AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

Waging and Fighting e-Jihad

by

Heidi L. Dexter, Maj, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor(s): Dr. Paul Springer and Maj Brian Tannehill

Maxwell Air Force Base, Alabama

December 2012

Disclaimer

The views expressed on this academic research paper are those of the author and do not reflect the official policy or position of the US Government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

On 11 October 2012, Defense Secretary Leon Panetta painted a grim picture of the emerging cyber threats to national security; warning of the possibility of a "cyber Pearl Harbor" should an aggressor nation or extremist group gain control of critical switches or infrastructure.[1] Panetta described an attack "as destructive as the terrorist attack on 9/11" which could "virtually paralyze the nation" with derailed trains, spilled chemicals, millions without power, and contaminated water, but is an extremist group capable of conducting attacks on critical infrastructure through cyberterrorism?[2] Cyberterrorism, defined as using "high technology to bring about political, religious, or ideological aims, actions that result in disabling or deleting critical infrastructure data or information," is a growing concern for the United States, but the majority of threats from extremist groups through the internet are of a low tech variety.[3] Terrorists do not have the ability to disable or delete critical data or information, rather they use the cyberspace to solicit funds, recruit and indoctrinate new members, reconnaissance for future attacks, brag about successes, or to communicate. A catastrophic cyberattack requires funding, advanced technological knowledge, and coordination. Terrorist organizations do not currently possess the skills necessary to hack into, and take control of a well-protected system. A more likely scenario involves a partnership between a terrorist group and a rogue hacker or well-funded and well-equipped nation state. The United States government drafted legislation to improve information sharing and the overall security posture, but more work is needed to maintain a technological advantage. Increased security for Supervisory control and data acquisition (SCADA) systems, better collaboration across the Global Information Grid, and monitoring and disrupting terrorist's ability to operate in cyberspace are necessary to continue to prevent the possibility of a cyberattack from an extremist group.

One of the primary ways terrorist exploit the internet is to raise funds to conduct operation. This is done by directly soliciting funds, or through credit card fraud, often referred to as "carding". "Cybercrime has now surpassed international drug trafficking as a terrorist financing enterprise."[4] Imam Samudra, an Indonesian terrorist executed in 2008 for his role in the 2003 Bali nightclub bombing, used carding as a means to fund his attacks.[5] In his autobiography, "Samudra urges fellow Muslim radicals to take the holy war into cyberspace by attacking U.S. computers, with the particular aim of committing credit card fraud."[6] He was reported to be extremely technologically savvy, adept at programming in several languages and, though he had grandiose ideas about penetrating vulnerable American networks, he was only successful in credit card fraud. Samudra was much more educated and capable than the average extremist, but his cybercrimes were relatively minor in the amount of damage caused to the United States public, and did not impact critical infrastructure at all.

The ability to conduct real-time communications around the world led terrorists to rely on the internet as a medium to communicate and plan operations. Osama bin Laden was extremely paranoid, and lived mostly off the grid in an effort to evade US forces but relied on email to communicate with his top leaders. To keep his emails from identifying his location, he did not have internet access at his compound, and communicated though emails drafted on thumbdrives and sent by couriers in internet cafés.[7] Even when messages were intercepted, US forces were only able to trace link to the café, and the operative was gone. The raid on his compound yielded thumbdrives, and personal computers that showed the back-and-forth messages between Bin Laden and his top lieutenants.[8]

The capabilities of government agencies are better known from their publicized successes, and terrorists are aware that their cell phone, email correspondence, and online

activities are being monitored. Email is not the only method of communicating across the internet, and terrorists have evolved to become more adept at covert communication. Web chat through on multiplayer online video games allows terrorist the ability to communicate in real-time with a relative amount of anonymity. These chat sessions take place in real time, and voice data are not recorded via electronic transcripts to be reviewed later, making detection and monitoring incredibly difficult. "Extremists choose realistic 'first person' conflict games, including 'Medal of Honor' and 'Halo,' because they can disguise their discussions as harmless web chat. In the games, players work through a complex simulation of war scenarios, carrying out missions and battling enemy fighters." Differentiating between planning a simulated attack for the game and an actual attack could be incredibly difficult.[9]

