The Journal of Public and Professional Sociology

Volume 6 | Issue 1 Article 2

February 2014

Psychological Operations and Terrorism: The Digital Domain

Rodger A. Bates
Clayton State University, rodgerbates@clayton.edu

Mara Mooney
Clayton State University, maramooney@clayton.edu

Recommended Citation
Bates, Rodger A. and Mooney, Mara (2014) "Psychological Operations and Terrorism: The Digital Domain," *The Journal of Public and Professional Sociology*: Vol. 6 : Iss. 1 , Article 2.
Available at: https://digitalcommons.kennesaw.edu/jpps/vol6/iss1/2

Psychological Operations and Terrorism: The Digital Domain

Cover Page Footnote

This paper was presented at the 2013 Mid-South Sociological Association Meetings in Atlanta, GA.

Introduction:

More than 2,000 years ago in China, Sun Tzu (2005) noted that the highest form of military leadership comes from breaking the enemy's resistance without fighting. In the asymmetric environment of terrorist movements targets are psychological and economic rather than military.

Historically, the application of psychological operations in one form or another has proven to be essential in successfully waging war. In spite of its long history of successful employment, the potential for using the power of persuasion through psychological operations as a force multiplier to achieve group or national objectives has been recognized by only the most perceptive leaders and statesmen (Baker, 2010). Furthermore, since World War II psychological operations (PSYOP*) have come into its own as an effective weapon system and has been employed by combatants and strategists of various nations and ideological groups. Increasingly, the digital domain has emerged as a critical environment in which terrorists and governments have attempted to influence the attitudes and behaviors of target audiences in support of their objectives. (*PSYOP – A term coined by the U.S. Army is plural and similar to the term UN which is plural and stands for the United Nations.)

Psychological Operations:

Psychological Operations are planned to convey selected information and indicators to audiences to influence emotions, motives, objective reasoning and ultimately the behavior of organizations, groups and individuals (Rouse, 2012). Psychological operations have involved a variety of tactics and technologies to influence target audiences (FM 33-1-1, 2003)

A psychological warfare campaign is a war of the mind. PSYOP can be disseminated by face-to-face communication, audio visual means (television), audio media (radio or loudspeaker), visual media or the digital domain. The weapon is not the delivery system, but the message it carries and how that message affects a target audience (Rouse, 2012).

There are three types of psychological operations: tactical, strategic and consolidation activities. Tactical PSYOP is targeted towards specific enemy combat groups to induce them to perform a specific action that will affect the current or short-range combat situation. Aimed at a larger audience, strategic PSYOP involves a carefully planned campaign against a larger target audience. The mission of consolidation PSYOP is to assist the civil and military authorities in consolidating their gains, by establishing and maintaining law and order and by re-establishing civil government in an occupied or liberated area (USDA, 1994). All three types of psychological operations have been employed by both governments and terrorist groups.

Regardless of the type of psychological operations used by governments or terrorist groups, propaganda is a major component of any psychological operations campaign. It is employed to influence various target groups. Modern propaganda is classified as white, gray, or black according to the degree to which the sponsor conceals or acknowledges its involvement (Gray and Martin, 2007). White propaganda is correctly attributed to the sponsor and the source is truthfully identified. Gray propaganda is unattributed to the sponsor and conceals the real source of the propaganda. The objective of gray propaganda is to promote viewpoints that are in the interest of the originator but that would be more acceptable to target audiences than official statements. Black propaganda, on the other hand, camouflages the sponsor's participation. While gray propaganda is unattributed, black propaganda is falsely attributed. Black propaganda is subversive and provocative; it is designed to appear to have originated from a hostile source in order to cause that source embarrassment, to damage its prestige, to undermine its credibility, or to get it to take actions that it might not otherwise pursue (DA-Pam 550-104, 1966).

Regardless of the type of propaganda, practitioners of psychological operations employ a variety of strategies to shape and influence the attitudes and behaviors of their target audiences. Common tactics include assertion (the enthusiastic advertisement of a fact that is not necessarily true but is presented as truth without substantiation), the band-wagon effect (convincing a group that everybody is on their side), the use of glittering generalities (or appealing to the emotions of a target audience through reference to universally pleasing concepts), name-calling, stereotyping and card-stacking (by presenting only one side of a contested issue). The use of testimonials, simplification and attitude transfer also are encountered (Lee and Lee, 1939). These tactics have been refined by social psychologists and specialists in collective behavior.

Terrorism:

As a social construct, terrorism takes place within a given historical and social context (Schmid, 1992). In 1999, the United States Department of State (22 U.S.C. § 2656f(d)) defined terrorism as “premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents, usually intended to influence an audience.” Terrorism enhances the ability of a less powerful group to influence a more powerful group through a variety of tactics related to psychological operations (White, 2012).

