National Security Program

Homeland Security Project

Countering Online Radicalization in America: Executive Summary

The Internet has revolutionized the way all of us communicate and do business. Its benefits to people everywhere have been enormous and will continue to drive progress in practically every area of life. At the same time, it should be recognized that, while being a force for good, the Internet has also come to play an important—and, in many ways, unique—role in radicalizing homegrown and domestic terrorists. Supporters of Al Qaeda, Sovereign Citizens, white supremacists and neo-Nazis, environmental and animal liberationists, and other violent extremist groups all have embraced the Internet with great enthusiasm and vigor. They are using it as a platform to spread their ideas, connect with each other, make new recruits, and incite illegal and violent actions.

We believe that this trend will continue and that future terrorist attacks against the United States and its interests will involve individuals who have been radicalized—at least in part—on the Internet. As a result, countering online radicalization should continue to be a major priority for the government and its Countering Violent Extremism (CVE) efforts.

The purpose of this report is to equip policy makers with a better understanding of how the Internet facilitates radicalization, in particular within the United States; an appreciation of the dilemmas and trade-offs that are involved in countering online radicalization within the United States; and ideas and best practices for making the emerging approach and strategy richer and more effective.

In doing so, this report builds on previous reports by the Bipartisan Policy Center's (BPC) Homeland Security Project, especially *Assessing the Terrorist Threat* (2010) and *Preventing Violent Radicalization in America* (2011).

The Strategy

In its 2011 counter-radicalization strategy and the subsequent implementation plan, the White House acknowledged that "the Internet has become an increasingly potent element in radicalization to violence," and promised to "develop a separate, more comprehensive strategy for countering and preventing violent extremist online radicalization and leveraging technology to empower community resilience." Nearly a year later, this still hasn't happened, and the report's first and most important recommendation is for the White House to complete its work on the strategy, make it public, and begin its implementation with alacrity.

In strategic terms, online radicalization can be dealt with in three ways:

Approaches aimed at *restricting freedom of speech and removing* content from the Internet are not only the least desirable strategies, they are also the least effective.

Instead, government should play a more energetic role in *reducing the demand for radicalization and violent extremist messages*—for example, by encouraging civic challenges to extremist narratives and by promoting awareness and education of young people.

In the short term, the most promising way to deal with the presence of violent extremists and their propaganda on the Internet is to *exploit, subject to lawful guidelines and appropriate review and safeguards, their online communications to gain intelligence and gather evidence* in the most comprehensive and systematic fashion possible.

Reducing the Supply

For reasons ranging from the political to the practical, approaches that are aimed at reducing the supply of violent extremist content on the Internet are neither feasible nor desirable. They also tend to conflict with the imperative of gaining intelligence that can be useful in pursuing terrorists and preventing terrorist plots.

Filtering of Internet content is impractical in a free and open society, taking down foreign-based websites should only be a very last resort, bringing prosecutions against propagandists often does more harm than good by publicizing their rhetoric, and relationships with Internet companies are more productive when based on partnerships, not confrontation.

The report's recommendations are as follows:

- Government should refrain from establishing nationwide filtering systems.
- Government needs to retain its capability for aggressive takedowns of foreign-based websites but only use it when doing so is absolutely essential to stop a terrorist attack and/or prevent the loss of life.
- The circumstances and legal framework governing the use of cyber-attacks need to be clarified.
- Prosecutions against violent extremist Internet entrepreneurs need to weigh the chances of success against the unintended consequence of drawing attention to their ideas and propaganda.
- Government should accelerate the establishment of informal partnerships to assist large Internet companies in understanding national security threats as well as trends and patterns in terrorist propaganda and communication.

Reducing the Demand

Much needs to be done to activate a virtual marketplace in which extremism, terrorism, and other bad ideas are drowned out by pluralism, democracy, and the peaceful means through which good ideas can be advanced.

The federal government can play a limited but positive role in helping to bring this marketplace about—for example, by helping to create awareness, convene relevant non-governmental actors, build capacity, and foster media literacy. While doing so, government needs to be realistic about its own role, the extent to which civic challenges to violent extremist ideologies can be engineered (especially on the Internet), and the time and resources that is required for them to become effective.

The report's recommendations are as follows:

- Government, in partnership with community groups, needs to continue to expand programs and initiatives that create awareness and spread information about online radicalization among educators, parents, and communities.
- Government should serve as an enabler, bringing together the private sector, foundations, philanthropists, and community groups to build capacity and to help potentially credible messengers—such as mainstream groups, victims of terrorism, and other stakeholders—to become more effective at conveying their messages. The forthcoming Internet strategy should spell out what the government will do and how success will be measured.
- The government's Internet strategy also needs to make clear what part of government will coordinate capacity building, engagement, and outreach efforts as well as what resources will be made available to support this task.

- The government should encourage school authorities to review and update their curricula on media literacy, consider violent extremism as part of their instruction on child-safety issues, and develop relevant training resources for teachers.

Exploiting Cyberspace

Rather than removing violent extremist content or trying to undercut the demand for it, a different approach for dealing with online radicalization is to take full advantage of violent extremists' and terrorists' presence in cyberspace and make maximum use of the information they are sharing with others.

This information can be used to gain strategic intelligence on terrorist groups' intentions and networks, on tactical intelligence on terrorist operations and the people who are involved in them, and on evidence that can be used in prosecutions.

Doing so is the most effective way of dealing with online radicalization in the short term, and government should pursue this approach more systematically. This, however, requires the clarification of existing laws and the creation of appropriate review and oversight mechanisms that will give domestic agencies more confidence to operate in cyberspace.

The report's recommendations are as follows:

- Government needs to review oversight procedures and clarify the legal framework under which domestic agencies are permitted to monitor, save, and analyze online communications.
- Government should increase the amount of online training offered to members of law enforcement and intelligence agencies, including state and local agencies.
- Given the rapidly changing nature of the online environment, government needs to periodically review the scope, sophistication, and appropriateness of the regulatory framework that governs data gathering and analysis in cyberspace, as well as the technological tools and capabilities that are used for doing so.

Arguably, the use of the Internet to radicalize and recruit homegrown terrorists is the single-most important and dangerous innovation since the terrorist attacks of September 11, 2001. This should remind us that dealing with online radicalization must not be a one-off effort. As the Internet keeps changing, so do the methods of those who want to use it to spread hate and incite terror.

National Security Program

Homeland Security Project

Countering Online Radicalization **in America**

December 2012

BIPARTISAN POLICY CENTER

ACKNOWLEDGMENTS

BPC would like to thank Gordon Lederman and C. Michael Hurley for their invaluable assistance in putting this report together.

DISCLAIMER

This report is the product of the Bipartisan Policy Center's Homeland Security Project. The findings and recommendations expressed herein do not necessarily represent the views or opinions of the Bipartisan Policy Center, its founders, or its board of directors.

Letter from the Co-Chairs

We are proud to serve as co-chairs of the Bipartisan Policy Center's (BPC) Homeland Security Project. We launched it to carry on the bipartisan work of the 9/11 Commission, cooperating with the administration, Congress, state and local authorities and the private sector on the most pressing homeland and national security issues.

In the days after 9/11, people asked "how did this happen?" and "what could we have done to prevent it?" When we agreed to lead the 9/11 Commission, our goal was to answer the first question in as clear and factual a way possible and to make, and see implemented, recommendations to prevent future attacks and keep the country safe. The second question is ongoing, because we need to constantly reassess, stay one step ahead of those who would do us harm, and take actions to thwart them before they strike.

Grave threats against our nation persist, though they differ in some respects from what we faced in the first years after the 9/11 attacks. We are now confronted with the sad fact that many of these threats exist within our borders. So-called homegrown lone wolf extremists, their minds poisoned by radical doctrines of hate and violence, have struck in our communities. In BPC's 2011 report *Preventing Violent Radicalization in America*, we examined this alarming trend and asked who inside our government was in charge of monitoring and preventing violent radicalization.

It became clear to us that a growing number of individuals find radical materials and mentors online, whether through direct searches or by chance. Through repeated online interactions with extremist materials, these people become more and more radicalized, develop violent beliefs in their own living rooms, and completely isolate themselves from contact with more moderate, non-violent influences.

This report asks what is online radicalization, how and why is it happening, how serious is the threat, and what can government do to prevent it. While misguided individuals who harbor violent tendencies will always exist and pose a threat, we believe there is an urgent need for revised policies as well as strengthened and retooled approaches that can make an impact, thereby lessening the chance that impressionable users of the Internet will find and respond to online hatred and calls to violence.

In a threat environment that continues to evolve and at times change rapidly, an important goal is to reduce the ability of our enemies to propagate and attract new followers. Implementing a robust and relevant strategy that decreases the likelihood an extremist can reach and convince a new recruit to join in violence, whether they are in the same town, same country or same continent, is one of the most powerful measures we can take to keep our country safe and secure.

Sincerely,

Thomas H. Kean

Former 9/11 Commission Co-Chair and
Governor of New Jersey

Lee H. Hamilton

Former 9/11 Commission Co-Chair and
Representative from Indiana

National Security Program
Homeland Security Project

Homeland Security Project

PROJECT CO-CHAIRS

Thomas H. Kean
Former 9/11 Commission Co-Chair and Governor of New Jersey

Lee H. Hamilton
Former 9/11 Commission Co-Chair and Representative from Indiana

PROJECT MEMBERS

Peter Bergen
National Security Analyst, CNN

Christopher Carney
Former Representative from Pennsylvania and Chair of the U.S. House Homeland Security Oversight Committee

Stephen E. Flynn, Ph.D.
Founding Co-Director of the George J. Kostas Research Institute for Homeland Security and Professor of Political Science at Northeastern University

Dr. John Gannon
Former Deputy Director of the CIA for Intelligence and President of BAE Systems' Intelligence & Security business

Dan Glickman
BPC Senior Fellow; Former Secretary of Agriculture; Former Chairman of the U.S. House Intelligence Committee

Dr. Bruce Hoffman
Director, Center for Peace and Security Studies, Georgetown University

Michael P. Jackson
Chairman and CEO, VidSys, Inc. and Former Deputy Secretary of the U.S. Department of Homeland Security

Ellen Laipson
President and CEO of the Stimson Center and member of the President's Intelligence Advisory Board

Michael E. Leiter
Senior Counselor to the Chief Executive Officer, Palantir Technologies and Former Director of the National Counterterrorism Center

Edwin Meese III
Former U.S. Attorney General, Ronald Reagan Distinguished Fellow in Public Policy and Chairman of the Center for Legal and Judicial Studies at The Heritage Foundation

Erroll G. Southers
Former Chief of Homeland Security and Intelligence for the Los Angeles Airports Police Department; and Associate Director of the National Center for Risk and Economic Analysis of Terrorism Events at the University of Southern California

Richard L. Thornburgh
Former U.S. Attorney General and Of Counsel at K&L Gates

Frances Townsend
Former Homeland Security Advisor and Deputy National Security Advisor for Combating Terrorism

Jim Turner
Former Representative from Texas and Ranking Member of the U.S. House Homeland Security Committee

HOMELAND SECURITY PROJECT STAFF

Carie Lemack
Director

REPORT AUTHOR

Dr. Peter Neumann
Founding Director, International Centre for the Study of Radicalisation at King's College London

National Security Program
Homeland Security Project

Table of Contents

National Security Program
Homeland Security Project

Executive Summary

The Internet has revolutionized the way all of us communicate and do business. Its benefits to people everywhere have been enormous and will continue to drive progress in practically every area of life. At the same time, it should be recognized that, while being a force for good, the Internet has also come to play an important—and, in many ways, unique—role in radicalizing homegrown and domestic terrorists. Supporters of Al Qaeda, Sovereign Citizens, white supremacists and neo-Nazis, environmental and animal liberationists, and other violent extremist groups all have embraced the Internet with great enthusiasm and vigor. They are using it as a platform to spread their ideas, connect with each other, make new recruits, and incite illegal and violent actions.

We believe that this trend will continue and that future terrorist attacks against the United States and its interests will involve individuals who have been radicalized—at least in part—on the Internet. As a result, countering online radicalization should continue to be a major priority for the government and its Countering Violent Extremism (CVE) efforts.

The purpose of this report is to equip policy makers with a better understanding of how the Internet facilitates radicalization, in particular within the United States; an appreciation of the dilemmas and trade-offs that are involved in countering online radicalization within the United States; and ideas and best practices for making the emerging approach and strategy richer and more effective.

In doing so, this report builds on previous reports by the Bipartisan Policy Center's (BPC) Homeland Security Project, especially *Assessing the Terrorist Threat* (2010) and *Preventing Violent Radicalization in America* (2011).

The Strategy

In its 2011 counter-radicalization strategy and the subsequent implementation plan, the White House acknowledged that "the Internet has become an increasingly potent element in radicalization to violence," and promised to "develop a separate, more comprehensive strategy for countering and preventing violent extremist online radicalization and leveraging technology to empower community resilience." Nearly a year later, this still hasn't happened, and the report's first and most important recommendation is for the White House to complete its work on the strategy, make it public, and begin its implementation with alacrity.

In strategic terms, online radicalization can be dealt with in three ways:

Approaches aimed at *restricting freedom of speech and removing* content from the Internet are not only the least desirable strategies, they are also the least effective.

Instead, government should play a more energetic role in *reducing the demand for radicalization and violent extremist messages*—for example, by encouraging civic challenges to extremist narratives and by promoting awareness and education of young people.

In the short term, the most promising way to deal with the presence of violent extremists and their propaganda on the Internet is to *exploit, subject to lawful guidelines and appropriate review and safeguards, their online communications to gain intelligence and gather evidence* in the most comprehensive and systematic fashion possible.

Reducing the Supply

For reasons ranging from the political to the practical, approaches that are aimed at reducing the supply of violent extremist content on the Internet are neither feasible nor desirable. They also tend to conflict with the imperative of gaining intelligence that can be useful in pursuing terrorists and preventing terrorist plots.

Filtering of Internet content is impractical in a free and open society, taking down foreign-based websites should only be a very last resort, bringing prosecutions against propagandists often does more harm than good by publicizing their rhetoric, and relationships with Internet companies are more productive when based on partnerships, not confrontation.

The report's recommendations are as follows:

- Government should refrain from establishing nationwide filtering systems.
- Government needs to retain its capability for aggressive takedowns of foreign-based websites but only use it when doing so is absolutely essential to stop a terrorist attack and/or prevent the loss of life.
- The circumstances and legal framework governing the use of cyber-attacks need to be clarified.
- Prosecutions against violent extremist Internet entrepreneurs need to weigh the chances of success against the unintended consequence of drawing attention to their ideas and propaganda.
- Government should accelerate the establishment of informal partnerships to assist large Internet companies in understanding national security threats as well as trends and patterns in terrorist propaganda and communication.

Reducing the Demand

Much needs to be done to activate a virtual marketplace in which extremism, terrorism, and other bad ideas are drowned out by pluralism, democracy, and the peaceful means through which good ideas can be advanced.

The federal government can play a limited but positive role in helping to bring this marketplace about—for example, by helping to create awareness, convene relevant non-governmental actors, build capacity, and foster media literacy. While doing so, government needs to be realistic about its own role, the extent to which civic challenges to violent extremist ideologies can be engineered (especially on the Internet), and the time and resources that is required for them to become effective.

