Radicalization:
Behind Bars and Beyond Borders

Frank J. Cilluffo*, Sharon L. Cardash, and Andrew J. Whitehead
Homeland Security Policy Institute
The George Washington University

The phenomenon of Islamic radicalization and recruitment of residents and citizens from Western countries has manifested itself in a series of terrorist attacks and activities including the bombings in Madrid (11 March 2004) and London (7 July 2005), and operations recently uncovered in Canada.[1] While resurgent, al-Qaeda in its classic form is now a degraded entity, with many of its remaining key figures on the run. However, it has franchised itself across the globe, with its franchises prepared to act locally and largely independently—in effect as a network of networks. Recently, we have seen the emergence of a leaderless movement, marked significantly by self-enlistment and taking its inspiration from "al-Qaeda classic" to join the global Salafi jihad.

Measures taken to combat this transnational insurgency have made it more difficult for extremist groups to recruit through mosques, and so the search for new and different areas of opportunity to expand their ranks is constant and outpacing many efforts to combat this threat.[2] This article focuses on two understudied but fertile grounds for radicalization in the United States: the nation's prison system and cyberspace. Until the bounds of the challenge in each of these contexts are better understood, effective, appropriately tailored prevention and response measures cannot be formulated and implemented.

Background

From the anarchist who assassinated President William McKinley, to the Ku Klux Klan, to the Unabomber, the United States is no stranger to homegrown terrorism. On 19 April 1995, Timothy McVeigh murdered 168 people in the United States' worst case

Frank J. Cilluffo is the director of the George Washington University Homeland Security Policy Institute (HSPI). Sharon L. Cardash is HSPI's associate director of research and education. Andrew J. Whitehead is a policy analyst at HSPI.

of domestic terrorism to date. However, U.S. counterterrorism efforts have been heavily focused on foreign threats. The roster of hijackers behind the 9/11 terrorist attacks explains why this is so: fifteen Saudis, two from the United Arab Emirates, an Egyptian, and a Lebanese. Though resilient and resurgent, al-Qaeda of 2001 is not al-Qaeda of the present. Having been driven out of its haven in Afghanistan in 2001, al-Qaeda has had to reinvent itself as a decentralized network of networks, relying on its component cells to operate locally and independently.

Ideology is the lifeblood of this movement, as anywhere this ideology takes root—even within the United States, among citizens born and raised here—a new cell can potentially arise. In this way, homegrown terrorism poses a unique set of threats, as potential terrorists could be anyone exposed and vulnerable (due to social, psychological, and other factors) to seduction by the jihadi-Salafist ideology and are often very difficult to detect until such individuals are ready to commit acts of violence.

Efforts to combat terrorism have of late relied strongly on military action even though the struggle against terrorism is as much a battle of ideas as it is a battle of bullets. As a result two potential avenues of radicalization have been understudied to date: the U.S. prison system and the Internet. Prison populations offer another entrée for extremist groups to promote their ideology.[3] The Internet, with its enormous reach and omnipresent role in modern society, provides a valuable means for extremists to spread their message. Given that ideology propels terrorists' recruitment, ideas—the winning of hearts and minds—must also be the driver underlying an effective response.

Radicalization in Prisons[4]

With the highest incarceration rate in the world, the United States is home to over two million inmates in jails and prisons. Millions more have spent time in prisons. The radicalization of even a small fraction of this population holds high-consequence potential.

