The Role of the Internet Post-9/11 in Terrorism and Counterterrorism

Dana Janbek
Assistant Professor
Lasell College

Valerie Williams
PhD Candidate
Lasell College

Terrorism, motivated by religious or political principles, is a tool used to instill fear in the enemy and to attract media attention to publicize a cause. Its targets could reside in places as varied as the terrorist group's home country or a foreign land. Outraged by U.S. foreign policy, some perceive the United States and the Western world as enemies and thus justify using violence against these governments. Others target those who offend the terrorists' religion or those who simply do not follow it. The motivations of terrorist groups vary, with each group having its own rationale for why terrorism is appropriate to achieve its goals. While beyond the scope of this paper, it is important to become familiar with the specific motivations and frustrations that drive individuals and groups to commit acts of terrorism. Despite their varying motivations, many terrorist groups and their networks have one tactic in common since 9/11: their use of the Internet to not only communicate with other members of their groups, but also with sympathizers and potential recruits.

Over the past 15 years, scholars and counterterrorism experts alike have contemplated the role of the Internet in terrorist attacks. Does the Internet help radicalize potential recruits? Does the Internet aid potential terrorists in organizing attacks? What about its role in counterterrorism? This article surveys

Dana Janbek is Assistant Professor of Public Relations at Lasell College in Newton, Massachusetts. Her research focuses on terrorist use of the Internet as a media outlet and the use of information and communication technologies in the Middle East including within refugee populations. Prior to entering academia, she worked for the Embassy of the Hashemite Kingdom of Jordan in Washington, D.C. Earlier in her career, she served as the Director of World Communities of Louisville. Dr. Janbek is the co-author of *Global Terrorism and New Media: The Post Al-Qaeda Generation* (2010, with Philip Seib).

Valerie Williams is a graduate student and research assistant at Lasell College. She will graduate May 2014 from Lasell with a Master of Science in Communication. An alumna of University of Massachusetts Lowell, her background is in writing and diversity programming.

terrorism-related cases that have surfaced since the 9/11 attacks on the United States. The first part of the paper examines the role that the Internet played in these cases. For many terrorist organizations, this role includes disseminating hate speech, planning attacks, connecting like-minded individuals or potential terrorists, connecting with and seeking inspiration from terrorist leaders, recruiting new members, and operating websites with terrorist rhetoric. Furthermore, it will highlight specific case studies in which the Internet was used to provide material supporting a terrorist organization. In cases of terrorism in which the Internet was used, it played an integral role in either the recruitment or planning of the terrorist act.

By using the Internet, potential terrorists unintentionally made themselves visible to the counterterrorism community. They became targets for organizations like the U.S. Federal Bureau of Investigation (FBI), which seek out potential terrorist suspects. As the uses of the Internet by terrorist groups continue to evolve, so do the strategies employed by counterterrorism officials to combat them. The second part of the paper examines the different strategies used and the controversies that surround them. Counterterrorism agencies rely on undercover operations and other investigative techniques to expose terrorist plots. Additionally, legislation since 9/11 has enabled law enforcement to employ advanced surveillance of online activity. This paper draws conclusions about how the Internet has been used over the past 13 years in cases of terrorism, how the Internet is used in counterterrorism strategies, and the government's controversial surveillance of online activity.

Uses of the Internet in Cases of Terrorism

Since 9/11, extremists have utilized the Internet in many ways such as inspiring potential recruits through online communication and mobilizing them to act on radical ideology. In addition to aiding the planning and execution of terrorist attacks, one of the Internet's most common uses today by terrorists is as a database of information to learn more about terrorist organizations and their causes. The use of the Internet as a communication medium by terrorists has historically taken place prior to terrorist attacks themselves. Extremists or potential terrorists use the Internet to frequent online extremist forums and websites. These websites usually offer a significant amount of information—including organizations' missions, doctrines, and histories—to their visitors, allowing terrorist organizations to communicate detailed information about themselves to potential recruits.[1] The organizations communicate their version of reality and