Today’s terrorists, both foreign and domestic, increasingly have turned to psychological operations as a significant tool and tactic in their asymmetric struggles. Essentially, terrorism is a communications process designed to influence audiences beyond that of the direct target (Matusitz, 2013). According to Tuman (2003), this process is interactive in which target audiences decode terrorist violence depending on the contexts, methods and tools it has for interpreting the situation. The responses and interpretations by the target audience provide feedback to terrorists. Terrorism is an act, process or plan intended to cause a response. As a violent vehicle for communication, terrorism exploits a variety of mediums.

Modern terror organizations place a high priority on the methods of psychological warfare and how to successfully increase fear within their target audiences (Ganor, 2002). Specifically, media technology as a force-multiplier is a frequently invoked tool of terrorists. Terrorists rely on the media to facilitate and enhance their efforts. Previously, the drama of terrorism has provided attention, recognition and even claims of legitimacy (Alexander and Wilkinson, 1979). Traditionally, newspapers, magazines, pamphlets, posters and other print media were the tools of dissemination. In the electronic age, movies, radio and television emerged as favored means of public influence and persuasion. With the emergence of the digital age, the symbiotic relationship between terrorism and the digital domain has reached a new zenith.

The Digital Domain:

The Internet is particularly well-suited for the spread of ideology to a global audience because communication channels are largely unfettered (Bolechow, 2006; Rothenberger, 2012). According to Weimann (2005), the Internet is an ideal platform for domestic and international terrorists because it affords easy access, minimal regulation and censorship, anonymity of communication, speed, low cost, a multimedia environment to combine text, graphics, audio, video and perhaps most significantly, the ability to shape coverage in the traditional mass media. Specifically, terrorists can bypass existing “selection thresholds” of traditional media to gain public attention by simply posting the controversial content themselves. One example of terrorist propaganda being spread through social media channels is the beheading by Abu Musab al-Zarqawi of an American businessman in Iraq. A video of the murder was uploaded to the Internet by al-Qaeda and was downloaded over 500,000 times within the first twenty-four hours of its online posting. The video with interactive comments is still accessible online (Liveleak.com, 2013).

Propaganda manifests through a vast web of Internet servers in the form of high-definition video productions, social networking sites and treatises that often showcase impassioned, articulate and educated leaders (Shephard, 2013). Popular digital platforms include blogs, Twitter, YouTube, online chat rooms, open and password-protected forums, social networking sites such as Facebook and Google+, photo-sharing sites such as Instagram and Tumblr, and periodicals available in digital and print format. The asynchronous features of social media are particularly attractive because the access and dissemination of material is not limited by traditional notions of time and place (Selwyn, 2011). Social media platforms, such as Twitter and Facebook, for example, have been likened to a “global town square for the digital age” (Kjuka, 2013), reaching over one billion active monthly users (McNaughton, 2013) who share information in a participatory and collective fashion.

For some groups devoted to a singular cause, the dissemination of violent imagery and combative messages has been a popular means through which to incite action for social and political ends (Ganor, 2002; Ryan, Vanderlick, & Matthews, 2006; Schmid, 2005). These strategies recruit new members, educate the public about a group’s ideology, generate fear, obtain financing and organize events that endorse the stated objectives of the group (Freiburger & Crane, 2008). While terrorists, for example, use an amalgam of force, fear and targeted attacks to stay relevant and to make an impression on the public, causing harm is often a secondary result of a terrorists’ primary objective to achieve a political goal (Ryan, Vanderlick, & Matthews, 2006). Therefore, while the substance of these messages is largely consistent, the form of the messages has evolved in the digital age.

The United States Army, the government agency charged with the conduct of most forms of psychological operations, noted that:

> the emergence of the cyberspace domain has created significant opportunities for PSYOP forces to perform mission essential functions ------- by utilizing the emergence of virtual worlds, mirror worlds and life-logging within the —multi-verse□, PSYOP can gain critical access to

> wider audiences leveraging the phenomenal of social influence/facilitation to influence their target audience while providing the target with a level of anonymity that doesn't exist in the physical world (Baker, 2010).

A 2012 study by the United Nations Office on Drugs and Crime identifies the following six areas in which the Internet is used to advance terrorist causes: (1) Propaganda (including recruitment, incitement, and radicalization); (2) Financing; (3) Training; (4) Planning (including secret communication and open-source information); (5) Execution; and (6) Cyberattacks. Examples of these methods are discussed below.

