Awareness Through Agility: Teenagers as a Model for Terrorist Development of Situational Awareness

Mr. Matthew J. Sheffer
Northrop Grumman Information Technology – Intelligence Group (TASC)
Defense Threat Reduction Agency
ATTN: NTT/Matthew Sheffer
8725 John J Kingman Road STOP 6201
Fort Belvoir, Virginia 22060-6201

ABSTRACT

What do terrorists, teenagers, and the individual soldier have in common? The need for agile communications in their tactical operations.

The agility exercised by teenagers in gathering situational awareness is a model for how insurgent terrorists communicate on the battlefield. Tactical decision making by Allied commanders is slowed by the application of strategic situational awareness concepts in tactical environments. Currently, tactical situational awareness is developed and transferred to the strategic common operational picture. Alternatively, the teenage communications model provides an evolutionary concept of operations for Allied forces to develop a highly flexible tactical situational awareness in urban environments leveraging commercial technologies and infrastructure. The forced technical interoperability between the tactical and strategic operations center hinder agility at the tactical level. The strategic/tactical model must be changed in the defense against terrorism. Allied forces must be able to keep pace with the enemy's rapid planning-and-attack cycle. By leveraging the teenage model to improve the flexibility and speed at which information is provided to the urban warfare environment we can, and must, change the "Cold War" communication paradigm. This paradigm shift will allow for tactics, techniques, and procedures (TTPs) to be developed more quickly which is critical in the urban warfare environment. Teenagers use situational awareness to make decisions regarding their interpersonal relationships in much the same way that military and civilian leadership make decisions. By using commercially available, collaborated and highly resilient communications capabilities, both teenagers and terrorist insurgents are able to develop situational awareness in an unconstrained manner. This paper will present possible solutions to merging agility with the necessary strategic/tactical secure infrastructure to gain urban warfighting superiority. Defeating terrorist insurgents will require that Allied commanders develop situational awareness in a way as efficient and agile as teenagers and terrorist insurgents.

1.0   INTRODUCTION

Effective situational awareness is essential to battlefield management. Terrorists, teenagers, and the individual soldier all require effective situational awareness to conduct operations. Terrorist situational awareness evolves through the use of covert communications. Given that there are a finite amount of communications methodologies that exist, it should be possible to discover how terrorists communicate without needing to know much about the content or the sender-recipient pair. Using the teenage communications paradigm as a model, it is possible to discover the communications methodologies being employed by terrorists. This understanding of how terrorists exchange information will give coalition forces the ability to respond more effectively by developing coalition strategic objectives that improve the likelihood that tactical situational awareness results in improved defences against terrorism. In order to defend against

terrorism coalition forces must be able to gain situational awareness faster than terrorist elements. Effective action depends on situational awareness.

2.0   THE TEENAGE COMMUNICATIONS PARADIGM

Teenagers are defined as youth between the ages of 13 and 19 (inclusive), however in American culture this label can be placed on youths as old as 21 or 22. Teenagers form unique social groupings that are often held together by both paranoia and friendship. Paranoia causes a teenager to gather a consistent stream of situational awareness regarding the members of their clique so that the motives of other members can be discerned and reacted to. Intelligence, often both actual and imagined, causes teenagers to constantly readjust their tactics, techniques, and procedures (TTPs). For teenagers situational awareness shapes the day-to-day structure of their social group.