Another way terrorist organizations evade messages from being monitored is through a technique known as electronic dead dropping. Spies have been using dead dropping for many years; exchanging information at a prearranged location, which prevents the parties from having to meet face to face. Electronic dead dropping puts a modern twist on this age-old technique. Using this method, geographically separated people can communicate with a smaller chance of being monitored by drafting a message on an email account known to both parties. The message is then left in the draft folder or placed in the deleted folder for the second person to access. Electronically sending the information to another address through multiple mail servers would allow the possibility for a third party to intercept it but this method allows the information to be stored on only the server where it was originally drafted. This method can also used to electronically store information a terrorist does not wish to carry for fear it will incriminate him or divulge information if captured.[10] Dead dropping is not limited to mail servers, cloud computing through applications such as EverNote, iCloud, Amazon Cloud, and many others all

allow a user to keep documents online so that they can be accessed anywhere in the world with the correct login information. Since the information is stored on a server, and not sent through multiple devices, detection and monitoring are that much more difficult.

Even if data are sent over the internet, there are methods to hide incriminating information to avoid discovery. Two related techniques to hide messages to evade detection are called steganography and alternate data streams. "Steganography replaces unneeded bits in image and sound files with secret data" while alternate data streams hide data behind a file name.[11] There is evidence Al Qaeda used steganography by "hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other websites."[12] Though it sounds complex, this technique requires very little computer knowledge as there are commercial tools available to hide information in any file format including audio, video, picture or other file formats. While the amount of data that can be hidden by using steganography is relatively small, alternate data streams, however, have no limit on the size of the information being hidden. One could hide a file or even directory and without being visible in a search. Alternate data streams are difficult to detect and a remarkable easy way to hide information with a little computer knowledge and a few commands.[13] This method can hide larger amounts of information in non-related files for peer-to-peer sharing. There is no evidence that this technique has been adopted by terrorists, but as terrorists gain computer skills, it may become another method to hide large amounts of data from detection.

Not all communications methods used by terrorists are covert. Al Qaeda in the Arabian Peninsula (AQAP) uses a widespread electronic magazine titled *Inspire* to recruit new members and promote its message to a wider audience.[14] *Inspire* is believed to be published by Al-Awaki, an American who defected to Yemen to join AQAP and led recruiting efforts until his death via a

CIA drone strike in Yemen. By publishing in English, *Inspire* focused its recruiting to Westerners, and targeted populations at war with Muslims, specifically the United States, Britain and France. Recent editions request stories from members on their successes against the West, and urge the widest possible dissemination, fearing the United States government is trying to block websites that publish the magazine. Terrorists also use social media websites such as Facebook, Twitter, YouTube, and various forums and blogs, to recruit and indoctrinate members to their cause. Social media sites have "been employed by terrorist organizations to radicalize new recruits, deliver operational training and resources for the radicalized, raise funds, highlight successes, and shape public perception regarding ongoing hostilities."[15] Posting deliberately inflammatory information, known as trolling, can begin to lay the framework of recruiting, or deliver a psychological blow to the American public. Social networks can also be used to indoctrinate new members and glorify attacks such as JihadJane, an American woman who "posted messages on YouTube and used jihadist websites and chat rooms to plan and facilitate an overseas attack."[16] Terrorists post violent footage of recent attacks to highlight recent successes and recruit new members through clips that extol the virtues of martyrdom. Though YouTube tries to keep this footage off its site, they are posted so frequently moderators have trouble restricting access. Many sites have explicit language in their user agreement prohibiting the depiction or promotion of terrorism, but attribution to a specific user can be difficult, as well as enforcing laws, especially if the user is not an American citizen or located in the United States.[17]

Technology has become so integrated with daily lives, as well as small and unobtrusive, that modern societies are no longer concerned over the constant monitoring or sometimes even aware when something is being watched. "Analog surveillance systems were difficult to hack

into by people who lacked the adequate knowledge, but IP [internet protocol] cameras … can be quite easily physically located and their stream watched in real-time by anyone who has a modicum of computer knowledge."[18] The abundance and unobtrusive nature of this technology can easily be exploited to a terrorist's advantage. A search in an internet search engine can help a novice hacker find a live view of an area, enabling detailed reconnaissance without raising suspicion. In some extreme cases, the webcams are not even secured, allowing the viewer to pan, tilt and zoom (PTZ). "PTZ functionality allows security staff to look around a sensitive area without physically being there, but when one is left unsecured, it becomes a toy for the Internet."[19] A would-be attacker can easily gather months worth of sensitive information from the privacy of their own home, such as determining what type of security measures are in place, how many guards are employed, times of shift change, peak hours, or monitor ingress and egress routes. Anything that would have previously aroused suspicion if someone was continuously monitoring and gathering notes can now be done without detection.[20]