Propaganda: Recruitment, Incitement, and Radicalization

As a group of like-minded individuals who seek to further their cause, jihad at its core is a modern-day public relations machine (Rothenberger, 2012). For example, Al-Qaeda employs a sophisticated media strategy and has utilized more than 4,000 web sites to reach its followers and threaten its enemies (Seib, 2008). Al-Qaeda owns a multimedia production company and released one particularly polished video montage, akin to the type of music video seen on Western television, set to the tune of popular music and featuring a "Top 20" review of graphic images of attacks on U.S. soldiers in Iraq (bestgore.com, 2008; Seib, 2008). United States military may also unwittingly contribute to the incitement and radicalization efforts of terrorists by posing for "trophy" photographs with Iraqi youth corpses and posting these photographs on the Internet. However, according to Weimann (2005), most terrorist-sponsored sites do not taut violent activities, but instead focus on freedom of expression issues designed to elicit sympathy from Western audiences and on the plight of political prisoners to justify terrorists' use of violence in the face of oppression. In *Jihad, Inc.*, Alexiev (2009) notes that propaganda is also used to further a primary goal of extremist Islam to proselytize, indoctrinate, infiltrate and recruit from the West by exploiting the rights and freedoms provided by democracy and by calling into question an individual's belief in certain collective social values.

Twitter, for example, is a popular terrorist platform that is steeped in the spirit of Western free speech ideals. The official Somali al-Qaeda affiliate al-Shabab maintained a popular Twitter handle, @HSMPress, with nearly 21,000 followers, but was administratively disabled in January 2013 for making a specific threat in violation of Twitter's terms of service. Within two weeks, however, a new handle, @HSMPress1, had opened and garnered over 5,767 followers (Twitter, 2013). It appears that disrupting a micro-blog or other social media feed may reduce the number of followers, at least temporarily, but may not have long-lasting effects on the ability of the terrorist organization to re-group and re-brand. The other leading social media platforms for terrorists are YouTube and Facebook, both of which contain videos and other content re-posted from major jihadi forums, such as Shumoukh Al Islam, known as the "New York Times of online jihad," and Jabhat Al Nusrah, the Syrian al-Qaeda affiliate (Verton, 2013). Google, which owns YouTube, has blocked some, but not all, terrorist-related content on its U.S. site, but has not blocked similarly violent content on its overseas platforms.

Lone Wolves and Unlikely Wolves

Terrorists often send messages to stoke anger in marginalized, younger people (Carpenter, Levitt & Jacobson, 2009) who are impressionable, disenfranchised and seeking a cause. (USDOC, 2012). A recent example of virtual recruitment and radicalization of terrorists is that of the accused 2013 Boston Marathon bombers, brothers Tamerlan and Dzhokhar Tsarnaev, whose actions killed three people and injured at least 260. The brothers' radicalization stemmed from watching images and accessing terrorist-related information on the Internet (Guarino, 2013). In 2009, Major Nidal Malik Hasan, who was also radicalized on the Internet, went on a shooting spree on a Fort Hood, Texas military base that killed thirteen people and injured 30, and another Internet self-radicalized terrorist, Umar Farouk Abdulmutallab, known as the Christmas Bomber, attempted to board and detonate an undergarments bomb on a Detroit-bound international flight.

While terrorism is generally associated with young men (Awan, Hoskins, & O'Loughlin, 2011), the digital domain has also provided a venue for the recruitment of female participants who are generally less attracted by messages of violence. For example, in *44 Ways to Support Jihad*, respected leader Anwar Al Awalki, who has been credited with the online radicalization of the Fort Hood shooter and the Christmas Bomber, implores non-violent supporters to disseminate jihadist literature and news through its "WWW Jihad" initiative (Al-Awalaki, 2010). He further encourages "nasheers," Islamic musicians and poets, to expand their audiences beyond Islam by performing in different languages and forums.

Most terrorists possess a controlled hate that is "disciplined, purposeful and intrinsically rewarding" and that is buoyed by their peers (Ryan, Vanderlick, & Matthews, 2006). Individualized interactions involving self-radicalized terrorists stem from the omnipresent deconstructed framework of modern terrorist organizations. This type of "leaderless resistance" has spawned a new generation of lone wolf terrorists who will die for their cause based upon ideological justifications (propaganda) and directions being dispensed from a distance (Bates, 2012). Lone wolves were also responsible for the first major acts of domestic terrorism: a midair plane bombing, product contamination and anthrax attacks (Thomson, 2013).

Financing

Fundraising is an ongoing concern for most organizations. As with most businesses, funds for domestic and international terrorist causes are obtained primarily through direct solicitation from investors and online stores that sell merchandise and accept payment through wire transfer, credit card and PayPal. Outside of traditional reals, money is also raised through the use of stolen identities and credit cards, and through donations made to shell corporations, such as the Benevolence International Foundation and the Global Relief Foundation, which are ostensibly philanthropic organizations that funnel money to terrorist activities (USDOC, 2012). In an effort to stem financing of terrorist activities, a major increase in the area of prosecution in the United States has been for "material support," wherein individuals are convicted for what they may have naively hoped was only tangential activity such as monetary or information donations related to terrorism. Material support for terrorism is defined as a war crime under the Military Commissions Act of 2006 (10 U.S.C. § 950t(25); see also 10 U.S.C. § 950v(b)(25), 2006). According to a report by the New York University School of Law Center on Law and

Security (Greenberg, 2011), the federal government will continue to use an increasingly aggressive interpretation of material support statutes to obtain high conviction rates.

