My Cyber Counter-jihad

How a Montana woman broke new counterterrorism ground

By Shannen Rossmiller; The Middle East Quarterly/Summer, 2007; Volume XIV, #3

On September 3, 2004, a nine-member officer's panel at Fort Lewis, Washington, found Specialist Ryan G. Anderson guilty of five counts of seeking to aid the enemy during a time of war and attempted espionage. The court martial subsequently sentenced him to five concurrent life terms for his crimes. To date, the sentence represents the most severe penalty meted out to a U.S. citizen in President George W. Bush's global war on terror. The case also marked the triumph of the new field of cyber counterterrorism, which I helped develop. Working from my home computer, I enabled Anderson's capture. There have since been more than 200 other cases.

Discovering Jihad Online

Before 9-11, I had no experience with the Middle East or the Arabic language. I was a mother of three and a municipal judge in a small town in Montana. But the terrorist attacks affected me deeply. I wondered how it could happen. What kind of people could carry out such an atrocity and why? I began to read vociferously about Islam, terrorism, extremist groups, and Islamist ideology.[1] Some of the books satisfied; many did not.

In November 2001, I saw a news report about how terrorists and their sympathizers communicated on websites and Internet message boards and how limited government agencies were in their ability to monitor these web communications. This news report showed me how extensively Al-Qaeda used the Internet to orchestrate 9-11 and how out of touch our intelligence agencies were regarding this Internet activity. Apparently, there were not procedures in place for tracking communications and activity on the Al-Qaeda websites and Internet forums at the time.

The Internet address named in the news report was "www.alneda.com." I wrote it down and proceeded to see for myself what all the fuss was about.

---

1 For example, see Reinhard Schulze, *A Modern History of the Islamic World* (New York: New York University Press, 2002); Ahmed Rashid, *Jihad: The Rise of Militant Islam in Central Asia* (New York: Penguin, 2003); Ahmed Rashid, *Taliban* (New Haven: Yale University Press, 2001); Karen Armstrong, *Muhammad: A Biography of the Prophet* (San Francisco: Harper San Francisco, 1993); Gilles Kepel, *Jihad: The Trail of Political Islam* (Cambridge: Belknap Press, 2003); Rohan Gunaratna, *Inside Al-Qaeda: Global Network of Terror* (Berkley: Berkley Trade, 2003).

I entered another world when I logged on to that site for the first time. I did not know Arabic, so I clicked away at random, looking at featured pictures depicting such things as dead bodies lying around in the aftermath of a car bombing and other atrocities.

Early in January 2002, I began taking an Arabic language course online for eight weeks from the Cairo-based Arab Academy,[2] which, that autumn, I supplemented with an intensive Arabic course at the State University of New York at Buffalo. As I learned more Arabic, the jihadi websites opened for me. Certain individuals stood out for either their radicalism or the information that they sent. I followed and tracked these individuals and kept notebooks detailing each website and person of interest.

Gradually, as I put to use the knowledge and skills I was developing of the Arabic language, I started posting messages on Internet forums and message boards. However, it was not until I was able to find an Arabic language translator through an online translation service[3] willing to assist me with constructing contextually accurate messages that I began to elicit responses from individuals at these Internet sites. As time went on, and through the process of trial and error, I eventually figured out what to say and how to say it to start the process of passing myself off as a jihadist sympathizer.

I created my first terrorist cover identity on the Internet on March 13, 2002, to communicate and interact with these targets. In my first chat-room sting, I convinced a Pakistani man that I was an Islamist arms dealer. When he offered to sell me stolen U.S. Stinger missiles to help the jihadists fighting the U.S. and coalition forces in Afghanistan, I used the Persian Gulf dialect of Arabic to ask him to provide me with information that I could use to confirm his claims, such as stock numbers. Within a couple of weeks, the missile identification numbers were in my computer inbox.

Stock numbers and the e-mail correspondence in hand, I intended to drive to the closest field office for the FBI here in Montana but was afraid that the FBI would not take me seriously. What were the chances of a Montana mom showing up at their door with information about an individual in Pakistan who was trying to sell Stinger missiles? Instead, I submitted the information to the FBI's online tips site.

A few days later, I received a telephone call from an FBI agent from New Jersey who proceeded to question me. It felt like an interrogation. Several days later, the same agent called to thank me and say that the stock number information for the Stingers did match some of the information that the government had about the missiles.

Encouraged by this success, I continued to communicate with these jihadis online and proceeded to gather more information.

Using various Muslim personalities and theatrics for cover, I began monitoring the jihadist chat rooms into the early hours of the morning while my family slept. Plunging in, I started making headway into the world of counterterrorism.

---

2 The Arab Academy maintains a website at http://www.arabacademy.com.

3 Translation Depot. http://groups.yahoo.com/group/translation_depot/

4 *BBC News*, May 13, 2003; "Saudi Bombing Deaths Rise" http://news.bbc.co.uk/2/hi/middle_east/3022473.stm

In 2003, the individuals interacting in known Al-Qaeda affiliated websites and Internet forums began to pass around information about private Internet forums used by Al-Qaeda and its sympathizers.