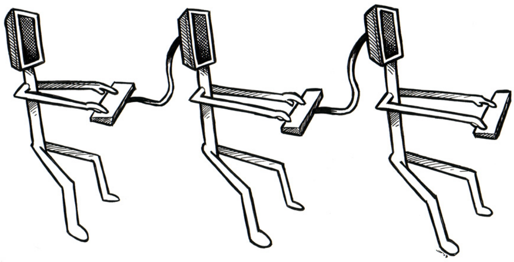
Historically, prisons have served as incubators of extreme ideas, and jihadists would not be the first to infiltrate and recruit from prisons. Right-wing extremist groups, including Posse Comitatus, the Order, Aryan Nations, and various militia movements, have been formed or recruited from U.S. prison populations for decades. This is because prisoners make inviting targets for extremists. Prisoners form a captive audience and often exhibit many characteristics that render them vulnerable to radicalization, including alienation, anti-social attitudes, cultural disillusionment, social isolation, and violent tendencies. Moreover, prisoners may be forced to join gangs in prison for the purpose of protection, giving extremists another opportunity to exert influence. Jihadists have adapted the efforts of other domestic extremist groups in order to further the spread of their own ideology among prisoners.

New Folsom State Prison in California offers a compelling illustration. A prisoner there, Kevin Lamar James, founded the extremist group Jam'iyyat Ul-Islam Is-Saheeh (Assembly of Authentic Islam, or JIS), and recruited fellow inmates while other members recruited outside the prison after having been paroled. The group planned a number of attacks on targets in the Los Angeles area, including U.S. military facilities, synagogues, and the Israeli consulate. The plot was ultimately discovered, though largely because a member of the group happened to drop a cell phone during a robbery.[5]

A prisoner's vulnerability to radicalization does not end after release from prison. Having served their sentences, individuals often leave prison with very little financial, emotional, or familial support. Where support does exist, it is often provided by community and religious groups; extremist groups can masquerade as legitimate support organizations in order to build ties with former prisoners. One extremist group, al-Haramain, maintained a database containing information on over 15,000 prisoners deemed vulnerable to the group's message, including names, release dates, and the addresses to which the individuals would be released.[6]

Radicalization and the Internet[7]

The Internet is cheap, pervasive, anonymous, unregulated, and uncensored; it allows for instantaneous communication with potentially huge audiences. Any group, no matter how small, can establish a major web presence through a professional-looking website that lends it an air of legitimacy, and almost every extremist group—there are hundreds or more—has a website.[8] Recruitment is not the only use extremists have made of the Internet; it has also proved a useful tool for (among other things) fundraising, training, planning, and attacking vulnerable computer systems and networked infrastructure belonging to perceived adversaries.[9] Radicalization and recruitment are, however, among the most important online activities for most extremists. Radicalization provides a pool of like-minded individuals from whom extremists can draw moral and material support, as well as recruits to replace losses and expand operations, which can produce new cells and groups from within.



The Internet grants extremists direct access to their audiences, allowing propagandists to bypass mainstream media outlets and institutions to which they have no access. Extremists have become very adept at using the Internet to craft their message and target audiences in increasingly sophisticated ways. Many terrorist websites are flashy, colorful, well-designed, and feature visually arresting graphic content. Many offer chat rooms, movies, and music, and some even feature online stores where users can buy t-shirts and CDs. In this way, terrorist groups target a computer savvy, media-saturated generation—specifically, youth. The features of the website are meant to attract an audience who can then be exposed to the extremist message, which is almost invariably about an Islam under attack, a West implacably hostile to Muslims, and the need to undertake jihad as a religious and moral imperative. Conveniently ignored is the fact that a significant proportion of the victims of terrorism are in fact Muslims.

In particular, extremists make extensive use of videos, circulated through their websites, to spread this simple message: Islam is under attack, and young Muslims have a personal duty to fight in defense of the *ummah*, or Muslim community. The videos make use of news footage from the Israeli–Palestinian conflict and conflicts in Iraq, Lebanon, Chechnya, Bosnia and Kosovo, and other hotspots around the world in order to depict the Muslim world as under attack. U.S. and allied troops and combat vehicles are framed as invaders, occupiers, and destroyers. Civilian casualties of those conflicts, especially Muslim women and children, are depicted as victims of Western aggression—sometimes in graphic detail. Muslim men are often depicted as part of a growing crowd angrily resisting Western aggression. The message is a direct appeal to Muslim youth around the globe to join the jihadi movement.

