

**ISIS ONLINE: COUNTERING
TERRORIST RADICALIZATION AND RECRUITMENT
ON THE INTERNET AND SOCIAL MEDIA**

HEARING

BEFORE THE

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

OF THE

COMMITTEE ON

HOMELAND SECURITY AND

GOVERNMENTAL AFFAIRS

UNITED STATES SENATE

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

JULY 6, 2016

Available via the World Wide Web: <http://www.fdsys.gov/>

Printed for the use of the
Committee on Homeland Security and Governmental Affairs



ISIS ONLINE: COUNTERING TERRORIST RADICALIZATION AND RECRUITMENT ON THE INTERNET AND SOCIAL MEDIA

**ISIS ONLINE: COUNTERING
TERRORIST RADICALIZATION AND RECRUITMENT
ON THE INTERNET AND SOCIAL MEDIA**

HEARING

BEFORE THE

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

OF THE

COMMITTEE ON
HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE
ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

JULY 6, 2016

Available via the World Wide Web: <http://www.fdsys.gov>

Printed for the use of the
Committee on Homeland Security and Governmental Affairs



U.S. GOVERNMENT PUBLISHING OFFICE

22-476 PDF

WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

JOHN McCain, Arizona	THOMAS R. CARPER, Delaware
ROB PORTMAN, Ohio	CLAIRE McCASKILL, Missouri
RAND PAUL, Kentucky	JON TESTER, Montana
JAMES LANKFORD, Oklahoma	TAMMY BALDWIN, Wisconsin
MICHAEL B. ENZI, Wyoming	HEIDI HEITKAMP, North Dakota
KELLY AYOTTE, New Hampshire	CORY A. BOOKER, New Jersey
JONI ERNST, Iowa	GARY C. PETERS, Michigan
BEN SASSE, Nebraska	

CHRISTOPHER R. HIXON, *Staff Director*

GABRIELLE A. BATKIN, *Minority Staff Director*

JOHN P. KILVINGTON, *Minority Deputy Staff Director*

LAURA W. KILBRIDE, *Chief Clerk*

BENJAMIN C. GRAZDA, *Hearing Clerk*

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

ROB PORTMAN, Ohio *Chairman*

JOHN McCain, Arizona	CLAIRE McCASKILL, Missouri
RAND PAUL, Kentucky	JON TESTER, Montana
JAMES LANKFORD, Oklahoma	TAMMY BALDWIN, Wisconsin
KELLY AYOTTE, New Hampshire	HEIDI HEITKAMP, North Dakota
BEN SASSE, Nebraska	

BRIAN CALLANAN, *Staff Director and General Counsel*

MARGARET DAUM, *Minority Staff Director and Chief Counsel*

KELSEY STROUD, *Chief Clerk*

CONTENTS

Opening statements:	Page
Senator Portman	1
Senator McCaskill	4
Senator Ayotte	15
Senator Lankford	17
Senator Heitkamp	19
Senator Baldwin	20
Prepared statements:	
Senator Portman	45

WITNESSES

WEDNESDAY, JULY 6, 2016

Michael Steinbach, Executive Assistant Director, National Security Branch, Federal Bureau of Investigation	6
George Selim, Director, Office of Community Partnerships, U.S. Department of Homeland Security, and Director, Interagency Task Force on Countering Violent Extremism	8
Meagan M. LaGrafte, Chief of Staff to the Coordinator and Special Envoy, Global Engagement Center, U.S. Department of State	10
Peter Bergen, Vice President, New America Foundation	33
Alberto M. Fernandez, Vice President, Middle East Media Research Institute ..	35

ALPHABETICAL LIST OF WITNESSES

Bergen, Peter:	
Testimony	33
Prepared statement	64
Fernandez, Alberto M.:	
Testimony	35
Prepared statement	82
LaGrafte, Meagan M.:	
Testimony	10
Prepared statement	59
Selim, George:	
Testimony	8
Prepared statement	54
Steinbach, Michael:	
Testimony	6
Prepared statement	51

APPENDIX

Images submitted by Senator Portman	49
Statement submitted for the Record by American-Arab Anti-Discrimination Committee	95
Responses to post-hearing questions for the Record	
Mr. Selim	100
Ms. LaGrafte	109

**ISIS ONLINE: COUNTERING
TERRORIST RADICALIZATION AND
RECRUITMENT ON THE INTERNET AND
SOCIAL MEDIA**

WEDNESDAY, JULY 6, 2016

U.S. SENATE,
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS,
OF THE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:07 p.m., in room SD-342, Dirksen Senate Office Building, Hon. Rob Portman, Chairman of the Subcommittee, presiding.

