Cyber Jihad: Terrorists as Knowledge Workers and Cyber Learners

Hwee-Joo Kam, D.Sc.  
Ferris State University

Pairin Katerattanakul, Ph.D.  
Western Michigan University

Greg Gogolin, Ph.D.  
Ferris State University

Abstract. Using multiple case studies approach, temporal analysis, and Social Network Analysis, this study examined the antecedents of knowledge management that drove Cyber learning in Cyber Jihad. By investigating the cases of “Jihad Jane” and “Terrorist 007”, this study discovered that knowledge management was driven by trust, social interaction ties, group identification, reciprocity norms, shared vision, shared language, and community well-being. In addition, personal outcome expectations were the effect, rather than the antecedent, of knowledge sharing among Cyber Jihadists. Furthermore, a high degree of knowledge management expanded the network of Cyber Jihad, enabling Cyber learning across multiple networks and supporting the intuitive learning culture. Hinged on these findings, this study presents counterterrorism strategies and theoretical implications.

Keywords. Cyber Jihad, Knowledge Management, Cyber Learning

Introduction

Terrorists have been using social networking sites to propagate their agendas, educate members on their ideologies, solicit funding, recruit new members, and secure International support (Ariely 2003; Ariely 2008; Rogan 2006). Social networking sites refer to well-known sites such as Facebook and any other sites that facilitate social interaction.

The Internet enables Cyber learning and knowledge management among terrorists, turning them into knowledge workers and Cyber learners (Ariely 2008). Cyber learning denotes online learning supported by online repositories (knowledge database), online media, and
social interaction in online forums (Kam and Katerattanakul 2014). On the other hand, knowledge management pertains to identifying and leveraging the collective knowledge in an organization to increase organizational competitiveness (Alavi and Leidner 2001).

Knowledge is more efficient than any suicide bombs as knowledge constitutes skills, competence, creative thinking, understanding, and integration of insightful information (Ariely 2003). Working with knowledge engenders knowledge management, which, in turn, promotes Cyber learning (Kam and Katerattanakul 2014). Cyber learning is critical as terrorists must learn fast to adapt to the volatile environment (Ariely 2008). Gradually, this nurtures an “intuitive” learning culture in Cyber Jihad (Ariely 2008). Understanding knowledge management in Cyber Jihad will unveil the use of knowledge among terrorists, discover how knowledge management shapes Cyber learning, and examines the intuitive learning culture. However, there are not many studies discussing how terrorists make use of knowledge management and Cyber learning to attain their goals (Ariely 2008). To fill in the gaps, this study investigated the antecedents of knowledge management that drove Cyber learning in Cyber Jihad. Hinged on the knowledge management framework (Chiu, Hsu and Wang 2006), this study ran case studies research on the cases of “Jihad Jane” and “Terrorist 007” followed by Social Network Analysis (SNA) and Temporal Analysis. The research findings then added to the counterterrorism strategies and theoretical implications.

**Literature Reviews**

**Cyber Jihad and Cyber Learning**

Cyber Jihad refers to “the general, often communicative and informative” aspect of the Internet used “by the jihadists for terrorist purposes” (Rogan 2006). Cyber Jihadists, ranging from non-violent, low hacking skills to devastating, strategic information attacks, are heavily motivated by the ideologies of Jihadism. They try to reach out to the audience by spreading propaganda in text, video, and audio format (Rogan 2006). Cyber Jihadists often use the In-
ternet to propagate their agendas, garner International support, solicit funding, recruit new members, communicate within groups, and share information (Ariely 2003, Ariely 2008, Rogan 2006) rather than equating Internet with a “suicide bomb” (Silke 2010). This is because many do not see Internet as an effective weapon to inflict fatal destruction (Silke 2010).

