Islamic Terror Networks Implementation of Network Technologies

Michael S. O'Neil
Diplomacy Department
Norwich University
Northfield, VT 05663-0367
michaeloneil23gmail.com

David H. Gray
Campbell University
Buies Creek, NC 27506
grayd@campbell.edu

Abstract

As the international community becomes more globalized so do Islamic terror networks. The technological advancements of the 21st century continue to aid Islamic terror networks in their ability to implement global communication strategies. Implementing worldwide communication strategies has brought the terrorists closer to achieving their desired end result, an Islamic caliphate. In order to impede any further advancement in their asymmetrical battle with the West, apostate Muslim regimes, Israel, and the counterterrorism community need to understand the threat before them. Through a thorough investigation of Islamic terrorist networks strategic communications approach alongside the use of network technologies it is the hope to better understand the capabilities of the 21st jihadist. By understanding the capabilities of the 21st century terrorist effective policy recommendations can be made to help counter future terrorist attacks and the establishment of an Islamic caliphate.

Key Words: Islamic terror networks, strategic communications, network technologies, Islamic caliphate, asymmetrical warfare

Introduction

There is no question that the effects of globalization have increased the interconnectedness of communities throughout the world. The continuous advancement of various technologies in areas such as communication and travel has assisted the increase of wealth, goods, and services through the international community. Nevertheless, there is a darker side to the era of globalization. The darker side of globalization is the proliferation of international terrorist organizations. Terrorism is not a new phenomenon, however, terrorist organizations' global influence is. Prior to the era of globalization terrorist organizations were confined to their domestic and regional areas. Now, the advancement of various technologies has increased the regional and global reach of terrorist organizations. By adopting various network technologies, terrorist organizations have been able to advance their recruiting techniques, communications, training, planning and targeting, and lastly, propaganda and persuasion. Similarly, by studying Islamic terrorist organizations' adoption

of network technologies provides insight into the operational abilities of global terrorist networks. Through this investigation it is the goal to identify the adaptation of pertinent network technologies to aid the continuance of terror networks, as well as ascertain how Islamic terrorist organizations evaluate the strengths and weaknesses of the various technologies they employ to maximize their potential. By recognizing the network technologies terrorist organizations adopt and evaluating how terrorist organizations use such technologies, policy recommendations for the counterterrorism community will be established.

Understanding Prominent Terrorist Networks of the 21st Century

On September 11, 2001 the United States of America received a series of coordinated suicide attacks by al-Qaeda operatives. The al-Qaeda operatives were able to successfully hijack four planes, three of which were flown into designated targets; the two World Trade Center buildings and the Pentagon. The last of the four planes did not reach its intended target but did crash into the ground at Shanksville, Pennsylvania, killing all on board. This comprehensive attack was the culmination of several previously attempted, but failed, attacks on the United States, the results of which set a new standard for future terrorist attacks throughout the world. The attacks of 9/11, the failed al-Qaeda "Millennium Plot," and the more recent Mumbai terrorist attacks draw attention to reoccurring trends of terrorism in the 21st century. Firstly, the attacks are becoming more extravagant. As was the case with 9/11 and Mumbai, terrorists are becoming more capable of attacking numerous targets simultaneously. Secondly, the operatives of the aforementioned attacks and countless numbers of others are not specifically from one distinct region of the world. Rather, operatives throughout the world have been recruited to a particular organization to fight for that organizations specific cause. For instance, the al-Qaeda terrorist network does not confine itself to recruiting persons of distinct nationalities, but rather looks for Muslims who are susceptible to their plight and willing to fight for their cause.