Training

The risks and costs associated with dwindling physical training facilities have contributed to an increase in virtual training grounds for students of terrorism. The Internet has become a vehicle to pair mentor and novice and to serve as a surrogate for traditional in-person encounter; previously unconnected individuals can develop their cultural identities and form social bonds (Schmidle, 2009). In the past, recruits were trained by teachings contained in the ultra-secretive *Encyclopedia of Jihand*, a collection of essays on weapons handling, bomb making, and military training, but the contents of this terrorist training manual, along with *The Terrorists Handbook* and *The Anarchist Cookbook*, are now widely available on the Internet (Weiman, 2005). The availability of online training materials may contribute to the creation of online cells of dissidents who may act in concert or solo. The conviction of Zachary Chesser, a young Virginia man who was admittedly schooled in terrorism techniques by Internet resources and is serving 25 years in prison on terrorist-related charges, is an example of how new models of virtual education are being employed (United States Senate Committee on Homeland Security and Governmental Affairs, 2012). However, doubt exists about the ability of Internet-trained militants to carry out larger scale strikes without formal training in a physical camp, and these formal camps still exist in more remote areas (Coll & Glasser, 2005; Kaplan, 2009).

Al-Qaeda and other organizations now maintain a decentralized set of online universities that do not confer diplomas but whose marketing brochures could boast the following enthusiastic recruiting language published by one student: “Al-Qaida is a university that is decentralized, respects no geographic boundaries and does not exist in any one location. And anyone who loves his religion can register. Praise be to God that the Al-Qaida University graduates [so many] heroes with various specializations.” This testimonial further states, “[t]his university even has various departments: one for electronic jihad, one for jihad against oneself (in other words, to overcome one's own inner resistance), one for the technology of explosives and others!” (Musharbash, 2012) These online training facilities are accessed through semi-centralized, password-protected forums, such as Ansar al-Mujahidin English Forum (AMEF) and the Ansar al-Mujahidin Arabic Forum (AMAF) (Zelin & Fellow, 2013).

Another terrorist training resource is *INSPIRE*, an online magazine that has been published by the al-Qaeda branch in Yemen since 2010 to help Muslim militants train at home. The Tsarnaev brothers ostensibly learned how to make pressure cooker bombs by reading articles in *INSPIRE*, and the Christmas Bomber and his accomplices credit the magazine with providing teaching and training for their mission (Cruickshank & Lister, 2013). The tenth edition of *INSPIRE*, published in March 2013, contained an article that called upon sympathizers in the West to pursue senior former politicians, such as George W. Bush, William Clinton, and Tony Blair, explaining why now is an ideal time to assassinate them (Global Jihad, 2013). An earlier edition of the magazine encouraged American students to open fire on crowded restaurants in Washington, D.C., to massacre U.S. government workers (Global Jihad, 2010).

Planning and Execution

Online communications are not dependent upon personal interactions developed in the traditional sense, and the digital domain plays a key role in the planning and execution of terrorist plots. According to the USDOC 2012 report, almost every prosecuted case of terrorism involved the use of Internet technology and virtual communications among several parties. Some examples of Internet usage by terrorists include translating and encryption of pro-jihadist materials, moderating terrorism-related websites (USDOC, 2012), using GPS mapping programs and photographs in the public domain to identify and study potential structural targets, and studying instructional videos of step-by-step guidance on executing a hostage-taking situation (Coll & Glasser, 2005). In a recent federal conviction resulting in a life sentence, Khalid Ali-M Aldawsari, a Texas resident, was convicted for acquiring ingredients through the Internet to build a weapon of mass destruction, for making violent and martyrdom statements on his blog, and for conducting online research of several potential U.S. targets (U.S. v. Aldawsari, 2012).

Resistance groups' use of data mining, such as accessing GoogleEarth to obtain images of potential sites and researching violent web sites to develop strategy (Verton, 2003), can also be accessed by authorities to thwart plots or amass evidence post-attack. Digital breadcrumbs, or cookies, provide a trail of virtual footprints which identify the Internet Provider addresses that have been accessed and the documents that have been downloaded to and created on a computer hard drive. Information can be recovered from the discs on which data is stored even if the hardware is damaged. Digital breadcrumbs left by Norwegian gunman Anders Behring Breivik, who confessed to killing 93 people, showed a history of attempts to join radical groups on Facebook, a series of online discussion posts and an online journal entry stating, "It would have saved me a lot of hassle if I could just 'borrow' a cup of sugar and 3 kg of C4 from my dear neighbor" (Sullivan & Golijan, 2013).