Cyber Jihadists benefit from social networking sites built on the Web 2.0 technology (Rogan 2006). Essentially, Web 2.0 empowers users to collaborate and learn together, develop and share content using various tools and resources, and re-use and organize content based on their preferences and needs (Downes 2006). Hence, Web 2.0 facilitates group learning and collaborative knowledge building to enable Cyber learning (Kam and Katerattanakul 2014). Social networking sites aid learning by storing the knowledge content in the centralized repositories (e.g., online database). In essence, centralized repositories retain collective knowledge derived from the collaborative effort of knowledge building, thereby rendering collective intelligence (Kam and Katerattanakul 2014). Thus, collective intelligence pertains to intelligence stemmed from the collaboration of many individuals (Gruber 2008). Collective intelligence facilitates Cyber learning when users retrieve knowledge from centralized repositories and later study the existing knowledge to gain new understanding (Kam and Katerattanakul 2014).

**Knowledge Management Framework**

Knowledge management identifies and leverages the collective knowledge in an organization to increase its competitiveness (Alavi and Leidner 2001) and to support organizational learning (Kam and Katerattanakul 2014). Knowledge management incorporates knowledge creation, sharing, application, and storage (Alavi and Leidner 2001). Similarly, Cyber Jihadists create, share, apply, and store knowledge. For example, as Cyber Jihadists shared the instructions for making bomb (knowledge sharing), other members would read the instructions to produce bombs (knowledge application); and meanwhile, some might just study the same
instructions (Cyber learning) stored in the online database (knowledge storage) and discover a better way to improve bomb production (knowledge creation).

A prior study proposed a theoretical framework (see Figure 1) of the antecedents of knowledge sharing in virtual communities (Chiu, Hsu and Wang 2006). Our study adapted this framework to analyze knowledge management and Cyber learning of Cyber Jihad by proposing that the same set of antecedents propels knowledge management of Cyber Jihad. The framework integrates two theories (Chiu, Hsu and Wang 2006): Social Capital Theory (Coleman 1988) suggests that the dynamic of relationships and resources embedded in the relationships affect knowledge sharing; and Social Cognitive Theory (Bandura 1982) posits that outcome expectations affects knowledge sharing (Chiu, Hsu and Wang 2006). Building on the Social Capital Theory, the framework captures three dimensions: the structural, the relational, and the cognitive dimensions (Nahapiet and Ghoshal 1998). Also, the Social Cognitive Theory presents outcome expectations constituting personal and community-related outcomes (Bandura 1982). Similarly, the adapted framework used in this study includes the three dimensions and the outcome expectations as shown in Figure 1. The definition of each component (e.g., social interaction ties, reciprocity norms, personal-related outcome) is discussed in the following subsection.

**Fig. 1. Knowledge Management Framework (Adapted from Chiu, Hsu and Wang 2006)**
Case Study Research

Case study approach discovered “how” and “why” (Yin 2003) knowledge management and Cyber learning occurred in Cyber Jihad. Particularly, this study adopted multiple case studies because cross case analysis (1) enables juxtaposition of all cases, stopping researchers to hastily draw conclusion through pattern searching and data comparison; and (2) allows researchers to examine the subtle similarities and differences between cases, thus dismantling simplistic frame for sophisticated understanding (Eisenhardt 1989).

Good case studies should contain frameworks (Yin 2003) so we adapted a priori framework (see Figure 1) to guide us on data collection and analysis. Although case studies are applicable for theory testing (Lee 1989), our intention was not to test the framework but we inductively elaborated the framework through emerging themes (Eisenhardt 1989). Finally, we collected data from news reports and court records of the United States District Court. Realizing that news reports may contain biases, we validated the data collected with more than one sources and did not include journalist’s interpretation into our study.