how they perceive the world. In many cases, they specify who their enemies are and justify the use of violence against them, often while boasting about previous operations against enemies that were allegedly successful. Photos and videos of specific terrorist operations ensure that the websites remain entertaining and engaging for their audiences. Through personally maintaining their online presence, terrorist organizations are able to communicate directly with their target audiences without their message being distorted by mainstream media. Extremist websites and forums are maintained by sympathizers who are responsible for posting relevant content. Mohamed Jarmoune, a Moroccan-Italian in his twenties, was accused in 2012 of using his web skills to disseminate terrorist propaganda. Jarmoune "spent all his time—up to 15 hours a day—online, disseminating jihadist materials and connecting with interested individuals around the world."[2] Additionally, he administered a Facebook group that showed that he agreed with jihadist ideology. Similarly, Babar Ahmad and Syed Talha Ahsan, two British citizens, maintained a family of websites operating out of London known as Azzam Publications.[3] The sites were utilized to solicit funds, personnel, and physical items like gas masks for the Taliban and other groups. The websites featured instructional training articles, biographies of *mujahideen*, as well as audio and video products for sale. The videos included actual footage of combat and deceased extremists. Ahmad and Ahsan's cases have been ongoing since 2004 and 2006 respectively. In a similar case in Sweden, Swedish citizen Oussama Kassir, who was hoping to establish a jihad training camp in Oregon, operated six websites since December 2001 that presented "instructions about how to make bombs and poisons."[4] Kassir was a fan of Osama bin Laden and had previously received jihadist training in Pakistan.[5] These cases serve as examples of how the Internet has been used by jihadist sympathizers to assist terrorist organizations in spreading their ideology online.

The Internet also serves as a networking tool for extremists to connect with like-minded individuals or even leaders with whom they can discuss their ideologies. Such is the case of Major Nidal Malik Hasan, who communicated with the infamous American-born Muslim cleric Anwar al-Awlaki.[6] Al-Awlaki represents a modern-day terrorist. He utilized online publications and videos, as well as individual emails, to recruit potential terrorists. During his search for spiritual guidance, Major Hasan became engaged with jihadist ideology posted online. His exchanges with Anwar al-Awlaki arguably further encouraged Hasan's thoughts of violence, leading to his ultimate decision to shoot several American soldiers in 2009 in Fort Hood, Texas. Major Hasan attacked a processing center where soldiers were preparing to deploy to Afghanistan, resulting in the deaths of

13 people.[7] The FBI intercepted emails between Hasan, who was a psychiatrist at the time, and the cleric about a year before the shootings took place. As a Muslim, Major Hasan was troubled by the war, which was causing the deaths of other Muslims in Afghanistan. After the attack, the cleric al-Awlaki praised Major Hasan for doing "the right thing."

Although al-Awlaki acknowledged communicating with Major Hasan, the cleric "said that he neither ordered nor pressured Maj. Nidal M. Hasan to harm Americans, but that he considered himself a confidant of the Army psychiatrist who was given a glimpse via email into Hasan's growing discomfort with the U.S. military."[8] In fact, this was not the first time that Major Hasan had come across the cleric. Back in 2001, Major Hasan worshipped at a mosque in Falls Church, Virginia, where al-Awlaki preached.[9] There, he was exposed to radical ideas. In other words, Major Hasan came across the extreme teachings of al-Awlaki eight years prior to the Ford Hood shootings. Years later, before the shootings took place, Major Hasan relied on the Internet to seek advice from a former leader. This is an example of how the Internet can not only facilitate direct communication between those interested in terrorism and those who seek to inspire them, but also how it can reinforce existing radical ideology.