Many Islamic terrorist groups exhibit an ideology that looks to restore an Islamic caliphate. For al-Qaeda its ideology hopes to restore a global Islamic caliphate, whereas organizations such as Hamas and Hezbollah want to restore its caliphate over its holy land, now wrongfully occupied by invaders, the Zionists. To recruit potential members such Islamic terrorist organizations create narratives based on Islamic ideals. Islam's universal mission is to establish a caliphate. However, there are discrepancies between Muslims on how to establish the caliphate and what regions it will rule over. On how to establish the caliphate, Marc Sageman (2004) notes there is the belief in numerous Muslim communities that Muslims "are required to engage in a jihad to expand dar al-Islam to the world that all humankind could benefit from living with a just social order." To expand upon this further, Sageman identifies there are two distinct types of jihad, the greater jihad and the lesser jihad. "The greater jihad is the individual nonviolent striving to live a good Muslim life," whereas, the lesser jihad "is the violent struggle for Islam (Sageman, 2004)." Islamic terrorist organizations who adhere to the lesser jihad often couple this with the controversial teachings of Sayyid Qutb, who preached western culture was to blame for the fall of Islam. In order to restore Islam, Qutb believed their God, Allah, bestows the "right to destroy all obstacles in the form of institutions and traditions (Sageman, 2004)" that hinder the establishment of an

Islamic caliphate. In the case of al-Qaeda, the obstacles that need to be destroyed are the West, Israel, and apostate Muslim regimes.

As a result, Islamic terrorist organizations tailor their narratives and ideologies by fusing revisionist Islamic history with controversial teachings to convince Muslims to join their fight against the evils in the world. However, to bestow their message and gain a devout following, Islamic terrorist organizations need to adopt continuously advancing technologies to increase their regional and global reach in hopes of achieving their goals. By adopting network technologies of the 21st century, to recruit and gain advantages in their operational capabilities, bring Islamic terrorist organizations one step closer in reaching their objectives. Thus, Islamic terrorist organizations are quite sophisticated. For the counterintelligence communities to effectively thwart future terrorist attacks it must understand the sophistication of Islamic terror networks.

Identifying the Functions of Terrorist Networks

In order for terrorist organizations to be successful they need to have a comprehensive game plan or business model to maintain their status quo. In their piece titled, *Network Technologies for Networked Terrorists*, Bruce W. Don et al. (2007) identify several components terrorist organizations need to have in order to be effective. The list of components is as follows: recruiting, acquiring resources, training, reconnaissance and surveillance, planning and targeting, communication, attack operations, and propaganda and persuasion. The central link of the aforementioned components of a terrorist organization is communication. Without effective communication a terrorist organization would not be able to successfully implement any other component and as a result, would likely falter. Quality communication is essential for terrorist organizations to: recruit new members; to solicit funding; to implement effective training; to plan successful attack operations, and to release the organizations grievances and a list of demands to their intended targets.

In the piece titled, *Communication and Media Strategy in the Jihadi War of Ideas*, Corman and Schiefelbein (2006) condense the rationale of why jihadis pursue advanced technologies. According to Corman and Schiefelbein (2006) Islamic terror networks pursue three strategic goals for communication against their operations which are: legitimize their cause; propagate their movement; and intimidate their opponents. To explain further Corman and Schiefelbein (2009) write, Islamic terror networks "must legitimate their movement by establishing its social and religious viability while engaging in violent acts that on their face seem to violate the norms of civilized society and the tenets of Islam." Secondly, Islamic terror networks must propagate "their visions, goals, and slogans by spreading messages to sympathizers in areas they want to expand (Corman & Schiefelbein, 2009)." And lastly, Islamic terror networks look to intimidate their opponents.

The three strategic goals of Islamic terror networks are a concerted effort to fight an asymmetrical war. Terror networks are keenly aware they do not match up, militarily, to their opponents. For example, terror networks such as al-Qaeda do not have the military prowess of their opponent, the United States. If al-Qaeda were to try to fight a symmetrical war they would be quickly disposed of and ultimately would not attain their goal of establishing a global Islamic caliphate. But, by engaging their enemy in an asymmetrical conflict the terror network seeks to create an imbalance that favors one's own side in order to win the campaign. In other words, the purpose of an asymmetrical conflict "is to hit the opponent at

his center of gravity or several conflict-determining centers and decide the conflict in one's own favor or reach one's own purposes (Bockstette, 2008)." The new dimension of network technologies, e.g., mass media and the internet has enabled terrorists to spread their message and attack their enemies with a multifaceted front, which has helped terror networks to tip the scales of the asymmetrical conflict in their favor.