Successful attacks by terrorist organizations have been mostly primitive denial of service (DOS) attacks and website defacement. DOS attacks flood the victim with thousands of requests which overload the server and render it incapable of processing any requests. Though there may be limited loss of revenue while the server is offline, there is no destruction of property, and the attacks are limited in scale. There are websites that provide information on how to conduct a DOS attack and even provide the ability to outsource through an online application which allows the user to identify the "target and launch a low-level cyberattack."[21] In 2005, Scotland Yard arrested Younis Tsouli, who went by the handle Irhabi007, Arabic for terrorist007, for conspiracy to commit murder and raising funds for terrorism. Tsouli was reportedly skilled at hacking, programming, and maintained a large online presence through password protected

websites associated with Al-Qaeda. He posted a message titled "Seminar for Hacking Websites," in an attempt to create "a network of technology-savvy terrorist disciples."[22] In addition to messages about how to exploit computer vulnerabilities, he posted videos with communications from Osama bin Laden and Zarqawi, and recent activity of Al Qaeda in Iraq, thereby using his computer knowledge to ensure messages were disseminated rather than as a means of attack. Even with his reportedly advanced knowledge of computer systems and vulnerabilities, Tsouli's efforts succeeded in distributing information, not in executing attacks. "Despite [his] ominous sounding label, Tsouli's skills were quite mundane by hacker standards: he was able to hack Web sites and servers using standard tool kits found on the Internet."[23] Any system connected to the internet is vulnerable to attack and intrusion attempts are common occurrence.[24] However, if even"the top jihadi expert on all things internet related," Tsouli relied solely on widely accessible tools to exploit known vulnerabilities, then it stands to reason that patching known vulnerabilities will protect from the sophistication of cyberattacks initiated by a terrorist organization. "While such attacks can work – they succeed all the time against poorly defended systems-it does mean that cyberattacks conducted by terrorists would have roughly the same impact as techniques used by ordinary hackers, hactivists and cyber criminals."[25]

Ironically, the group that shows the greatest skill in cyberspace is one the United States government does not even consider a terrorist organization. Anonymous is a group of hactivists, people who hack to promote awareness or influence opinion of a specific cause. They succeeded in several distributed denial of service (DoS) attacks and website defacement attacks against US and foreign government websites, as well as various cybercrimes such as stealing credit card numbers to donate to charity in 2011.[26] Arguably the most technology savvy organization, they have only caused limited financial damage, and are not responsible for any loss of life.

Anonymous' goal is not to overthrow the government or harm noncombatants, rather they disrupt the targeted government websites to express dissatisfaction with government policy. Destructive cyber activity from Anonymous includes the Op_Israel campaign that called for DoS attacks against and defacement of Israeli websites because of Israel's alleged targeting of children in Gaza.[27] Though they affected over 3,000 websites, the strategic scope of such an attack pales in comparison with the psychological and economic impact of 9-11.[28]

Should a hacker like an Anonymous member become disgruntled enough to conduct cyberterrorism, it is possible that he could splinter from the group and become a hacker-for-hire and assist a terrorist organization in conducting a cyberattack. The recent recruiting efforts in English aimed at well-educated western men show this could be a valid concern. Additionally, as computers become more common and computer literacy spreads, "the chances that a terrorist group will be able to recruit people with strong computer skills (or induce potential recruits to obtain such skills" will likely increase over time."[29] Recent reports show that terrorists in the Middle East and South Asia may be "increasingly collaborating with cybercriminals."[30] Since terrorist do not currently possess the technical skills necessary to conduct a cyberattack, collaboration with hackers, cybercriminals or nation state sponsorship may be a logical approach to conducting cyber terrorism. A partnership is advantageous for the terrorist group because it would not require they have the technical knowledge to develop or implement an attack. Similarly, this may be advantageous to the hacker or criminal who would be well paid for their skills, or the nation who would like to covertly attack American interests without fear of reprisal. However, there is a fundamental difference in the goals of the terrorist and hactivist or cybercriminal. A hactivist or criminal is not interested in destroying nations, rather, they "rely heavily on several US structures such as telecommunications and financial services, to conduct

their operations."[31] Additionally, cybercriminals prefer to make money and not get caught while a terrorist group brags about successes. This fundamental difference in approach may dissuade such partnership. A union between an extremist group and a nation state is a more likely scenario, and many nations have shown the ability to develop and conduct attacks in cyberspace. Stuxnet, a worm targeted at nuclear command and control system in Iran, has not been publically claimed by any nation, but the complexity of the code led experts to attribute it to a nation.[32] Cyberattacks are a sophisticated, complex and costly endeavor, and remain far beyond the scope of a terrorist organization.