Faisal Shahzad, more famously known as the Times Square Bomber who intended to set off a bomb in Times Square in 2010, used the Internet to connect with extremists. As Professor John Mueller notes, "The Internet was crucial for Shahzad's entrance into the domain of religious fanatical terrorism. He initiated contact with Tehrik-i-Taliban Pakistan over the Internet. Through the initial connection, he was in communication with many jihadist contacts including Anwar al-Awlaki."[10] Similar to the case of Major Hasan, Shahzad was also troubled by the U.S. role in Muslim countries, the use of drones, and the killings of Muslims abroad, and used the Internet to connect with experienced jihadists who gave him both the necessary push and practical knowledge to pursue his attack. Both Major Hasan's and Shahzad's cases demonstrate the important role that the Internet played in connecting extremists. International organizations working on counterterrorism acknowledge that "the reach of the Internet provides terrorist organizations and sympathizers with a global pool of potential recruits."[11]

The Internet is also used to sway those who have some interest in extremist ideologies. Speeches by extremist leaders are posted online and can be accessed by anyone interested in their rhetoric. Nigerian Umar Farouk Abdulmutallab became known as the "Underwear Bomber" for his attempt to blow up a Michigan-bound flight in 2009 with material hidden in his underwear. He, too,

had connections with the late al-Awlaki. U.S. government documents reveal that Abdulmutallab sought out al-Awlaki, who later trained him.[12] The government argued that Abdulmutallab was manipulated by extremist lectures posted online. This case demonstrates the not inconsiderable potential influence of Internet videos in the radicalization process.

In addition to connecting like-minded individuals and inspiring others to commit violent action, terrorist networks use the Internet to recruit new members. One of the cases that drew media attention was that of Colleen LaRose, more popularly recognized as "Jihad Jane" or Fatima LaRose.[13] In 2008, LaRose, linked to other extremists online in Europe, had conspired to kill a Swedish cartoonist who depicted Prophet Muhammad in a negative light.[14] This case captured the attention of many in the United States and Europe, especially since the accused was a white American female who had converted to Islam as an adult. LaRose used the Internet to successfully recruit and convince other women, such as Jamie Paulin Ramirez, to join her jihadist mission. According to the U.S. Department of Justice, "LaRose and her co-conspirators used the Internet to establish relationships with one another and to communicate regarding their plans…in order to wage violent jihad."[15] Here, the Internet took on the role of recruiting potential terrorists for an international terrorist plot. As demonstrated in this case, "the Internet becomes a virtual "echo chamber"—acting as a radicalization accelerant while creating the path for the ultimate stage of Jihadization."[16]

The Internet can also be used to communicate during the process of planning an attack. Najibullah Zazi, a Colorado resident responsible for planning an attack against the New York subway system in 2009, communicated with his contact in Pakistan via email to design the foiled attack.[17] In addition to other recruits from the United Kingdom involved in the case, the two exchanged messages concerning the making of the bomb and the progress of the plot using coded language. Before heading to New York to execute his plot, Zazi wrote to his contact, letting him know that "the marriage is ready"—signaling that the attack was ready.[18] The two used the term "wedding" to refer to the attack. They also used coded language to refer to explosives. In this example, the Internet was used by individuals to communicate the details and the logistics of their planned attack.

Since 9/11, the Internet has been used to spread terrorist group rhetoric, connect like-minded extremists, inspire and radicalize terrorist sympathizers, recruit potential terrorists, and plan attacks. In the surveyed cases, the Internet played a significant role in the radicalization and planning processes in terrorism.

The aforementioned cases also show that in addition to the Internet, there are a number of other factors that contributed to the radicalization and planning processes, such as disagreeing with a country's foreign policy. Although one cannot isolate the Internet as the main or only factor that causes individuals to commit an act of terrorism, one can confirm from documented cases that the Internet has been used in various ways to facilitate different aspects of terrorism. That said, "despite increasing international recognition of the threat posed by terrorists' use of the Internet in recent years, there is currently no universal instrument specifically addressing this pervasive facet of terrorist activity."[19]

The FBI now allocates approximately half of its resources to counterterrorism and the remaining half to all other criminal activity.