The report's recommendations are as follows:

- Government, in partnership with community groups, needs to continue to expand programs and initiatives that create awareness and spread information about online radicalization among educators, parents, and communities.
- Government should serve as an enabler, bringing together the private sector, foundations, philanthropists, and community groups to build capacity and to help potentially credible messengers—such as mainstream groups, victims of terrorism, and other stakeholders—to become more effective at conveying their messages. The forthcoming Internet strategy should spell out what the government will do and how success will be measured.
- The government's Internet strategy also needs to make clear what part of government will coordinate capacity building, engagement, and outreach efforts as well as what resources will be made available to support this task.

- The government should encourage school authorities to review and update their curricula on media literacy, consider violent extremism as part of their instruction on child-safety issues, and develop relevant training resources for teachers.

Exploiting Cyberspace

Rather than removing violent extremist content or trying to undercut the demand for it, a different approach for dealing with online radicalization is to take full advantage of violent extremists' and terrorists' presence in cyberspace and make maximum use of the information they are sharing with others.

This information can be used to gain strategic intelligence on terrorist groups' intentions and networks, on tactical intelligence on terrorist operations and the people who are involved in them, and on evidence that can be used in prosecutions.

Doing so is the most effective way of dealing with online radicalization in the short term, and government should pursue this approach more systematically. This, however, requires the clarification of existing laws and the creation of appropriate review and oversight mechanisms that will give domestic agencies more confidence to operate in cyberspace.

The report's recommendations are as follows:

- Government needs to review oversight procedures and clarify the legal framework under which domestic agencies are permitted to monitor, save, and analyze online communications.
- Government should increase the amount of online training offered to members of law enforcement and intelligence agencies, including state and local agencies.
- Given the rapidly changing nature of the online environment, government needs to periodically review the scope, sophistication, and appropriateness of the regulatory framework that governs data gathering and analysis in cyberspace, as well as the technological tools and capabilities that are used for doing so.

Arguably, the use of the Internet to radicalize and recruit homegrown terrorists is the single-most important and dangerous innovation since the terrorist attacks of September 11, 2001. This should remind us that dealing with online radicalization must not be a one-off effort. As the Internet keeps changing, so do the methods of those who want to use it to spread hate and incite terror.

National Security Program
Foreign Policy Project

Chapter 1: Introduction

The killing of six worshippers at a Sikh Temple in Wisconsin in early August 2012 was the second most deadly terrorist attack in the United States since September 11, 2001.[1] Wade Michael Page, the gunman, was a neo-Nazi who had been deeply immersed in America's white supremacist counterculture. A rock singer whose body was covered in racist tattoos, he had been a member of several white-power bands that played at festivals across the country.[2] When he wasn't on tour, however, he spent much of his time online, promoting his music and hanging out with other skinheads and neo-Nazis on websites like the white supremacist online forum Stormfront. There is no evidence Page became radicalized on the Internet, but it made him feel involved and important, and it connected him to people who were thinking the same way. On one website alone, he had posted more than 250 comments, often urging others to act on their convictions and "stop hiding behind the computer or making excuses."[3]

On the one hand, no one should be surprised that violent extremists like Page are using the Internet: In 21st-century America, practically everyone is using the Internet, and violent extremists are no exception. That said, violent extremists and terrorists have embraced the new technology with particular enthusiasm and vigor. The most prominent example is the late Anwar Al Awlaki, the Yemen-based, U.S.-born cleric whose entire strategy revolved around inspiring, inciting, and directing Americans to attack their own country. He did so by using e-mail, blogs, discussion forums, chat rooms, video, and the English-language online magazine *Inspire*, which told its readers "how to build a bomb in the kitchen of your mom." Awlaki was the inspiration behind a dozen terrorist plots,[4] and he was involved in a lengthy exchange of e-mails with Major Nidal Hasan, who killed 13 people at Fort Hood in November 2009, the most devastating terrorist attack on U.S. soil after the September 11 attacks.[5]

With Awlaki in mind, the White House's counter-radicalization strategy, published in August 2011, acknowledged "the important role the Internet and social networking sites play in advancing violent extremist narratives."[6] The strategy's implementation plan, which came out in December 2011, stated that "the Internet has become an increasingly potent element in radicalization to violence"[7] and that new "programs and initiatives" had to be "mindful of the online nature of the threat."[8] Crucially, it also committed the administration to formulate a strategy in its own right:

> [B]ecause of the importance of the digital environment, we will develop a separate, more comprehensive strategy for countering and preventing violent extremist online radicalization and leveraging technology to empower community resilience.[9]

By the time this report went to print, however, no such online strategy had been published, and no date for publication had been set.

As with previous reports, the Homeland Security Project's intention with this document is to offer fresh ideas and—in doing so—support the government's efforts to protect the American people from homegrown terrorism:

- The project's 2010 report, *Assessing the Terrorist Threat*, highlighted the increasingly homegrown nature of the threat and called on the administration to do more to protect young Americans from being radicalized and recruited by Al Qaeda. At the time, the report argued that the absence of a coherent approach in this area was "fundamentally troubling."[10]
- The project's 2011 report, *Preventing Violent Radicalization in America*, anticipated—and welcomed—the publication of the 2011 domestic counter-radicalization strategy.[11] It surveyed best practices, and offered ideas and practical recommendations for making

the White House's strategy more systematic and effective.

This latest report pursues a similar approach. Its purpose is to equip policy makers with a better understanding of how the Internet facilitates radicalization, in particular within the United States; with an appreciation of the dilemmas and trade-offs that are involved in *countering* online radicalization within the United States; and with ideas and best practices for making the emerging approach and strategy richer and more effective.

This report will show that the Internet is a unique and challenging environment, in which terrorist radicalization and recruitment takes place, and that understanding and penetrating this environment are essential to preventing homegrown terrorism. (For key terms and definitions, see Box 1.)

From the author's interviews with government officials and other stakeholders,[12] it seems clear that as of fall 2012 online radicalization should continue to be a major priority for the government and its Countering Violent Extremism (CVE) efforts. While the killing of Anwar Al Awlaki, who had pioneered the use of the Internet to radicalize young Americans, has removed one of the main drivers of Al Qaeda–related radicalization in recent years, this does not diminish the role of the Internet as a vehicle through which radicalization efforts are conducted. Indeed, based on project interviews, there seems to be a strong consensus among different government departments and agencies as well as independent analysts and experts that the growing importance of the Internet in radicalization is the single most significant innovation to have affected homegrown radicalization since the September 11 attacks in 2001. Furthermore, as the Internet keeps evolving, so do the methods of those who want to use this technology to incite terror, and it is vitally important, therefore, for law enforcement and intelligence agencies to be effective at combating the terrorist threat in this new and rapidly changing arena.

Preventing online radicalization requires a balanced and sophisticated approach:

- First comes the recognition that—for constitutional, political, and practical reasons—it is impossible to remove all violent extremist material from the Internet and that most efforts aimed at *reducing the supply* of violent extremist content on the Internet are costly and counterproductive.
- More important, therefore, are measures that seek to *reduce the demand* for radicalization and violent extremist messages: for example, by discrediting, countering, and confronting extremist narratives or by educating young people to question the messages they see online.
- Another key component is *exploiting* online content and interactions for the purpose of gathering information, gaining intelligence, and pursuing investigations.

Most measures aimed at removing content and/or restricting access to the Internet are neither practical nor desirable, and they must not, therefore, become the central plank of the government's strategy. The federal government must play a more energetic role in facilitating and encouraging civic challenges to extremist ideas, and it should help, where possible and appropriate, to inoculate young people against their appeal. Moreover, law enforcement and intelligence agencies need to become more systematic and sophisticated in exploiting the Internet for investigations and intelligence, which may be the most effective approach for dealing with online extremism in the short term.

Box 1: Key Terms and Concepts[13]

Radicalization is the process whereby groups or individuals become political extremists. The concept of extremism, however, is ambiguous: It may refer to extremist ideas (ideas and ideologies that oppose a society's core values and principles) or extremist methods ("showing disregard for the life, liberty, and human rights of others").[14] As a result, experts distinguish between cognitive radicalization (extremist ideas) and violent radicalization (extremist methods). Many governments describe terrorists and insurgents as "violent extremists"—a term that stresses the violent, rather than purely cognitive, nature of their extremism.

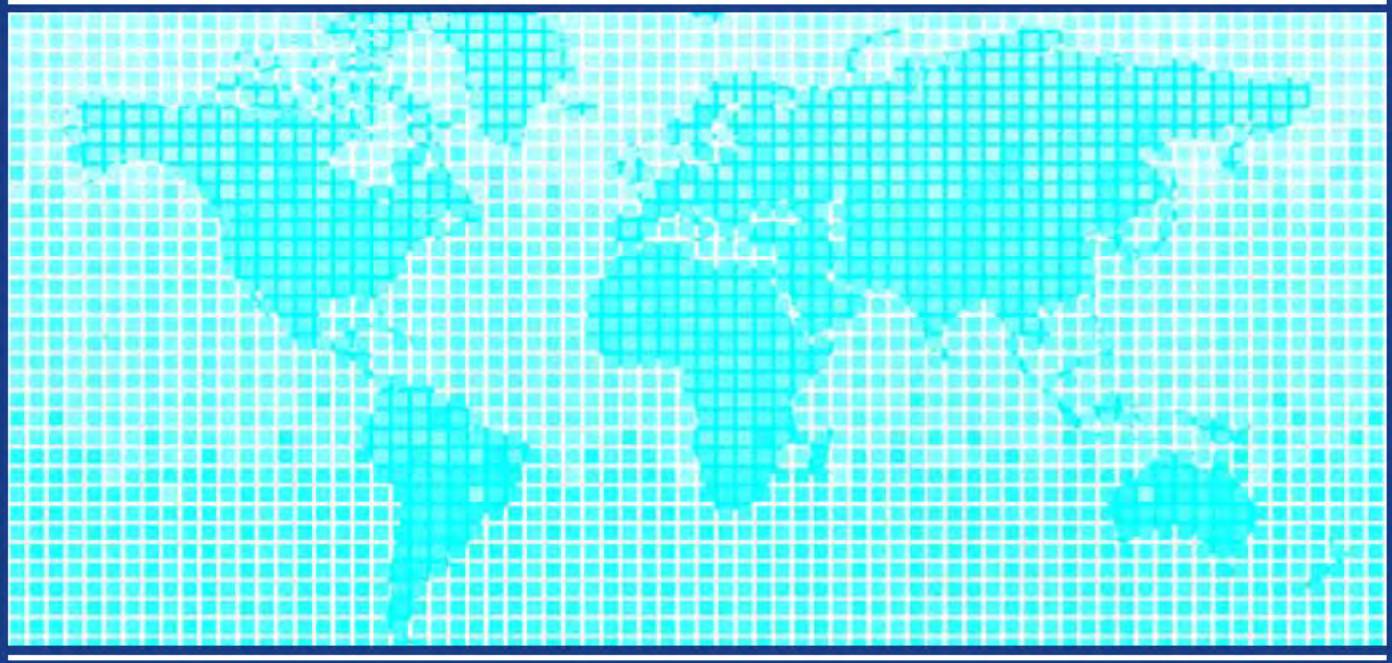
Counter-radicalization seeks to prevent non-radicalized populations from being radicalized. The objective is to create individual and communal resilience against cognitive and/or violent radicalization through a variety of non-coercive means. The U.S. government uses the term "Countering Violent Extremism" (CVE) to describe its foreign and domestic counter-radicalization efforts.

Cyberspace is the total landscape of technology-mediated communication. This includes not only the Internet and the World Wide Web, but also mobile- and fixed-phone networks, satellite and cable television, radio, the Global Positioning System (GPS), air-traffic control systems, military rocket guidance systems, sensor networks, etc. As more devices come online by being linked to each other, cyberspace is rapidly covering more of the physical world and its channels of communication and expression.

The Internet, a subset of cyberspace, is a system of interconnected computer networks. It comprises both hardware and software that facilitate data transfer across a network of networks, ranging from local to global and incorporating private, public, corporate, government, and academic networks. Functioning primarily as a data-exchange system, the Internet carries a wide range of resources, such as e-mail, instant messaging, file transfer, virtual worlds, peer-to-peer file sharing, and the World Wide Web.

The World Wide Web (www or Web) is a more recent development than the Internet, with its origins in the academic community of the late 1980s. The Web is one of many services that relies on the Internet. It consists of an assembly of files (audio, video, text, etc.), each assigned an address, which are connected to one another through hyperlinks (more commonly, links). The contents of the Web are (usually) accessed via the Internet using software known as browsers.

National Security Program
Homeland Security Project



Chapter 2: Online Radicalization

The first American extremists to embrace cyberspace were white supremacists. As early as 1983, a neo-Nazi in West Virginia created a "computerized bulletin board system," which connected far-right activists across the country.[15] A year later, the prominent white supremacist Louis Beam set up a bulletin board system on behalf of his group, Aryan Nations. Judging by his first message, the original intention was not to radicalize people, but—rather—to enable debate, connect activists, and pool resources among those already committed to the cause:

> Finally, we are all going to be linked together at one point in time. Imagine if you will, all of the great minds of the patriotic Christian movement linked together and joined into one computer. All the years of combined experience available to the movement …[16]

Whatever Beam's original intentions, it soon became clear that being "joined into one computer" was changing the movement's dynamics. In its 1985 report about "computerized networks of hate," the Anti-Defamation League observed that the majority of Beam's users were not veteran neo-Nazis but "impressionable young people vulnerable to propaganda." [17] It also noted that "the [linking] together [of] hate group activists coincides with an escalation of serious talk … about the necessity of committing acts of terror." [18]

People like Beam were quick to understand the potential of the new technology. Long before Awlaki created *Inspire* magazine, Beam started making the case for leaderless resistance. Writing in 1992, he called for the empowerment of small groups or lone actors ("one man cells") who, instead of relying on formal orders, would "take their cue from others" and stay connected via "newspapers, leaflets, [and] computers."[19]

The history of online extremism in the United States is longer, therefore, than commonly imagined. The purpose of this section is to bring together the latest research on how terrorists, past and present, have used the Internet and what role the Internet plays in radicalizing people. It argues that, like Beam, terrorists have embraced the technology's communicative aspects, helping them to spread their message and create (virtual) constituencies, and that such (virtual) communities are the places in which extremist behaviors are learned and normalized, enabling mobilization into violence to become possible.

How Terrorists are Using the Internet

As mentioned in the introduction, there is nothing unusual about terrorists using the Internet. Nor is there anything strange or surprising about *how* they use it: Like everyone else, they disseminate their ideas and promote their causes, they search for information, and they connect and communicate with like-minded people, often across great distances.[20] What makes terrorists different from the general online pubic is the *purpose* for which they go online. Experts, therefore, distinguish between activities that aim to build support and generate publicity (communicative), and those that facilitate acts of terrorism (instrumental).[21]

Instrumental Uses

When looking at instrumental uses, it becomes obvious that many online activities by terrorists are unexceptional. For example, terrorists frequently use online tools for logistics and reconnaissance: They e-mail, chat, and instant-message; search for addresses and pictures; look up maps; and book flights online. None of these behaviors and activities, however, are unique to terrorists, and in most cases, they are difficult to distinguish from the online behaviors of ordinary people.