While they may be unaware, teenagers perform every action in the intelligence cycle[1] in order to produce the situational awareness required. The teenage communications paradigm is primarily concerned with the collection aspect of the intelligence cycle. In order to collect situational awareness teenagers use two technological tools – computers and cell phones – as well as human intelligence gathered through daily interactions with those around them.
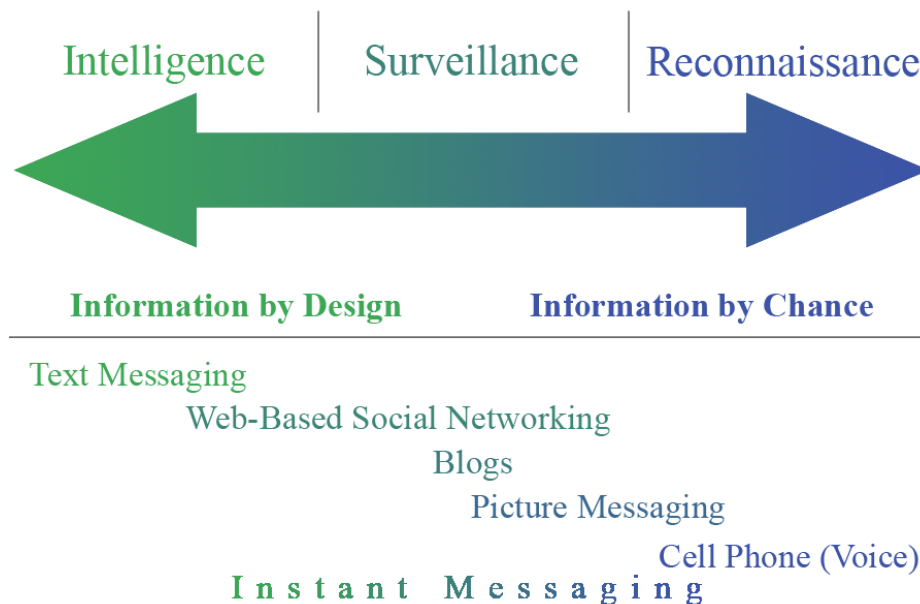
Intelligence | Surveillance | Reconnaissance

Information by Design   **Information by Chance**

Text Messaging
Web-Based Social Networking
Blogs
Picture Messaging
Cell Phone (Voice)
Instant Messaging

**Figure 1: Identifying teenage situational awareness technology by the type of intelligence
"operation" that it can be used for.**

It is also important to realize that teenagers primarily distribute information horizontally. By horizontally disseminating situational awareness a teenager is able to have a greater perception of their surroundings without having to request information from "higher headquarters." Unlike the military, there is very little resistance to the flow of information between independent elements due to the fact that vertical information distribution is essentially non-existent.

---

[1] Central Intelligence Agency, "The Intelligence Cycle," [http://www.cia.gov/cia/ciakids/who_we_are/cycle.shtml], April 2006.
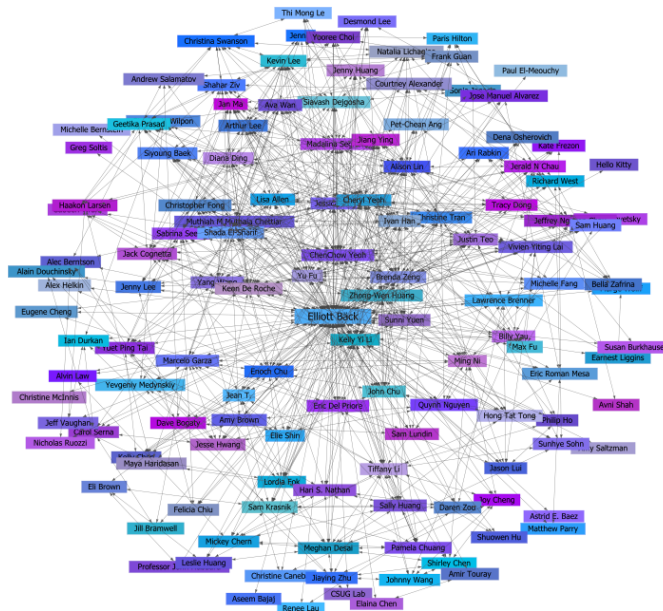
**Figure 2: A large social network as seen on Facebook. The user requesting this diagram is located
in the center of the sphere and the nodes with the fewest links are on the outer edge.**

2.1 Computer Based Situational Awareness

Computers have become an important resource in situational awareness development by teenagers. So called "Social Networking" sites such as MySpace and Facebook have permanently changed the way in which teenage cliques are organized and managed. Social networking over the Internet allows for effective information gathering and denial-and-deception operations. Web logs, or blogs, have also become an integral part of information dissemination and collection. Internet sites such as Blogger, LiveJournal, and Blogspot leverage advertising revenue to provide free Internet accessible space. Instant messaging – provided by companies such as America Online (AOL Instant Messenger), Microsoft (MSN Messenger), and Yahoo! (Yahoo! Messenger) – allows for real-time communications in either a one-to-one or one-to-many mode over the Internet.[2]

2.1.1 Web-Based Social Networking

Web-based social networking allows for the definition of groups online by connecting people using a defined relationship. Two of the most popular social networking sites are Myspace.com and Facebook.com. MySpace is currently the world's fifth most popular English language Internet site.[3] MySpace allows teenagers, and anyone else with Internet connectivity, to post pictures and textual information for free. By adding other MySpace users to one's list of friends relationships can be defined and information collected and disseminated appropriately. With MySpace it is possible to conduct "covert" collection activities on any member without needing an account or validating an existing relationship. This allows teenagers to gain situational awareness without disclosing sources and methods.