The common belief among the security experts is that "it would take a dedicated and well-financed team several years of effort to prepare a truly serious strategic attack on U.S. infrastructures."[33] If terrorist do not currently possess the skills, partnerships are filled with potentially unnecessary risks, and routine security measures would deny most attacks a terrorist is capable of launching, why would they go through the effort? An obvious reason is the actual damage that could be inflicted to the United States infrastructure and the second order impact to the economy and psychological fear that would be inflicted from this large-scale attack. Attackers have not been successful in an attack on American soil since the strike on September 11, 2001. There have been numerous attempts such as Faisal Shahzad, who attempted to detonate an Improvised Explosive Device (IED) in Time Square in 2010, and Umar Farouk Abdulmutallab, who was subdued by passengers and flight crew on Christmas day 2009 after smuggling explosive material onto the flight in his underwear, but was unable to get the device to explode.[34] A successful cyberattack would not only inflict kinetic damage, it would be a successful psychological win for the terrorist in telling the American people that they are vulnerable and an attack can come at any time, from anywhere. The resulting panic and distrust

of the infrastructure could have even wider impacts. Even small successes benefit terrorists due to the resulting publicity brought to the organization, and possible funding and recruiting gain thereafter. [35] The recent coverage of the vulnerabilities might lead terrorists to believe that "even a marginally successful cyberattack directed at the United States would garner considerable publicity" which would be advantageous to promote their cause.[36]

The most common reaction from the government when an inflammatory website is found has been to remove the website; however, the FBI is increasingly leaving the websites functional because of how easily a replacement site can be established, and to monitor activity as a counterterrorism measure.[37] This method uses the known defamatory website as a honeypot, a website with false information to spread disinformation such as "a bomb that will detonate prematurely, or incorrect intelligence," and to help identify members who should be placed on watch lists.[38] Using known terrorist sites as a counterterrorism measure has proved successful. In 2012, Barry Bujol Jr, an American in Texas, was sentenced to 20 years in prison for trying to provide personnel, equipment, and funding to Al Qaeda in the Arabian Peninsula.[39] He was arrested after providing government documents and supplies to an FBI agent posing as an Al Qaeda recruiter he met online.[40] Though honeypots have been successful, the "tactic must be used sparingly …or else officials risk 'poisoning a golden pot [of information]' about how terrorists operate."[41]

Attribution and retaliation are two major concerns the United States faces when trying to track and prosecute people who host or contribute to inflammatory websites or conduct criminal activity using the internet. A crime against an American such as data theft for carding may be committed by a person sitting in another country, using infrastructure that is located in a third country. The United States may or may not have agreements in place to trace the evidence

through the equipment used as well as the agreements to extradite and prosecute. Cyber law and treaties are emerging but "the ability of the U.S. National Security Agency to monitor such individuals inside the United States has been the subject of a heated political and legal debate. The United States has tried to prosecute webmasters who run terrorist websites in the West, but has run into opposition from advocates of free speech."[42] This sparked a debate about the NSA collecting on American citizens without sufficient cause, infringing on first and fourth amendment rights and spying on allied nations when infrastructure used by the terrorists are not located on their home soil. To alleviate some problems with attribution within the United States, the government proposed, but failed to pass laws that facilitated information sharing between Internet Service Providers and federal agencies in exchange for classified and unclassified cyberthreats to protect their infrastructure.[43] Ultimately, such measures lacked support from civil rights groups for being too vaguely worded, giving federal entities access to information protected by the Federal Wiretap Act and Electronic Communications Privacy Act without prior judicial review. President Obama is working toward proactive measures in cyberspace, attempting to create national policy more proactive than reactive. In addition to the policy review, he signed a directive titled Presidential Policy Directive 20, which enables the military to act offensively in cyberspace while also looking to protect US citizens' and partner nations' data according to national law.[44]

The increasingly use of covert technology to communicate makes gathering electronics intelligence by government agencies difficult. To counter this, the government became more focused on information sharing within United States industries and across partner nations. The Defense Industrial Base added cybersecurity measures to strengthening the collective cyber defenses. President Bush began the Comprehensive National Cybersecurity Initiative in January