Other instrumental behaviors are ineffective or have been exaggerated. Terrorist-linked websites encourage readers to raise money, and some provide buttons and links to make

online contributions, but it remains unclear how much money has been raised in this way. The Dutch intelligence service—so far the only Western intelligence agency to have published a detailed assessment on the issue—does not believe that terrorists attempts at online fundraising have been significant or successful.[22] Similarly, terrorist groups have produced training manuals and videos that try to teach would-be lone actors and unaffiliated groups how to make bombs, procure weapons, and other skills and techniques involved in terrorist attacks. Many researchers, however, doubt that such materials are genuinely useful,[23] and not a single terrorist plot in any Western country has substantially relied on them.[24] Lastly, there have been attempts by terrorists to use the Internet as a weapon, and protest groups like Anonymous and other so-called "hacktivists" keep demonstrating the enormous potential of online disruption. That said, to date, the number of instances of cyber-terrorism can still be counted on one hand, and—so far—no terrorist group has pursued a systematic or large-scale campaign.[25]

This is not to say that terrorists will not, in future, become more effective or that instrumental behaviors and activities should be of no interest to prosecutors, law enforcement, and intelligence services. On the contrary, intercepted e-mails and other forms of electronic communication have been crucial in preventing plots and convicting terrorists in court, and they will remain a powerful source of intelligence and evidence. Likewise, there is no inherent reason why terrorists would not, at some point, become interested in cyber-terrorism. No doubt, terrorist intentions and capabilities in all these areas must be monitored carefully. At the same time, it should be recognized that instrumental activities are not the only—or principal—reason why terrorists have populated cyberspace.

Communicative Uses

As long as the Internet has been in existence, violent extremists and terrorists have used the technology to publicize their causes, generate political support, and recruit new followers.

In the 1990s, many groups established static websites. The idea was to make available alternative platforms, circumventing the mainstream media's censorship, conveying unfiltered news, and disseminating ideological texts and materials that, previously, had been difficult and (sometimes) expensive to obtain. The websites didn't offer spaces for dialogue and interaction, but they still mattered as first ports of call for news, information, and authoritative announcements. To this day, many groups maintain a variety of such sites, now including personal sites for leaders and prominent ideologues, as well as memorial sites, which tell the stories of prisoners, fallen fighters, and martyrs.[26]

During the same period, many groups started online forums, of which bulletin board systems represented a first (and very primitive) version. For a while, forums existed as part of mainstream platforms (Yahoo and AOL, for example), but they gradually established their own independent presence, which no longer relied on the hosting of large Internet companies. The forums turned into virtual town squares, where people met, bonded, and talked to each other—and where even the most controversial issues could be debated without fear of retribution. Though launched, in many cases, by the groups themselves, the day-to-day running of forums has typically been left to those who populate them. This means that sites like the white supremacists' Stormfront or Al Ansar and Al Shmukh, which both support Al Qaeda, provide participants with a real sense of ownership and empowerment.

Another milestone was the dissemination of multi-media products, especially video. Until the early 2000s, most

of the communication on websites and forums had to be text-based, because Internet bandwidth and people's dial-up connections could not cope with large downloads. When, eventually, this became possible, audio and—then—video emerged as powerful drivers of Internet traffic. For supporters of Al Qaeda, for example, clips from jihadist battlefronts such as Iraq and Afghanistan—depicting suicide attacks, improvised explosive device (IED) explosions, and beheadings—became essential viewing that spurred debates and generated constant excitement.[27]

By the mid-2000s, social networking and user-generated content had arrived, and violent extremists and terrorists took full advantage of what became known as Web 2.0. Violent extremist content started popping up on mainstream blogging, social-networking, video-sharing, and instant-messaging platforms. Rather than being tucked away in the darkest corners of the Internet, it became possible for people to virtually stumble into extremist propaganda on sites like YouTube, Twitter, Paltalk, Facebook, and WordPress. This enabled violent extremists and terrorists to reach more people and engage new demographics, especially women.[28] It also has coincided with an increase in English-language videos and literature supporting Al Qaeda.[29]

The proliferation of cheap production and editing tools, which corresponded with the rise of Web 2.0, created an entirely new kind of activist. So-called "jihobbyists"—and their neo-Nazi, Sovereign Citizen, animal liberationist, and other equivalents—are not members of violent extremist groups, but they are actively advancing their agendas in online forums and on social-networking sites. According to the analyst Jarret Brachman, who coined the term:

> By hosting Jihadist websites, designing propaganda posters, editing al-Qaida videos, recording soundtracks, … compiling speeches from famous Jihadist shaikhs and packaging them into easily downloadable files or writing training manuals, these individuals help to form the base that keeps the movement afloat.[30]

Jihobbyists, in other words, are both consumers and producers of violent extremist content, and they think of themselves as active and valued members of their movements who make important contributions to the struggle.

If extremism online continues to mirror the trends and developments that apply across the Internet, the next step will be for violent extremists and terrorists to exploit the smartphone revolution, which experts believe will lead to a gradual merging of mobile telephony and the traditional, PC-based Internet.[31] If so, extremist-produced apps, instant messaging, and other tools are likely to become more important, including for instrumental uses such as fundraising.

How Online Radicalization Works

There are numerous examples of people who have radicalized with the help of the Internet (see Box 2). Experts have identified six processes and dynamics that explain online radicalization—that is, how the Internet promotes extremist beliefs and/or violent methods.

The first two of these processes deal with the consequences of being exposed to extremist content. No single item of extremist propaganda is guaranteed to transform people into terrorists. Rather, in most cases, online radicalization results from individuals being immersed in extremist content for extended periods of time, the amplified effects of graphic images and video, and the resulting emotional desensitization. According to one expert, social psychologist Tom Pyszczynski, for example, constant exposure to discourses about martyrdom and death—combined with videos of suicide operations and beheadings—can produce "mortality salience," an overpowering sense of one's own

mortality, which increases support for suicide operations and other, often excessively brutal, terrorist tactics.[32] Similarly, the powerful and (often) emotionally arousing videos from conflict zones—for example, those depicting alleged incidents of torture, rape, and other atrocities by Western troops—can induce a sense of moral outrage, which another expert, terrorism analyst Marc Sageman has identified as an important trigger for mobilization into violent action.[33]

The third and fourth explanations of online radicalization emphasize the social environment in which people are exposed on the Internet. For Sageman, this is the most significant—and most problematic—aspect of the Internet:

> [I]t is based on interactivity between the members, which makes the participants in the [extremist online] forums change their mind. Some of the participants get so worked up that they declare themselves ready to be terrorists. … Since this process takes place at home, often in the parental home, it facilitates the emergence of homegrown radicalization, worldwide.[34]

One reason why extremist forums whip up such enthusiasm is that participants are surrounded by other extremists. If people end up spending too much of their time in virtual communities, the online forums come to function like one of sociologist Edwin Sutherland's "criminogenic environments," in which deviant and extreme behaviors are learned and absorbed and in which extreme ideas come to seem normal because of constant interaction with people who hold similar—and similarly extreme—views. Online forums become like echo chambers, in which all moderating influences are removed and violent voices are amplified.[35] As a result, people acquire a skewed sense of reality so that extremist attitudes and violence are no longer taboos but—rather—are seen as positive and desirable. In the words of Elizabeth Englander, director of the Massachusetts Aggression Reduction Center:

> Without the Internet, … you might have a few people in a community with a very extremist view, but there wouldn't be anybody else who shared their view. They might come to the conclusion that these extremist views are wrong or incorrect or kooky. With the Internet, they can always find others who share their views. Suddenly there is [an entire] community that says, "You're not crazy, you're right." That's very powerful.[36]

Closely related to these dynamics are inherent features and characteristics of the Internet, most importantly a sense of anonymity that allows people to believe they can hide their real identities and avoid responsibility for their actions. (On the Internet, "no one can punch you in the nose!")[37] The effect is what psychologist John Suler has referred to as "online disinhibition," which leads to groups becoming more hostile and polarized and which may spill over into aggressive behavior offline.[38]

The fifth process involved in online radicalization is an offshoot of explanations that emphasize the social and interactive nature of the Internet. As researcher Katherine Bessière has shown, cyberspace enables people to role-play their idealized selves, projecting traits and characteristics they aspire to but do not possess.[39] According to Jarret Brachman and Alix Levine, over time, this process of role-playing becomes painful and depressing as people realize the discrepancy between their actual selves and the roles they are playing:

> [A]fter recognizing the gap between their avatar's mobilization and their own physical mobilization, many online participants begin taking steps to reconcile the gap. … [A] select few … will try to live up to their virtual, extremist, and pro-violent selves in the real world.[40]

In Brachmann and Levine's view, the need to "relieve the pain of dissonance"—or, stated differently, mobilization through role playing—is a consequence of the increasing "gamification" of cyberspace, involving not just extremist forums and social-networking sites but multiplayer online role-playing games[41] like World of Warcraft and virtual-life simulations like Second Life.[42]

The sixth explanation for online radicalization is far more basic. It relates to one of the Internet's core functions, namely connecting people with similar interests, even across great distances and with no prior interaction. Accordingly, the Dutch domestic intelligence agency (and others) has argued that, with the help of the Internet, people find it easier to meet terrorists and connect into terrorist networks, especially those who have no real-world contacts in the violent extremist milieu. In the absence of radical mosques (or their non-jihadist equivalents), so-called self-starters and people in remote areas rely on the Internet to link up with terrorist structures and turn their terrorist aspirations into reality. For terrorist recruiters, in turn, the Internet offers a pool of potential members that can be tapped into with less risk than would be involved in approaching an individual in the real world.[43]

It seems obvious, therefore, that the Internet has evolved into a unique and significant arena in which radicalization plays out. Violent extremists themselves have recognized this and become adept at using the new technology to their advantage. What the U.S. government and other actors can do to counter their efforts—both online and offline—will be discussed in the following sections.

Box 2: Online Radicalization: Jihadist Case Studies

Five men from northern Virginia (the "Virginia Five"), aged between 18 and 24, were arrested in December 2009 and given ten-year sentences for supporting terrorism. Their aim had been to go to Afghanistan, where they wanted to join the Taliban or Al Qaeda. American citizens of Pakistani, Arab, and African descent, the five men displayed few outward signs of radicalization. In the year prior to their arrest, however, they had become deeply involved in the world of online jihad, both watching and producing video clips that were posted in extremist forums and on YouTube. In August 2009, they were contacted by a Taliban recruiter who had seen their videos and claimed that he could facilitate travel to Afghanistan. In late November, they set off for Pakistan, hoping to meet their contact close to the Afghan border.[44]

Major Nidal Hasan was 39 years old when he went on a shooting spree at the U.S. Army base in Fort Hood, Texas, in November 2009, killing 13 and wounding 29 in the most devastating terrorist attack on U.S. soil since September 11, 2001. Hasan had been radicalized for a number of years: His extremist views first attracted attention in 2003, during his residency at Walter Reed hospital, and subsequently prompted several investigations by the FBI.[45] From what is known, Hasan had no public associations with violent extremists but made extensive use of the Internet. Between December 2008 and June 2009, he sent 20 e-mails to Anwar Al Awlaki, sharing his thoughts, expressing his admiration, and, importantly, seeking permission to carry out the attack.[46] Accordingly, Awlaki, who responded to two of Hasan's e-mails, was described as a "virtual spiritual sanctioner" in the U.S. Senate Homeland Security Committee's report on the shooting.[47]

Box 2: Online Radicalization: Jihadist Case Studies Continued

Roshonara Choudry was a 21-year-old British university student when she attempted to kill her local member of Parliament in May 2010 because of his support for the Iraq war. Her transformation from English Literature student to terrorist happened in less than six months. A daughter of immigrants from Bangladesh, Choudry wanted to learn more about her religion, but—in doing so—stumbled across jihadist literature and the sermons of Anwar Al Awlaki on YouTube and on the U.S.-based website Revolution Muslim (which has since been closed). She downloaded the entire set, around 100 hours of video. It was Awlaki, she later claimed, who taught her that "we shouldn't allow the people who oppress us to get away with it," and videos of another jihadist icon, Sheikh Abdullah Azzam, who convinced her that "even women are supposed to fight."[48] By the time she had finished watching Awlaki's sermons, in late April, she decided that something had to be done. She had no real-world associates and acted entirely on her own.

Arid Uka was 21 years old when he shot dead two United States airmen at the Frankfurt airport in Germany in March 2011. During his trial, it became clear that Uka had radicalized within just "a few weeks." The trigger for his action was a YouTube video that contained scenes from a fictional movie that showed Muslim women being raped by American soldiers, which Uka thought was real. Like Choudry, he seems to have been a lone perpetrator whose entire radicalization happened online. Uka was a member of several extremist forums and maintained a Facebook page under the name Abu Reyyan, where he displayed links to the websites of many extremist websites and preachers. Though he corresponded with the leader of an extremist, albeit non-violent, group in Frankfurt, there is no evidence that he ever attended the group's meetings.[49]

Zachary Chesser was 20 years old when he was arrested and charged with material support for the Somali group Al Shabaab, an Al Qaeda affiliate. (He has since been convicted and sentenced to 25 years in prison.) Prior to his arrest, he had attracted the FBI's attention because of an online threat he had made against the creators of the animated series "South Park," and he was considered one of the most active promoters of violent jihad on the Internet, running several blogs, YouTube channels, as well as Twitter and Facebook accounts. Based in northern Virginia, Chesser's own radicalization was driven by materials he found online, especially the sermons of Anwar Al Awlaki, which he discovered shortly after converting to Islam in the summer of 2008. Through Awlaki's blog, he also met the woman who would become his wife and—through her—established a network of contacts and associations with U.S.-based jihadists.[50]

Colleen LaRose—better known as "Jihad Jane"—was 46 years old when police charged her with conspiracy to murder a Swedish cartoonist who had published drawings of the Prophet Mohammed in October 2009, causing outrage in parts of the Muslim world where this was considered a grave insult. Having pled guilty, she now faces a life sentence. LaRose converted to Islam in 2005, but her involvement in online jihad began in June 2008, when she started commenting on YouTube videos about conflicts in the Middle East. Based in a small town in Pennsylvania, and with few, if any, real-world Muslim contacts, she became immersed in jihadist websites and extremist forums. On MySpace and other social-networking sites, she announced her desire to help "suffering Muslims" and, beginning in December 2009, declared that she wanted to become a martyr, "dying in Allah's cause."[51] These statements prompted several Al Qaeda associates, based on both sides of the Atlantic, to approach her and suggest she should kill the cartoonist—a mission she embraced and was determined to carry out.[52]

National Security Program
Homeland Security Project

Chapter 3: Reducing the Supply

Samir Khan, who was killed in a drone strike in Yemen in September 2011 that targeted Anwar Al Awlaki, was one of Al Qaeda's most prolific online propagandists. Khan had been one of Awlaki's closest collaborators since his arrival in Yemen in late 2009 and was responsible for editing Al Qaeda's English-language online magazine *Inspire*, which American officials described as Al Qaeda's "most downloaded" publication.[53] The first issue of *Inspire* came out in June 2010 and featured stories such as "How to Build a Bomb in the Kitchen of Your Mom" and "What to Pack When You Leave for Jihad." Another edition encouraged readers to "blow up Times Square [and] pull off [a] Mumbai[-style attack] near [the] White House till martyrdom."[54]

Inspire was not Khan's first online venture. As early as 2004, he had started running pro–Al Qaeda blogs from his parents' house in Charlotte, North Carolina. Having grown up in Saudi Arabia, Khan initially made his name by publishing translations of Al Qaeda materials. Later, he also published graphics, video clips, and comment pieces about the situation in Iraq and Afghanistan. His most successful website, *Inshallahshaheed*, which he ran for about a year prior to joining Awlaki in Yemen, had as its aim the revival of "the love, spirit and knowledge of Jihad."[55] It featured essays about religious and political topics, glowing endorsements of Al Qaeda leaders, and practical advice on what readers should do to support "jihadist battlefronts."[56] In the end, Khan followed his own instructions and made his way to Yemen, despite several attempts by his father and Muslim community leaders to convince him otherwise.[57]

Why did American authorities not arrest him or take down his websites? The answer is simple: because Khan had not broken any U.S. laws. His vocal support and advocacy for the organization that had killed nearly 3,000 Americans on September 11, 2001, was protected by the First Amendment of the U.S. Constitution, and Khan knew this: In 2004, he had consulted a lawyer who advised him to avoid specific threats and to avoid open and direct incitement to violence.[58] He never crossed those lines. American prosecutors' hands were tied.