---

[2] Duffy, Michael, "A Dad's Encounter with the Vortex of Facebook,"
[http://www.time.com/time/archive/preview/0,10987,1174704,00.html], March 27, 2006.

[3] Alexa Internet, "Top English Language Sites," [http://www.alexa.com/site/ds/top_sites?ts_mode=lang&lang=en], April 2006.

Figure 3: A user's homepage on Facebook, a popular web-based social networking service.

A more structured web-based social network is Facebook. Only teenagers with validated credentials (a college e-mail address or invitation from previously authenticated high school student) can access Facebook content. Within Facebook preliminary associations are made based on school affiliation; allowing for only cursory information – such as name, school affiliation, and a small user-posted picture – to be collected. Facebook's tiered security limits "covert" collection, however once a relationship has been defined users can see all posted information regarding one another. With a sense that their content is more protected, Facebook users often post more detailed information and far more unedited pictures than what might be seen on MySpace.

2.1.2   Blogging

Blogging has revolutionized the way in which information is disseminated. Teenagers, once seemingly averse to writing, have begun to author online journals in the form of blogs. Authoring blogs allows teenagers to express themselves and, in some cases, gain limited notoriety. Blogs differ from web-based social networking sites as the information is more personal and the publication's author may be anonymous to all but a small social group.

In both web-based social networking and blogging situational awareness is obtained from user-posted information and comments left by visitors. In web-based social networking increased intelligence can be collected by following a trail of comments between users; much like an e-mail trail results from multiple messages sent back-and-forth among a group.

Figure 4: Popular blog creation sites Blogger.com and LiveJournal.com. Both sites have thousands of active users and offer free content hosting.

2.1.3 Instant Messaging

Instant messaging allows for short, real-time messages to be sent between users over the Internet. Numerous applications exist to exploit this capability; some of which include AOL Instant Messenger (AOL IM), MSN Messenger, and Yahoo! Messenger. The intelligence benefits of instant messaging are twofold. First, instant messaging allows for rapid, informal communications in order to disseminate or collect targeted information. Secondly, instant messaging services often allow users to post information in a profile that can be read by any user. Profiles are frequently updated and will often include information regarding the location of the user. When intelligence can be collected against a number of targets it is possible to build relationship structures and develop situational awareness based on critical information requirements.

2.2 Cell Phone Based Situational Awareness

Teenagers use three applications of cell phone technology to collect intelligence: text messaging, picture messaging, and voice communications. Text messaging allows teenagers the same rapid, informal communications as instant messaging, but without the ability to post static "profiles" that are common in instant messaging. This means that cell phones are used to gather targeted intelligence by asking carefully crafted questions or collecting intelligence via information disseminated by reliable sources. Picture messaging allows users to send an image taken from a normally low resolution camera located on the phone to anyone with a cell phone or e-mail address capable of receiving them. Voice communications using cell phones are a primary means of collaboration between teenagers, however this means of communication is not as agile and is more time consuming than the previous two.

2.2.1 Text and Picture Messaging

Teenage use of text messaging is increasing on a daily basis. Text messaging provides teenagers an informal way to send information such that no direct interaction with the recipient is required. Coordination of event information, brief single-topic discussions, and information verification are just some of the potential uses of text messaging among teenagers. Text messaging is changing the way that information is disseminated by reducing the energy and time expended in the exchange of ideas. As the phone revolutionized the information exchange that once took days or weeks via the Postal Service, text messaging is now poised to further reduce the time-to-delivery. Text messaging is also seen as a discreet form of communications that allows for conversations to develop in constrained environments where cell phone based voice communications are prohibited.

Picture messaging is used by teenagers in the same way that imagery intelligence is used by military organizations. Through photo interpretation teenagers can gain situational awareness. Photo interpretation may provide details about the subject's location and acquaintances. Alternatively, information about the person taking the photo can also be gleaned. In this way a picture can often tell a teenager who is participating in an activity, where and when that activity is taking place, and what ancillary activities are occurring simultaneously.