Present: Senators Portman, Lankford, Ayotte, Sasse, Johnson, McCaskill, Tester, Baldwin, Heitkamp, and Carper.

OPENING STATEMENT OF SENATOR PORTMAN

Senator PORTMAN. This hearing will come to order. We are here to talk about an incredibly important issue, a critical issue that affects the security of our country and the security of our families.

When the Subcommittee first began planning this hearing, of course, we did not know it would fall just 3 weeks after the most deadly terrorist attack on American soil since September 11th. The evil terrorist attack in Orlando last month that targeted the lesbian, gay, bisexual and transgender (LGBT) community was yet another reminder of the urgent need to reexamine and redouble our government's efforts to combat violent Islamic jihadism both at home and abroad—and particularly to disrupt and ultimately destroy the so-called Islamic State of Iraq and Syria (ISIS). There is no room for complacency on this issue. It warrants continuous scrutiny and oversight from Congress as our government's understanding of the enemy evolves. And we will hear some about that today.

ISIS, of course, specializes in savagery—violence inspired by delusions of sectarian conquest from another age. Yet it has effectively deployed modern technology of the information age to spread its propaganda and recruit killers to its cause. ISIS has developed a sophisticated information warfare capability. It has pioneered a distinctive strategy of targeted online recruitment, while disseminating sleek viral videos and messages, primarily from two media centers—Al-Hayat and Al-Furqan—through a constantly evolving set of online platforms. As the Federal Bureau of Investigation (FBI) Director James Comey has noted, even if we were able to

keep foreign terrorists physically out of the United States, online communication and social media allow ISIS to, as he said, “enter as a photon and radicalize somebody in Wichita, Kansas.” ISIS has weaponized online propaganda in a new and very lethal way.

The damage wrought by that weapon is considerable: Orlando, 49 dead; San Bernardino, 14; Fort Hood, 13 dead; the Boston Marathon, 3 dead and hundreds wounded. Each of these killers was reportedly radicalized to some degree by online jihadist content. And so many other attacks inspired by means of social media have, thank God, been thwarted. Indeed, experts tell us that throughout last year, social media played some part in the radicalization of all of the 60 people arrested in the United States for criminal acts in support of ISIS. Again, we may hear more about that today. Most recently, of course, the FBI has publicly stated that it is “highly confident” that the Orlando killer, Omar Mateen, was “radicalized at least in part through the Internet.”

One longstanding aim of the ISIS propaganda machine is to attract foreign fighters to ISIS-controlled territory. Often ISIS tells its recruits tales of high adventure, joined with false narratives of Islamic extremism as a utopia. The bizarre images behind me over here,¹ for example, appear in a ISIS film exhorting Muslims around the world to join the Islamic State; rather than show ISIS fighters for what they are—murderers of innocent victims who are themselves overwhelmingly Muslim—they are shown playing with laughing children and shopping in local marketplaces.

Appeals like these have helped draw an estimated 30,000 foreign fighters, including at least 6,000 Westerners, to take up arms with ISIS. The good news is that the Defense Department (DOD) reports a significant decrease in the flow of foreign fighters to ISIS territory. At the same time, however, ISIS has increasingly shifted its propaganda efforts to inciting sympathizers to commit acts of terror in the West—including right here in the United States.

Online propaganda, amplified by social media and Peer-2-Peer (P2P) communication, is now a key weapon in ISIS’ arsenal. We should, of course, resist oversimplifying the problem. Not all radicalization in the United States occurs online, and in-person interaction often reinforces the process. But unlike the more common European pattern of jihadist radicalization in clusters, neighborhoods, or in prison, the U.S. threat so far is predominantly that of the lone-wolf terrorist—an individual radicalized on his own, often in front of his computer screen with access to online jihadist content and videos that create a sort of virtual training camp.