Network Technologies Defined

Bruce W. Don et al. (2007) in their piece, *Network Technologies for Networked Terrorists*, define network technologies "as command, control, communication, computer intelligence, surveillance, and reconnaissance (C4ISR) technologies in military parlance, as well as the consumer-orientated technologies that can often provide the functionality needed for terrorist operations." More specifically, these technologies can include, but are not limited to, "connectivity technologies (e.g. wireless routers), mobile computing (e.g. laptop computers), personal electronic devices (e.g. personal assistants and cell phones), IT services and Internet access, and video recordings (Don et al., 2007)." The most crucial network technology for Islamic terror networks is the internet. The internet is considered crucial for two reasons. One, the internet is the underlying, fundamental component that makes the other previously mentioned network technologies function. Secondly, the internet is capable of connecting network technologies the world over. This is especially important for Islamic terror networks to enact their three strategic goals: legitimize; propagate; and intimidate in their efforts to defeat the West, Israel, and apostate Muslim regimes.

Linking Network Technologies with Islamic Terror Networks Three Strategic Goals

The first strategic goal of Islamic terror networks is the pursuit of legitimizing their movement. Islamist terror networks must spend due diligence in legitimizing their movement because their violent attacks kill innocent people. Killing innocent people contradicts the tenants of Islam, thus, "legitimacy and the ostensible demonstration of compliance with Islamic law are prominent in their communication strategy (Bockstette, 2008)." Moreover, Islamic terror networks must "portray their movement as one of freedom fighters, forced against their will to use violence due to a ruthless enemy that is crushing the rights and dignity for their community (Bockstette, 2008)." So, prior to and after terrorist attacks it is imperative for Islamic terror networks to disseminate a persuasive rationale to their followers and potential followers so as to not alienate them.

To better understand how Islamic terror networks disseminate the legitimization of their violent actions one must ask what devices or network technologies are Islamic terror networks using to do so? Islamic terror networks use a variety of network technologies to spread their rationale which include, but are not limited to, video, chat rooms, radio messages, podcast, and websites. Such Islamic terror networks rationale's found in various network technologies can be summarized by the spoken words of Abu Musab-al Zarqawi in a 2006 interview:

> "Our political agenda, […] is that of the saying of the Prophet (peace be upon him), I have been sent the sword, between the hands of the hour, until Allah is worshipped alone…this is what determines our political goal. We fight in the way of Allah, until the law of Allah is implemented, and the first step is to

> expel the enemy, then establish the Islamic state, then we set forth to conquer, the lands of Muslims to return them back to us, then after that, we fight, the kuffar (disbelievers) until they accept one of the three. I have been sent with the sword, between the hands of the hour; this is our political agenda (Bockstette, 2008)"

A particular technological advancement that is capable of globally disseminating Islamic terror network leaders' words of legitimization, similar to the one above, is the internet. The quote above is the rhetoric of a former al-Qaeda leader Abu Musab-al Zarqawi. Al-Zarqawi was part of a terror network that understands the immense potential of the internet. Thus, al-Qaeda has devoted and continues to devote much time and money to their established media wing, as-Sahab. As-Sahab is known to have produced 97 original videos and disseminates such material through Internet "clearinghouses." To define, Mark Dubowitz (2009) writes clearinghouses "act as middlemen in distributing terrorist media to mirror sites." To explain further Dubowitz provides an example of a clearinghouse, al-Fajr Media Center. Al-Fajr, operates almost entirely virtually and is responsible for moving as-Sahab content to pre-selected sites at which point, the videos have the potential of going viral. Viewers of as-Sahab productions have the ability to download the video from al- Fajr and repost it to other sites, potentially reaching such websites as Archive.com and YouTube where there is a high volume of users (Dubowitz, 2009). Once, as-Sahab productions reach websites such as YouTube they have the immense potential to reach more audiences and viewership through other network technologies as well.

The second of the three strategic communication goals of Islamic terror networks is to propagate visions and slogans to targeted audiences. Again, the preferred method of network technology is the internet. The internet is a vast sea of various media formats capable disseminating material. The key reason for internet being a reoccurring choice for terror networks is that the internet is decentralized and provides almost perfect anonymity. Also, the internet in many countries is not subjected to controls or restrictions and consequently, may be accessed by anyone (Weimenn, 2010). Furthermore, the internet affords jihadis the opportunity to use sophisticated communication methods that draw comparisons to the modern methods of communication and public relations (Corman & Schiefelbein, 2006). Meaning, Islamic terror networks such as, al-Qaeda, Hamas, and Hezbollah are capable of tailoring their slogans and visions to specific audiences in effort to gain optimal results. Corman and Schiefelbein (2006) note, sympathizers and potential sympathizers of both the near and far movements are primarily targeted with social and religious legitimization messages. Face-to-face personally delivered speeches and sermons are the preferred method, however, a recording of such an event and consequent posting of it on the internet is a beneficial substitute.