Khan's case illustrates one of the principal limitations of dealing with homegrown online radicalization by removing content or restricting access to the Internet: the protections afforded by the First Amendment. The First Amendment, however, is not the only limitation—and may not even be the most significant. This section argues that—for reasons ranging from the political to the practical—approaches that are aimed at reducing the supply of violent extremist content on the Internet are neither feasible nor desirable and that they tend to conflict with the imperative of gaining intelligence that can be useful in pursuing terrorists and preventing terrorist plots. Indeed, this section will show that the filtering of Internet content is impractical in a free and open society, taking down websites should only be a very last resort, bringing prosecutions against propagandists often does more harm than good, and relationships with Internet companies are more productive when based on partnership, not confrontation.

The Limits of Online Censorship

In contrast to the United States, many foreign countries have procedures for preventing people from accessing certain websites, files, or locations in cyberspace. Their argument is that the Internet must not be beyond the law, and that whatever domestic laws apply to newspapers and TV stations should also be enforced in cyberspace. In reality, however, censoring the Internet is rarely effective, except in the most repressive countries, which have full control over Internet access and devote massive resources to policing its use. In the United States, constitutional, political, and practical constraints make this impossible.

Constitutional free speech protections in the United States are extensive, which means that the vast majority of the

content that qualifies as extremist or radicalizing would be protected under the First Amendment. For a statement to be illegal, it needs to "[contain] a direct, credible 'true' threat against an identifiable individual, organization or institution; [meet] the legal test for harassment; or [constitute] incitement to imminent lawless action likely to occur."[59] As a result, promoting the aims and methods of a terrorist organization is not illegal, nor is it forbidden to incite lawbreaking or violence as long as doing so will not result in "imminent lawless action."[60] Federal courts have consistently erred on the side of free speech, including in cases where public order was under threat and the exercise of free speech was likely to cause significant emotional distress.[61] Indeed, even critics of what may be called "free speech absolutism" concede "the First Amendment is so central to our self-conception" that it has come to define what being American means.[62]

In its foreign policy, the United States has become a global champion of Internet freedom and the free flow of information, with Secretary of State Hillary Clinton repeatedly speaking out against electronic curtains, firewalls, and other kinds of online censorship in countries like Syria, North Korea, China, and Iran.[63] Congress has been united in opposing attempts to regulate cyberspace or give governments or international institutions control over the Internet.[64] Using the same kinds of methods that are used by dictatorships—however different the reasons and context—would undermine America's leadership by vindicating the practices of rogue regimes and inspiring others to follow their example.

Domestically, any formalized, network-level system for removing content or restricting access would have to be subject to oversight and be open to judicial challenges. In other words, someone in government would have to maintain blacklists of banned websites that would become public, generate political controversy, inspire conspiracy theories, and—worst of all—draw attention to the very content that the government does not want people to see. Given that no technical system for removing content from the Internet is perfect, and that even children seem to be able to circumvent sophisticated filtering systems,[65] the likely outcome would be to increase, not reduce, the number of people that view violent extremist content on the Internet.[66]

Indeed, the rise of instant-messaging, blogging, video-sharing, and social-networking platforms has made it more difficult to remove or restrict particular types of content in practical terms. Rather than static websites, which serve only one purpose at a time and may be filtered, the interactive platforms that carry much of today's online traffic have hundreds of millions of users uploading, posting, and re-posting terabytes of data every minute. Furthermore, the majority of violent extremist content is now embedded in privately owned platforms—YouTube or Facebook, for example—which the U.S. government would never consider shutting down. Indeed, even the most sophisticated censorship systems—such as China's "Great Firewall," which consists of a highly complex system of formalized and informal controls that are maintained at great expense[67]—can barely keep up with removing objectionable content of this or any kind.

Based on these constraints, most of the traditional means for reducing the supply of violent extremist content would be entirely ineffective or of very limited use in the U.S. context. Their nature, implications, and likely consequences are described in the following parts of this section.

Nationwide Filtering

The most drastic measure to reduce the supply of violent extremist content is the introduction of nationwide filters, which drop requests to access websites or content that has been blacklisted. This technique is possible because the vast majority of Internet users receive their online

services from a small number of Internet service providers (ISPs)—the virtual bottlenecks through which all Internet traffic flows. Consequently, the governments of China and Saudi-Arabia, for example, have made sure that all Internet users in their countries are connected to the Internet via government-controlled ISPs, which filter content according to government policy. Even in the United States, more than 80 percent of users are receiving their Internet from just ten ISPs, with Comcast alone providing access for nearly a quarter of all American Internet users.[68]

Internet traffic can be filtered by domain name, the full Web page address, specific keywords, or the Internet protocol (IP) address of the computer and/or Web host for which the information is destined. On their own, these methods are likely to result in over-blocking (in addition to violent extremist and terrorist content, they also block legitimate websites) or slowing down Internet traffic. Mixed methods, such as hybrid IP/proxy filtering, avoid some of these problems, but are expensive and easy to circumvent. Like all other methods, they only deal with static websites, not the dynamic and interactive platforms on which violent extremist content can increasingly be found. Furthermore, in contrast to China and Saudi-Arabia, they would require the U.S. government to maintain and publish blacklists of banned websites, prompting legal challenges and raising myriad political and constitutional issues, ranging from free speech to the perception that only certain ethnic or religious communities are singled out for censorship.[69]

In practice, therefore, network-level filtering would make only a small part of violent extremist online content unavailable but would open a Pandora's box of issues and come at enormous financial and political cost. All Western governments that have considered the idea of introducing network-level filters for violent extremist content—such as Australia, the United Kingdom, and the European Union—have eventually discarded it for being too costly and controversial.[70] For the United States, the cost-benefit analysis would be even clearer: with its long and cherished tradition of free speech, the creation of a nationwide system of censorship is virtually inconceivable.

Legal Takedowns

An alternative to filtering *all* online traffic is for specific websites to be disabled or removed from the Internet in accordance with domestic laws. While no provisions for doing so exist in the United States, several European countries have established procedures that facilitate the taking down of websites:

- In 2010, the British government created the Counterterrorism Internet Referral Unit (CTIRU), which acts on tips from the public, the police, and the intelligence services. Websites that are suspected of being in breach of the law (which, in Britain, includes laws against the glorification of terrorism, the dissemination of terrorist materials, and the incitement of radical hatred) are examined by a team of specialists and members of the Crown Prosecution Service.[71] If CTIRU concludes that the content in question is illegal, it can "[serve] notices on website administrators, Web hosting companies, Internet Service providers (ISPs) and other relevant parties within the UK, to modify or remove any unlawful content."[72] During its first year of operation, 156 websites were shut down according to this procedure.[73]
- The Netherlands's notice-and-takedown regime places more emphasis on self-regulation. It allows government agencies and members of the public to report objectionable content to relevant website or hosting providers, who—in turn—have committed themselves to investigating and responding to complaints as well as to acting swiftly to remove content that is considered illegal or that violates their terms of use.[74] If providers refuse to remove content, then claimants may report the matter to the police, who will investigate and bring

prosecutions if doing so "serves the public interest."[75] In operation since 2008, the regime relies on voluntary agreements with website and hosting providers, and only applies in "situations in which the laws of the Netherlands are applicable."[76] At the time of writing, no figures were available on how many extremist or terrorist websites have been removed as part of the procedure.[77]

The principal weakness of these procedures is that they only apply to websites that are hosted or administered domestically. By definition, neither the British nor the Dutch government have powers to remove websites that are situated in jurisdictions other than their own. As a result, even if a violent extremist or terrorist website is shut down in accordance with Dutch or British regulations, its owners can simply move the content to a foreign hosting service from where it will, once again, be available to Internet users in the Netherlands or in Britain. In fact, the British government recently conceded that its domestic takedown procedures deal with no more than "a fraction of the problem."[78]

In the United States, the scope for legal takedowns would be even more limited, because the First Amendment is likely to protect many of the websites that violate domestic hate-speech laws in Britain and the Netherlands. In practice, therefore, the practical effect of introducing legal takedowns in the United States would be negligible.

Aggressive Takedowns

One way of overcoming the limitations of legal takedowns with respect to websites not hosted inside the United States is through cyber-attacks. The U.S. government has the capacity to carry out so-called "distributed denial of service" attacks[79] and also maintains other, technically sophisticated means for knocking down websites.[80] In the fall of 2008, for example, the Pentagon's Joint Functional Component Command-Network Warfare at Fort Meade, Maryland, reportedly disabled three Al Qaeda–linked online forums, hoping that would limit the ability of Iraqi terrorist and insurgent groups to coordinate attacks against American troops.[81]

However, like many aspects of cyber-warfare, the legal framework for carrying out such operations remains unclear. For example, do they constitute acts of force under international law, and if so, who needs to authorize them?[82] Equally important, their effectiveness is questionable. Like filtering and legal takedowns, cyber-attacks can disable individual websites but do not capture dynamic content like blogs, videos, social networking, and instant messaging, which is embedded in larger online platforms. Nor can they knock down specific videos or documents, such as *Inspire* magazine, which are posted (and re-posted) in so many locations on the Internet that attacks on a small number of static websites would make little difference.

The most powerful objection to shutting down violent extremist websites is that valuable sources of tactical and strategic intelligence will be destroyed. In 2008, *The Washington Post* reported that the Central Intelligence Agency (CIA) strongly opposed the Pentagon's plans to take down the three Al Qaeda forums, arguing that the benefits would be short-term disruption at best. One of its officials told the *Post*:

> [We] understood that intelligence would be lost, and it was; that relationships with cooperating intelligence services would be damaged, and they were; and that the terrorists would migrate to other sites, and they did.[83]

Contrary to popular imagination, therefore, the applicability and effectiveness of aggressive takedowns is limited, and their negative effects can be profound. The lesson is clear: While the U.S. government needs to retain its capability for carrying out cyber-attacks, it should only be used when doing so is absolutely essential to stop a terrorist attack and/or prevent the loss of life.

Prosecutions

An entirely different approach is to target, not the content, but its producers by bringing prosecutions against extremist Internet entrepreneurs—such as Samir Khan or Don Black, the founder of the white supremacist forum Stormfront—based on the idea that their online activism is crucial to the production and dissemination of violent extremist content.

This approach suffers from severe limitations. First, it requires that people are located within the United States, which means that foreign-based propagandists such as Awlaki (who lived in Yemen at the time of his greatest online reach and influence) are unaffected. Second, for prosecutions to be successful, individuals need to have broken the law. As mentioned earlier, the free-speech protections within U.S. law are so extensive that only a tiny percentage of extremist online content is likely to be classified as illegal. Indeed, to be prosecutable, it is not sufficient for content to be offensive, degrading, or in support of illegal or violent organizations: It needs to contain threats or acts of incitement that are directed at *specific* individuals and are likely to be carried out as a *direct result* of the statements made.[84] In cyberspace, the legal threshold is even higher: Because "speaker and listener are separated and often do not even know each other," courts have repeatedly rejected the argument that online threats ever qualify as true or that Internet-based "call[s] to arms … would result in immediate violence."[85]

Furthermore, instead of reducing the supply of violent extremist content, criminal prosecutions can have the unintended consequence of giving it more attention. A good example is the so-called "lyrical terrorist," Samina Malik, a 23-year-old woman from London, England, who had published poems expressing her desire to be a suicide bomber. Prior to her prosecution in the United Kingdom, the poems had been seen by less than 100 members of an extremist online forum, but the attention that resulted from the trial turned Malik into a minor celebrity. The poems can now be found on several thousand websites and may have been read by hundreds of thousands of people. Meanwhile, Malik is a free woman whose conviction was overturned on appeal.[86]

As a result, American prosecutors have been reluctant to bring incitement and communicating threats as stand-alone charges. Where such charges have been brought, they were linked to other, more substantive offenses, which have helped to underline the threats' immediacy and trueness. Zach Chesser, for example, who was running pro–Al Qaeda blogs and websites and planned to join an Al Qaeda affiliate group (see Box 2), was convicted of providing material support to a foreign terrorist group *in addition* to communicating online threats.[87] This way of combining online offenses with other, more substantive charges is both sensible and realistic: It uses the law where possible and appropriate while recognizing the limitations and constraints of policing speech within the U.S. legal and constitutional system.

Commercial Takedowns

Other ways of limiting the supply of violent extremist content rely on the cooperation of the private sector, especially Silicon Valley–based Internet companies like Google, Facebook, Twitter, and Paltalk, the platforms of which have been used by violent extremists and terrorists. Since 2008, lawmakers such as Senator Joe Lieberman (I-Conn.) have repeatedly urged these companies to take down content that supports terrorism and criticized them for failing to do so more vigorously.[88]

Silicon Valley's response has been mixed. Google has argued that it would be impossible for the company to pre-screen all 72 hours of content that is uploaded onto its video-sharing site, YouTube, every minute.[89] Instead, YouTube re-structured and re-launched its Abuse and

Safety Center, making it easier for users to bring hateful content" to the attention of the company's takedown team.[90] It also formed a partnership with the Anti-Defamation League, which has trained members of the takedown team to understand the nature of hateful content and to distinguish among videos that are legitimate, hateful, and illegal.[91] In late 2010, YouTube created a button that allows users to flag content specifically for supporting terrorism[92] and has since hired additional content managers to oversee the removal of hate-speech content.[93]

Despite these efforts, it remains easy to find content on YouTube that violates the company's community guidelines against hate speech[94] and/or explicitly promotes terrorism. This includes Awlaki's complete set of lectures; promotional videos by terrorist and insurgent groups in Somalia, Chechnya, Iraq, and Afghanistan; and step-by-step instructions for making phone detonators.[95] Indeed, Google is fully conscious that YouTube's takedown efforts have been imperfect and that the massive volume of clips and their constant re-posting continue to make it difficult to keep the site clean.[96]

Google is not alone in having struggled to reconcile politicians' calls for a tougher policing of hate speech with questions of technical capacity and their own libertarian instincts, according to which maximum access to information—whatever information it may be—is always a good thing. Companies like Facebook and Twitter have faced the same dilemmas and trade-offs, and—like Google—they rely on their users to flag violations of their codes of acceptable online behavior and content, which are reviewed by takedown teams and may result in the removal of content depending on the teams' sizes and competencies and the restrictiveness of each company's terms of use.[97]

Through interviews conducted for this report, it became clear that the larger, more established Silicon Valley companies like Google and Facebook want to act responsibly and are genuinely receptive to information and guidance on how to identify violent extremist and terrorism-related content on their platforms. Government agencies should strive to create and, where appropriate, strengthen informal partnerships with Internet companies whose platforms have been used by violent extremists. The objective would be to assist their takedown teams—through training, monthly updates, and briefings—in understanding national security threats as well as trends and patterns in terrorist propaganda and communication. As a result, online platforms such as Facebook and Google would become more conscious of emerging threats, key individuals, and organizations, and could align their takedown efforts with national security priorities.