Under one of my terrorist identities, I was able to infiltrate some of these private sites where the communication and interaction was much more radical than what I had earlier encountered. In March 2003, I aligned myself with a few of the more prolific individuals at one of these forums. During this time, there was a lot of communications being passed around about how the "brothers" had perfected the use of cell phones as remote bomb detonators and how they would share the information. When I received the "perfected" schematics for use of cell phones as remote bomb detonators, the "brothers" at the Internet forum stated that the next big attacks would incorporate the use of cell phones detonators for car bombing in the Arab peninsula. I again forwarded this information to the FBI.

Over the next couple months, it became clear that Al-Qaeda would next target Western interests in Saudi Arabia. On April 30, 2003, while chatting online in Arabic with terrorist "friends," a jihadi indicated that the selected targets for new attacks would be Western housing complexes or hotels frequented by Westerners in the kingdom. After further conversations over the next few days, I became convinced that the attack would be within a week, in Riyadh. On May 12, 2003, four days after the FBI had been tipped off, Al-Qaeda carried out its attacks. Terrorists drove two cars, a pickup, and an SUV through Riyadh. Two of the vehicles carried heavily armed assault teams, and three of the four were also packed with explosives.[4] Their targets were three compounds: the Durat al-Jadawil, a compound owned by MBI International and Partners; Al-Hamra Oasis Village compound; and a compound owned by the Vinnell Corporation, a Virginia-based defense contractor that was training the Saudi national guard. The Islamists killed thirty-four people in and around the compounds.[5]

Then, four days later on May 16, 2003, Al-Qaeda struck in Casablanca, setting off five explosions killing at least twenty people and injured 100. The attacks targeted a Jewish community center, a Spanish restaurant and social club, a hotel, and the Belgian consulate.[6] Subsequent to the attacks, FBI investigators confirmed that terrorists used cell phones as remote detonators in both operations.[7]

Two months later, while posing as a courier, I indicated that I was in Mosul, Iraq, and wanted to assist the jihadis fighting the Americans there. I informed them that I could travel between Jordan, Turkey, and Iraq and could take money or information to people in those countries to help the cause.

After a couple of weeks, I had gained enough trust in the chat room that I was asked if I could get a letter and some money into Jordan for certain members of Saddam's fedayeen.

I was given a "scanned" copy of a letter that was said to be written by Saddam Hussein and intended as a communiqué for former elements of his regime that had relocated to Jordan

---

5 *CNN.com*, May 13, 2003; "Riyadh Bombings," *Online NewsHour*, Public Broadcasting Service (PBS), accessed Feb 26, 2007.

6 CNN, May 19, 2003.

7 "Homeland Security Report," no. 127, Homeland Security Group, Apr. 5, 2004, p. 6.

after the fall of Baghdad to coalition forces. I was later told by federal authorities that they believed the letter to have been in fact written by Saddam Hussein.[8]

Capturing Ryan Anderson

It was soon after that I learned that I was not the only American surfing the chat rooms. In October 2003, while monitoring Arabic Islamist websites for threat-related information and activity, I saw a message posted in English by a man calling himself Amir Abdul Rashid. He said he was a Muslim convert who "was in a position to take things to the next level in the fight against our enemy (the U.S. government)." He further requested that someone from the mujahideen contact him for details. I was suspicious because Rashid posted his message in English on an Arabic website and was openly seeking contact from the mujahideen. I traced his IP address back to an area outside of Seattle, Washington. Over time, it also became apparent to me that he was a member of the U.S. military.

I posed as an Algerian with ties to that country's Armed Islamic Group, which I indicated was closely aligned and working with elements of groups associated with Al-Qaeda, and sent Rashid an e-mail in English with the subject line "A Call to Jihad." Rashid responded by asking if it was possible that a "brother fighting on the wrong side could sign up or defect, so to speak." Over a period of four months, Rashid and I exchanged a series of thirty e-mails in English. I learned he was a member of the Army National Guard from Washington State, whose tank battalion unit was scheduled to be deployed to Iraq in February 2004. Through the course of our e-mail exchanges, Rashid provided me with information and materials on the weaknesses and vulnerabilities of the M1-AI and M1-A2 Abrams tanks as well as U.S. troop locations in Iraq. At all times during our communications, Rashid perceived me to be a mid-level Al-Qaeda operative.

After our fifth e-mail exchange, I contacted the Department of Homeland Security, which put me in contact with my local FBI office. During the next four months, I worked closely with the FBI and the criminal investigation division of the Army. On February 12, 2004, just eight days shy of deploying with his National Guard unit; the FBI arrested Spec. Ryan G. Anderson and turned him over to the Army for prosecution.