Case Study 1: Jihad Jane

Colleen R. LaRose (aka “Jihad Jane”), a former prostitute and drug addict, radicalized after watching YouTube videos that showed the killing of Palestinian children (Shiffman 2012). She met a man online whose username was “Eagle Eye”. He lured LaRose to travel to Sweden to kill Lars Vilks, a Swedish cartoonist who angered the Muslim community by drawing the Prophet Mohammad’s head on a dog (The United States District Court for the Eastern District of Pennsylvania 2010). This case also involved:

- Mohammed H. Khalid (aka Hassan), 19: Khalid, a permanent resident of the United States, emigrated from Pakistan at 14. He became an honor student in a high school in Maryland. At 16, he supported LaRose’s activities of Jihad (Shiffman 2012).
• Jamie P. Ramirez (aka Jihad Jamie), 34: Ramirez, a single mom from Colorado, established an online friendship with LaRose. Upon meeting Ali Damache online, she agreed to join his Jihad and travel to Ireland to marry him (Shiffman 2012).

• Ali C. Damache (aka “Black Flag”), 47: Born in Algeria and raised in France, Damache immigrated to Ireland in his late 30s. He persuaded LaRose and Ramirez to join him in jihad in Waterford, Ireland. Later, he married Ramirez (Shiffman 2012).

• Eagle Eye: “Eagle Eye” was an online username used by an alleged al-Qaeda operative from Pakistan. U.S. authorizes accused him of keeping LaRose in touch with Damache and commanding her to kill Lars Vilks (Shiffman 2012).

Case Study 2: Younes Tsouli

In 2005, Younes Tsouli, a 22-year-old Morocco-born West Londoner and son of diplomat, was suspected of participating in an alleged bomb plot and working as an online recruiter for the Al-Qaeda. His online name was Irhabi007. Irhabi means terrorist in Arabic (Site Institute 2006). He connected with terrorists from Sweden, Canada, and USA. Since 2004, Tsouli became a member of the password protected al-Qaeda affiliated online forum known as Muntada al-Ansar al-Islami (Islam Supporters Forum) and al-Ekhlas (Sincerity) (Site Institute 2006). Gradually, he earned a reputation as a computer expert (Site Institute 2006). In July 2004, Tsouli hacked an FTP server run by the Arkansas Highway and Transportation Department to upload dozens of jihadist video files (Smith and Destint 2007). Around summer 2005, Tsouli stole people’s credit card identities to pay for better Web hosting services (Site Institute 2006). He worked with his accomplices - Waseem Mughal, 24, from Kent and Tariq al-Daour, 21, from West London (Krebs 2007). They made more than $3.5 million in fraudulent charges by stealing credit card accounts via phishing scams (Krebs 2007).

Multiple Case Studies Analysis
Identification is a sense of belonging and positive feeling that engenders loyalty and citizenship (Bagozzi and Dholakia 2002), creating support for knowledge sharing (Chiu, Hsu and Wang 2006). On December 8, 2008, an unidentified online user (John Doe) emailed Colleen R. Larose, asking her to wage Jihad and become a “shahed” (martyr), which she agreed (The United States District Court for the Eastern District of Pennsylvania 2010). Again, on January 2, 2009, Ali Damache advised her to become a martyr (The United States District Court for the Eastern District of Pennsylvania 2010). These requests enabled LaRose to shape positive affiliation with the Cyber Jihadist’s group. She then used words like “ummah” (Muslim community) and “kufar” (non-believer) to connect with the Jihadist’s group (The United States District Court for the Eastern District of Pennsylvania 2010). Gradually, LaRose formed identification with the group.

In the second case study, on April 25, 2004, Younes Tsouli was the first one to reply to an online post made by Abu Maysara, the official spokesman of Abu Musab al-Zarqawi (an insurgent leader in charge of beheading) (Site Institute 2006). Tsouli offered words of support and Maysara responded in a similar fashion (Site Institute 2006). This event showed that Tsouli was noticed by a prominent member of Jihad, enabling him to shape a positive affiliation with the Cyber Jihadist’s group. Eventually, Tsouli formed identification with the group and began serving the group by hacking into the FTP server operated by the Arkansas Highway Department for uploading dozens of jihadist videos (Site Institute 2006).