Conveniently ignored is the fact that a significant proportion of the victims of terrorism are in fact Muslims.

As the videos become increasingly sophisticated, they have become more tailored to their target audience of young Muslims. Some videos, for example, include hip-hop and rap musicians who extol jihadism and calls to violence. The importance of these videos to the jihadist movement is evident both in their abundance on extremist websites and also from the statements of the extremists themselves. One extremist wrote that "in many cases, the camera has more importance than the weapon and in many cases it surpasses the weapon in terms of its effect and power,"[10] while another said that one video is "worth more than a thousand sermons."[11] These websites provide a wealth of information about the extremists, as they conduct their business—communicating, debating, recruiting, and so on—openly on the Internet. In discussions online, jihadists promote the videos as the most valuable tool for recruitment, and in many cases, the jihadists identify the videos as their own inspiration for joining the movement in the first place.

In order to recruit, extremists who run these websites have developed ways of identifying which of these visitors are most receptive to their messages. A visitor's online activity is tracked by the website's operators and those who seem most interested are identified and targeted. Extremists will then contact the potential recruit via e-mail, on a forum, through a chat room, or through voice chat. In this way, they can engage a visitor one-on-one, indoctrinating directly. Extremists can also vet potential recruits in this manner, weeding out those who are not serious or trustworthy, as well as potential intelligence agents, by asking questions about Islam, the Arabic language, and extremist ideology. This gives extremists a chance to determine, through one-on-one contact, a potential recruit's dedication to the cause and willingness to sacrifice for it. Once a candidate for jihad has been deemed legitimate and worthy, he will receive instructions on the next steps, such as how to travel to Iraq, construct explosives, and fight against U.S. troops.[12] These websites often include information on conducting operations and constructing weapons.

The Internet provides an excellent environment for creating a community of like-minded extremists which may, in turn, spur additional self-enlistment and the formation of new cells. Whereas the Internet once promised a forum for untrammeled free speech and the free exchange of ideas, extremists have learned to manipulate the Internet in order to discourage dissension and deviation from their ideological line. Visitors to one extremist website are directed to visit other such sites. Internet forums and chat rooms, rather than fostering free and open discussion in which extremist ideas are challenged by competing ideas, often form echo chambers in which extremists find their ideas reinforced by others who hold equally aberrant views. New visitors and fence-sitters have their doubts assaulted and eroded by constant affirmations of the extremist viewpoint by like-minded users of the forum. Users who disagree with the extremist message are banned, and disagreements are discouraged.[13]

Responses

Jihadists rely on radicalization to create the pool from which their movement grows, spreads, and replenishes itself. A significant component to any response, then, will involve stopping the spread of this message of hate and violence.

In prisons, this means protecting a population vulnerable to this sort of message by denying extremists access to prisons. Some steps have already been taken toward this goal. The Federal Bureau of Prisons (FBOP) has changed some of its policies on certifying Muslim religious services providers to include more thorough background checks and more rigorous standards in order to weed out extremists from legitimate applicants. Very recently, however, the FBOP has relied on just ten Muslim chaplains for the entire federal prison system. These ten chaplains were responsible for vetting and endorsing contractors and volunteers who enter prisons to provide religious services, a Herculean task when one considers the thousands of contractors and volunteers who enter prisons each month.

FBOP staff members have also received training on Islamic beliefs, putting prison officials in a better position to identify and ban extremist materials from their facilities. That said, overstretched prison staff would be hard pressed to review each and every document entering prisons to determine whether it contains a message of violence and extremism. Calls to violence may be scattered throughout a text and become evident only upon a close reading. There exist, for example, a number of English-language translations of the Qur'an which, through selective interpretation and insertions in the text, footnotes, and appendices, transform the book into a call to jihadism.[14]

Efforts have been made to improve information and intelligence sharing. By way of illustration, the California state government has created several Joint Regional Intelligence Centers (JRICs) and Regional Threat Assessment Centers (RTACs) which are composed of representatives from prison staffs, the Los Angeles County Sheriff's Department, the Los Angeles Police Department, the Federal Bureau of Investigation, the Drug Enforcement Agency and the assistant U.S. attorney for the area. However, the JRICs and RTACs meet only infrequently, and are designed to study the problem from a strategic perspective rather than to support operations against extremist groups.[15]

Just as a prisoner's vulnerability to radicalization does not end with release, so too must countering prisoner radicalization look beyond prison walls. It is therefore crucial to identify steps to effectively reintegrate former inmates into the larger society. The problems faced by prisoners after release are not new, but they take on a new dimension when jihadism enters the picture.