Another effective tool jihadis have used to for their strategic communication goals is to propagate disinformation. Such disinformation propagated by jihadis has included rumors that cast the apostates, Jews, and the West in a negative fashion. The rumors are tailored in a way that will appeal to 'the prejudices of the jihadis' audience, making them more receptive to legitimating and propagation arguments. Examples of such rumors are variations of: the U.S. Marine Corps barbequed Somali babies; 4000 Jews were warned by the CIA/MOSAD not to come to work at the World Trade center on 9/11; and the Indonesian Tsunami was caused by a nuclear bomb detonated by the U.S. Navy (Corman & Schiefelbein, 2006). Such

rumors do not need a strong push from the media wings of Islamic terror networks; rather rumors like these are capable of spreading virally at rapid rates throughout the internet. Rumors may be spread through social media websites such as Facebook and Twitter, or be harnessed in the interactive capabilities of chartrooms, instant messenger, blogs, and self-determined online communities (Weismann, 2010). Nevertheless, rumors are another cog in the wheel of serving the jihadis legitimization strategy. The rumor casts its enemies, the West, Israel, and apostates as evil and encourages Muslims to rise up, resist, and fight against the tyranny ruling over the Muslim ummah.

The third communication strategic function of Islamic terror networks is to intimidate their opponents. One of the premier methods jihadis use to intimidate their opponent within the frameworks of strategic communication techniques is video recordings. Videos produced that serve the role of intimidation are: suicide attacks, beheadings, hostage taking, and direct messages aimed at the enemy. These types of messages provide a very direct and clear message to the enemy that the jihadis are capable and willing to do what they believe is necessary to win the asymmetrical conflict. With this message it is the hope of Islamic terror networks to instill fear and regret into their enemies. Striving to instill these two emotions in the enemy the jihadis hope that their message will convince the enemy to acquiesce to their demands.

The intimidation videos mentioned above can be grisly videos, especially videos depicting suicide attacks and beheadings. To better understand how videos of suicide attacks, beheadings, hostage taking, and direct messages aimed at the enemy portray intimidation it is necessary to break them down. For instance, suicide attack videos are often used to "illustrate the systematic approach of planning, preparation, execution, and the outcome of a suicide bombing (Salem et al., 2008)." The frightening part of each stage of a suicide video is the resolve of the jihadis to carry out what they believe is right. Moreover, the time and effort spent systematically planning and preparing for a suicide operation displays malice and intent. Similarly, beheading videos do much of the same. Of the beheading videos included in the Salem et al (2008) study, the videos follow a similar model to that of suicide attack videos. Often a beheading video will follow a protocol, for instance, the beginning starts with a message from the hostage which is followed by a verdict or warning by the hostage takers. Ultimately, the video concludes "with a grisly beheading or shooting of the hostage (Salem et al., 2008)." As for hostage taking videos and videos with direct messages they also follow a similar pattern as the previously described videos. Nevertheless, each type of video is for the intended use of instilling fear and regret into the enemy.

Adjusting Network Technologies to Target Broader & Specific Audiences

To this point, the three strategic communication techniques used alongside networked technologies have been identified and defined. However, networked communications serve a broader role for Islamic terrorist groups throughout the world. As discussed earlier, global terror networks seek to induce change throughout the world by recruiting, fundraising, and violently attacking their enemies. But to have a truly global influence they must adapt their strategic communication techniques to welcome greater audiences and not alienate potential sympathizers. To do so, global terrorist organizations are keenly aware of advancements in communication technology so as to stay in sync with the constantly advancing technology of the globalized world. It is important to identity the astute abilities of global terror networks in

communication because as Islamic terrorist Abu Musab al-Zarqawi, describes, "More than half of this battle is taking place in the battlefield of the media. We are in a media battle in a race for the hearts and minds of Muslims (Bockstette, 2008)." By identifying the capabilities of Islamic terror networks and the asymmetrical conflict they are trying to win the West, apostate Muslims, and Israel can create effective countermeasures.