Social Interaction Ties signify the power of the relationships and the amount of time invested and communication regularity among members (Chiu, Hsu and Wang 2006). Strong social interaction ties support knowledge sharing (Chiu, Hsu and Wang 2006). Colleen R. LaRose built an online friendship with Jamie P. Ramirez. On July 30, 2009, Ramirez emailed LaRose, saying “you need to talk to me urgently. What is going on sister?” (The United States District Court for the Eastern District of Pennsylvania 2011). Then, on August 1, 2009,
they chatted before LaRose left for Europe (The United States District Court for the Eastern District of Pennsylvania 2011). LaRose told Ramirez that “When our brothers defend our faith [and] their homes, they are terrorist. Fine, then I am a terrorist and proud to be this” (The United States District Court for the Eastern District of Pennsylvania 2010). This proved that the social interaction ties between LaRose and Ramirez enabled LaRose to share her personal knowledge on terrorism.

In the second case, around July 2004, Tsouli established a relationship with Abu Maysara (Corera 2008). They communicated online regularly and Tsouli helped Abu Maysara to find the storage space to upload the online video of Al-Zarqawi’s (Corera 2008). This case shows that social interaction ties facilitate knowledge storage.

**Norm of Reciprocity** or mutual reciprocity justifies the time and effort that members spend in a virtual community (Chiu, Hsu and Wang 2006). Additionally, mutual reciprocity engenders knowledge sharing (Chiu, Hsu and Wang 2006). On July 17, 2009, the Federal Bureau of Investigation (FBI) questioned Colleen R. LaRose, asking her about her involvement in Cyber Jihad (The United States District Court for the Eastern District of Pennsylvania 2010). She lied to the FBI and later informed the other Cyber Jihadists about her FBI visit, urging them to delete any online posts that would incriminate them (The United States District Court for the Eastern District of Pennsylvania 2010). On July 19, 2009, Ali Damache reciprocated, stating: “We’re willing to die in order to protect her no matter what the risk is” (The United States District Court for the Eastern District of Pennsylvania 2010). This evidence demonstrated that LaRose’s efforts was recognized and rewarded, encouraging her to share more information. After that, she shared the information of online recruiting with other Cyber Jihadists (The United States District Court for the Eastern District of Pennsylvania 2010). In the second case, Tsouli shared his computer knowledge to educate other Cyber Jihadists on video posting and anonymous browsing (Site Institute 2006). In August 12, 2004, he was
praised by a senior member of Al-Ansar forum for his good work (Site Institute 2006):

“....Our brother Irhabi 007, you have shown very good efforts in serving this message board... we ask God to keep you in his care...” (Site Institute 2006). The praise reciprocated Tsouli’s efforts, deepening his commitment in knowledge management of Cyber Jihad. He later became the administrator of al-Ansar, a password-protected web forum for sharing knowledge about the production of explosive devices (Site Institute 2006).

**Shared Vision** enables organizations to integrate resources and the collective goals of their members (Chiu, Hsu and Wang 2006). Members who share the same vision are more willing to share knowledge for reaching their common goals (Chiu, Hsu and Wang 2006). Colleen R. LaRose and “Eagle Eye” conspired in the murdering plot of Lars Vilks. On February 20, 2009, LaRose, emailed “Eagle Eye” to state that her white skin and green eye would allow her to “blend in with many people” (The United States District Court for the Eastern District of Pennsylvania 2010). “Eagle Eye” then shared his way of murder, wanting her to stab Lars Vilks six times in the chest (Shiffman 2012). That is, knowledge sharing occurred when both LaRose and “Eagle Eye” shared their same vision of Jihad. LaRose shared her look and “Eagle Eye” shared his way of murdering Lars Vilks.

This study also found evidences supporting that shared vision fostered Cyber learning. With the shared vision of murdering Lars Vilks, LaRose conducted online searches to learn more about Lars Vilks on September 3, 2009 (The United States District Court for the Eastern District of Pennsylvania 2010).