Responding to extremist recruitment over the Internet requires a different approach. Whereas responses to prisoner radicalization may take the form of denying extremists access to inmates, the nature of the Internet prevents a similar approach. Websites can be quickly and easily established from anywhere in the world, and attempts to shut them down can be easily thwarted through a number of methods: site owners can switch servers faster than authorities can find them and shut them down; hide files on legitimate websites, using proxy servers to create an electronic mask; encrypt communications with obscure dialects and codes; and so forth.[16] Authorities can and sometimes do try to identify and shut down extremist websites used to radicalize and recruit, but we cannot rely on this effort alone to have a decisive impact. Rather than trying to close off extremists' access to their target audience, it may be more productive to work towards attempting to disrupt and counter the extremist message itself.

It may be more productive to work towards attempting to disrupt and counter the extremist message itself.

One potential countering effort would borrow a page from the extremists, and display the victims of terrorism online. Extremists have had great success in energizing their ranks through photographs and videos that depict the Muslim victims of Western violence. Civilian casualties in Iraq, for example, are depicted in gory detail as victims of U.S. atrocities. Conversely, an online campaign designed to create a counter-presence on the Web would focus on depicting the human costs of terrorism. New websites could be created to carry this message. Officials could also take advantage of the interactive features of many websites, such as chat rooms and forums, and supply images of the costs of terrorism directly to the target audience. Indeed, campaigns against popular support for terrorism have been waged in the past. In Saudi Arabia, for example, as part of a government effort, banners depicting the victims of terrorism were hung over busy streets. Notably, according to an advisor to the Saudi government, support for al-Qaeda in that country has dropped and the group's physical presence there has been largely eliminated—though it is not certain that a jarring visual display of the sort described was exclusively responsible.[17] Further, prior to 9/11, the Spanish Ministry of the Interior issued, in four different languages, a 22-minute counter-propaganda VHS tape titled "The Face of ETA."

Another possible course of action involves utilizing the nature of the Internet against extremists. The anonymity provided by the Internet has been a boon to extremists, as it has allowed them to work in the open and still avoid identification. Yet this same feature may permit counterterrorism officials to infiltrate online extremist discussions, thereby offering an opportunity to disrupt the relevant online community. Contributors to extremist websites, despite their anonymous nature, may become trusted sources of information through the volume and quality of their involvement.[18] Through careful and patient work, an intelligence officer could infiltrate an online extremist community in the same way.

While an officer or even a team of officers operating anonymously is unlikely to bring down an extremist group through forum postings and chat room discussions, such groups require trust in order to function. Counterterrorism officials may be able to exploit this to sow doubt, confusion, and distrust in order to begin dissolving the ties that bind individual extremists into a cohesive and dangerous group. Accusations of spying can be leveled by an actual spy against a true believer just as easily as the reverse. Accusations of being a tool of the enemy, while unlikely to be taken at face value from an anonymous contributor, can begin to plant the seeds of distrust between security-conscious extremists. Officers could accuse extremists of posting virus-laden files, providing faulty bomb-making instructions, or attempting to recruit turncoats for the authorities—anything to erode trust and disrupt the groups' online activities. Teams of intelligence officers working the same online groups might, over time, turn the extremists' entire effort into a shouting match over trust and betrayal until the dedicated members give up in disgust.