The Uses of the Internet in Counterterrorism

The way in which terrorists utilize the Internet has continuously evolved since 9/11. U.S. intelligence, law enforcement, and security agencies have responded by significantly expanding their counterterrorism workforce, conducting undercover operations, and increasing surveillance of communications and online activity. Collaboration between these agencies has been vital to the nation's counterterrorism efforts; information gathered by the National Security Agency (NSA)'s surveillance technology is shared with the FBI for use in investigations.[20] Though these strategies have arguably stopped potential attacks on U.S. soil, media outlets have questioned the ethics behind undercover operations and advanced surveillance technologies.

Due to varying motivations, levels of expertise, and tactics of extremist groups and individuals, the FBI acknowledges terrorism as a complex threat. As a response, the agency has increased its number of agents by 40 percent and now allocates approximately half of its resources to counterterrorism and the remaining half to all other criminal activity.[21] Between 2001 and 2011, the agency has almost tripled its intelligence analyst workforce.[22] It has also increased the number of Joint Terrorism Task Force (JTTF) partnerships from 35 to over 100.[23] JTTF partnerships exist between law enforcement agencies across the country that share essential information with each other. These partnerships contribute resources, enhance operational capability, and significantly expand the FBI's intelligence base. According to the FBI, "JTTFs have been instrumental in breaking up cells…[and] they've foiled attacks on the Fort Dix Army base

in New Jersey, on the JFK International Airport in New York, and on various military and civilian targets in Los Angeles."[24]

In addition to expanding its labor force, the FBI has adapted its investigative approach to more proactive, intelligence-led strategies to combat terrorist attacks. These strategies are specifically tailored to the targeted suspect, requiring agents to utilize unique skill sets and language abilities for undercover operations. The FBI implements a variety of undercover tactics on the Internet, at times creating terrorist-network recruiting websites convincing enough to attract potential terrorists. When 18-year-old would-be terrorist Abdella Ahmad Tounisi was searching the Internet for Jabhat al-Nusra, an al-Qaeda branch in Syria, he found one of these sites. Created and maintained by the FBI, the page featured pictures and videos of armed fighters in masks and fatigues intended to depict terrorist training.[25] A section of the site, titled "A Call for Jihad in Syria," urged visitors to "come and join your lion brothers of Jabhat Al-Nusra who are fighting under the true banner of Islam, come and join your brothers, the heroes of Jabhat Al-Nusra."[26] When Tounisi contacted the website's recruiter, who in reality was an FBI agent, they exchanged email messages in which the teen divulged his detailed plan to engage in jihad in Syria. As a result of this communication, the agency was able to arrest Tounisi in 2013 at Chicago's O'Hare International Airport before his flight across seas. Tounisi was ultimately charged with attempting to provide material support to a foreign terrorist organization and lying to federal authorities.

The FBI utilizes specially trained undercover agents to befriend and earn the trust of domestic terror suspects similar to Tounisi. This strategy allows agents to monitor terrorism plots in their beginning stages and intercept forum posts and emails from individual suspects before they catch the attention of authentic extremist organizations. For example, after posting violent messages on an online extremist forum, teenaged Texas resident Hosam Maher Husein Smadi was befriended by an Arabic-speaking FBI agent posing as a member of an al-Qaeda sleeper cell.[27] Within months, Smadi and three undercover agents devised a plot to bomb a 60-story corporate building in Dallas, Texas. On the last day of the sting operation in 2009, Smadi attempted to detonate the fake bomb provided by the FBI and was immediately arrested.

Once an agent befriends a targeted suspect, plans are developed and if necessary, resources are provided at the target's request. Throughout this process, FBI agents attempt to dissuade the suspect, offering him or her a chance to abandon the plan.[28] If the individual is adamant in completing the mission—at times seen in attempts to purchase weapons, to leave the country, or to detonate an