2.2.2 Voice Communications

Teenagers love to talk on the phone. This traditional method of communications is still a primary means to gather information. In a recent Pew Internet and American Life Project survey, 63% of teenagers surveyed reported phone-based voice communication as their primary means of collaboration with friends.[4] Voice communications over cell phones allows for situational awareness to be gained based on more perceptual

---

[4] Lenhart, Amanda et. al., "Teens and Technology," [http://www.pewinternet.org/pdfs/PIP_Teens_Tech_July2005web.pdf], 27 July 2005

signals such as voice inflection. Voice communications also allows dialogue to direct situational awareness. With the understanding that "you don't know what you don't know," it is often impossible to ask every question which might provide situational awareness. Dialogue between teenagers over a cell phone allows for situational awareness to be developed without being constrained by limited prior knowledge.

2.3   Information Dissemination

In order to be collected, information must first be disseminated. Between teenagers dissemination can be either unintended or offensive in nature. Both unintended and offensive information propagation can be accomplished using any of the means mentioned in this section. An example of an unintended dissemination of intelligence information among teenagers can be illustrated using the following example:

> *John, Walt, Roger, and Paige are friends and members of a social group. John wants to invite his friends to attend a concert that evening. John decides to send each friend an instant message via AOL Instant Messenger (AOL IM) in lieu of a formal invitation or phone call. A user on AOL IM can exist in three states: active, inactive, and away. If a user is "away" they must leave a message that will display when another user sends a message. Away messages, as they are called, often describe where and with whom the user currently is (although this is not a formal requirement) and the length of time the user has been away. When John sends a message to Walt, Roger, and Paige he finds that all three are away. The away messages that are returned to John read:*

> *Walt: "I'm at the Bright Star Bowling Alley." [34 minutes]*

> *Roger: "Out of the house" [34 minutes]*

> *Paige: "Spending time with Roger and Walt" [34 minutes]*

> *Through these away messages John is able to deduce that his friends decided to go bowling without him. This intelligence increases John's situational awareness and aids in his future decision making.*

The use of offensive information is normally in the form of rumors and speculation. This information can be posted to web-based social networking sites, blogs, or instant messaging profiles; pictures that are taken out of context can be sent via cell phone picture messaging. Denial and deception campaigns should also be considered offensive information dissemination.

3.0   THE TEENAGE-TERRORIST MODEL

To describe the terrorist communications paradigm would be to repeat the teenage communications paradigm listed above with only minor changes. Terrorists have a somewhat more increased need to exercise operational security (OPSEC) due to their communications being actively targeted by coalition forces. This OPSEC requirement has forced terrorists to employ TTPs that are meant to hide both actual communications and the individual components of their collaborative environment. Through open source analysis of discovered communications it is possible to infer an analogous relationship in the communications paradigms exercised by both teenagers and terrorists.

While terrorists may not use Facebook or MySpace, use of the Internet for mission planning and information dissemination has been demonstrated in the past.[5] Terrorists have also demonstrated a keen understanding of cell phone technology; making cell phones useful in both mission planning and weapons triggering.[6]

---

[5] "Terrorists' Web Chatter Shows Concern About Internet Privacy," *The Washington Post*, 13 April 2006, A14.

[6] Appelbaum, Jacob, "IED in Iraq," [http://ioerror.livejournal.com/177534.html], April 2006.

Terrorists use technology in a way similar to that of a teenager. While the collaborate environments of terrorists may look different from those used by teenagers, their underlying capabilities are nearly identical.

3.1   Internet Based Communications

Terrorists need covert communications between geographically disparate cells to affect situational awareness and mission planning. The anonymity of the Internet seems to offer the widest range of services while providing the greatest opportunity for OPSEC. Each Internet based communications technology used by teenagers has been employed by terrorist elements. The continued reliance on technology as a force multiplier and agility enabler will decrease the length of the terrorist planning-and-attack cycle and increase the ability for geographically disparate participants to engage in terrorist activities.

While not as commercial as those services used by teenagers, terrorist Internet usage is just as sophisticated. The Internet has improved the ability for terrorist groups to gather and distribute critical information for the production of situational awareness.

Figure 5: The Internet site for the Army of Ansar Alsunnah. (Image Source: Associated Press)

3.1.1   Web-Based Social Networking

Younis Tsouli, also known as "Irhabi 007," was skilled in the art of networking over the Internet to further the goals of Islamic fundamentalist terrorism. Using a myriad of "underground" websites and password protected chat rooms Irhabi 007 linked numerous geographically disparate terrorist entities, and their potential recruits, via the World Wide Web. While Irhabi 007 was captured in November of 2005, he provided all of the resources necessary for continued terrorist use of Internet resources for social networking and recruiting.[7]

According to the website TrackingTheThreat.com, which provides link analysis between suspected terrorists, many terrorists can be linked even though they are located in geographically separate areas.[8] It can be inferred from these links that web-based social networking plays a part in the organization of terrorist structures.