The second case study also showed the shared vision of propagating Jihadism. On February 15, 2005 (Steele 2007), Tsouli received the following message: “We are 45 doctors and we are determined to…take the battle inside damaged America...our experience of preparing car-bombs is zero” (Smith and Destint 2007). Tsouli then emailed them the instructions of making car bombs (Steele 2007) to share knowledge. This demonstrated that the shared vi-
sion of propagating Jihadism between Tsouli and the doctors propelled knowledge sharing.

Also, learning occurred as these doctors learned how to make car bombs as they shared the common goal of attacking the United States.

**Shared Language** refers to coded language (Chiu, Hsu and Wang 2006). It facilitates understanding among members and helps constructing common vocabulary in their domains (Chiu, Hsu and Wang 2006). Shared language also facilitates knowledge sharing through the efficiency of communication (Chiu, Hsu and Wang 2006). The first case showed the use of coded language - “packages” - to infer the U. S. passports stolen by Colleen R. LaRose from her boyfriend. LaRose later mailed the passports to Mohammad H. Khalid (The United States District Court for the Eastern District of Pennsylvania 2011). On August 4, 2009, Ali Damache emailed Khalid, asking Khalid to use a “fake name” to send him the “packages” (The United States District Court for the Eastern District of Pennsylvania 2011). Khalid understood the coded language and mailed the passports to Damache (The United States District Court for the Eastern District of Pennsylvania 2011), showing that shared language facilitated information exchange about the delivery of passports.

In the second case, on April 2005, Younes Tsouli communicated with two American Jihadists named Ehsanul I. Sadequee and Syed H. Ahmed (The United States District Court for the Northern District of Georgia 2008). The district court of Northern Georgia reported that they “used coded language…to evade surveillance” (The United States District Court for the Northern District of Georgia 2008). Coded language also supported knowledge sharing and storage in that Sadequee sent Tsouli video clips of federal buildings in Washington D. C. for storage (The United States District Court for the Northern District of Georgia 2008).

**Trust** exists as members in a virtual community adhere to the firm values and norms (Chiu, Hsu and Wang 2006). Trust is an antecedent of knowledge sharing (Bock et al. 2005). The court records revealed that Colleen R. LaRose and “Eagle Eye” communicated online be-
tween 2008 and 2009 (The United States District Court for the Eastern District of Pennsylvania 2010). Without meeting “Eagle Eye” in person, LaRose followed his order to kill Lars Vilks (The United States District Court for the Eastern District of Pennsylvania 2010). We argued that trust culminated when she flew to Amsterdam on August 23, 2009 to train to kill (The United States District Court for the Eastern District of Pennsylvania 2010) because she trusted “Eagle Eye” up to the extent that her belief turned into action. LaRose trusted “Eagle Eye” so she accepted the knowledge transmitted to her from “Eagle Eye” and performed real-life actions accordingly.

Likewise, in the second case, Younes Tsouli, Waseem Mughal, and Tariq al-Daour had never met in person. In summer 2005, they stole credit cards via phishing scams and used at least 72 stolen cards to buy better web hosting (Krebs 2007). They made more than $3.5 million in fraudulent charges (Krebs 2007). As trust enables cooperation among members (McAllister 1995), it would be impossible to run such a massive credit card fraud without good cooperation built on trust. In this case, trust promoted knowledge application supporting good cooperation through a coordination of fraudulent activities.

**Personal-related outcome** or sense of self-worth denotes the extent to which individuals feel good about themselves based on their competence, power, or efficacy (Gecas 1971), thus attributing to personal outcome expectations (Chiu, Hsu and Wang 2006). Personal-related outcome or sense of self-worth was hypothesized to support knowledge management as shown in the knowledge management framework in Figure 1; however, no significant effect was found (Chiu, Hsu and Wang 2006). In contrast, our multiple case study analysis suggested the contrary. That is, components of knowledge management (e.g., knowledge sharing) could increase sense of self-worth among Cyber Jihadists.

