave the websites online and use them for intelligence purposes." And if it wasn't the U.S. government? "Other possible responsible parties might include the governments of France and Israel, as well as more skilled cybervigilantes."

Britain brought down jihadist websites in 2010, but did not admit to doing so until this year. So it is likely that the responsible party, whomever it is, will not be confessing anytime soon. But more significant than its origins may be what the attack reveals about al-Qaeda. "People in some intelligence agencies believe the organization is very weak," says analyst Zelin. "And the length and breadth of this outage seems to support that."

That's not to say, however, that these jihadist networks no longer pose a threat. "It's definitely a setback for al-Qaeda's communication network," says Kohlmann. But "if the past can serve as example, other trusted, authenticated forums will simply step up and take its place."

Team Poison hacks MI6 —then calls to boast

Source:http://www.msnbc.msn.com/id/47032601/ns/technology_and_science-security/#.T4hYKdmRQ4k

The hacktivist collective calling itself Team Poison (TeaMp0isoN) unleashed an automated 24-hour "phone bomb" assault against MI6, the United Kingdom's Secret Intelligence Service, and then called the agency to boast.

The barrage of phone calls tied up MI6's phone lines, effectively preventing any legitimate calls from getting through. Each time an MI6 official answered the phone, a robot voice said "Team Poison," the news site Softpedia reported.

To keep from being traced, the calls were automated through a script run on a compromised server in Malaysia, Softpedia said.

Taunting authority

Following the phone bombing, Team Poison leader "TriCk" called the secret intelligence service directly to taunt it. In a YouTube video uploaded Tuesday, TriCk, speaking with a British accent, tells the MI6 representative, "You're being phone-bombed right now, mate."

TriCk, who said he is 16, also calls himself Robert West, and tells the two MI6 representatives on the line that he's "got some terrorism here."

When asked about Team Poison's philosophy, TriCk answers, "Knowledge is power. We embarrass governments," and he curses the police. TriCk also tells the MI6 representative that Ryan Cleary, a 19-year-old British hacker arrested last June for a string of hacks against government agencies, is his brother.

MI6 responds that the information TriCk has disclosed "is being passed to the FBI."

Watching the watchers

Team Poison posted another video to YouTube today on Thursday. This

video, according to the hackers, captures a conversation between MI6 and the FBI. MI6 admits in the taped call that it has received about "700 calls over the last couple nights."

In a statement posted along with this second video, TriCk said his hacking group targeted MI6 "purely because they help lock up innocent people who they themselves label as terrorists with no proof at all."

TriCk cites "Babar Ahmad, Adel Abdel Bary & a few others" and says: "The people who have been extradited have done nothing wrong to be extradited to the U.S."

Adel Abdel Bary is an Egyptian militant wanted in connection with the 1998 bombing of the U.S. embassy in East Africa. He has been in custody in the U.K. since 1999. Babar Ahmad has been in custody in the U.K., and is believed to have been involved in supporting Chechen and Afghan insurgents. On April 10, the European Court of Human Rights ruled that Ahmad can be extradited to the U.S.

"The US is calling it a 'global war on terror' which in my opinion is a cover up for 'global war on Islam," Team Poison wrote. "The real terrorists are the guys sitting in 10 Downing Street and the Whitehouse (sic)."

Hackers join Anonymous' anti-extradition campaign

Team Poison's involvement in anti-government campaigns coincides with the recent efforts of Anonymous, which last weekend launched a denial-of-service attack against the U.K.'s Home Office website.

That attack, part of the hackers' "Operation Trial at Home," was carried out in protest of the extradition of three suspected U.K. cybercriminals.

Yesterday, Anonymous said it would launch a similar offensive Saturday against the website of the Government Communications Headquarters, the intelligence agency that, along with MI6, protects U.K. government agencies from cyberthreats.