In addition to a clear military strategy and vigilant law enforcement efforts here at home, the United States and our allies need a more robust, coordinated strategy to expose the enemy’s lies, counter its false narratives, and encourage credible voices to tell the truth to those most susceptible or receptive to the ISIS lies. And that is true both of foreign and U.S. audiences. Although the ISIS online radicalization threat is well recognized, there is a range of opinion on how best to combat it, and the U.S. Government’s efforts are still in their early stages, as we will hear about today. Today we are going to examine the countermessaging initiatives

¹ The images referenced by Senator Portman appears in the Appendix on page 49.

that show promise—and where the government has fallen short and could accelerate those efforts.

In January, the State Department began a revamp of its counter-terrorism messaging and coordination efforts with the launch of what is called the “Global Engagement Center”—a better funded and, at least on paper, more empowered version of its predecessor, the Center for Strategic Counterterrorism Communications. We have had testimony in this room before regarding the Global Engagement Center, and we look forward to getting deeper into that today.

Previous efforts to address this threat have struggled to overcome bureaucratic hurdles, unclear authorities, and a lack of inter-agency communication and a unity of effort. These structural deficiencies will continue to hinder future administrations—both Republican and Democrat—unless they are addressed. That is why I recently introduced legislation with Senator Murphy to help resolve some of these issues and the impact they have on our ability not only to counter propaganda and disinformation from extremist groups like ISIS but also the equally pressing challenges posed by some nation States and their sponsored propaganda.

The Department of Homeland Security (DHS) also recently consolidated its countering-violent-extremism (CVE), efforts in a new office call the “Office of Community Partnerships (OCP).” Again, we have heard about this in this hearing room. We look forward to digging deeper today. We will be hearing more about these efforts, and I will be interested in exploring whether these initiatives are backed by sufficient authorities and sufficient resources.

In addition, social media firms including Facebook and Twitter have stepped up their voluntary efforts to police their own terms of service, which prohibit incitements to terrorism. Twitter has closed more than 100,000 ISIS-linked accounts, for instance, and Facebook has actively worked to remove offending users while working in various ways to promote content to counter jihadist propaganda. These actions have helped to degrade ISIS’ social media megaphone, according to the Middle East Media Research Institute, but its online presence remains strong.

So let us be very clear: To defeat ISIS, it is necessary to destroy the enemy where they live and prosper—in Iraq and in Syria and elsewhere—in their major cells around the world. Online counter-messaging is no substitute for a clearly defined and vigorously executed military strategy. But a military strategy must be reinforced by a coordinated effort to undermine and disrupt the powerful disinformation spread by Islamic jihadists. Today we are going to hear from three Federal agencies involved in that effort, and I appreciate our three witnesses before us today. We are also going to hear from some distinguished experts who have been engaged on these issues for many years.

With that, I will turn to my colleague Senator McCaskill for her opening statement.

OPENING STATEMENT OF SENATOR MCCASKILL

Senator MCCASKILL. Thank you, Chairman Portman.

I think the topic of today's hearing is extremely important. Figuring out how to stop the Islamic State of Iraq and the Levant (ISIL)-inspired attacks at home and abroad is vital to our national security, and it is a topic on which the Homeland Security and Governmental Affairs Committee has an important role.

I would like to particularly note the efforts by Chairman Johnson and Ranking Member Carper who have held a number of oversight hearings in this Committee on this very topic and who have worked on relevant legislation during this Congress.

This Subcommittee has a long and proud tradition of the finest investigative work Congress has ever done, from work on war profiteering and Mafia racketeering to the U.N. Oil for Food Program and the financial crisis. And contrary to Senator Rand Paul's assertion at our cable hearing last month, during this Congress the Chairman and I have conducted many in-depth bipartisan investigations of government agencies as well as the private sector.

But today's hearing is not a typical PSI hearing. Because of the short timeframe of planning for this hearing, we were unable to speak with some of the people who I would like to see participate in our discussion: social media companies, local law enforcement groups, and those, importantly, directly involved on the ground with the pilot programs that we are currently funding through the Department of Homeland Security. Having the opportunity to hear from these other groups is especially important because, as today's government witnesses will point out, we still have a lot to learn about how to best counter the messages of violent extremism in this country from ISIL and otherwise.