---

[7] "Terrorist 007, Exposed," *The Washington Post*, 26 March 2006, B01.

[8] Tracking The Threat, [trackingthethreat.com], April 2006.

For example, Orkut, a web-based social networking site affiliated with Google, is gaining popularity in the Middle East. Orkut's popularity in the Middle East is most evident when searching through its social communities based on support for specific terrorists or terrorist networks.[9] These communities are formed much like communities on Facebook or MySpace except that rather than support for a university or sports team, the relationships are built on support for terrorism. If this trend continues to grow, these communities could be used to create recruiting and sympathizer lists.

3.1.2   Blogging

While pervasive use of blog technology by terrorists has not been demonstrated, a similar capability exists in message forums which are a well documented way in which terrorists have collaborated. Message forums allow users to post messages and have other users respond. These messages are often displayed in a hierarchy based on "threads." A new thread is similar to a post on a blog, while the replies to a thread are almost identical to comments left on blogs.

Terrorist message forums, many started by Irhabi 007, provide a collaborative capability to terrorists where situational awareness can be disseminated rapidly between geographically disparate users. Terrorists have been known to use message forums to collaborate on tactics and weapons; including weapons of mass destruction.[10]

3.1.3   Instant Messaging

Instant messaging would allow terrorists to rapidly initiate collaborative sessions from almost any connected device. Instant messaging services offer a flexible framework for communications in a one-to-one or one-to-many collaborative environment. Due to the myriad of instant messaging service providers, it is conceivable that anonymity would be increased by "service hopping" or rapidly developing new aliases, referred to as screen names. Encryption technology[11] also offers a measure of privacy that would be required for terrorist communications. Given the technology's availability it should be inferred that terrorists have the potential to use instant messaging in planning and attack coordination.

3.2   Cell Phone Based Communications

Cell phones provide an invaluable communications tool for terrorist organizations. The prevalent use of cell phones is indicated by their discovery as both a situational awareness tool and a weapons trigger. The use of communications equipment in effects based operations has highlighted the insecurity of cell phone communications among enemies of the coalition. It should be understood that terrorists have received the warning regarding cell phone usage for critical operations, however this technology is so pervasive throughout society that it would be hard to operate completely without the use of a cell phone. Terrorists must be considered a subset of any population in which they reside. As cell phones are a common means of communication in much of the world, it should be inferred that some percentage of terrorists use cell phones, roughly equivalent to the cell phone using population of a given region.

---

[9] Hunt, Kasie, "Osama Bin Laden Fan Clubs Build Online Communities," [http://www.usatoday.com/tech/news/2006-03-08-orkut-al-qaeda_x.htm], 08 March 2006.

[10] SITE Institute, "Message Posted To Jihadist Message Board provides Instruction Booklet for Home-Made Chemical Weapon," [http://siteinstitute.org/bin/articles.cgi?ID=publications12204&Category=publications&Subcategory=0], March 2004.

[11] JonyTech, "Encrypted Messenger," [http://www.johnytech.com/home.asp], April 2006.

**Figure 6: An image of a cell phone triggered IED that did not successfully detonate. (Image Source:
Jacob Appelbaum)**

3.2.1 Text and Picture Messaging

Text messaging is prevalent in areas where terrorists operate, however information on the use of picture messaging is generally unavailable. Terrorist use of text messaging generally seems to occur on "throw away" cell phones – cell phones either purchased using false names or used for only a short period of time.[12] Just as teenagers use text messaging to organize events, terrorists in Australia are charged with planning meetings using cell phone text messaging.[13]

The ability to rapidly disseminate information in a one-to-many manner is valuable to both terrorists and teenagers. In Iraq it is clear that cell phone communications using text messaging are being actively used by the local population to report crimes to the Iraqi Police Service.[14] Given that this technology is being actively used to expose terrorism, it should be inferred that this technology could be used by terrorists in Iraq.