Cyberattacks

The term "cybercrime" encompasses "any crime that is facilitated or committed using a computer, network or hardware device" in which the computer or the device serves as an agent, facilitator, or as a target of the crime (Gordon & Ford, 2006). A recent example of a PSYOP cyberattack occurred in Israel in 2012 when several symbolic Israeli institutions, such as the country's stock exchange and the national airline, were hacked (USDOC, 2012). These attacks are aimed at targets at a macro- or micro-level through hacking, persistent threats, computer viruses, malware, or "phlooding," (overloading servers), and on a related scale, aiming to destroy or undermine infrastructures or natural resource supplies (USDOC, 2012). One prominent al-Qaeda leader who specializes in teaching poisoning techniques maintains that computer proficiency is a critical component of terrorist education and has published an online manual that instructs prospective students to study the Koran and computers (Coll & Glasser, 2005).

<u>Domestic and Other Online Terrorists:</u>

Jihadists are not the only terrorist groups to have embraced the digital domain, as domestic terrorists also maintain an active online presence. According to Congress:

> Domestic terrorism involves groups or individuals who are based and operate entirely within the United States or its territories without foreign direction, and whose acts are directed at elements of the U.S. government or population. Domestic terrorist groups can represent right-wing, left-wing, or special interest orientations. Their causes generally spring from issues relating to American political and social concerns (18 U.S.C. § 2331).

According to former FBI Director John Lewis, eco-terrorists, such as the Earth Liberation Front, and animal rights terrorists, such as the Animal Liberation Front, are the number one domestic terror threat in the United States (Federal Bureau of Investigations, 2008). Though these groups are often decentralized and have not engaged in larger scale extreme acts of violence, they are listed as significant terrorist groups by the Department of Homeland Security for smaller scale acts of destruction, like torching homes to protest woodland encroachment, and have an active online presence through web sites, blogs and the full array of social media. Another domestic group with a significant digital footprint is the Aryan Nation, a White Supremacist neo-Nazi group in existence since the 1970s, with a Twitter feed and whose website contains pro-racist videos and contact information for a “Minister of Propaganda” (Aryan-nation.org, 2014).

While the above groups have operated under the auspices of some degree of umbrella organization, the anti-abortion movement, however, has spawned a number of web sites which have been linked to self-radicalization and a number of attacks on abortion clinics and practitioners. Emerging in the 1980s, this form of single-issue violence peaked a decade later with numerous bombings, arsons, murders and attempted murder. Though not as prominent as the Timothy McVeigh and Terry Nichols Oklahoma City bombing example, which at its time accounted for 80% of all deaths even caused by domestic terrorism, the anti-abortion movement has continued to manifest itself as a significant source of domestic terrorism (Anti-Defamation League, 2012).

Theoretical Implications:

The digital domain has clearly become an active environment for psychological operations and terrorism. In an attempt to influence both tactical and strategic target audiences, terrorists have sought to influence and mobilize large numbers of individuals. The goal of the collective manipulation of the public through threat or violence creates an opportunity to better understand this process through the study of collective behavior.

Traditionally, crowd behavior has been a primary topic of collective behavior (Le Bon, 1895). The emotional contagion and lack of rationality of the mob evolved into the analysis of the various forms of crowd behavior, as noted by Blumer (1937) in the 1930’s. Orrin Klapp (1972) noted that the existence of systemic tensions and new social definitions create environments conducive to acts of collective behavior. Turner and Killian added the role of norming acts which reflect the adaptation of a new, if only temporary, definition of a situation which occurs during a crisis (Miller, 1985). Finally, Smelser's Value-Added Perspective combined many of these previous perspectives into a series of requisite stages necessary for the emergence of a collective behavior episode (Miller, 1985).

These theoretical perspectives all required structurally conducive situations of physical proximity as a prerequisite for the collective behavior. Historically, they reflected the environment of the mid twentieth century. However, with the advent of the personal computer and its subsequent iterations, the nature of structurally conducive environments has changed. Never has society been so isolated and connected at the same time. The creation of virtual communities requires a re-visitation of the field of collective behavior. Virtual mobilization isolates the individual from external societal controls and may foster a lack of accountability coupled with a cult mentality. For example, crowd swarming has evolved as a result of the ease with which news and information can be shared electronically throughout the world. Structurally conducive environments are no longer physically limited. Technology has made events such as the Arab Spring, a string of decentralized democratic uprisings that occurred in the Middle East and North Africa, with its crowd behavior and emotional contagion, possible (Verton, 2013). Thus the digital domain, with its ability to create virtual communities, has created a new and dynamic environment for the development of a more modern study of collective behavior (Bates, 2013).

The field of collective behavior provides a theoretical environment for increased understanding of terrorism and its use as a tool of psychological operations. Though the field needs to update its perspectives to take into consideration the technological advances which have occurred with the digital domain, it appears that many of the basic premises of the field provide a solid starting point in trying to understand the conditions associated with the manipulation of groups within an online social situation.

Conclusions:

With the advent of the Internet, psychological operators, including terrorists, utilize the digital domain to spread propaganda via videos, web-sites, blogs, tweets and the full array of social media. In addition to the propaganda themes directed at specific target audiences, online environments serve as virtual meeting places for diverse individuals who share a common cause or belief. In a virtual space, the manipulation and mobilization of many is possible.