Moreover, recognizing that not all the violent extremist and terrorist content can ever be eliminated from very large user-driven platforms like YouTube and Facebook, government agencies need to become more sophisticated at using these websites for the purpose of gathering intelligence and pursuing investigations (see Section 5).

Hiding

Another approach involving the private sector is to make it more difficult for people to find violent extremist content—for example, by manipulating search results or deleting recommended links or suggestions for websites and videos that are known to promote terrorism or hate speech. This may not prevent determined individuals from finding such content, but it could stop people who are not radicalized from stumbling into it when searching for keywords like "Islam" or "Holocaust."

The experience of European countries, where the local versions of Google, Bing, YouTube, and other websites are subject to laws about Holocaust denial, demonstrate that hiding content is technically possible and that Internet companies will do so when left with no choice. In the

United States, however, where the vast majority of extremist content is protected by the First Amendment and content-oriented laws are therefore generally unconstitutional, by all indications, Internet companies would be unwilling to comply with government demands to hide content. In their view, the effort required to manipulate search results or to remove links would be similar to the effort involved in removing content, which means that they would be faced with the same problems related to capacity and volume. Moreover, for companies like Google and Microsoft, the integrity of their search technology, which is based on algorithms that anticipate user interest and relevance, not the nature of content, is one of the cornerstones of their business—thus they are reluctant to undermine it, however good the reason.[98]

Rather than hiding violent extremist content, a more productive approach would be to promote websites and messages that counter it. Internet companies should be encouraged to donate sponsored links and share their knowledge about search-engine optimization with groups that oppose extremism. More generally, in a constitutional and political environment in which the U.S. government has little leverage (or desire) to interfere with the exercise of free speech, approaches that reduce the demand for violent extremist and terrorist ideas are more promising than efforts aimed at suppressing their supply. The means and methods for doing so will be explored in the next section.

National Security Program
Homeland Security Project

Chapter 4: Reducing Demand

On January 21, 2009, the day after President Barack Obama was sworn into office, Keith Luke, a 22-year-old neo-Nazi from Brockton, Massachusetts, went on a racist shooting spree. He forced his way into a former neighbor's apartment, handcuffed and raped a 22-year-old woman who had emigrated from the African nation of Cape Verde, and then shot and killed her sister. While fleeing, he shot and killed a 72-year-old homeless man, who was also from Cape Verde, and set off for a local synagogue where he wanted to kill "as many Jews as possible during bingo night," which had been scheduled for that day. The police stopped and arrested him.[99] Since going to prison, Luke has carved a swastika into his forehead and twice attempted to commit suicide.

From what Luke has told the police, he had never joined a neo-Nazi organization, nor had he ever attended neo-Nazi rallies, meetings, or concerts. According to his own statements, his entire radicalization took place online, where he spent much of his time on far-right forums, reading threads, writing messages to others, and watching videos. He said to officers that his favorite site was Podblanc, a white-supremacist online forum that encourages its users to become involved in lone-wolf terrorism and that features videos on how to construct bombs, organize shooting sprees, and carry out beheadings. It was here that Luke learned about his "duty" to save the "white race" from extinction, and that doing so required the "[killing of] 'non-white people' such as African Americans, Hispanics and Jewish people."[100]

What might have stopped Luke? Removing the website from which he drew his inspiration would have been difficult. At the time of Luke's crime, Podblanc was hosted and registered outside the United States, and Craig Cobb, its owner and administrator, lived in the Baltic republic of Estonia.[101] Furthermore, the site's content would, in any case, have been legal under the First Amendment—which, again, protects political speech unless it contains true or imminent threats. A more promising approach might have been to systematically expose Luke to anti-extremist ideas, make him question his assumptions, and prompt those around him—his family, friends, and colleagues—to engage him in discussions and debates. This approach may not have changed all of his beliefs, but it might have sown enough doubt to make him reconsider engaging in violence.

By definition, methods and approaches that challenge violent extremist ideas will not diminish the *supply* of violent extremist ideas but—rather—seek to reduce the *demand* for them. As this section will show, much needs to be done to activate a virtual marketplace in which extremism, terrorism, and other bad ideas are drowned out by pluralism, democracy, and the peaceful means through which good ideas can be advanced. It argues that government can play a limited but positive role in helping to bring this marketplace about—for example, by helping to create awareness, convene relevant non-governmental actors, build capacity, and foster media literacy. While doing so, government needs to be realistic about its own role, the extent to which civic challenges to violent extremist ideologies can be engineered (especially on the Internet), and the time that is required for such challenges to become effective.

Activating the Marketplace of Ideas

In the U.S. tradition, the rationale that underlies freedom of speech is the notion of a marketplace of ideas, in which truth prevails as long as good and bad ideas are allowed to compete. Bad ideas—even falsehoods—will eventually be crowded out, while the truth will emerge as stronger and more robust, having been tested in a free, fair, and—sometimes—fierce contest. Accordingly, Thomas Jefferson argued in his first inaugural speech that "error of opinion" should be accepted "where reason is left free to combat it"[102] and various Supreme Court opinions have subsequently developed what Justice Oliver Holmes Jr. called the "free trade in ideas."[103]

At first glance, the Internet seems to have made this marketplace more effective. Prior to its creation, not everyone had the opportunity to participate in the trade of ideas. Access to the mass media was expensive and controlled by gatekeepers—journalists, editors, and proprietors—who had a tendency to filter out cranks, extremists, and conspiracy theorists. The Internet turned the situation on its head: It gave everyone access, reduced the cost of publishing to virtually zero, and eliminated the reliance on journalistic middlemen.

Even so, the rise of the Internet has created its own share of distortions and market failures:

- The enthusiasm gap: Instead of having extremist views drowned out by opposing views, the Internet has amplified extremists' voices. Whether on YouTube, blogging platforms, or in newspaper comment sections, the cranks, extremists, and conspiracy theorists now seem to be everywhere, and—rather than being crowded out by moderates—they are the ones doing the crowding out. Their enthusiasm, energy, and excitement is unmatched by the political mainstream: According to experts like psychologist John Suler, this allows them to dominate discussions and it conveys the impression that they are the majority.[104]
- The pluralism gap: Far from creating more—and more vigorous—debate, the Internet has created ever-smaller ghettos for ideas and discourses, which, in turn, have reduced the number of spaces in which extremist and/or controversial ideas are openly contested. The best examples are extremist forums, which have thousands of users arguing about tactics and strategy but who rarely challenge each others' assumptions. These forums serve as echo chambers, in which extremist attitudes are hardened, not challenged. In the words of Mark Potok of the Southern Poverty Law Center, "There is no real exchange of ideas on whitepower.com."[105]
- The skills gap: Young people are said to be digital natives who feel comfortable using information technology,[106] but they often lack the skills to evaluate and contextualize online content—whether because some parents are intimidated by the online environment and take a hands-off approach or because schools are not teaching analytical skills sufficiently.

The capacity of government to close these gaps and—in doing so—activate a fully functioning marketplace of ideas is limited due to laws and political conventions that prevent the U.S. government from interfering in the domestic political discourse.[107] This does not mean, however, that the government's hands are tied completely. As will be shown, the federal government can play a positive role in creating an environment in which civic actors feel empowered to challenge violent extremist and terrorist propaganda. It can also spread information, facilitate the exchange of experiences and best practices, and bring together different stakeholders, such as private business and community groups, who can take positive action.

Creating Awareness

Just because the Internet is a technology does not mean that the remedy for every problem caused by the Internet needs to be technological. Online extremists may spend much of their time in cyberspace and may maintain friendships and relationships with people they have never met in person, but they still have a real-world existence: They interact with their parents, fellow students, workmates, and friends; they go to school, shopping, and attend community events. Indeed, people like Roshonara Choudry (see Box 2), who are completely isolated and refuse to share their views with anyone, continue to be the exception, not the rule.

However, civic challenges to violent extremist online propaganda can only work if communities know—and understand—what they are meant to challenge. It is important, therefore, for the government to spread awareness about online radicalization among parents, teachers, and community leaders, so they are able to detect, report, and—if necessary—intervene in processes of online radicalization.

Indeed, in recent years, both government (including the Department of Homeland Security and the FBI) and community groups have become involved in efforts to educate communities about online radicalization. For example, the U.S. National Counterterrorism Center (NCTC)—the U.S. government's premier counter-terrorism analytic center, created at the 9/11 Commission's recommendation—has developed a community-awareness briefing that is used in roundtables and town-hall meetings with Muslim communities. The briefing consists of a slide show and several video clips, highlighting the messages and methods that are used by Al Qaeda propagandists to radicalize young Americans. It urges parents to take an interest in their children's online activities and to be ready to challenge their behaviors.[108]

In addition, NCTC—in collaboration with other government agencies and Muslim community groups—has run three Internet Safety Workshops in northern Virginia and Seattle, Washington,[109] which have combined sessions about online extremism with information about how to protect children from online predators and pornography. Aimed at Muslim parents, government representatives deliver briefings on the nature of the threat while Muslim community representatives focus on how parents can detect radicalization and "step in early … [in order to] counter the terrorist theology."[110]

The community awareness briefing and Internet Safety Workshops seem to have been received positively by the audiences that have been exposed to them.[111] Moreover, the involvement of community groups and the combination of counter-radicalization with other Internet safety issues have been effective at generating local interest and buy-in. There should be more of these events, and the workshops should be complemented by an online resource that can be accessed by smaller and/or more disconnected communities and individuals.

Building Capacity

One of the key challenges in fully activating the marketplace of ideas is to ensure alternative voices are heard. This involves creating interest and excitement among mainstream groups, so they can overcome the enthusiasm gap. It also means equipping those groups with the skills and knowledge to craft an appealing message and disseminate it among the people who are susceptible to online radicalization.

Targeting foreign audiences, the State Department has run a number of programs that seek to empower, network, and train moderate voices in foreign countries:

- Earlier this year, officials hosted a series of Web-based seminars ("webinars") for Somali bloggers in Europe, Canada, and Africa. The initiative helped online activists exchange ideas on how to make their websites more attractive and to reach wider audiences. It also generated a network of mainstream Somali bloggers who have made it their mission to challenge the narratives of violent extremist groups in Somalia.[112]
- In April, the State Department launched its Viral Peace campaign, which has trained young influencers in Southeast Asia to use social media as a way of promoting community involvement and peaceful change.[113] According to the program's coordinator, the aim is to help people craft online strategies that use a whole range of tools—including "logic, humor, satire, [and] religious

arguments"—to match the violent extremists' energy and enthusiasm.[114]

The legal constraints on manipulating the domestic political discourse make it difficult—if not impossible—for the federal government to run such programs *inside* the United States. Domestically, therefore, the government should focus its role on being a convener—that is, bringing together interested parties such as private business, foundations, think tanks, and community groups to facilitate their developing approaches, priorities, and messages on their own. Rather than telling people what to do, the aim—in the words of American officials—is to connect "good people," build capacity, and make it possible for "good things to result."[115] For example:

- In early 2013, the New America Foundation will run a series of online workshops for Muslim community leaders in Washington, D.C., Houston, Detroit, and San Francisco. They will be hosted and paid for by some of the most prominent companies in the technology business, including Microsoft, Facebook, Google, and Twitter. The purpose is to "empower [Muslim American] thought leaders" to become more effective at using informational technology, especially "social media, search engine optimization, application for free advertising and grants, and multimedia design."[116] Government officials have participated in meetings and assisted with contacts, encouragement, and strategic advice but are not involved in selecting participants, running, or funding the program.
- In 2011, Google's think tank, Google Ideas, launched a global network, Against Violent Extremism (AVE), which brings together former extremists, victims of terrorism, and other important stakeholders, such as private business, foundations, and experts.[117] The idea is to create a global network and—in doing so—make available knowledge, experience, and resources to groups that are too small and too locally focused to benefit from international exposure.[118] AVE is privately funded and entirely independent of government influence, though government officials have attended the network's launch conference and helped with advice and contacts where needed.

In principle, the government's approach is well thought out and appropriate. In practice, however, it remains to be seen how energetically the government will pursue its self-declared role. The government's forthcoming Internet strategy needs to spell out clearly what being a convener entails, what kinds of concrete and measurable actions it will undertake, and what resources will be devoted to this effort.

Counter-messaging

Counter-messaging takes capacity building one step further. The idea is to expose people to messages that are specifically designed to counter the appeal of extremism. In cyberspace, these messages can be delivered through websites, blogs, videos, Facebook groups, Tweets, and other types of online media.

Over the past decade, there have been numerous conferences and workshops on counter-messaging, and governments have conducted extensive research on the kinds of messages that may help to undermine Al Qaeda specifically.[119] Broadly speaking, counter-messaging may involve challenges to the violent extremists' ideology and to their political and /or religious claims; messages that aim to "mock, ridicule or somehow undermine their credibility";[120] contrasts between violent extremists' grandiose claims and the reality and/or consequences of their actions; or positive alternatives that cancel out or negate the violent extremists' ideology or lifestyle.

Government is not the most effective conveyor of these messages. It has a role to play in dispelling rumors and

false claims that relate to its own actions,[121] but—for the most part—it should act as enabler, supporting mainstream community groups and the victims of terrorism to become more effective at telling their stories and reaching the audiences that are potentially vulnerable to becoming radicalized.

This could involve, for example:

- Bringing together community groups with public relations, advertising, and media-production companies, who can help craft better, more powerful messages and turn them into attractive media products.
- Setting up prizes and competitions for online projects that promote civic participation and alternatives to violence.
- Encouraging foundations, philanthropists, and private business to launch a grassroots start-up fund for initiatives seeking to counter extremism and terrorism on the Internet.[122]

As with capacity building, the idea that government should take a backseat role and focus on enabling others' actions is a very good one in principle, but it must not be used as an excuse for inaction. The government's forthcoming Internet strategy should set out clearly what the government intends to do, what resources will be devoted to the effort, and how its actions should be evaluated.

Engagement

The most immediate way to confront violent extremist online propaganda is to go to the virtual places where extremist messages are being purveyed and engage actual and potential violent extremists in dialogue and discussion. This approach rests on the assumption that violent extremist arguments are often based on falsehoods and conspiracy theories and that exposing them will sow doubt in the minds of violent extremists and dissuade them from violence.

As mentioned earlier, this is particularly important in cyberspace because extremist forums and websites are like echo chambers where people's views are constantly reinforced and their underlying assumptions are rarely challenged.

The U.S. government is conducting engagement with foreign audiences through the State Department's Center for Strategic Counterterrorism Communications and programs funded by the Department of Defense. The State Department focuses on mainstream forums where extremists are present but not dominant, arguing that these are spaces that had previously been ceded to violent extremists and where minds can still be swayed.[123] In contrast, the Defense Department's programs are active in extremist forums and routinely engage with hardened terrorist supporters. Both are mostly conducted in foreign languages (especially Arabic and Urdu), and officials are instructed to back off when there is any indication that American citizens are involved.[124]

Within the United States, no government agency is currently involved in engaging violent extremists or potential violent extremists in cyberspace. Such programs would raise political and legal concerns about the U.S. government trying to interfere with domestic political discourse. In addition, in interviews conducted for this report, American officials disagreed on whether doing so would be effective and on how or where such efforts should be conducted.[125] Mainstream Muslim groups have offered to challenge violent extremist narratives in U.S.-based or English-language jihadist forums, but they require financial resources and assurances by the FBI and other relevant agencies that they will not be caught up in counter-terrorism investigations for doing so.[126]

Accordingly, the government's approach in this area needs to be clarified. Rather than speculating about the potential effects of online engagement, the government should

determine whether this tactic is effective and—if so—how and where its positive effects can be maximized. For engagement with American citizens, lawmakers also need to clarify the rules under which domestic government agencies can engage violent extremists without breaking the law or political conventions, and how non-governmental actors, such as community groups, can populate extremist forums without being considered extremists themselves.