Prior to the advancements of Islamic terror networks' communicative abilities they were using traditional communicative means. Traditional communicative means can be considered as journalist interviews, fax, face-to-face assemblies, and press conferences. However, by the end of the 20th century there was a shift in the communication means of terrorist networks due to technological advancements. Recognizing the availability of highly sophisticated communicative means, Islamic terrorist organizations started to develop and devote more time to media outlets. For example, in the fall of 2006 the terrorist organization, Hamas, sought to broaden their reach of its media wing al-Aqsa. Hamas noticed the success a rival faction, Hezbollah, was having in inciting hatred and violence among its worldwide viewership. Also, Hezbollah's media wing, al-Manar, was able to effectively recruit children and adults as terrorists by broadcasting to an estimated 10-15 million worldwide viewers during the height of its popularity. Consequently, Hamas developed their television broadcast station, al-Aqsa, to do the same. Prior to the fall of 2006, al-Aqsa had only broadcasted within the Gaza strip. Hiring the same satellite distribution company as Hezbollah, Hamas was also able to spread their message of hatred throughout Europe, the Middle East, and Europe (Dubowitz, 2009).

Although al-Manar and al-Aqsa broadcasts have been capable of meeting Hamas' and Hezbollah's "organizational goals: subverting the peace process, raising funds, disseminating movement propaganda, inculcating terror, and recruiting suicide bombers (Dubowitz, 2009)," counterterrorism forces have been able to effectively erode their influences. For instance, the Israeli Air Force has bombed al-Manar stations and infrastructure weakening Hezbollah's influence. Another effective countermeasure for counterterrorism forces has been to criminally charge satellite providers who transmit productions from known Islamic terrorists' media wings. For instance, the European Union successfully argued that the al-Manar's incitement to violence, racist remarks, and anti-Semitism found in their programs violated European law. Therefore, European satellite providers were compelled to cease transmission of al-Manar programs. Lastly, counterterrorism efforts have been able to hit terror networks radio broadcasting stations where it hurts the most, in the pocket. States in the European Union alerted unaware and reputable companies their brands were being advertised on terrorist stations. Once, companies like Coca-Cola, Pepsi, Proctor & Gamble, and Western Union were notified their brand was helping fund terrorist organizations they quickly pulled their advertisements (Dubowitz, 2009).

Although counterterrorism efforts have been able to impede Islamic terrorism networks' ability to broadcast their three strategic goals with continued success, the same cannot be said with counterterrorism efforts attacking the promulgation of terroristic messages throughout the internet. The internet is decentralized, provides almost perfect anonymity, it is difficult for authorities apply controls and restrictions, and can be accessed by anyone. Islamic terror networks use this for an advantage in researching and coordinating their attacks, expand the reach of their propaganda, to recruit, to communicate with international sympathizers, and solicit donations (Weimann, 2010). Providing a pertinent

case study Weimann (2010) offers the story of Younes Tsouli more commonly known by his pseudonym "Irhabi007."

Between the years 2003 through 2007 Younes Tsouli used the internet to spread Islamic terrorist's propaganda and organize attacks. At first Tsouli limited himself to joining terrorist internet forums in which he upload and published videos, pictures, and instruction manuals on computer hacking. It was not long before he caught the attention of al-Qaeda. Al-Qaeda wanted Tsouli to provide logistical support for their online operations. By 2005 al-Qaeda placed Tsouli in charge of a forum called al-Ansar. It was on the al-Ansar forum that Tsouli began publishing bomb making instructions and "how-to" instructions for suicide bombing operations. Tsouli was eventually caught, but not before he was able to successfully manipulate the internet for the benefit of al-Qaeda (Weimann, 2009). Furthermore, other internet savvy persons were able to learn from his mistakes.

Posting videos online has become a critical tool for Islamic terror networks strategic communications game plans. For Salem et al. (2008), videos serve several important functions:

> "The organizational sage is emphasized when the viewers replay videos (reinforcement), store images and radical messages (e.g. usage of IEDs), hear expert commentary [dubbed or subtitles in different languages] (suicide attack planning and execution), view interactions (social and emotional support with hugging), in the planning and execution (mega cognitive event), and listen to devoted players in an operational environment (social event)."