Terrorists use propaganda to gain attention and notoriety (Maras, 2013). Al Qaeda, FARC, the Earth Liberation Front, Hamas and other extremist groups use their web sites and other online platforms to publicize their attacks and to increase their visibility and perceived power. The digital domain facilitates recruitment, radicalization, training, planning, fund-raising and cyber-attacks.

A study by Ressler (2006) supports the premise that terrorist organizations are among the most omnipresent social networks of this century, with a "widely dispersed, loosely integrated, [and] decentralized" structure. Accordingly, the decentralized nature of terrorist social networks garners heightened attention when coupled with the fact that terrorists do not approach warfare in a traditional sense of combat. According to the Office of Security Technology of the

Transportation Security Administration, jihadi terrorists are embracing digital mediums in an unprecedented manner and emerging as leaders in the field of open-ended warfare (Kunkle, 2012). Policy and decision makers should take into account the strategic psychological damage that can be caused by a counter-terrorism policy that fails to recognize the influence of terror attacks on the morale of innocent citizens and on terrorists (Ganor, 2002).

In seeking to better understand the new environment of psychological operations and terrorism within the digital domain, looking at some of the underlying processes from the collective behavior perspective may provide important insights as to the strengths and weaknesses of the actions of terrorists and those seeking to counter their threat.

To minimize the spread of terrorist ideologies in the digital domain, it is very important that online communities be empowered to self-regulate and to participate in government strategies to reach these ends. Governments must also work to restrict the production of extremist materials and actively create a hostile online environment for extremist perspectives online (Maras, 2013). Counter-terrorism activities must compete more successfully in the digital domain to challenge the messages of terrorists and to provide narratives which discredit terrorists and their causes. In addition, an active cyber-security and cyber-warfare commitment is required to challenge the initial dominance of terrorists in the digital domain.

Some leaders in Western-sympathetic countries and leaders in extremist circles maintain that a digital war is being waged. Ban Ki-moon, Secretary General of the United Nations, has urged that," [t]he Internet is a prime example of how terrorists can behave in a truly transnational way; in response, States need to think and function in an equally transnational manner" (UNODC, 2012). Various jihadist ideologues rely upon historical or religious justifications for engaging in a "media battle." They point to the Prophet Muhammad's sanctioning of various types of warfare and popular online manuals, such as *39 Ways to Serve and Participate in Jihad*, which encourages "performing electronic jihad" as "a blessed field" by which to spread news, defend ideas and reach the people through discussions and computer hacking (Awan, 2010). No longer singularly a physical battle, it has been advocated that superior knowledge (Ressler, 2006) and, according to Pakistani Foreign Minister Hina Rabbani Khar (2013), a unification of the international community, be used to counter terrorist propaganda.

By combining the fields of psychological operations, sociology, collective behavior and communications technology, a deeper understanding of the digital domain and the struggle between the forces of extremism and moderation can be achieved. The development of successful strategies to deal with the new terrorist threat in the digital domain is a critical goal. Without a proactive approach to weighing costs, risks and benefits, we risk the consequences of extremism replacing moderation while governments struggle to address the growing needs of national security and its relationship to liberty and human rights.

References:

Al Awlaki, Anwar (2009) "44 Ways to Support Jihad." Retrieved from http://www.hoor-al-ayn.com/Books/Anwar_Al_Awlaki_-_44_Ways_To_Support_Jihad.pdf.

Alexiev, A. (2009) "Jihad, Inc." Retrieved from http://mashable.com/2013/01/23/state-social-media-propaganda/.

Anti-Defamation League (2012) “Anti-abortion Violence: America’s Forgotten Terrorism.” Retrieved from http://www.adl.org/combating-hate/domestic-extremism-terrorism/c/anti-abortion-violence-americas-forgotten-terrorism-1.html.

Aryan-nation.org (2014) “Aryan Nation World Headquarters.” Retrieved from aryan-nation.org.

Awan, A. (2010) “The Virtual Jihad: An Increasingly Legitimate Form of Warfare.” Retrieved from htt://www.ctc.usma.edu/posts/the-virtual-jihad-an-increasingly-legitimate-form-of-warfare.

Awan, A., Hoskins, A., & O’Loughlin, B. (2011) *Radicalization and Media: Connectivity and Terrorism in the New Media Ecology.* New York: Routledge.

Baker, P. (2010) “Psychological Operations within the Cyberspace Domain”. Unpublished Paper. Air University.

Bates, R. (2012) Dancing with Wolves: Today’s Lone Wolf Terrorists. *The Journal of Public and Professional Sociology, 4*(1). Retrieved from http://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1023&context=jpps.

Bates, R. (2013) “The Evolution of Collective Behavior: A Dramaturgical Presentation” Georgia Sociological Association Annual Meeting. Jekyll Island, Georgia.