Intelligence agencies could also establish "honey pots"—websites which resemble extremist websites and which would allow intelligence officers to spread disinformation directly to the same audiences targeted by extremists, as well as gather demographic information about visitors to the websites, which can help in the crafting of effective counter-messages. Unfortunately, personnel and time are less than abundant resources for intelligence agencies. As the Internet is not restricted to any national boundary or geographical location, these methods would apply to both foreign and domestic anti-terrorism efforts.

With regard to countering radicalization both in prisons and over the Internet, there are existing models (tailored to other settings) from which we can draw lessons that may inform and shape our responses in the present context. In the case of prisons, officials have been combating recruitment by violent gangs for decades. In the case of the Internet, officials have grappled for years with the control of dangerous online behavior such as child pornography. While precedents may not fit perfectly, there may be "best practices" that can be adapted and used to help develop a comprehensive strategy to counter these means of radicalization.

In both cases, local communities must play a significant role in countering radicalization. With regard to prisons, for example, over 90 percent of inmates in the U.S. prison system are in state and local prisons and jails.[19] Local communities are best positioned to identify broader avenues of dialogue with Muslim communities and to develop and implement outreach programs in order to better foster mutual respect and understanding.

Looking Ahead

Extremist recruitment of all kinds, in part, preys on alienation. The threat of violent Muslim fundamentalist movements recruiting in the United States is smaller than in Western Europe, since Muslims living the United States are, on average, more integrated, more prosperous, and therefore less alienated. However, the face of extremism is not necessarily foreign to Americans. Adam Gadahn for instance—an American from California—has become the English-language spokesperson for al-Qaeda by broadcasting propaganda over the Internet.[20] Starting in a better position than West European countries, the United States can address the areas of prison recruitment and the information war of the Internet to prevent future extremism in force.

In both cases, the problem is complex, and therefore professionals from no single discipline alone are equipped to handle it. The face of terrorism is always transforming, propelled by developments in a variety of areas, including technology, terrorist leadership, political reform in relevant countries, the availability of safe havens, and even U.S. efforts to prevent and combat terrorism, to which extremists are constantly adapting. A multidisciplinary approach that includes the diverse perspectives of religion, criminal justice, law, intelligence, information science, network theory, and behavioral science is vital for analysis of these phenomena. Also vital will be a better understanding of the radicalization process, in order to develop metrics and better identify this phenomenon when it occurs. An effective response to terrorism will require not only multidisciplinary analysis, but also seamless coordination among federal, state, and local authorities, as well as with international partners. Response efforts referenced above offer only a thumbnail sketch of a handful of key measures; the discussion was not intended to be exhaustive.

It is only by challenging ideas with ideas, both within and beyond prison walls or the Internet, that hearts and minds may ultimately be changed.

** This article is dedicated to the memory of Robert Kupperman—a mentor and a dear friend. Together, we contributed "Between War and Peace: Deterrence and Leverage" to the inaugural edition of the* Brown Journal of World Affairs.

Notes

[1] "Two key processes pave the way towards actual terrorism: radicalisation and recruitment. Radicalisation is a social process, while recruitment is a form of 'direction' that taps into radicalisation and seeks to channel it in the direction of violence." National Coordinator for Terrorism, "What is Terrorism?" Netherlands Ministry of the Interior and Kingdom Relations, Netherlands Ministry of Justice, http://english.nctb.nl/what_is_terrorism/introduction.

[2] U.S. Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, (12 April 2004), 263, http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf. For the purposes of this paper, "insurgency" refers to "an organized movement aimed at the overthrow of a constitutional government through the use of subversion and armed combat." Al-Qaeda and the global Salafi jihad should be viewed as a transnational insurgency, seeking to overthrow and replace the governments of the Muslim world and beyond, and making use of terrorism as one of many tools to achieve their objectives.

[3] U.S. Department of Justice Office of the Inspector General, *Analysis of the Response by the Federal Bureau of Prisons to Recommendations in the OIG's April 2004 Report on the Selection of Muslim Religious Service Providers*, July 2004. For the purposes of this paper, radicalization refers to "the process by which [people] adopt extreme views, including beliefs that violent measures need to be taken for political or religious purposes."