The increased availability of sophisticated, easy-to-use, cheap video capturing hardware and editing tools has enabled terrorist networks like Hamas, Hezbollah, and Liberation Tigers of Tamil Eelam (LTTE) to broaden their influence via the Internet. In 2009, LTTE posted of 100 videos alone and has even introduced their own version of YouTube, TamilTube. The videos are not solely aimed at Middle Eastern Muslim youths. Given that many of their videos are dubbed in English or provide English subtitles suggest LTTE is targeting western sympathizers as well (Weimann, 2009).

Network Technologies Used for Operational Means

Not only have network technologies been used for the communication of Islamic terrorist networks strategic purposes but also for operational purposes. Operational purposes may include training videos such as: how to build a bomb, surveillance and reconnaissance techniques, and real footage of actual suicide and attack operations. Such videos serve two purposes, to train and to serve as a learning tool. Using the footage as a learning tool is a vital aspect to the continued success of terrorist attacks. By reviewing footage of operations the terrorists are able to analyze and assess the procedure carried out by the operative. Those analyzing the video footage may assess tactical and procedure errors as well as positives from the operations. Thus, terrorist networks are able to learn from past mistakes and make improvements so as to avoid similar mistakes for future operations.

Other operational means for network technologies help the processes of leading up to an impending operation, during, and after the operation as well. Depicting all three phases may be portrayed by the case of the failed Manchester Plot. The Manchester Plot's central

figure was Abid Neseer, a Pakistani national residing in the United Kingdom. In 2006, Neseer moved to the United Kingdom to study at one of the universities, however, he became disenchanted with his educational pursuits. By 2008, Neseer returned back to Pakistan where he opened an email account under the name humaonion@yahoo.com on November 14. Sixteen days later Neseer started receiving emails from another account opened by a man known as "Ahmad." It was believed that Ahmad was a third party who was passing messages along from the al-Qaeda leader Salah al-Somali. The correspondence between the two email accounts revealed many exchanges of an ongoing discussion of possible 'girlfriends.' British authorities believed 'girlfriends' was a code word for bomb ingredients. By April 2009 the discussion ramped up and security services believed there would be an attack in the middle of the month. The security services quickly acted and arrested Neseer. Upon arresting Neseer and other accomplices police were able to find photos of potential targets and detailed maps of the photographed sites. Police also recovered mobile phones and surveillance footage of the potential targets (Pantucci, 2010).

Policy Recommendations

Corman and Schiefelbein (2006) offer four detrimental aspects the internet poses to the counterterrorism community: the internet is decentralized and is not subject to easy control by authorities, laws have not caught up to the continuously updating formats found within the internet, governments have a difficult time keeping pace with private companies constantly updating technologies for the internet, rapid technologic advancements create new and unpredictable developments. As a result, the internet is extremely advantageous for Islamic terror networks. Counterterrorism authorities are in a tough position trying to keep pace with the continuously advancing internet. Nevertheless, this does not mean effective counterterrorism efforts are impossible.

Abu Musab al-Zarqawi stated "More than half of this battle is taking place in the battlefield of the media. We are in a media battle, in a race for the hearts and minds of Muslims (Bockstette, 2008)." Zarqawi clearly states how Islamic terror networks are trying to tip the asymmetrical conflict in their favor. The counterterrorism community needs to apply their own media battle to win the hearts and minds of those who could be susceptible to the indoctrination of terror networks. Governments considered being enemies of Islamic terror networks should strive to develop their own comprehensive media campaign focused on improving their credibility with the ummah. To restore credibility the West needs to focus on three key factors: highlight the contradictory nature of Islamic terror networks interpretation of the Quran, and continue to erode their communication and media strategies by targeting their media outfits.