The efforts being undertaken by the Department of Homeland Security's Office of Community Partnerships and the Department of State's Global Engagement Center are just getting off the ground. I hope to hear today what their plans are; how they are specifically working with the private sector, whether through grants, contracts, or other agreements; and how we can best support them going forward, while also keeping taxpayers and our oversight obligations in mind. This is a chance for Congress to do oversight on the front end rather than the back end after something has already gone wrong and massive amounts of taxpayer dollars maybe have been wasted.

Further, as we will hear from our witnesses today, it is absolutely vital that any effort our government undertakes to counter violent extremism is done in partnership with and with the full engagement of the Muslim community. After all, this was one of the core rationales for establishing the DHS Office of Community Partnerships in the first place. In order to combat ISIL's propaganda, we must have a healthy, inclusive dialogue with Muslim and other community leaders as well as ensure that resources are available to families and friends that may have concerns about loved ones who have become attracted to extremist rhetoric.

Unfortunately, some of the rhetoric we hear from politicians, including the national leader of the Republican Party and their presumptive nominee for President, is completely and utterly at odds with this policy approach. Instead of inclusivity, the presumptive

Republican candidate for President is proposing that we bar all Muslims from immigrating to the United States, even those who are trying to escape the horrors of ISIL abroad. He also campaigns on the suggestion that the entire Muslim community is complicit in violent extremism, going so far as to suggest that Muslim neighborhoods must be “policed” and subjected to special surveillance for no other reason than their religious belief.

Not only is this strategy in opposition to recommendations from every expert that our staffs have spoken with, it is also in complete conflict with American principles and values. And, most importantly, it would actually make the United States of America less safe.

This extremist rhetoric plays right into ISIL’s hands and supports its propaganda’s key message that this country hates Muslims, making it more difficult for the government partners we have today in this country to work with the Muslim community to combat extremism.

Finally, as the mass shootings we hear about on a far too regular basis remind us, we also need to make sure guns stay out of the hands of terrorists and mentally unstable individuals from all political and religious backgrounds. This is a simple, common-sense idea that nearly all Americans support.

Regrettably, we are still not ready to pass small steps, reasonable and sensible, to keep guns out of the hands of terrorists and making sure terrorists are not exploiting the online and gun show loopholes for background checks. So if we really want to counter violent extremism, we also need to spend less time stirring up anti-Muslim rhetoric and more time working on these issues and working with the majority of the Muslims who are peaceful in this country and around the world.

Although the work of the agencies represented at this hearing is important and is one part of the strategy to defeat extremism in this country, there are steps we can take immediately to make us safer starting today.

I thank the witnesses for being here, and I look forward to their testimony.

Senator PORTMAN. Thank you, Senator McCaskill.

We will now call our first panel of witnesses for this afternoon’s hearing.

Michael Steinbach is the Executive Assistant Director of the National Security Branch of the Federal Bureau of Investigation. Previously, Mr. Steinbach held multiple positions with the FBI, including serving in Afghanistan as the FBI’s deputy on-scene commander for operations and as the assistant section chief for international terrorism operations in the Counterterrorism Division. Thank you for being here.

George Selim some of you know from his exposure to the Committee through his work at the Department of Homeland Security. He is Director of the Office of Community Partnerships at DHS. He also leads the Countering Violent Extremism Task Force. Prior to his time at DHS, Mr. Selim worked at the White House on the National Security Council staff as Director for Community Policing, where he was responsible for policies related to domestic and global security threats. Before the White House, Mr. Selim was a Senior

Policy Adviser at DHS' Office for Civil Rights and Civil Liberties. Thank you for being here.

Meagen LaGraffe is the Chief of Staff for the Global Engagement Center at the State Department, which was developed to disrupt and undermine extremism propaganda, as we talked about. Prior to joining the State Department, she was Chief of Staff for Special Operations and Low-Intensity Conflict in the Office of the Secretary of Defense. Ms. LaGraffe previously served as Special Assistant to the Secretary of Homeland Security and as an aide to Senator Ted Kennedy.

I appreciate all of you for being here this afternoon and look forward to your testimony. It is the custom of this Subcommittee to swear in all of our witnesses, so at this time I would like you to stand and raise your right hand. Please repeat after me. Do you swear that the testimony you are about to give before the Subcommittee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. STEINBACH. I do.