3.2.2 Voice Communications

Terrorist use of wireless voice communications technology in support of situational awareness is well documented. Osama Bin Laden's satellite phone was under surveillance by the United States National Security Agency prior to the exposure of that fact. As early as 2003 security services were unraveling terrorist networks based on the phone numbers of associates stored in captured terrorist cell phones.[15] The prevalence of cell phones and their network infrastructure has only increased, and it can be inferred that while this network is under continued surveillance its importance in situational awareness gathering and dissemination is still important.

---

[12] Harnden, Toby et. al., "UK Terrorists Got Cash From Saudi Arabia Before 7/7,"
[http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2005/08/07/nsaud07.xml], 08 July 2005.

[13] The Sydney Morning Herald, "The Case Against the Sydney Accused," [http://www.smh.com.au/news/national/case-against-the-sydney-accused/2005/11/14/1131951103465.html?page=fullpage#contentSwap1], 15 November 2005.

[14] Knickmeyer, Ellen, "Text Messaging Lets Iraqis Tip Authorities to Attacks From a Safe Distance," [http://www.sfgate.com/cgi-bin/article.cgi?f=/news/archive/2005/01/21/international1353EST0546.DTL], 21 January 2005.

[15] Isikoff, Michael et. al., "Like Clockwork," [http://www.msnbc.msn.com/id/5821599/site/newsweek/], 25 August 2004.

4.0 COALITION STRATEGIC OBJECTIVES

Correlation of the teenage communications paradigm with that of the terrorists allows for the development of two coalition strategic objectives (CSOs). First, mitigate the speed at which terrorists gain situational awareness by developing the same agility within coalition forces. Second, respond to the terrorist use of efficient, cost effective technology by fielding similar systems within the coalition structure. Effective management of these CSOs will result in more effective operations.

Current statistics show that tactical forces are young. Youth allows a coalition military to leverage their knowledge of situational awareness tools – such as Facebook, MySpace, blogs, and instant messaging – to mitigate the agile terrorist communications methodologies. According to the Population Reference Bureau approximately 42% of Army and Navy personnel are below the age of 25 compared with just 15% of the civilian labor force in the United States.[16] Exploiting the pre-existing knowledge that these military youths have would be extremely valuable in tactical environments supporting the defense against terrorism.

4.1   Coalition Strategic Objective: Mitigate

Mitigating the speed at which terrorists gain situational awareness requires that coalition situational awareness be collected and disseminated at similar speeds. Current military strategy is to coalesce situational awareness at the strategic level; requiring vertical information dissemination. The need to protect sources and methods requires that some of the most important information remains bogged down in a bureaucracy of classification.

Counter-terrorist operations are conducted at the tactical level on a daily basis by coalition forces. Due to the vertical distribution of information, tactical users often have far less situational awareness on their target than strategic commanders. Only when information is distributed both horizontally and vertically will the tactical soldier be able to operate with critical situational awareness in-hand.

4.2   Coalition Strategic Objective: Respond

Rather than developing technology for soldiers to use, the coalition should use tools that soldiers know. Responding to the technology of the terrorists requires similarly user-intuitive tools to be employed at the tactical level. Coalition soldiers use, or have used, situational awareness tools throughout their young adult lives. Current military strategy is to develop technological tools because young soldiers understand technology. However, using technological tools that young soldiers understand could be of staggering consequence. For instance, in conjunction with CSO Mitigate, what if coalition forces developed a "Terrorist Facebook" that looks and feels like today's Facebook tool used by teenagers? This Terrorist Facebook armed with the same tools currently available – such as social network linking, biographical display, multiple image storage – would give the tactical soldier the situational awareness needed to find terrorists in a given soldier's area of operation.

5.0 CONCLUSION

The teenage communications paradigm provides a model for understanding how terrorists gain situational awareness. A terrorist communications infrastructure based on the tools used by teenagers must be defeated by using similarly agile technologies within coalition military forces. One way to improve upon tactical

---

[16] Segal, David et. al., "America's Military Population,"
[http://www.prb.org/Template.cfm?Section=Population_Bulletin1&template=/ContentManagement/ContentDisplay.cfm&ContentID=12460], December 2004.

situational awareness is to use the technology that soldiers, mostly teenagers themselves, understand and have used. Improving the agility and efficiency of coalition military situational awareness development in tactical environments will create an environment in which soldiers can respond as quickly as terrorists. It is nearly impossible to defeat an enemy using commercial, publicly available, Internet-based technology to develop and disseminate situational awareness. However, by using similar technologies to improve horizontal information flow it is possible for tactical forces to mitigate the speed at which terrorists operate.