Promoting Media Literacy

The most long-term—yet potentially most important—means of reducing the demand for online extremism is to promote digital literacy. In recent years, educators and policy makers have recognized the unique risks and challenges posed by the Internet. Most efforts have focused on protecting children from predators and pedophiles, with the result that—in practically every school—kids are now being taught to avoid giving out personal details and to be suspicious of people in chat rooms.[127] Little, however, has been done to educate young people about violent extremist and terrorist propaganda.

Online extremism can be dealt with as a child-safety issue, using the same methods and approaches that are used in educating children about predators and pedophiles. This may include, for example, warnings about grooming behavior (that is, actions intended to establish trust between a child and an online predator), information about the likely consequences of becoming involved in violent extremist activity, and reminders to always question people's online identities. It can also be embedded in the wider curriculum on media literacy that teaches young people how to use media critically, to evaluate and question sources, and to distinguish information that is plausible and trustworthy from information that is not.[128] In either case, school authorities need to catch up: They have started addressing digital media in their lesson plans only recently, and they very rarely tackle the specific challenges posed by user-generated and dynamic content, such as social-networking and video-sharing sites where most violent extremist activities take place and where the vast majority of propaganda can be found.[129] School systems must review and update their curricula and ensure that teachers receive the training that is required to teach these subjects.

Other stakeholders play important roles, too. Rather than being content with installing filtering software on their children's computers, parents should be encouraged to take an active interest in their children's Internet activities and to learn to use new online platforms *with* them.[130] Internet companies need to update parental-filtering software to include websites that are openly promoting violent extremism and need to devote adequate resources to moderating chat rooms and online forums. Given their influence and resources, Internet companies should play leading roles in promoting child-safety issues and should serve as information hubs for parents and schools. Indeed, both Google and Facebook have made positive efforts to tackle child-safety issues,[131] efforts that can and should be broadened to address online extremism and terrorist propaganda, especially by adapting their educational materials, case studies, advice, and software to account for this threat.

None of the measures that are outlined in this section are likely to reach every person who is potentially vulnerable—especially individuals who are particularly isolated socially. Nor—like media literacy and capacity building—will these measures be immediately effective. Accordingly, the next section deals with how terrorists' online activities can best be exploited in the short term.

National Security Program
Homeland Security Project

Chapter 5: Exploiting Cyberspace

In April 2012, Antonio Martinez, a 25-year-old construction worker from Baltimore, Maryland, was sentenced to 25 years in prison for plotting to bomb a military recruitment center. His plan was to detonate a truck packed with explosives that he had parked outside the facility on the morning of December 8, 2010. As it turned out, the people who provided Martinez with the truck and (what he believed were) explosives were undercover FBI agents. When Martinez pressed the button, no explosion happened. Instead, he was surrounded by counter-terrorism officers, arrested, and charged with the attempted murder of federal officers and attempted use of a weapon of mass destruction.[132]

What makes the case different from other sting operations is how Martinez came to the FBI's attention. Having converted to Islam less than six months before his arrest, Martinez had few extremist connections in the real world, but he maintained a public Facebook page that he used to advertise his ideas about violent jihad and the need to confront anyone who "opposes Allah and his prophet."[133] An FBI confidential source noticed Martinez's profile and contacted him—again, through Facebook—to find out if he had any plans to become involved in violent jihad. According to the FBI, Martinez told the confidential source that it was his "dream to be among the ranks of the mujahideen, and that he hoped Allah would open a door for him because all he thinks about is jihad."[134] Indeed, it was Martinez's idea to target the recruitment station, which he told the confidential source he had visited years earlier when he wanted to join the military.[135]

The FBI's actions against Martinez highlight a third approach for dealing with online radicalization: Rather than removing violent extremist content (see Section 3) or trying to undercut the demand for it (see Section 4), the aim is to take full advantage of violent extremists' and terrorists' presences in cyberspace and make maximum use of the information they are sharing with others. As this section shows, this information can be used to gain strategic intelligence about terrorist groups' intentions and networks, tactical intelligence on terrorist operations and the people who are involved in them, and evidence that can be used in prosecutions.

Exploiting the Internet to gather intelligence and/or evidence is the most effective way of dealing with online radicalization in the short term, and government should pursue this approach more systematically. Doing so, however, requires the clarification of existing laws and the creation of appropriate review and oversight mechanisms that will give domestic agencies more confidence to operate in cyberspace.[136]

Setting Rules for Cyberspace

In theory, the idea that law enforcement and intelligence agencies should take advantage of the information that violent extremists and terrorists put on the Internet is attractive and entirely uncontroversial. Even the American Civil Liberties Union (ACLU) has endorsed the approach. At a congressional hearing in May 2010, its executive director argued that, rather than censoring the Internet, "we can and should be using [terrorists'] online communications to learn as much as is lawfully possible about those who should do us harm and their activities and motives."[137]

At the same time, the ACLU—and others—have made it clear that any action in cyberspace should be conducted "following proper law enforcement and intelligence procedures and with appropriate judicial oversight."[138] This, of course, is where the problem lies: The current procedures and oversight mechanisms are not sufficient, adequate, or consistent. The rise of the Internet and the massive expansion of data storage over the past two decades have outpaced the ability of policy makers to formulate rules for what law enforcement and intelligence agencies can and cannot do. As a result, government

agencies are often unsure to what extent they can use, process, and interact with publicly available information on the Internet. For example, the use of online sources by the Department of Homeland Security relies on two sets of guidelines, one of which dates from 1999.[139] These guidelines are mostly based on translating the rules and principles that apply to collecting information from public meetings, paper-based information, and interactions with people "in person or over the telephone"[140] and—in doing so—fail to address some of the key characteristics of the Internet:

- What is domestic? From surveillance to engagement, U.S. government rules for counter-terrorism and counter-radicalization distinguish between domestic and foreign. The transnational nature of the Internet, however, makes such distinctions difficult: A website may be registered in one country, its content hosted in a second, the producer based in a third, and the user in a fourth. What rules should apply?
- What is public? U.S. government guidelines for online monitoring and surveillance apply rules for (real-world) public places to the Internet. Yet cyberspace is often, and increasingly, more difficult to categorize. While static websites are public, most of the content that has emerged as part of Web 2.0 falls somewhere in between. What about online forums? Facebook profiles where some content is public, some private? Instant-messenger communication and Twitter? Pictures on photo-sharing sites?
- What rules for data mining? Unlike real-world communication, online communication can be monitored, stored, and analyzed electronically, and there are virtually no technical limits anymore for doing so. This can produce stunning insights, but the routine monitoring of non-suspicious communication may also be considered overly intrusive, inappropriate, and, in certain circumstances, illegal. Reviewing existing laws and regulations, a 2010 report by the Constitution Project identified a "patchwork of [legal] protections," with "only one federal statute explicitly [contemplating] data mining as it relates to privacy, and none [providing] direct guidance on implementing these activities."[141] It concluded that "the current legal regime fails to clearly or uniformly regulate government data mining activities," making it more difficult "to harness the vast seas of information for our collective benefit and simultaneously protect the delicate relationship our Constitution established between the government and the governed."[142]

Having appropriate rules, oversight, and review mechanisms will not be an obstacle to making full use of the Internet in countering homegrown terrorism, but will enable a more systematic exploitation of this resource. As this section shows, the potential benefits and opportunities are numerous.

Gaining Strategic Intelligence

For many terrorist groups, the Internet has come to be more than just a platform on which they present their ideas: It is a center of gravity, holding together disparate and often unconnected people in different cities, countries, sometimes even continents. It facilitates strategic discussion and debate, and it allows for new ideological currents to emerge and be articulated. According to terrorism analyst Marc Sageman, the Internet has become the virtual glue providing cohesion and coherence for movements like Al Qaeda.[143] As a result, trying to understand the conversations that happen online and who is involved may be just as important as spying on a terrorist group's leadership or interpreting their official announcements and statements.

One of the focal points for strategic intelligence efforts is what experts call "text analytics" and "sentiment analysis,"

each of which can range from expert analysts looking at individual postings and making highly informed judgements about individual pieces of text to computerized analytics through which thousands of posts can be sifted and wider trends and dynamics can be discovered. In either case, the aim is to track and analyze online platforms—static websites, online forums, blogs, Twitter, videos, and discussion threads—to detect shifts in intentions and priorities, pick up on arguments, cleavages, fault lines, and new tactics.[144] In Al Qaeda's case, for example, the systematic analysis of sentiment on the principal online forums associated with the jihadist movement could reveal people's changing interest in various battlefronts, which may—in turn—help to predict changing patterns of foreign fighter traffic.[145] Text analytics, on the other hand, could provide early warning of new modus operandi, such as the lone-wolf attacks that started becoming more frequent after Awlaki and his lieutenant, Samir Khan, had promoted this tactic via *Inspire*.[146]

Equally important is "network analysis," which seeks to understand connections between people. Social-networking sites, for example, can help to identify the people who are involved in processes of radicalization and recruitment. At the most basic level, they show whose opinions are most "liked," "followed," "shared," and disseminated across certain media platforms. This may, then, provide information about key nodes that are involved in distributing terrorist propaganda across the online chain and enable analysts to make sense of how online magazines like *Inspire* or propaganda videos are being passed around and what kind of media items are likely to be influential with certain audiences.[147] Indeed, it is precisely when sentiment and network analysis are combined that law enforcement and intelligence agencies can gain reliable predictors of radicalization and—possibly—derive models for predicting Internet-inspired terrorist action.

Needless to say, none of this is entirely new. Yet, from conversations held with government officials in preparation of this report, it seems that police forces and intelligence agencies still have not truly—and fully—embraced cyberspace as a critical source of this type of intelligence:

- Local police forces, for example, may never have the resources to engage in sophisticated forms of network and sentiment analysis. But they should be conscious that violent extremist groups in their area are likely to have an Internet presence and that good community policing requires keeping an eye on the virtual (not just the physical) locations in which those communities gather.[148] They need to know what those locations are and how to use them.
- At the national level, interviews conducted with government officials for this report suggest that the scope, sophistication, and success of on-going efforts need to be periodically reviewed and, where necessary, changed and improved in order to reflect the rapidly changing nature of cyberspace. The aim is for national law enforcement and intelligence agencies to (always) possess the latest technological tools and capabilities and to have absolute clarity regarding their authorities in cyberspace.

Gaining Tactical Intelligence

Compared with strategic intelligence, tactical intelligence may—at first sight—seem more difficult to obtain. After all, once a decision has been taken to launch an attack, most terrorists will be careful not to reveal their intentions, never mind advertising them in public forums. That said, even publicly available information from websites and online forums can turn out to be useful in foiling terrorist plots and preventing terrorist attacks.

For example, extremist forums and social-networking sites are essential for identifying lone actors with no real-world

connections into extremist milieus. Like Antonio Martinez, lone actors often have a long history of online activism: They maintain Facebook profiles, run blogs, and post messages in online forums. In other words, they are leaving plenty of virtual traces that enable investigators and analysts to identify who they are and chart their interests, passions, and intentions. Most importantly, their online activism makes it possible to pick up on sudden changes in behavior, escalating (and increasingly specific) threats, requests for bomb-making instructions, contacts with foreign-based insurgent groups, or announcements of imminent action.

This does not mean that every member of an extremist online forum should be under police observation, nor does it imply that there is always a correlation between the intensity of online behavior and the likelihood of someone taking violent action. But there are plenty of cases in which people—for whatever reason—decided to share and discuss their intentions with others. Take, for instance, Mohamed Osman Mohamoud, the 19-year-old Somali American from Portland, Oregon, who attempted to blow up the tree-lighting ceremony in his hometown in 2010 and who had been in touch with Samir Khan, the editor of *Inspire*, for nearly two years. Mohamoud was a member of several Al Qaeda–supporting online forums and had published three articles in Khan's first online magazine, *Jihad Recollections*, including one in which he described how to get "physically [fit] for jihad." Aged 18, he used his online contacts to facilitate foreign fighter travel, but was prevented from doing so by the FBI, which—at this point—had been alerted to Mohamoud's behavior and began to involve him in a sophisticated sting operation.[149]

Where potential terrorists are not entirely on their own, their online activism makes it possible to identify networks of associates. As in any criminal investigation, the discovery of one suspected criminal immediately raises the question if there are other people they are connected to and, possibly, with whom they have conspired. This can be vitally important in preventing further acts of terrorism, which may have been at the planning stage but were missed or overlooked by investigators and analysts. It can also reveal wider networks and/or connections with recruiters and facilitators who are based abroad.

The most obvious way in which networks of associates can be established is through people's Facebook friends, the people they follow on Twitter, and their posts and messages on YouTube and in open-forum threads. Once a formal criminal investigation has been launched and legal authorities have been granted, investigators may also look at suspects' e-mails and the messages they have received and sent on various social platforms and instant-messenger systems. Given the ubiquity of electronic communications and the importance of cyberspace to virtually every violent extremist movement, it becomes possible, then, to re-construct a suspect's entire social universe, including their extremist associates and fellow plotters.

As with strategic intelligence, this is not entirely new territory for domestic law enforcement and intelligence agencies. Indeed, it raises familiar questions and dilemmas:

- To what extent can the activities of extremist, albeit mostly non-violent, countercultures, such as white supremacists and supporters of violent jihad, be monitored and mined for intelligence? What laws and policies should govern government activity, and should laws and policies be different for federal versus state/local law officials?
- What are the factors and indicators that cause an individual to go from speech to (violent) action, and at what points is it lawful, reasonable, and legitimate for government to intervene?
- If intervention is appropriate, who in government should intervene, and how? What level of government should do the intervention—is this matter a state/local responsibility given that state/local officials tend to know

their local areas better, or is this a federal matter? And what part of government should do an intervention—law enforcement officials, government officials who focus on providing services (social work, psychological, education, job training, etc.), or some combination? Or should government officials hand off the matter to community members—and, if so, what is the mechanism for doing so and maintaining public-private coordination?

The existence of these dilemmas reinforces the argument that government and legislators need to clarify the rules and frameworks that govern tactical intelligence gathering, both online and offline. Yet it also demonstrates that—in principle—cyberspace needs to be no more off limits than any of the real-world locations in which tactical intelligence gathering has been carried out in the past. Cases like Martinez's and Mohamoud's show that the FBI has begun to penetrate this environment with great success.[150] If anything, therefore, government needs to encourage law enforcement and intelligence agencies to continue this process and alleviate the legal, political, and other obstacles that stand in the way of exploiting cyberspace in the most systematic and comprehensive fashion possible.

Gathering Evidence

If cyberspace is a potentially fruitful source for tactical and strategic intelligence, it can also provide evidence for prosecutions. As mentioned above, terrorists will be careful to limit their public online profile once they have decided to become operational, and one should not, therefore, expect to find large amounts of evidence of attack planning on Facebook profiles, Twitter feeds, or even extremist online forums. Yet, because online communications have become so routine and essential to anyone living in a modern, industrialized country like the United States, it will be unusual not to find *any* evidence of attack planning in a terrorist's personal communication.[151] Instead of Facebook and Twitter, those conversations will mostly happen on e-mail and instant messenger, and may, occasionally, spill into more public forums. As a consequence, there is a significant chance that law enforcement and prosecution will be able to establish motive and circumstances, as well as piece together a substantial amount of attack planning from the online traces that the suspects have left.