FBI-provided bomb—he or she is arrested and tried for the crime. This scenario is not uncommon; there have been several cases of homegrown violent extremism fueled by extremist websites, even in individuals as young as 14.[29] In cases like these, the FBI asserts that if an individual is susceptible to an undercover agent, he or she would be just as susceptible to an extremist group.[30] Although sting operations have been used by law enforcement for decades, this process of befriending and working with potential terrorists online has sparked an ethical debate. Furthermore, some have questioned whether sting operations are the best use of counterterrorism resources. Some consider these operations to be entrapment since the FBI partially devises the plan and provides money, fake bombs, and even vehicles to suspects. In a recent *New York Times* article, author David Shipler questioned the legitimacy of cultivating potential terrorists instead of finding real ones.[31] Shipler dismisses some terror suspects as "incompetent wannabes looking for a cause that the informer or undercover agent skillfully helps them find."[32]

Cases like that of Hosam Smadi exemplify these arguments; Smadi's defense team described him as a troubled youth who suffered from depression and schizophrenia.[33] According to the defense, Smadi was motivated by the undercover agents' praise and companionship.[34] Despite their efforts to portray him as a misguided victim of entrapment, Smadi was charged in 2010 with one count of attempting to use a weapon of mass destruction and one count of bombing a public place. He was sentenced to 24 years in prison and deportation upon release. According to investigative journalist Trevor Aaronson, no terrorism defendant since 9/11 has won an acquittal using entrapment as a defense.[35] Collaborating with prosecutors, undercover operatives determine strategies to prove the suspect's predisposition to committing the crime. Working together, prosecutors and FBI employees document proof to use in court later.[36] Though its ethical standards are in question by the public, the FBI's strategies have been successful under legal standards.

No terrorism defendant since 9/11 has won an acquittal using entrapment as a defense.

Undercover operations represent just one investigative technique for identifying terrorists and their networks. FBI operatives also investigate activities of known terrorist organizations, interview locals, and monitor foreign press for intelligence. These traditional, preventative policing techniques are employed in collaboration with online data to compile evidence necessary to prosecute terrorists.[37] Although controversy surrounds the agency's sting operations, the FBI reports that it has removed more than 20 of al-Qaeda's top 30 leaders

due to the FBI's improvements since 9/11.[38] These changes hinder al-Qaeda's efforts in fundraising, recruiting, training, and planning attacks outside their local region. The FBI also says that every major al-Qaeda affiliate has lost its key leader.[39] Although these leaders can be replaced, al-Qaeda is forced to use less experienced leaders, degrading their overall efficiency. The FBI credits their achievements to their expansion in intelligence and access to digital records, due in part to post-9/11 legislation.

The FBI reports that it has removed more than 20 of al-Qaeda's top 30 leaders due to the FBI's improvements since 9/11.

Post-9/11 legislation, including the PATRIOT Act and the FISA (Foreign Intelligence Surveillance Act of 1978) Amendments Act, enables the NSA to gain access to individuals' online activity, employ advanced surveillance technology, and increase the use of National Security Letters. National Security Letters, commonly used in counterterrorism investigations, enable agents to collect non-content consumer information including Internet records, telephone records, and credit reports from third party service providers. Additionally, section 215 of the PATRIOT Act permits the FBI to seize anything tangible from a person for investigations against international terrorism.[40] Intelligence officials admit that "the National Security Agency is searching the contents of vast amounts of Americans' email and text communications into and out of the country" for mentions of foreign terrorist suspects under surveillance.[41] Relevant data collected by this surveillance is shared with the FBI and their JTTFs to aid investigations.[42]

As government organizations continue to monitor personal online activity in the name of national security, privacy has become a growing concern for citizens and organizations like the American Civil Liberties Union (ACLU). In December 2013 the ACLU filed a lawsuit against the NSA, demanding that it disclose details of its surveillance program and what protections, if any, the NSA provides to American citizens.[43] The NSA has been accused of conducting surveillance without probable cause or individualized suspicion and spying on American citizens despite their commitment to monitoring only valid foreign suspects.[44] Many mainstream media outlets have also created an open discussion about the NSA, providing classified documents and quotes from anonymous intelligence officials in extensive investigative reports. While detailing the nation's counterterrorism strategy and objectives, President Barack Obama acknowledged that it is essential to respect civil liberties and rights to privacy in order to maintain the public's support.[45]