While I preferred to continue my work anonymously, my undercover life became public because of my involvement in the Anderson case. During his prosecution, I was called to testify, and so my work and identity was exposed in U.S. court records.[9]

After the media picked up my identity at Anderson's Article 32 hearing in May 2004, I received numerous threats and, on December 5, 2004, someone stole my car out of my family's garage. It was later found wrecked two counties away from my home, riddled with bullet holes. As a result, I now have permanent security.

I have still continued my online sleuthing. After the Anderson case, I worked to capture members of an Al-Qaeda affiliate in Lebanon seeking to sneak chemical weapons into Iraq. Believing me to be a jihadist banker, the group said that they had already killed twenty-four

---

8 See mention in *The Washington Post*, May 4, 2003.

9 "United States of America, Department of the Army v. Specialist Ryan G. Anderson, Fort Lewis, Army Base, Washington State,"**;** *The Seattle Post-Intelligencer*, Feb. 13, 2004.

British troops, wanted to attack U.S. soldiers with weapons of mass destruction, and needed money to buy the materials on the black market. Because of the hard work of a number of investigative bureaus in the United States and abroad, they never got the chance.

In January 2005, I came upon another individual here in the United States who claimed to have knowledge and skills in nuclear physics and was offering his abilities online to Al-Qaeda to carry out terrorist attacks here on U.S. soil. The individual's online tracks traced back to several public library locations in Ohio. I began communicating with this individual in English and transliterated Arabic, who I later identified as Mohammed Radwan Obeid. During the course of our communications, Obeid talked about nuclear weapons and other weapons attractive to the mujahideen as well as his desire to recruit people to start or join a terror cell. In March of 2005, the FBI arrested Obeid, a Jordanian and illegal alien pretending to be a Jehovah's Witness. He has since been sentenced to a year in prison, followed by deportation.[10]

Finally, in October 2005, I came into contact with another U.S. citizen intending to harm the United States for al-Qaeda. Michael C. Reynolds was arrested on December 5, 2005, outside of Pocatello, Idaho.[11] He thought he was conspiring with an Al-Qaeda operative online seeking to cause a major disruption in the U.S. economy and its foreign policy objectives abroad by bombing sections of the Alaska transcontinental pipeline and other U.S. oil and energy installations. On October 3, 2006, a federal grand jury in Scranton, Pennsylvania, indicted Reynolds on six counts of attempted terrorism activities.[12] Reynolds remains in federal custody in Pennsylvania pending judgment.[13]

Terrorist Use of Internet and Technology

More than five years after 9-11, a growing number of terrorist movements harness the Internet and employ technology in their fight against the West. However, as Jarret Brachman, director of research for the Combating Terrorism Center at the United States Military Academy, points out, "It is the strategic—not operational—objectives of the jihadi movement's use of technology that engenders the most enduring and lethal threat to the United States over the long term." He argues, "If Western governments made reading the online statements posted by Al-Qaeda ideologues a priority, they would better realize how the jihadi movement is not simply using technological tools to recruit new members, receive donations, and plan attacks.

In actuality, Al-Qaeda's use of the Internet and other new technologies has also enabled it to radicalize and empower armies of new recruits by shaping their general worldview."[14]

---

10 *Dayton Daily News, July 8, 2006.*

11 *CBS News,* Feb. 11, 2006; *The Washington Post*, Feb. 13, 2006.

12 Middle District of Pennsylvania, United States of America vs. Michael Curtis Reynolds, no. 3: CR-05-493, Oct. 3, 2006; *The New York Times,* Oct. 5, 2006.

13 My involvement is mentioned in: *The Washington Post*, June 4, 2006; *ABC News*, June 5, Oct. 3, 2006; *The Telegraph* (London), June 27, 2006.

14 Jarret M. Brachman, "High-Tech Terror: Al-Qaeda's Use of New Technology," *The Fletcher Forum of World Affairs*, Summer 2006.

The process that I started in early 2002 would eventually become a template for the government in the new and developing field of fighting terrorism online called "cyber-counterintelligence." It would be counterproductive, though, to ongoing investigations to comment further on the institutionalization of the field or its sources and methods.

Yet my efforts have been worth the personal sacrifice. After hundreds of cases, I continue to challenge myself to out-think and out-maneuver the terror enemy—by forging new and untested methods in the field of cyber-counterintelligence to always gain the upper hand in an operation. Whenever I set out to ensnare any terrorist operative or group, I always have one main motivating factor in sight: simply said, I cannot and will not ever forget the painful memory of 9-11 and the death and destruction brought to bear upon the United States and the world.

If we are to defeat Al-Qaeda and all it encompasses, governments need to develop a better understanding of the ways Al-Qaeda and its affiliates use the Internet and technology. Intelligence agencies must be allowed to "think outside the box" and incorporate creative strategies that allow them to anticipate where the terrorist movements might next carve their path on the Internet. Western governments are behind in Internet cyber-warfare with Al-Qaeda. If they do not catch up, they will not gain the upper hand in the war on terror.

##

Shannen Rossmiller *retired from the bench as a municipal court judge in Montana in September 2006 and has since taken a position as the senior civil litigation specialist for the Montana Attorney General's Office.*