Colleen R. Larose shared the information that her green eyes and white skin would allow her to blend into the Western countries (The United States District Court for the Eastern District
of Pennsylvania 2010). Later, she was picked by “Eagle Eye” to murder Lars Vilks. On September 30, 2009, she emailed “Eagle Eye”, telling him that it was “an honour & great pleasure to die or kill for” him (The United States District Court for the Eastern District of Pennsylvania 2010). This inferred that LaRose earned the honor of getting chosen to become an assassin. That is, her sense of self-worth was resulted from her knowledge sharing.

In the second case, Tsouli became a notorious Cyber Jihadist from his successful attempt of hacking into the FTP server (owned by the state of Arkansas) for storing and sharing Jihad videos (Corera 2008). Then, on September 6, 2005, the New York Post published an article entitled “U.S. Shaken by Qaeda 007”, presenting the Cyber threat posed by Tsouli whose identity still remained unknown (Lathem 2005). Tsouli kept a cutting of the article (Corera 2008). His decision to keep the article suggested his good feeling related to sense of self-worth caused by his efforts of enabling knowledge storage and sharing.

Community-related outcome or community well-being refers to one’s judgment about the possibility of attaining one’s ideal outcomes of knowledge sharing on the community (Chiu, Hsu and Wang 2006). In short, the expectation of enhancing community well-being could promote knowledge sharing (Chiu, Hsu and Wang 2006). On August 11, 2009, Mohammed H. Khalid helped the community to recruit by sharing his questionnaire. In the questionnaire, he stated “Are you a European citizen and do you live in Europe? Do you have a European passport?” (The United States District Court for the Eastern District of Pennsylvania 2011). He emailed the questionnaire to Colleen R. LaRose, wanting her to forward the message (The United States District Court for the Eastern District of Pennsylvania 2011). This exemplified attempts of serving the Jihadist’s community by sharing the knowledge of recruitment.

In the second case, on June 25, 2005, Younes Tsouli posted a long message entitled “Seminar on Hacking Websites” in the Ekhlas forum to educate Cyber Jihadists on hacking into the legitimate sites so that they could upload extremist’s videos (Site Institute 2006). Tsouli’s
effort of knowledge sharing was meant to help the Jihadist’s community to propagate Jihadism via online videos. This suggested that Tsouli’s expectation of improving community well-being encouraged his knowledge sharing.

Temporal Analysis

Temporal analysis sequentially presents a storyline of events through chronological order of events (Chow et al. 2007). Crime investigators adopt temporal analysis to study the trend of crime over time so that they could identify the crime patterns (Chow et al. 2007). Using IBM Analyst’s Notebook, we drew temporal charts to rebuild the sequential events in each case to discover the similar temporal patterns emerged in both case studies. This would then enable us to augment the findings of case studies. A temporal chart had events and actors. Each event, called event frame entity, had a date and a brief description. Each event frame entity was linked to all the actors involved. For example, in the event dated December 8, 2008, an unidentified online user (John Doe) emailed Larose, asking her to wage Jihad and become a “shahed” (martyr) (The United States District Court for the Eastern District of Pennsylvania 2010); this event was shown as an event frame entity in the temporal chart (see Figure 2 below).

**Fig. 2. Event Frame Entity and Actors**

Then, each event frame entity was mapped to an antecedent of knowledge management based on the multiple case study analysis discussed in the aforementioned subsection 3.3. For example, according to the discussion in the multiple case study analysis, the event frame entity
in the Figure 2 suggested that LaRose formed identification with the Jihad group; thus, this *event frame entity* was mapped to the “identification”, an antecedent of knowledge management as shown in the following Figure 3.

**Fig. 3.** Mapping an Event Frame Entity to an Antecedent

The temporal charts for the case study 1 and case study 2 are shown in the following Figure 4 and Figure 5, respectively. By comparing these two temporal charts, we could identify similar temporal patterns that emerged in both cases. We discovered that identification surfaced at the beginning of the timelines in both cases but trust showed up at the end. Also, trust emerged after social interaction ties, reciprocity norms, shared language, and shared vision in both cases as well.