In August 2013 Obama announced the creation of the Review Group on

Intelligence and Communications Technologies (RGICT), intended to protect citizens' liberty and security. In December 2013 the group released a total of 46 recommendations including stricter regulations for the use of National Security Letters, more transparency of the NSA's authority and actions, and the development of a more targeted surveillance system.[46] Internet freedom is an important aspect of U.S. policy, with protection against intrusive surveillance and repression among its central themes. In fact, in 2012 the United States successfully pushed for human rights to be protected online to the same extent as in real life. The RGICT reports "[the] U.S. Government has consistently spoken out against the arrest and persecution of bloggers and online activists in countries including Azerbaijan, China, Cuba, Egypt, Ethiopia, Iran, Russia, Saudi Arabia, Thailand, Venezuela, and Vietnam."[47] Some see a clear contradiction between the United States pushing for freedom of speech abroad, while engaging in surveillance programs at home. Though many U.S. citizens have taken a stance against widespread surveillance, the impact of the ACLU's lawsuit and the RGICT's recommendations is yet to be seen.

In summary, the anonymity of the Internet makes it equally accessible to both the innocent and the guilty. While some suspects are more dangerous than others, in combating the global threat of terrorism, it is difficult to distinguish which targets are the biggest threats. As terrorists and their networks' use of the Internet has expanded, so have the strategies of the FBI and its counterparts in other agencies. Today, terrorist groups use the Internet to spread rhetoric, inspire, recruit, radicalize, network with like-minded extremists, and plan attacks. Many cases since 9/11 have documented this growing and creative use of the Internet as a tool to serve terrorism purposes. The Internet plays a critical role in cases of terrorism and to counter this threat, counterterrorism officials have resorted to questionable investigative strategies. This has provoked a debate concerning civil liberties, as some argue that the government's war on terror entraps citizens and infringes on their rights to online privacy. The FBI, in order to combat the anonymous and elusive nature of how terrorists use the Internet, regard it necessary to pass legislation that impacts the privacy of innocent citizens. This notion, however, has been challenged by citizens, mainstream media, and now the court of law. With pending lawsuits against the NSA, there may be a change in surveillance regulations in the future. This will affect the way the counterterrorism community addresses current and future threats resulting from terrorist groups' use of the Internet. The Internet will continue to be a key part of counterterrorism efforts, as it is an integral part of some terrorist organizations' strategies and operations.