2008 to enhance information sharing while protecting civil liberty.[45] President Obama further expanded on this initiative when he accepted the recommendations of the Cyberspace Policy Review in May of 2009 which identified 12 initiatives to strengthen the overall cyber security posture of the United States, among them are "deploy an intrusion detection system of sensors across the Federal enterprise, connect current cyber ops centers to enhance situational awareness, increase the security of our classified networks, and expand cyber education."[46]

Though terrorists are incredibly successful using the internet to raise funds, recruit, plan, and communicate, the ability to launch and sustain an attack against critical infrastructure remains beyond their capability. Increased collaboration with cyber criminals and recruiting better educated members moved their technological knowledge forward, but any damage from an attack in the near future will be "comparable to that which takes place daily from Web site defacements, viruses and worms, and denial of service attacks. While the impact of these attacks can be serious, they are generally not regarded as acts of terrorism."[47] Robert Mullen III, the director if the FBI acknowledges that "terrorists have not used the Internet to launch a full-scale cyberattack, but we cannot underestimate their intent."[48] Measures should still be enacted to prevent this threat from growing and to counter the known threat from nation states. Sanctions and threat or retaliation will not deter terrorist groups who do not recognize the government and are not frightened by the threat of a large war. Attribution needs to improve to deter would-be attackers and prevent nations from covertly collaborating with extremist groups. Collaboration within industries across the United States and among partner nations needs to improve across the global information grid so that critical infrastructure will be able to stand when tested. Though terrorist groups do not possess the skills or equipment to conduct a large scale cyber terrorist attack that is capable of wide spread destruction, the Unites States should still look towards

securing critical infrastructure systems from known vulnerabilities. “The Internet has presented investigators with an extraordinary challenge. But our future security is going to depend increasingly on identifying and catching the shadowy figures who exist primarily in the elusive online world.”[49]

---

[1] Panetta, Leon E., “Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City.” http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136
[2] Ibid.
[3] Tafoya, William L., “Cyber Terror.” FBI Law Enforcement Bulletin 80, no. 11 (November 2011): http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2011/november-2011-leb
[4] Theohary Catherine A. and John Rollins. “Terrorist Use of the Internet: Information Operations in Cyberspace.” http://www.carlisle.army.mil/dime/documents/Terroist%20Use%20of%20Internet%20IO.pdf
[5] Sipress, Alan. “An Indonesian's Prison Memoir Takes Holy War Into Cyberspace In Sign of New Threat, Militant Offers Tips on Credit Card Fraud.”http://www.washingtonpost.com/wp-dyn/articles/A62095-2004Dec13.html
[6] Ibid.
[7] Stanglin, Douglas. “Bin Laden used thumb drives to send and receive email.” http://content.usatoday.com/communities/ondeadline/post/2011/05/bin-laden-used-thumb-drives-to-send-and-receive-email/1
[8] Allan, Mike. “Osama bin Laden raid yields trove of computer data.” http://www.politico.com/news/stories/0511/54151.html
[9] Willetts, David and Tom Wells. “TERRORISTS are using online war games like Call of Duty to plot attacks, The Sun can reveal.” http://www.thesun.co.uk/sol/homepage/news/4205896/Terrorists-play-online-games-like-Call-of-Duty-to-plan-attacks.html#ixzz2E2lOCwjd
[10] Daily News and Analysis. “Headley used 'electronic dead drop' method for communication.” http://www.dnaindia.com/india/report_headley-used-electronic-dead-drop-method-for-communication_1324633
[11] Radcliff, Deborah. “QuickStudy: Steganography: Hidden Data.” http://www.computerworld.com/s/article/71726/Steganography_Hidden_Data
[12] McCullagh, Declan. “Bin Laden: Steganography Master?” http://www.wired.com/politics/law/news/2001/02/41658?currentPage=all
[13] Cook, Rick. “Alternate Data Streams: Threat or Menace?” http://www.informit.com/articles/article.aspx?p=413685
[14] Access ADL. “Al Qaeda’s Inspire Magazine Resurrected!” http://accessadl.blogspot.com/2012/05/al-qaedas-inspire-magazine-resurrected.html
[15] The Soufan Group. “TSG Intel Brief: Cyber Series: Terrorism and Social Media.” http://www.soufangroup.com/briefs/details/?Article_Id=272
[16] Ibid.
[17] Ibid.
[18] Slashdot.org. “Unsecured IP Cameras Accessible To Everyone.” http://hardware.slashdot.org/story/11/01/18/1829230/unsecured-ip-cameras-accessible-to-everyone
[19] Conner, Tom. “Peep show: inside the world of unsecured IP security cameras.” http://arstechnica.com/gadgets/2011/01/one-mans-journey-through-the-world-of-unsecured-ip-surveillance-cams/2/
[20] Ibid.
[21] Theohary Catherine A. and John Rollins. “Terrorist Use of the Internet: Information Operations in Cyberspace.” http://www.carlisle.army.mil/dime/documents/Terroist%20Use%20of%20Internet%20IO.pdf
[22] Kaplan, Eban. “Terrorists and the Internet.” http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005