Regarding prosecutions, the true challenge for law enforcement is not the lack of evidence but the massive amounts of data that need to be analyzed in order to identify the pieces that are relevant. A typical suspect may well have accumulated several Terabytes of data on his or her computer, external hard drives, e-mail accounts, and Internet-based data storage, containing thousands of hours of video and audio, as well as documents, e-mails, and messenger communication. In addition, the suspect may have participated in thousands of conversations and threads in online forums, and left months' worth of comments on people's Facebook and YouTube pages. Indeed, in a recent British case, it took the high-tech unit of London's Metropolitan Police half a year and 16 officers to sift through the contents of one terrorism suspect's computer.[152] This included not just tens of thousands of pages of conversation in various online forums, but also many documents in foreign languages that needed to be translated before they could be assessed.

This shows that the phenomenal increase in computing power in recent years has changed the situation on both sides of the counter-terrorism equation. It has given law enforcement and intelligence agencies new and powerful tools, because potential suspects' statements and conversations are electronically recorded and can be traced long after they have taken place. At the same time, the amounts of data produced require additional resources—both human and technological—for review and assessment. The actions that should be taken to deal with this new and evolving phenomenon will be described in the next—and final—section.

National Security Program
Homeland Security Project

Chapter 6: Recommendations

The Internet has revolutionized the way people communicate and do business. Its benefits to users everywhere have been enormous and will continue to drive progress in practically every area of life. At the same time, it should be recognized that, while being a force for good, the Internet has also come to play an important—and, in many ways, unique—role in radicalizing homegrown and domestic terrorists. Supporters of Al Qaeda, Sovereign Citizens, white supremacists and neo-Nazis, environmental and animal liberationists, and other violent extremist groups all have embraced the Internet with great enthusiasm and vigor. They are using it as a platform to spread their ideas, connect with each other, make new recruits, and incite illegal and violent actions. It seems clear that this trend will continue and that future terrorist attacks against the United States and its interests will involve individuals who have been radicalized—at least in part—on the Internet.

The Strategy

In its 2011 counter-radicalization strategy and the subsequent implementation plan, the White House acknowledged that "the Internet has become an increasingly potent element in radicalization to violence"[153] and promised to "develop a separate, more comprehensive strategy for countering and preventing violent extremist online radicalization and leveraging technology to empower community resilience."[154] One year later, this still hasn't happened, and this report's first and most important recommendation is for the White House to complete its work on the strategy, make it public, and begin its implementation with alacrity.

In strategic terms, online radicalization can be dealt with in three ways. Approaches aimed at *restricting freedom of speech and removing content* from the Internet are not only the least desirable, they are also the least effective. Instead, the federal government should play a more energetic role in *reducing the demand for radicalization and violent extremist messages*—for example, by encouraging civic challenges to extremist narratives and by promoting awareness and education of young people. In the short term, the most promising way for dealing with the presence of violent extremists and their propaganda on the Internet is to *exploit their online communications to gain intelligence and gather evidence* in the most comprehensive and systematic fashion possible.

Reducing the Supply

As shown in Section 3 of this report, the legal, political, and practical options for removing violent extremist content from the Internet are limited. This report's recommendations are as follows:

- Government should refrain from establishing nationwide filtering systems, which are unconstitutional, ineffective, and likely to open a Pandora's box of controversial political issues.
- Government needs to retain its capability for aggressive takedowns of foreign-based websites but only use it when doing so is absolutely essential to stop a terrorist attack and/or prevent the loss of life. The circumstances and legal framework governing the use of cyber-attacks need to be clarified.
- When bringing prosecutions against violent extremist Internet entrepreneurs, government should always weigh the chances of success against the unintended consequence of drawing attention to their ideas and propaganda.
- Government should accelerate the establishment of informal partnerships to assist large Internet companies in understanding national security threats as well as trends and patterns in terrorist propaganda and communication, so that such companies become more conscious of emerging threats, key individuals, and organizations, and

find it easier to align their takedown efforts with national security priorities.

Reducing the Demand

As demonstrated in Section 4, the long-term aim must be to create resilient populations, which resist the appeal of violent extremist online propaganda and mount civic challenges to counter its influence. To achieve this goal, the report recommends the following:

- Government, in partnership with community groups, has an important role to play in creating awareness and spreading information about online radicalization among educators, parents, and relevant communities. Existing programs and efforts that serve this purpose need to be continued and expanded.
- While government agencies are restricted in their ability to become involved in counter-messaging, they should serve as enablers, bringing together the private sector, foundations, philanthropists, and community groups to build capacity and help mainstream groups, victims of terrorism, and other stakeholders become more effective at conveying their messages. The White House's forthcoming Internet strategy should spell out what the government will do, what resources will be devoted to this effort, and how success will be measured.
- The government's Internet strategy also needs to make clear what part of government will coordinate capacity building, engagement, and outreach efforts and what resources will be made available to support this task. If NCTC, whose small global-engagement unit has led several initiatives in this area, is to assume the overall lead, its staffing and resources will have to be increased.
- Government needs to adopt a consistent policy on engaging with violent extremists and vulnerable populations in online forums. It needs to review and, if necessary, clarify existing rules, so community groups that are willing to populate online forums and engage with violent extremists can do so without running the risk of being caught up in counter-terrorism investigations.
- Government should encourage school authorities to review and update their curricula on media literacy, consider violent extremism as part of their instruction on child-safety issues, and develop relevant training resources for teachers. Internet companies should broaden their efforts to promote child safety to include threats from online extremism and terrorist propaganda—for example, by adapting their educational materials, case studies, advice, and software to account for this threat. Parents should be encouraged to take an active interest in their children's Internet activities and learn to use the Internet *with* them.

Exploiting Cyberspace

Section 5 showed that there are numerous benefits to—and opportunities for—exploiting terrorists' online communication and interactions to gain intelligence and gather evidence. The report recommendations are:

- Government needs to review oversight procedures and clarify the legal framework under which domestic agencies are permitted to monitor, save, and analyze online communications. The lack of a sufficiently clear legal framework, judicial-review mechanism, and congressional-review mechanism has prevented domestic agencies from making maximum use of the Internet as an investigative tool.
- Government should increase the amount of online training offered to members of law enforcement and intelligence agencies, including state and local agencies, so they are conscious of the increasingly virtual nature of the threat and can use online resources to gather information about violent extremist communities in their local areas.

- Given the rapidly changing nature of the online environment, government needs to periodically review the scope, sophistication, and appropriateness of the regulatory framework that governs data gathering and analysis in cyberspace, as well as the technological tools and capabilities that are used for doing so.

Arguably, the use of the Internet to radicalize and recruit homegrown terrorists is the single most important and dangerous novelty since the terrorist attacks of September 11, 2001. As *The 9/11 Commission Report* showed, the September 11 attackers used the Internet for searches, to buy tickets, and book hotels, but the new technology played little role in their radicalization.[155] Back then, the rise of online communities and the dissemination of near-professional propaganda videos via video-sharing and social-networking sites was hard to imagine and impossible to predict. If anything, this should remind us that dealing with online radicalization must not be a one-off effort. As the Internet keeps changing, so do the methods of those who want to use it to spread hate and incite terror.


threat

Endnotes

1. For an overview of all terrorist attacks on U.S. soil since September 11, 2001, see "The Homegrown Threat," an online database maintained by the New America Foundation and Syracuse University; available at http://homegrown.newamerica.net/.
2. Joe Heim, "Wade Michael Page Was Steeped In Neo-Nazi 'Hate Music' Movement," The Washington Post, August 7, 2012.
3. BBC News, "Profile: Wisconsin Sikh Temple Shooter Wade Michael Page," August 7, 2012.
4. Interview with Alexander Hitchens, International Centre for the Study of Radicalisation (ICSR), King's College London, August 2012.
5. See Jarret M. Brachman and Alix N. Levine, "You Too Can Be Awlaki!" The Fletcher Forum of World Affairs, 35(1) (2011), pp. 27-32. Also "A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government's Failure to Prevent the Fort Hood Attack," A Special Report by the U.S. Senate Committee on Homeland Security and Governmental Affairs, February 2011, pp. 20-21.
6. "Empowering Local Partners to Prevent Violent Extremism in the United States," White House, August 2011, p. 6.
7. "Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States," White House, December 2011, p. 20.
8. Ibid., p. 5.
9. Ibid., p. 20.
10. National Security Preparedness Group, Assessing the Terrorist Threat (Bipartisan Policy Center: Washington, 2010).
11. National Security Preparedness Group, Preventing Violent Radicalization in America (Bipartisan Policy Center: Washington, 2011).
12. Research for this report involved several meetings with staff and members of the Homeland Security Project; a systematic review of the academic literature and relevant think tank reports, congressional testimonies, conference summaries, and other printed materials; and interviews with nearly 40 individuals, representing the U.S. government, Congress, foreign embassies, industry, academia, think tanks, and public interest groups. The interviews were carried out by phone or in person, mostly during the months of July and August 2012, and included individuals associated with the following institutions and entities (in alphabetical order): American Civil Liberties Union; Anti-Defamation League; Community Security Trust; Constrat; Center for Naval Analyses; Center for Strategic and International Studies; Department of Homeland Security; Embassy of the Netherlands, Washington; Embassy of the United Kingdom, Washington; Google; Hogan Lovells LLC; Institute for Strategic Dialogue; International Centre for the Study of Radicalization, King's College London; Muslim Public Affairs Council; Morningside Analytics; Muflehun; National Consortium for the Study of Terrorism and Responses to Terrorism (START), University of Maryland; National Counterterrorism Center; New America Foundation; Office of Senator Susan Collins; Palantir; Senate Committee on Homeland Security and Governmental Affairs; State Department; Southern Poverty Law Center; and WORDE.
13. The definitions of radicalization and counter-radicalization are from the Homeland Security Project's 2011 report on counter-radicalization; see National Security Preparedness Group, Preventing Violent Radicalization, p. 16. The definitions of cyberspace, the Internet, and the World Wide Web can be found in Tim Stevens and Peter Neumann, Countering Online Radicalization: A Strategy for Action (London: ICSR, 2009), p. 10; available at http://www.icsr.info/news-item.php?id=21.
14. See Roger Scruton, The Palgrave Macmillan Dictionary of Political Thought, 3rd ed. (Basingstoke: Palgrave Macmillan, 2007).
15. Brian Levin, "Cyberhate: A Legal and Historical Analysis of Extremists' Use of Computer Networks in America," American Behavioral Scientist 45(6) (2002), p. 960.
16. Cited in ibid., pp. 961-2.
17. David Lowe, Computerized Networks of Hate: An ADL Fact-Finding Report (New York: ADL, 1985). Cited in Levin, "Cyberhate," p. 963.
18. Ibid.
19. Louise Beam, "Leaderless Resistance," The Seditionist, February 1992.
20. Stevens, Countering Online, p. 11.
21. See, for example, Gabriel Weimann, Terror on the Internet: The New Arena, the New Challenges (Washington: United States Institute for Peace Press, 2006), Chapters 3 and 4.
22. See, for example, National Coordinator for Counterterrorism, Jihadists and the Internet: 2009 Update (The Hague: NCTb, 2009), p. 11.
23. See, for example, Michael Kenney, "Beyond the Internet: Metis, Techne, and the Limitations of Online Artifacts for Islamist Terrorists," Terrorism and Political Violence, 22(2) (2010), pp. 177-197; Anne Stenersen, "The Internet: A Virtual Training Camp," Studies in Conflict and Terrorism 20 (2008), pp. 215-233.
24. Interview with Gary Ackerman, research director, National Consortium for the Study of Terrorism and Responses of Terrorism (START), University of Maryland.
25. Ibid. Also Evan Kohlmann, "The Real Online Terrorist Threat," Foreign Affairs, September 2006, pp. 115-116; National Coordinator, Jihadists and, Chapter 2; William Tafoya, "Cyber Terror," FBI Law Enforcement Bulletin, November 2011.
26. See Brynjar Lia, "Al Qaeda Online: Understanding Jihadist Internet Architecture," Jane's Intelligence Review, December 2005.
27. See Daniel Kimmage, The Al-Qaeda Media Nexus (Washington: Radio Free Europe/Radio Liberty, 2008).
28. Adam Bermingham, et al., "Combining Social Network Analysis and Sentiment Analysis to Explore the Potential for Online Radicalisation," Proceedings of the International Conference on Advances in Social Network Analysis and Mining, 20-22, July 2009, Athens, Greece, pp. 231-236.
29. National Coordinator, Jihadists and, p. 12.
30. Jarret Brachman, Global Jihadism: Theory and Practice (London: Routledge, 2009), p. 19.
31. See, for example, John J. Barton, Shumin Zhai, and Steve B. Cousins, "Mobile Phones Will Become the Primary Personal Computing Devices," 7th IEEE Workshop on Mobile Computing Systems and Applications, April 6-7, 2006, Semiahmoo, WA; available at http://www.almaden.ibm.com/u/bartonjj/jbarton-PhoneBeatsPC.pdf.
32. Tom Pyszczynski, et al., "Mortality Salience, Martyrdom and Military Might: The Great Satan Versus the Axis of Evil," Personality and Social Psychology Bulletin 32(4) (2006), pp. 525-537.
33. Marc Sageman, Leaderless Jihad: Terror Networks in the Twenty-First Century (Philadelphia: University of Pennsylvania Press, 2008), Chapters 3 and 4.
34. Marc Sageman before the U.S Senate Committee on Homeland Security and Governmental Affairs, Hearing on Violent Islamist Extremism: The European Experience, June 27, 2007, pp. 1-2.
35. See Edwin H. Sutherland and Donald R. Cressey, Principles of Criminology, 4th ed. (Chicago: Chicago University Press, 1947). In the online context, extremist forums have frequently been described as echo chambers. On echo chambers, see Sanne Gerraerts, "Digital Radicalisation Of Youth," Social Cosmos 3(1) (2012), pp. 26-27.