Notes

1. Philip Seib and Dana Janbek, *Global Terrorism and New Media: The Post Al-Qaeda Generation* (New York: Routledge, 2011), 43–60.
2. Lorenzo Vidino, "The Evolution of Jihadism in Italy: Rise in Homegrown Radicals," *CTC Sentinel*, November 2013, 19.
3. "Two British nationals plead guilty to terrorism-related charges in New Haven federal court," U.S. Attorney's Office: District of Connecticut, December 10, 2013.
4. "Swedish Citizen Oussama Kassir Found Guilty of Providing Material Support to al Qaeda," U.S. Attorney's Office: Southern District of New York, May 12, 2009.
5. Ibid.
6. "Anwar al-Awlaki Fast Facts," CNN Library, August 23, 2013.
7. David Johnston and Scott Shane, "U.S. Knew of Suspect's Tie to Radical Cleric," *New York Times,* November 9, 2009.
8. Sudarsan Raghavan, "Cleric Says He Was Confidant to Hasan," *Washington Post,* November 16, 2009.
9. Philip Sherwell and Alex Spillius, "Fort Hood Shooting: Texas Army Killer Linked to September 11 Terrorists," *The Telegraph*, November 7, 2009.
10. John Mueller, *Terrorism since 9/11: The American Cases* (Columbus, OH: Mershon Center, 2013), 435.
11. "The Use of the Internet for Terrorist Purposes," United Nations Office on Drugs and Crime, September 2012, 5.
12. "Government's sentencing memorandum," United States District Court, Eastern District of Michigan, Southern Division, February 10, 2012.
13. "Colorado Woman Pleads Guilty to Conspiracy to Provide Material Support to Terrorists," U.S. Department of Justice: Office of Public Affairs, March 8, 2011.
14. "Leader of Revolution Muslim Pleads Guilty to Using Internet to Solicit Murder and Encourage Violent Extremism," U.S. Attorney's Office: Eastern District of Virginia, February 9, 2012.
15. "Federal Judge Sentences 'Jihad Jane' to Serve 10 Years in Prison for Role in Plot to Commit Murder Overseas," U.S. Department of Justice: Office of Public Affairs, January 6, 2014.
16. United States Senate Committee on Homeland Security and Governmental Affairs, "Violent Islamist Extremism, The Internet, and the Home Grown Terrorist Threat," Majority & Minority Staff Report, May 8, 2008, 11.
17. "Charges Unsealed Against Five Alleged Members of al Qaeda Plot to Attack the United States and the United Kingdom," U.S. Department of Justice: Office of Public Affairs, July 7, 2013.
18. Ibid, 7.
19. "Use of the Internet," United Nations Office on Drugs and Crime.
20. Robert S. Mueller, III, "Working Together to Defeat Cyber Threats," Federal Bureau of Investigation, February 28, 2013.
21. Jerome P. Bjelopera, "The Federal Bureau of Investigation and Terrorism Investigations," Congressional Research Service, April 24, 2013.
22. Ibid.
23. "Protecting America: National Task Force Wages War on Terror," Federal Bureau of Investigation, August 19, 2008.
24. "Protecting America from Terrorist Attack: Our Joint Terrorism Task Forces," Federal Bureau of Investigation, 6.
25. United States District Court Northern District of Illinois Eastern Division. "Government's appeal of Magistrate Judge's Order Concerning Detention Pursuant to 18 U.S.C.§ 3145(a)(1)," May 2, 2013.
26. Ibid.
27. "FBI Arrests Jordanian Citizen for Attempting to Bomb Skyscraper in Downtown Dallas," U.S Department of Justice, September 24, 2009.
28. David J. Gottfried, "Avoiding the Entrapment Defense in a Post-9/11 World," Federal Bureau of Investigation, January 2012.
29. Mark Giuliano, "The Bureau's Response to Evolving Threats," Federal Bureau of Investigation,

April 14, 2011.
30. David J. Gottfried, "Avoiding the Entrapment Defense in a Post-9/11 World," Federal Bureau of Investigation, January 2012.
31. David K. Shipler, "Terrorist Plots, Hatched by the F.B.I.," *New York Times*, April 28, 2012.
32. Ibid.
33. Mueller, *Terrorism since 9/11*, 2.
34. Ibid., 4.
35. "Interview: 'The Terror Factory: Inside The FBI's Manufactured War On Terrorism,'" Radio Free Europe Free Liberty, February 26, 2013.
36. David J. Gottfried, "Avoiding the Entrapment Defense in a Post-9/11 World," Federal Bureau of Investigation, January 2012.
37. "The Use of the Internet for Terrorist Purposes," United Nations Office on Drugs and Crime, September 2012.
38. Daniel Benjamin, "Global Counterterrorism: A Progress Report," U.S. Department of State, December 18, 2012.
39. "Remarks of John O. Brennan, Assistant to the President for Homeland Security and Counterterrorism, on Ensuring al-Qa'ida's Demise," The White House, June 29, 2011.
40. PATRIOT Act, United States Congress, January 1, 2001.
41. Charlie Savage, "N.S.A. Said to Search Content of Messages to and From U.S.," New York Times, August 8, 2013.
42. Mueller, "Working Together."
43. "ACLU v. Clapper—Challenge to NSA Mass Call-Tracking Program," American Civil Liberties Union.
44. "How the NSA's Surveillance Procedures Threaten Americans' Privacy," American Civil Liberties Union; "Valid Foreign Intelligence Targets Are the Focus," National Security Agency, October 31, 2013.
45. "National Strategy for Counterterrorism," The White House, June 2011.
46. Review Group on Intelligence and Communications Technologies. "Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies," December 12, 2013.
47. Ibid.