**Fig. 4.** Temporal Chart for Case Study 1
To highlight the social networks of both cases, this study adopted Social Network Analysis (SNA). SNA studies the relationships among actors within a network by analyzing relational patterns of nodes (actors) and relations (ties) (Hulst 2009). SNA describes network of relations, detects prominent patterns in networks, and discovers the impacts on these relations on organizations (Hulst 2009), making it appropriate to track terrorist network. In this study, we used IBM Analyst’s Notebook for SNA.

We collected additional data from the Homeland Security reports (Majority and Minority Staff of Homeland Security and Governmental Affairs 2012) to include actors who were not initially mentioned in the two case studies so as to provide a more comprehensive view of social network in each case. This would then help us to compare the complexity of network structure between cases. For example, in the social network chart for the first case study (see Figure 6), an external network is linked to a convicted Jihadist named Emerson Begolly whose direct contacts were several American Jihadists, including LaRose, Khalid, and
The social network chart for the second case study (see Figure 7) exhibits that Younes Tsouli was directly linked to 7 external networks including Abu Maysara (the official spokesman of Abu Musab al-Zarqawi), Mirkad Bektasevic (Sarajevo Al-Qaeda), the “Toronto 18” (18 Jihadists from Canada), Ehsanul I. Sadequee (American Jihadist), Syed H. Ahmed (American Jihadist), Aabid H. Khan (British Jihadist), a group of 45 doctors and the Al-Qaeda (Krebs 2007; Latham 2005; Site Institute 2006, Smith and Destiny 2007). Moreover, both “Eagle Eye” from the first case and Tsouli from the second case linked to the Al-Qaeda. Therefore, we could combine the social network charts of both cases to yield a comprehensive social network as shown in the Figure 8 below.

Finally, in SNA, network centrality is a key concept that reflects the nature and level of connectedness among actors (Hulst 2009). Thus, in the comprehensive social network, we assessed the centrality of (1) degree to identify the actor with high direct links to other actors (Freeman 1979), (2) betweenness to identify the actor who played a center role in facilitating
communication flow (Freeman 1979), (3) closeness to identify the actor who had quicker access to the other actors (Freeman 1979), and (4) eigenvector to identify the well-connected actor with direct influence on other actors (Bonacich 1987).

Table 1 outlines the top 5 players in the comprehensive social network. Younes Tsouli from the second case ranked #3. Interestingly, although Colleen R. LaRose was a key player in the first case, she did not show up among the top 5 players.

Fig. 7. Social Network Chart for Case Study #2

Fig. 8. Comprehensive Social Network Chart
Table 1. Top 5 Players in the Comprehensive Social Network

<table>
<thead>
<tr>
<th>Rank</th>
<th>Case #</th>
<th>Actors</th>
<th>Betweenness</th>
<th>Closeness</th>
<th>Degree</th>
<th>Eigenvector</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1 &amp; 2</td>
<td>Al-Qaeda</td>
<td>100.00%</td>
<td>100.00%</td>
<td>8</td>
<td>52.75%</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>Anwar al-Aulaqi</td>
<td>49.18%</td>
<td>81.87%</td>
<td>7</td>
<td>11.64%</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>Younes Tsouli</td>
<td>46.97%</td>
<td>86.42%</td>
<td>13</td>
<td>100.00%</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>Eagle Eye</td>
<td>44.60%</td>
<td>81.87%</td>
<td>5</td>
<td>13.13%</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>Abu Musab al-Zarqawi</td>
<td>40.41%</td>
<td>76.92%</td>
<td>10</td>
<td>19.49%</td>
</tr>
</tbody>
</table>