36. Cited in Larry Keller, "Experts Discuss the Role of Race Propaganda after White Massachusetts Man Kills Two African Immigrants," Intelligence Report, Summer 2009; available at http://www.splcenter.org/get-informed/intelligence-report/browse-all-issues/2009/summer/from-hate-to-hurt.
37. Howard Rheingold, The Virtual Community: Homesteading on the Electronic Frontier (New York: Harper Collins, 1994), p. 4.
38. John Suler, "The Online Disinhibition Effect," CyberPsychology and Behavior 7(3) (2004), pp. 321-326.
39. See Katherine Bessière, A. Fleming Seay, and Sara Kiesler. "The Ideal Elf: Identity Exploration in World of Warcarft," CyberPsychology and Behavior 10(4) (2007), pp. 530-535.
40. Jarret Brachman and Alix Levine, "You Too Can Be Awlaki!," Fletcher Forum of World Affairs 35(1) (2011), pp. 41-2.
41. The official term is "massively multiplayer online role-playing games" (MMORPG).
42. Ibid., p. 43.
43. AIVD, Jihadism on the Web: A Breeding Ground for Jihad in the Modern Age (The Hague: Ministry of the Interior and Kingdom Relations, 2012), p. 17.
44. Scott Shane, "Web Posts Began Tale of Detained Americans," The New York Times, December 13, 2009.
45. "A Ticking Time," Chapter IV.
46. For a full account of the e-mails, see "Anwar Al Awlaki Email Exchange with Fort Hood Shooter Nidal Hasan," Intelwire, July 19, 2012; available at http://news.intelwire.com/2012/07/the-following-e-mails-between-maj.html.
47. "A Ticking Time," pp. 20-21.
48. Quoted in Vikram Dodd, "Roshonara Choudry: Police Interview Extracts," The Guardian, November 3, 2010.
49. Matthias Bartsch, Matthias Gebauer, and Yassin Musharbash, "The Radical Islamist Roots of the Frankfurt Attack," Spiegel Online, March 3, 2011; available at http://www.spiegel.de/international/germany/facebook-jihad-the-radical-islamist-roots-of-the-frankfurt-attack-a-748910.html; also Gerhard Piper, "Der Frankfurter Pistolenschütze und seine Kontakte," Telepolis, March 3, 2011; available at http://www.heise.de/tp/blogs/8/149375.
50. "Zachary Chesser: A Case Study in Online Islamist Radicalization and Its Meaning for the Threat of Homegrown Terrorism," Senate Committee on Homeland Security and Governmental Affairs, February 2012, p. 13.
51. United States v. Colleen R. LaRose (2010); available at http://media.nbcphiladelphia.com/documents/JihadJane.pdf.
52. Ibid.
53. Conversation with U.S. government official, June 2011.
54. See National Security, Preventing Violent, p. 12.
55. "Samir Khan: American Blogger and Al Qaeda Propagandist," Anti-Defamation League, February 8, 2008; available at http://www.adl.org/main_Terrorism/samir_khan.htm?Multi_page_sections=sHeading_2.
56. Ibid.
57. Dina Temple-Raston, "American Editor Brings U.S. Savvy to Jihad Outreach," NPR, October 12, 2010.
58. Cited in ibid.
59. Anti-Defamation League, Combating Extremism in Cyberspace: The Legal Issues Affecting Internet Hate Speech (New York: ADL, 2000), p. 3.
60. Ibid., p. 5.
61. This included, for example, the case of a neo-Nazi march through a Jewish suburb of Chicago (Collin v. Smith, 7th Circuit, 1978) and that of an anti-gay church group from Kansas picketing soldiers' funerals (Snyder v. Phelps, 2011).
62. Dartmouth philosophy Professor Susan Brison, cited in Sasha Dudding, "Brison Discusses Free Speech Limits," The Dartmouth, January 17, 2012; available at http://thedartmouth.com/2012/01/17/news/brison.
63. See "Remarks on Internet Freedom," U.S. Department of State, January 21, 2010; available at http://www.state.gov/secretary/rm/2010/01/135519.htm.
64. See Eliza Krigman, "Hill Tries To Foil Plot Against The Net," Politico, September 22, 2012; available at http://www.politico.com/news/stories/0912/81552.html.
65. Victoria Kempf, "Kids Circumventing Fences to the Internet," ScreenRetriever, June 25, 2011; available at http://www.screenretriever.com/2011/06/kids-circumventing-fences-to-the-Internet/.
66. Stevens, "Countering Online," pp. 20-21.
67. In addition to the "Great Firewall"—a nationwide system of network filters that is maintained by tens of thousands of government employees—the Chinese government has imposed draconian sanctions, including prison, on Internet users promoting "harmful" online content. State and local governments all have units responsible for monitoring online content and usage in their areas. Internet companies operating in China are liable for illegal content posted by their customers. See Lacey Alford, The Great Firewall of China: An Evaluation of Internet Censorship in China (Dusseldorf: VDM, 2010).
68. "ISP Usage and Market Share," Stat Owl; available at http://www.statowl.com/network_isp_market_share.php.
69. Stevens, "Countering Online," pp. 15-18.
70. Confidential conversations with E.U. and U.K. government officials.
71. Interview with Duncan Fulton, British Embassy, Washington, August 2012.
72. "Prevent: Tackling Terrorism and Violent Extremism on the Internet," Association of Chief Police Officers, March 2010; available at http://www.acpo.police.uk/documents/TAM/CTRIU%20factsheet.pdf.
73. HM Government, Contest: The United Kingdom's Strategy for Countering Terrorism (London: Stationery Office, 2011), p. 76.
74. Interview with HP Schreinemachers, Embassy of the Netherlands, Washington, August 2012.
75. "Notice-and-take-down Code of Conduct," ECP, October 2008; available at http://www.ecp-epn.nl/sites/default/files/NTD_Gedragscode_Engels.pdf.
76. Ibid., p. 7.
77. Interview with HP Schreinemachers.
78. Cited in "UK 'Blacklist' Of Terrorist Supporting Websites Should Be Developed, Government Says," Out-Law.com, June 8, 2011; available at http://www.out-law.com/page-11988.
79. Distributed Denial of Service attacks typically aim to flood a website with communication requests, thereby causing the site to shut down. See "distributed denial-of-service attack (DDoS)," Search Security, November 2010; available at http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack.
80. Ellen Nakashima, "Dismantling Of Saudi-CIA Website Illustrates Need For Clearer Cyberwar Policies," The Washington Post, March 19, 2010.
81. Ibid.
82. See, for example, J. Nicholas Hoover, "Cyber Warfare Still Poses Legal Questions," Information Week, September 19, 2012; available at http://www.informationweek.com/government/security/cyber-warfare-still-poses-legal-question/240007560.

83. Ibid.
84. Interview with Christopher Wolf, Hogan Lovells LLC, August 2012.
85. ADL, Combating Extremism, p. 5.
86. The appeal court judges concluded that the jury had not been properly instructed and that the verdict might therefore be unjust. The British Crown Prosecution Service decided not to request a retrial. See "Lyrical Terrorist' Wins Appeal," BBC News, June 17, 2008.
87. See "Virginia Man Sentence to 25 Years in Prison for Providing Material Support and Encouraging Violent Jihadists to Kill U.S. Citizens," United States Attorney's Office, February 24, 2011; available at http://www.justice.gov/usao/vae/news/2011/02/20110224chessernr.html.
88. See, for example, "Lieberman to YouTube: Remove al-Qaeda videos," CNN, May 20, 2008.; available at http://edition.cnn.com/2008/POLITICS/05/20/youtube.lieberman/.
89. Interview with Bob Boorstin, Google, August 2012.
90. "YouTube Opens Enhanced Abuse and Safety Center," TechCrunch, December 11, 2008; available at http://techcrunch.com/2008/12/11/youtube-opens-abuse-and-safety-center/.
91. Anti-Defamation League, "YouTube Taps ADL As Partner In Fight Against Hate," December 11, 2008; available at http://www.adl.org/PresRele/Internet_75/5416_75.htm.
92. Brian Bennett, "YouTube is letting users decide on terrorism-related videos," Los Angeles Times, December 12, 2010.
93. Correspondence with Mike Whine, Community Security Trust, September 2012.
94. "YouTube Community Guidelines," YouTube; available at http://www.youtube.com/t/community_guidelines.
95. For examples of what was found when searching for terms like "Al Awlaki," "Chechnya mujahideen," "Iraq mujahideen," or "how to make detonator" in mid-September 2012, see http://www.youtube.com/results?search_query=anwar+al+awlaki&page=1; http://tinyurl.com/92htwa2; http://tinyurl.com/9lk7hut; http://www.youtube.com/verify_age?next_url=/watch%3Fv%3D8ttroowu6_w.
96. Interview with Bob Boorstin.
97. Like Google, Facebook does not permit hate speech, whereas Twitter only draws the line at threats of violence directed at specific people. See "Facebook Community Standards," Facebook; available at https://www.facebook.com/communitystandards; "The Twitter Rules," Twitter; available at http://support.twitter.com/articles/18311-the-twitter-rules.
98. Interview with Bob Boorstin.
99. "White Supremacist Shooting Spree Leaves Bloody Trail in Massachusetts," Anti-Defamation League, January 22, 2009.
100. David Holthouse, "Website Read by Accused Racial Killer Encouraged 'Lone Wolf' Murders," Extremist Crime, January 23, 2009.
101. Larry Keller, "U.S. Neo-Nazi, Back From Estonia, Bedevils Montana," Southern Poverty Law Center, 25 August 2010; available at http://www.splcenter.org/blog/2010/08/25/u-s-neo-nazi-back-from-estonia-bedevils-montana/#more-4664.
102. Cited in Barbara Oberg (ed.), The Papers of Thomas Jefferson, Volume 33: 17 February to 30 April 1801 (Princeton, N.J.: Princeton University Press, 2006), pp. 143-8.
103. Abrams v. United States, Supreme Court, 1919.
104. Suler, "Online Disinhibition."
105. Mark Potok, "Hate on the Internet and the American Legal System," Briefing of the Commission on Security and Cooperation in Europe, May 15, 2008; available at http://tinyurl.com/9c9e73f._
106. Marc Prensky, "Digital Natives, Digital Immigrants," On the Horizon 9(5) (2001).
107. The most frequently cited example is the Smith-Mundt Act of 1948, which restricts the domestic dissemination of information—produced typically by the State Department and the Department of Defense—that is aimed at foreign audiences. See Josh Rogin, "Much ado about State Department 'propaganda,'" Foreign Policy, May 23, 2012; available at http://thecable.foreignpolicy.com/posts/2012/05/23/much_ado_about_state_department_propaganda.
108. See Jerome Bjelopera, "American Jihadist Terrorism: Combating a Complex Threat," Congressional Research Service, December 7, 2010, p. 130.
109. Interview with Humera Khan, Muflehun, August 2012.
110. "ADAMS Center Event Report," National Counterterrorism Center, 2012 (unpublished document).
111. Participants were asked to evaluate the second workshop that was held at the ADAMS center in northern Virginia: 90 percent said they either found it "useful" or "learned a lot," with 60 percent saying they "learned a lot." See ibid.
112. Interviews with Shahed Amanullah and Humera Khan, August 2012.
113. Ibid.
114. Amanullah, quoted in Spencer Ackerman, "Newest U.S. Counterterrorism Initiative: Trolling," Wired, July 18, 2012.
115. Interview with government officials, August 2012.
116. Correspondence with Brian Fishman, New America Foundation, September 2012.
117. Against Violent Extremism; website available at http://www.againstviolentextremism.org/about.
118. Interview with Ross Frenett, Institute for Strategic Dialogue, September 2012.
119. The global leader in this respect has been the United Kingdom, whose Research, Information and Communications Unit has undertaken extensive research on online behavior and counter-terrorist messages.
120. "Radicalisation: The Role of the Internet: A Working Paper of the PPN," Institute for Strategic Dialogue, p. 9.
121. An example of good practice is the Transportation Security Administration's (TSA) "Blogger Bob," who takes on rumors about the work of TSA on "The TSA blog"; available at http://blog.tsa.gov/.
122. See Stevens, "Countering Online," pp. 43-46.
123. Interview with Ambassador Alberto Fernandez, August 2012.
124. Interview with Constrat representatives, August 2012.
125. Interview with government officials, July and August 2012.
126. Interview with Haris Tarin, MPAC, and government officials, July and August 2012.
127. Stevens, "Countering Online," pp. 36-37.
128. Ibid., pp. 38-39.
129. Ibid.
130. Ibid., pp. 39-40.
131. See Elliot Schrage, "Online child safety initiatives," Google Blog, February 16, 2007; available at http://googleblog.blogspot.co.uk/2007/02/online-child-safety-initiatives.html; "Family Safety Center," Facebook; available at https://www.facebook.com/safety.

132. "Maryland Man Arrested in Plot to Attack Armed Forces Recruitment Center," U.S. Attorney's Office, December 8, 2010; available at http://www.fbi.gov/baltimore/press-releases/2010/ba120810.htm.
133. Ibid. Also "Baltimore Man Arrested for Attempting to Bomb Military Recruitment Centre," Anti-Defamation League, December 9, 2010; available at http://www.adl.org/main_Terrorism/Antonio_Martinez.htm.
134. "Maryland Man," U.S. Attorney's.
135. "Baltimore Man," Anti-Defamation.
136. Interview with John Gannon, August 2012.
137. "Statement of Anthony D. Romero, Executive Director, American Civil Liberties Union before the House Committee on Homeland Security," American Civil Liberties Union, May 26, 2010.
138. Ibid.
139. "Written Testimony of Mary Ellen Callahan, Chief Privacy Officer, and Richard Chavez, Director, Office of Operations Coordination and Planning, U.S. Department of Homeland Security before United States House of Representatives," Committee on Homeland Security," Department of Homeland Security, February 16, 2012; pp. 10-11.
140. Ibid.
141. The Constitution Project, Principles for Government Data Mining (Washington DC: The Constitution Project, 2010), p. 16; available at http://www.constitutionproject.org/pdf/DataMiningPublication.pdf. Also, Fred H. Cate, "Government Data Mining: The Need for a Legal Framework," Harvard Civil Liberties-Civil Rights Law Review, 43(2) (2008), pp. 435-488.
142. Ibid., p. 4.
143. Marc Sageman, Leaderless Jihad: Terror Networks in the Twenty-First Century (Philadelphia: Pennsylvania University Press, 2008), p. 144.
144. Interview with John Kelly, Morningside Analytics, and representatives of Constrat, August 2012.
145. See Alexander Meleagrou-Hitchens, Shiraz Maher, and James Sheehan, Lights, Camera, Jihad: Al Shabaab's Western Media Strategy (London: ICSR, 2012); available at www.icsr.info.
146. See Alexander Meleagrou-Hitchens, As American as Apple Pie: How Anwar al-Awlaki Became the Face of Western Jihad (London: ICSR, 2011); available at www.icsr.info.
147. Interview with Will McCants, August 2012.
148. Interview with government officials, August 2012.
149. See Caryn Brooks, "Portland's Bomb Plot: Who Is Mohamed Mohamoud?," Time, November 28, 2010; available at http://www.time.com/time/nation/article/0,8599,2033372,00.html. Also Bob Drogin and April Choi, "Teen held in alleged Portland bomb plot," Los Angeles Times, November 28, 2010; available at http://articles.latimes.com/2010/nov/28/nation/la-na-portland-bomb-plot-20101128.
150. "Testimony of William McCants, Analyst for the Center for Naval Analyses," Subcommittee on Counterterrorism and Intelligence, House Homeland Security Committee, December 6, 2011; available at http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20McCants.pdf.
151. To our knowledge, there has not been a single terrorism prosecution in the United States in recent years that has not relied, to a greater or lesser extent, on defendants' personal electronic communications.
152. Conversation with British officials, London, October 2012.
153. "Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States," White House, December 2011, p. 20.
154. Ibid.
155. See National Commission on Terrorist Attacks on the United States, The 9/11 Commission Report (New York: WW Norton, 2004), pp. 157, 222; available at http://www.9-11commission.gov/report/911Report.pdf.

Founded in 2007 by former Senate Majority Leaders Howard Baker, Tom Daschle, Bob Dole and George Mitchell, the Bipartisan Policy Center (BPC) is a non-profit organization that drives principled solutions through rigorous analysis, reasoned negotiation and respectful dialogue. With projects in multiple issue areas, BPC combines politically balanced policymaking with strong, proactive advocacy and outreach.

BIPARTISAN POLICY CENTER

1225 Eye Street NW, Suite 1000
Washington, DC 20005
(202) 204-2400

WWW.BIPARTISANPOLICY.ORG