[4] For a more detailed discussion of prisoner radicalization, see Frank Cilluffo, Gregory Saathoff, and others, "Out of the Shadows: Getting Ahead of Prisoner Radicalization," report by the George Washington University's Homeland Security Policy Institute and the University of Virginia's Critical Incident Analysis Group, 19 September 2006. Figures, concepts, and certain passages herein are drawn from that report. See also "Prison Radicalization: Are Terrorist Cells Forming in U.S. Cell Blocks?" (testimony, Senate Committee on Homeland Security and Governmental Affairs, 19 September 2006).

[5] United States vs. Kevin James, U.S. District Court for the Central District of California, October 2004.

[6] Daveed Gartenstein-Ross, "Prison Radicalization: Are Terrorist Cells Forming in U.S. Cell Blocks?"

(testimony, Senate Homeland Security and Governmental Affairs Committee, 19 September 2006).

7. See, for example, Marc Sageman, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004); Reuven Paz, "Reading Their Lips: The Credibility of Jihadi Web Sites in Arabic as a Source for Information," http://www.e-prism.org/images/Read_Their_Lips.doc; and Stephen Ulph, "The Next Stage in Counter-terrorism: Jihadi Radicalisation on the Web," http://www.jamestown.org/docs/JR-Slides.pdf. See also Frank Cilluffo, Gregory Saathoff, and others, "NETworked Radicalization: A Counter-Strategy," report by the George Washington University's Homeland Security Policy Institute and the University of Virginia's Critical Incident Analysis Group, 3 May 2007. Figures, concepts, and certain passages herein are drawn from that report.

8. Bruce Hoffman, "The Use of the Internet by Islamic Extremists" (testimony, Select Committee on Intelligence, U.S. House of Representatives, 4 May 2006); Gabriel Weimann, "www.terror.net: How Modern Terrorism Uses the Internet," *United States Institute of Peace* (Mar 2004): 2.

9. Maura Conway, "Terrorist 'Use' of the Internet and Fighting Back," (lecture, Oxford Internet Institute, 10 Sep 2005).

10. Unknown author, "Jihadi Iraq—Hopes and Risks: Analysis of the Reality, Overview of the Future and Practical Steps on the Way of the Blessed Jihad," published on the Global Islamic Media website on 10 December 2003.

11. Javier Jordan and Nicola Horsburgh, "Mapping Jihadist Terrorism in Spain," *Studies in Conflict and Terrorism* (May–June 2005): 176–177.

12. Gabriel Weimann, "www.terror.net": 8.

13. S.J. van Hulst, "Violent Jihad in the Netherlands: Current Trends in the Islamist Terrorist Threat." Netherlands Ministry of the Interior and Kingdom Relations, http://english.nctb.nl/Images/Violent%20jihad%20in%20the%20Netherlands%202006_tcm127-112471.pdf.

14. Cilluffo, Saathoff, and others, "Out of the Shadows," 6.

15. Ibid., 11.

16. "Examining the Cyber Capabilities of Islamic Terrorist Groups," Institute for Security Technology Studies at Dartmouth College, http://www.ists.dartmouth.edu/TAG/ITB/ITB_032004.pdf.

17. Anthony Cordesman and Nawaf Obaid, *Al-Qaeda in Saudi Arabia: Asymmetric Threats and Islamist Extremists* (Center for Strategic and International Studies: 2005), 23.

18. Nadya Labi, "Jihad 2.0," *Atlantic Monthly* (Jul/Aug 2006): 103.

19. Office of Justice Programs, Bureau of Justice Statistics, *Prison Statistics*, Department of Justice, http://www.ojp.usdoj.gov/bjs/correct.htm.

20. Raffi Khatchadourian, "Azzam the American: The Making of an Al-Qaeda Homegrown," *New Yorker* (22 January 2007).