Bestgore.com (2013) “Beheading highlights.” Retrieved from bestgore.com/all-the-gore.

Blumer, H. (1937) “Collective Behavior,” in Robert Park (ed.), *Principles of Sociology.* New York: Barnes and Noble.

Bolechow, B. (2006) “Internet As a Flexible Tool of Terrorism.” In T. Pludowski (Ed.), Terrorism, Media, Society (pp. 33-44). Tonrun: Adam Marszalek.

Carpenter, J.S., Levitt, M. & Jacobson, M. (2009) Confronting the Ideology of Radical Extremism. *Journal of National Security Law & Policy, 3*, 301 – 327.

Coll, S. & Glasser, S.B. (2005) “Terrorists Turn to the Web as Base of Operations.” *The Washington Post*, August 7, 2005. Retrieved from: http://www.washingtonpost.com/wp-dyn/content/article/2005/08/05/AR2005080501138.html.

Cruickshank, P. & Lister, T. (2013) “From the Grave, the Cleric Inspiring a New Generation of Terrorists (April 24, 2013). Retrieved from http://www.cnn.com/2013/04/24/us/boston-awlaki-influence.

DA-FM 33-1-1 *Psychological Operations: Tactics, Techniques and Procedures.* Washington, D.C., Department of the Army.

DA-Pam 550-104 (1966) *Human Factors Considerations in Underground Insurgencies.* Washington. D.C., Department of the Army.

Federal Bureau of Investigations (2008) “Putting Intel to Work Against ELF and ALF Terrorists.” Retrieved from http://www.fbi.gov/news/stories/2008/june/ecoterror_063008.

Freiburger, T. & Crane, J.S. (2008) A Systematic Examination of Terrorist Use of the Internet. *International Journal of Cyber Criminology, 2*(1), 309-319.

Ganor, B (2002) “Terror as a Strategy of Psychological Warfare. Retrieved from http://212.150.54.123/articles/articledet.cfm?articleid=443.

Gordon, S. & Ford, R. (2006) On the definition and classification of cybercrime. *Journal in Computer Virology 2*, 13–20.

Gray, T and Martin, B. (2007) Backfires: White, Black and Grey. Journal of Information Warfare. Volume 7, Issue 1.

Greenberg, K.J. (ed., 2011) “Terrorist Trial Report Card: September 11, 2001 – September 11, 2011,” New York University School of Law Center on Law and Security. Retrieved from http://www.lawandsecurity.org/Portals/0/Documents/TTRC%20Ten%20Year%20Issue.pdf.

Guarino, M (2013) "Teenagers, Social Media, and Terrorism: A Threat Level Hard to Assess," The Christian Science Monitor, May 5, 2013, retrieved from http://www.csmonitor.com/USA/Justice/2013/0505/Teenagers-social-media-and-terrorism-a-threat-level-hard-to-assess/(page)/2.

Inspire (2013) "Global Jihad: The 21st Century's Phenomenon: Al-Qaeda New Online English-speaking Magazine." Retrieved from: http://globaljihad.net/view_news.asp?id=1535.

Kaplan, E. (2009) "Terrorists and the Internet." Council on Foreign Relations, retrieved from http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005.

Khar, H.R. (2013) "Pakistani Minister Says Terrorists Using Social Media to Radicalize Populations," Radio Free Europe, January 15, 2013, retrieved from http://www.rferl.org/content/pakistani-foreign-minister-social-media-terrorists/24824901.html.

Kjuka, D. (2013) "When Terrorists Take to Social Media." The Atlantic. February 20, 2013, retrieved from http://www.theatlantic.com/international/archive/2013/02/when-terrorists-take-to-social-media/273321/.

Kunkle, J. (2012) "Social Media and the Homegrown Terrorist Threat." *The Police Chief 79* (June 2012), 22 – 28.

LeBon, G. (1895) *The Crowd.* New York: Viking Press.

Lee, A. and Lee, E. (1939) *The Fine Art of Propaganda: A Study of Father Coughlin's Speeches.* New York: Harcourt and brace.

Liveleak.com (2013), retrieved from http://www.liveleak.com/view?i=299_1320002757.

Maras, M. (2013) *Counterterrorism.* Bartlett, MA: Jones and Bartlett

Martin, G. (2006) *Understanding Terrorism. Challenges, Perspectives, and Issues*. Thousand Oaks: Sage.

McNaughton, M. (2013) "Social Networking Stats: 59% of Top Brands on Instagram, #RLTM Scorecard." Retrieved from http://therealtimereport.com/2013/02/22/social-networking-stats-59-of-top-brands-on-instagram-rltm-scoreboard/.

Musharbash, Y. (2012) *The New Al-Qaida*. Germany: Kiepenheuer & Witsch GmbH, excerpt retrieved from http://www.rickross.com/reference/alqaeda/alqaeda75.html.

Powell, B., Carsen, J., Crumley, B., Walt, V., Givson, H. & Gerlin, A. (2005) "General Jihad." *Time, 166*, 56-59.