Mr. SELIM. I do.

Ms. LAGRAFFE. I do.

Senator PORTMAN. Great. Let the record reflect that the witnesses answered in the affirmative. And to our witnesses, all of your written testimony will be printed in the record in its entirety. I would ask you to keep your comments to 5 minutes so that we will have a good opportunity for some questions and answers. Mr. Steinbach.

**TESTIMONY OF MICHAEL STEINBACH,¹ EXECUTIVE ASSISTANT
DIRECTOR, NATIONAL SECURITY BRANCH, FEDERAL BU-
REAU OF INVESTIGATION**

Mr. STEINBACH. Good afternoon, Chairman Portman, Ranking Member McCaskill, and Members of the Subcommittee. Thank you for the opportunity to appear before you today to discuss the challenge of combating the widespread reach of terrorist propaganda.

Preventing terrorist attacks remains the FBI's top priority. In today's hyperconnected world, this mission is tightly intertwined with technology and the ability it provides to reach out to anyone, anywhere, anytime.

Just as we use technology throughout the course of our day, so do the bad guys. The widespread use of technology propagates the persistent terrorist message to attack U.S. interests, whether in the homeland or abroad.

Many foreign terrorist organizations use various digital communication platforms in an effort to reach individuals they believe may be susceptible and sympathetic to the message. But no group has been as successful at drawing people into its message as ISIL. ISIL's extensive reach through the Internet and social media is most concerning as the group continues to aggressively employ the latest technology as part of its nefarious strategy.

ISIL's messaging blends both officially endorsed sophisticated propaganda with that of informal peer-to-peer recruitment through digital communication platforms. No matter the format, the mes-

¹ The prepared statement of Mr. Steinbach appears in the Appendix on page 51.

sage of radicalization spreads faster than we imagined just a few years ago. Like never before, social media allows for overseas terrorists to reach into our local communities to target our citizens as well as to radicalize and recruit.

From a threat perspective, we are concerned with three areas: those who are inspired by terrorist propaganda and feel empowered to act out and support; those who are directed by members of foreign terrorist organizations to commit a specific directed act in support of a group's ideology or cause; and those who are enabled to act after gaining inspiration from extremist propaganda and communicating with members of foreign terrorist organizations who provide guidance on method or target.

A bad actor can fall into any of the above categories or span the spectrum, but in the end the result is the same: innocent men, women, and children killed, and families, friends, and whole communities left to struggle in the aftermath.

To identify and disrupt these bad actors, we must overcome two challenges: volume and encryption.

The issue of volume is no surprise to those of you who have heard Director Comey's remarks over the last year and a half. The digital world knows no bounds. We do not just look at a person's physical associates, but now we must, too, look to their digital connections and from that assess who is a passive connection versus an active connection.

The digital world has fostered a global neighborhood of new people to meet and new ideas to follow. It is up to us to sort through the noise and identify those signals that are most concerning. Sifting through the numerous online monikers and communication platforms is not a light lift. It requires both technical capabilities and eyes-on analysis. This takes time—time we do not always have.

Not only do we face the overwhelming volume of information we have uncovered; the second challenge is the lack of accessible information when a person is using encrypted communications. Encryption takes many forms. Encryption hides stored digital communications, sometimes it masks the trail of communications, and at other times it erases the content. In many cases, we have seen concerning individuals connect via publicly available communication platforms and then switch to private encrypted applications. These apps make conversations more secret than ever before. We know that bad actors have used encrypted communication platforms prior to conducting attacks, as was the case in Garland, Texas, in May 2015, where to this day we still do not know the content of the pre-attack text messaging.

To successfully combat today's threats, we must adapt and confront these challenges. We are not in this alone. We rely heavily on the strength of our Federal, State, and local partners as well as our international partnerships. The key part of these partnerships includes an emphasis on streamlining information sharing. In today's threat environment, it is not sufficient to say information sharing is important. It is the speed of information sharing which is critical to our success. Law enforcement and the U.S. intelligence community (IC) will continue to utilize the Joint Terrorism Task Forces (JTTF) and the fusion centers to do just that. There is not

a body of people more unified and more dedicated to the singular mission of protecting our communities. Having all member agencies collocated, working the same threats, and bringing their agency's skills and resources collectively to work the investigations is powerful. We must now work to develop the same success internationally.