[23] Lachow, Irving"Cyber Terrorism, Meance or Myth?" in "Cyberpower and National Security"
[24] Tafoya, William L., "Cyber Terror." FBI Law Enforcement Bulletin 80, no. 11 (November 2011): http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2011/november-2011-leb
[25] Lachow, Irving "Cyber Terrorism, Meance or Myth?" in "Cyberpower and National Security"
[26] http://allthingsd.com/20111226/anonymous-plays-robin-hood-with-stolen-credit-cards/
[27] @Op_Israel 27 Nov 2012; 26 Nov 2012
[28] @Op_Israel 26 Nov 2012
[29] Lachow, Irving "Cyber Terrorism: Menace or Myth?" in "Cyberpower and National Security"
[30] Theohary Catherine A. and John Rollins. "Terrorist Use of the Internet: Information Operations in Cyberspace." http://www.carlisle.army.mil/dime/documents/Terroist%20Use%20of%20Internet%20IO.pdf
[31] Lachow, Irving"Cyber Terrorism, Meance or Myth?" in "Cyberpower and National Security"
[32] Theohary Catherine A. and John Rollins. "Terrorist Use of the Internet: Information Operations in Cyberspace." http://www.carlisle.army.mil/dime/documents/Terroist%20Use%20of%20Internet%20IO.pdf
[33] Lachow, Irving "Cyber Terrorism: Menace or Myth?" in "Cyberpower and National Security"
[34] The Federal Bureau of Investigation. "Umar Farouk Abdulmutallab Sentenced to Life in Prison for Attempted Bombing of Flight 253 on Christmas Day 2009."http://www.fbi.gov/detroit/press-releases/2012/umar-farouk-abdulmutallab-sentenced-to-life-in-prison-for-attempted-bombing-of-flight-253-on-christmas-day-2009
[35] Theohary Catherine A. and John Rollins. "Terrorist Use of the Internet: Information Operations in Cyberspace." http://www.carlisle.army.mil/dime/documents/Terroist%20Use%20of%20Internet%20IO.pdf
[36] Ibid.
[37] The Soufan Group. "TSG Intel Brief: Cyber Series: Terrorism and Social Media." http://www.soufangroup.com/briefs/details/?Article_Id=272
[38] Kaplan, Eban. "Terrorists and the Internet." http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005
[39] Associated Press. "Texas man gets 20 years in prison for trying to give al-Qaida drone, GPS documents."http://www.msnbc.msn.com/id/47557311/ns/us_news-security/t/texas-man-gets-years-prison-trying-give-al-qaida-drone-gps-documents/
[40] Ibid.
[41] Kaplan, Eban. "Terrorists and the Internet." http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005#p8
[42] Ibid.
[43] Vijayan, Jaikumar. "FAQ: What you need to know about CISPA." http://www.computerworld.com/s/article/9226684/FAQ_What_you_need_to_know_about_CISPA
[44] Nakashima, Ellen. "Obama signs secret directive to help thwart cyberattacks." http://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html
[45] National Security Council. "The Comprehensive National Cybersecurity Initiative." http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative
[46] Ibid.
[47] Lachow, Irving "Cyber Terrorism: Menace or Myth?" in "Cyberpower and National Security"
[48] Cowley, Stacy." FBI Director: Cybercrime will eclipse terrorism." http://money.cnn.com/2012/03/02/technology/fbi_cybersecurity/index.htm
[49] Sipress, Alan. "An Indonesian's Prison Memoir Takes Holy War Into Cyberspace In Sign of New Threat, Militant Offers Tips on Credit Card Fraud."http://www.washingtonpost.com/wp-dyn/content/article/2006/03/25/AR2006032500020.html