Undoubtedly, the most difficult task of the aforementioned policy recommendations is for the counterterrorism community to erode Islamic terror networks' media outfits. The counterterrorism community needs to create a task force comprised of members with in-depth knowledge of information technology systems. This team could work to sabotage Islamic terrorist networks pursuits virtually. Secondly, the counterterrorism community needs to partner up with reputable businesses to create controls on their websites that increase the difficulty of terrorists and their sympathizers from using their websites. For instance, YouTube has been known to put restrictive controls on their site that only allows for certain types of materials to be uploaded and disseminated. Other websites should follow

suit. However, this could prove to be more difficult for email services; often terrorists will create emails using alias and set up accounts using fake personal information. This will continue to prove problematic; however, it may be a worthy effort to research if it is possible to put tighter restrictions on those who look to create new email accounts. One possible measure may be to require individuals who seek an email account to provide more personal information than currently required.

Lastly, and more importantly, it is imperative for the West to establish quality ties with reputable domestics leaders of the Muslim community. Creating strong bonds between the government, law enforcement, and the Muslim community will help to erode the influence and the promulgation of radicals. Having a close working relationship with the Muslim community may help in identifying those who are displaying, or starting to show signs of radicalization. Such individuals need to be identified and brought to the attention to the appropriate law enforcement agencies so they may be monitored.

Conclusion

The 21st century Islamic terror network is a formidable force. The acquisition of a strong strategic approach and the adoption of network technologies have increased the capabilities of jihadis. The modern version of Islamic terrorism has created a truly global network capable of disseminating their ideology, recruiting, carrying out attacks, and fundraising. So long as modern terrorism is able to continue disseminating material in the aim of establishing their goals they will remain a force with which to be reckoned. It is of the utmost importance for Islamic terror networks' enemies to create effective policies to counter the influence of such groups. Undoubtedly, the Islamic terror networks have gained an upper hand in this asymmetrical conflict but the counterterrorism community must start their own effective media campaign. The campaign needs to target current radicalized Muslims and Muslims who have the potential of being radicalized by winning their hearts and minds.

References

Bockstette, Carsten. "Jihadist Terrorist Use of Strategic Communication Management Techniques." *George C. Marshall European Center for Security Studies: Occasional Paper Series*. Nov 2008. <http://www.dtic.mil.library.norwich.edu/cgi-bin/GetTRDoc?AD=ADA512956&Location=U2&doc=GetTRDoc.pdf>

Croft, Stuart and CerwynMoore. "The Evolution of Threat Narratives in the Age of Terror: Understanding Terrorist Threats in Britain." *International Affairs*. 86.4 (July 2010): 821-835.

Corman, Steven R. and Jill S. Schiefelbein. "Communication and Media Strategy in the Jihad War of Ideas." *Consortium of Strategic Communication*. 2006. <http://comops.org/publications/CSC_report_0601-jihad_comm_media.pdf>

Don, Bruce W., David R. Frelinger, Scott Gerwehr, Eric Landree, and Brian A. Jackson. "NetworkTechnologies for Networked Terrorists: Assessing the Value of Information and Communication Technologies to Modern Terrorist Organizations." *Rand Homeland Security Program.* (2007). <http://www.dtic.mil.library.norwich.edu/cgi-bin/GetTRDoc?AD=ADA473460&Location=U2&doc=GetTRDoc.pdf>

Dubowitz, Mark. "Wanted: A War on Terrorist Media." *The Journal of International Security Affairs*, 0.17 (Fall 2009). <http://www.ciaonet.org.library.norwich.edu/journals/jisa/v0i17/09.html>

Pantucci, Raffaelo. "Manchester, New York, and Oslo: Three Centrally Directed al-Qa'ida Plots." *CTC Sentinel*, 3.8 (Aug 2010). <http://www.ctc.usma.edu/posts/manchester-new-york-and-oslo-three-centrally-directed-al-qaida-plots>

Sageman, Marc. *Understanding Terror Networks*. Philadelphia: University of Pennsylvania Press, 2004.

Salem, Arab, Edna Reid, and Hsinchun Chen. "Multimedia Content Coding and Analysis: Unraveling the Content of Jihad Extremist Groups' Videos." *Studies in Conflict & Terrorism*. 31 (2008): 605-626. <http://floodhelp.uno.edu/uploads/Content%20Analysis/Salem.pdf>

Weimann, Gabriel. "Terror on Facebook, Twitter, and Youtube." *Brown Journal of World Affairs*. 16.2 (Spring/Summer 2010): 45-54.