Ressler, S. (2006) Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research, *Homeland Security Affairs, II*(2) (July 2006). Retrieved from http://www.hsaj.org.

Rothenberger, L. (2012) Terrorist Groups: Using Internet and Social Media for Disseminating Ideas. *Revista Commmunicare*, 7-23.

Rouse, E. (2012) "Psychological Operations/Warfare." Retrieved from http://www.psywarrior.com/psyhist.html.

Ryan, C., Vanderlick, J. & Matthews, W. (2006) A Paradoxical Analysis of Social Learning Theory as Applied to the Potential Reform of Terrorist Offenders. *Professional Issues in Criminal Justice 2*(1). Retrieved from http://picj.org/vol2_1.aspx.

Schmid, A. (2005) Terrorism as psychological warfare. *Democracy and Security, 1*, 137-146.

Schmidle, R.E. (2009) Positioning theory and terrorist networks. *Journal for the Theory of Social Behavior, 40*(1), 65-78.

Seib, P. (2008) The Al-Qaeda Media Machine. *Military Review*, *88*(3). U.S. Army Command Combined Arms Center. Retrieved from http://www.highbeam.com/doc/1G1-179133572.html.

Selwyn, N. (2011) "Social Media in Higher Education: The Europa World of Learning." Retrieved from http://www.educationarena.com/pdf/sample/sample-essay-selwyn.pdf.

Shephard, M. (2013) Terror Groups Turn to Twitter, Facebook, YouTube to Gain Support, Analysts Say, *National Security Reporter*, February 14, 2013. Retrieved from http://www.thestar.com/news/world/2013/02/14/terror_groups_turn_to_twitter_facebook_youtube_to_gain_support_analysts_say.html.

Stalinski, S. (2013) "The Jihad and Terrorism Threat Monitor." Retrieved from http://www.memrijttm.org/.

Sullivan, B. & Golijan, R. (2013) "Terrorists May Leave 'Digital Breadcrumbs' for Investigators." Retrieved from http://usnews.nbcnews.com/_news/2013/04/21/17852502-terrorists-may-leave-digital-breadcrumbs-for-investigators?lite.

Sun Tzu (2005) *The Art of War – Special Edition.* Translated by Lionel Giles. El Paso, Texas: El Paso Norte Press.

Thompson, M. (2013) The Danger of the Lone-Wolf Terrorist. *Time*, February 27, 2013. Retrieved from: http://nation.time.com/2013/02/27/the-danger-of-the-lone-wolf-terrrorist/.

Tuman, J. (2003) *Communicating Terror: Rhetorical Dimensions of Terrorism.* Thousand Oaks, CA: Sage.

Twitter (2013). Retrieved from https://twitter.com/HSMPRESS1.

United States Code, 10 U.S.C. § 950t(25), 2006.

United States Code, 10 U.S.C. § 950v(b)(25), 2006.

United States Code, 22 U.S.C. § 2656f(d), 1999.

United States Code, 18 U.S.C. § 2331, 1999.

United States Senate Committee on Homeland Security and Governmental Affairs (2012) "Zachary Chesser, A Case Study in Online Islamist Radicalization and Its Meaning for the Threat of Homegrown Terrorism." Retrieved from https://www.hsdl.org/?view&did=701274.

University of Arizona Dark Web Portal (2013) "Artificial Intelligence Laboratory: Dark Web and Geopolitical Web Research." Retrieved from http://ai.arizona.edu/research/terror/.

UNODC: United Nations Office on Drugs and Crime (2012) *The Use of the Internet for Terrorist Purposes.* New York: United Nations.

U.S. v. Aldawsari, U.S. District Court for the Northern District of Texas, June 27, 2012. Retrieved from http://images.politico.com/global/2012/02/aldawsaridefexperts.pdf.

Verton, D. (2013) Terrorists' Use of Web, Social Media Expanding Rapidly. *Homeland Security Today*. February 6, 2013. Retrieved from http://www.hstoday.us/blogs/critical-issues-in-national-cybersecurity/blog/terrorists-use-of-web-social-media-expanding-rapidly/fa6512335287c102954b03e8f2b3c1e2.html.

Weimann, G. (2005) How Modern Terrorism Uses the Internet. *The Journal of International Security Affairs*, Spring 2005 (8). Retrieved from http://www.securityaffairs.org/issues/2005/08/weimann.php.

White, J. (2012) *Terrorism and Homeland Security, Seventh Edition.* Belmont, CA.: Wadsworth.

White, J. (2013) *Terrorism and Homeland Security, Eighth Edition.* Belmont, CA: Wadsworth.

Zelin, A.Y. & Felllow, R.B. (2013) The State of Global Jihad Online. *New American Foundation*. Retrieved from http://www.newamerica.net/sites/newamerica.net/files/policydocs/Zelin_Global%20Jihad%20Online_NAF.pdf.