Discussion, Conclusion, and Implications

This study adopted the knowledge management framework (Chiu, Hsu and Wang 2006) to analyze multiple case studies related to Cyber Jihad. We found that (1) social interaction ties fostered knowledge sharing among Cyber Jihadists; (2) identification, reciprocity norms, and trust established that Cyber Jihadists met online to seek friendship, support, and sense of belonging (Andrews, Preece, Turoff 2002) other than sharing knowledge; (3) shared vision drove knowledge sharing and Cyber learning; that is, as Cyber Jihadists shared the same vision of propagating Jihadism, they shared knowledge to support their learning; (4) shared language aided information exchange among Cyber Jihadists; and (5) Cyber Jihadists shared knowledge to benefit the Jihad community. Finally, results of the multiple case study analysis suggested that knowledge sharing could lead to sense of self-worth. This result could be corroborated by the results in temporal analysis wherein sense of self-worth appeared at the end of the timelines in both cases (see Figure 4 and 5).

Additionally, results of temporal analysis suggested that Cyber Jihadists first formed identification with the online community before investing in knowledge management. Also, in both cases, trust emerged after social interaction ties, reciprocity norms, shared language, and shared vision. These results were consistent with those in the prior studies in that personal connections, shared vision, and shared language generate trust (Abrams, Cross and Levin 2003) and that reciprocity predicts trust (King-Casas et al. 2005).
Finally, other than revealing the top players in the social network of Cyber Jihad, SNA shed light on the effect of knowledge management in the social network. That is, in Cyber Jihad, active investment in knowledge management would promote Cyber learning and eventually expand its social network. For example, Tsouli in the second case actively facilitated knowledge management in Cyber Jihad. First, he shared knowledge about hacking (Site Institute 2006) to enable other members applying the knowledge (knowledge application). Next, Tsouli enriched the knowledge database (centralized repositories) by contributing knowledge from his computer expertise. He also stored the same contents in many servers (Site Institute 2006) so that if one of the servers crashed, the other servers would still be up for video uploads (knowledge storage) and video search (knowledge retrieval). Gradually, Tsouli became a “hub” of Cyber Jihad’s knowledge management and learning. His network expanded and connected to 7 different external networks. In contrast, Colleen R. Larose from the first case had much less involvement in knowledge management so she connected to only one external network.

For theoretical implications, this study elaborates the knowledge management framework (Chiu, Hsu and Wang 2006) in that (1) shared vision, shared language, social interaction ties, and reciprocity norms determine trust in Cyber Jihad; and (2) sense of self-worth ascribed to personal outcome expectations is the effect, rather than the antecedent, of knowledge sharing among Cyber Jihadists. Additionally, this study adds to the notion of “intuitive” learning culture in terrorism (Ariely 2008). That is, the “intuitive” learning culture is supported by shared vision and active knowledge management for network expansion. Consequently, this empowers Cyber Jihadists to hone the necessary skills with ease given individual’s motivation to learn and easy access to knowledge resources.

This study also proposes three counterterrorism strategies. First, the intelligence community should minimize individual’s identification with Cyber Jihad by discrediting jihadists who
claimed to hold prominent positions so as to prevent newcomers from building associations with the powerful figures. Second, as trust facilitates knowledge sharing (Bock et al. 2005), authorities may want to dismantle trust building by diluting reciprocity norms which are the predictor of trust (King-Casas et al. 2005). To deter reciprocity norms, authorities could first acknowledge an individual’s effort of knowledge sharing to develop social interaction ties and gain the individual’s acceptance followed by doubting the individual’s quality of knowledge sharing. Third, the intelligence community should degrade knowledge quality by injecting contradictory messages as knowledge in poor quality will not support effective knowledge management for Cyber learning and network expansion.

References
Mandak, J 2013.: Emerson Begolly Sentenced to 8 1/2 Years For Promoting Terrorist Attacks on American Soil. Huffington Post.
The United States District Court for the Eastern District of Pennsylvania. 2010. United States of America V. Colleen R. Larose, a/k/a “Fatima LaRose,“JihadJane”.