Chairman Portman, Ranking Member McCaskill, and members of the Subcommittee, I thank you for the opportunity to testify concerning terrorists' use of the Internet and social media. I am happy to answer questions you may have.

Senator PORTMAN. Thank you, Mr. Steinbach. Mr. Selim.

TESTIMONY OF GEORGE SELIM,¹ DIRECTOR, OFFICE FOR COMMUNITY PARTNERSHIPS, U.S. DEPARTMENT OF HOMELAND SECURITY, AND DIRECTOR, INTERAGENCY TASK FORCE ON COUNTERING VIOLENT EXTREMISM

Mr. SELIM. Good afternoon. Thank you, Chairman Portman, Ranking Member McCaskill, and distinguished Members of the Subcommittee, for the opportunity to testify here today. I welcome the opportunity to appear before you to discuss priorities and key actions that the Department of Homeland Security is conducting to address ISIL and other terrorist's attempts at online recruitment and radicalization to violence.

I have considerable personal and professional equities in protecting our homeland. By way of background, I have spent over a decade as a civil servant at the Department of Homeland Security. I have also served as the Department of Justice (DOJ) and on the National Security Council staff at the White House. In addition, I am a commissioned officer in the United States Navy Reserve and view the call to public service as one of the greatest honors our country offers all people, regardless of race, religion, or nationality.

As Secretary Johnson has stated, we are in a new phase of the global terrorist threat. The threat today is more decentralized, more complex, and difficult to detect. We have moved from a world of terrorist-directed attacks to a world of increasingly terrorist-inspired attacks. ISIL and other terrorist groups are turning to the Internet to inspire lone offenders. This is a pattern we saw last December in San Bernardino and most recently in Orlando.

By their nature, attacks involving self-radicalized individuals are harder for intelligence and law enforcement officers to detect, and they could occur with almost little or no warning. So what are we doing about it?

The threat from homegrown violent extremism requires going beyond traditional counterterrorism approaches and focusing not just on mitigation efforts but also on preventing and intervening in the process of radicalization. This prevention framework is known as "countering violent extremism," or the acronym CVE.

In 2015, Secretary Johnson announced the creation of the Office for Community Partnerships at DHS. This is the office that I lead and is focused on the Department's efforts in countering violent extremism and working to build effective partnerships with communities across the country for that explicit purpose. Our CVE efforts depend on working in a unified and cohesive manner across the

¹ The prepared statement of Mr. Selim appears in the Appendix on page 54.

U.S. Government. That is why we have established the CVE Task Force, currently headquartered at DHS, to organize all CVE Efforts across the U.S. domestically. This new task force could not be possible without the strong partnership from the Department of Justice who have appointed my Deputy Director and several key staff on the task force.

A unified efforts is necessary given the threat environment we face today. Terrorist groups such as ISIL have undertaken a deliberate strategy of using social media to reach individuals susceptible to their message and recruit and inspire them to violence. The Office of Community Partnerships and the CVE Task Force depend on our stakeholder partners to reach these individuals before they become radicalized.

Our partners in Federal, State, and local governments and law enforcement, civic and faith-based organizations, educators, social service organizations, mental health providers, and the private sector are essential to this mission. Our efforts are federally driven, but they are locally focused. Our goal is to empower credible voices within communities that are targeted by violent extremists.

Research has proven that young people, Millennials, victims of terrorists, and community-based organizations are the most credible voices to discourage those in danger of being radicalized to violence, and our role in the Federal Government should be to give those community partners the tools and support to raise their voices. Some of those tools can be provided by key technology companies. We are engaging with the private sector to encourage efforts to counter ISIL online as well as other groups.

The Department of Homeland Security and the Department of Justice, including Secretary Johnson and Attorney General Lynch, have also engaged with social media industry representatives in the past year-plus. One of our efforts, the Peer-2-Peer Challenging Extremism competition, empowers university students around the world to develop their own authentic narratives to counter violent extremist recruitment through social media.

Facebook became the first technology partner to join the Peer-2-Peer project in the summer of 2015. Facebook's participation has allowed the initiative to expand to many more international schools. In addition to the Peer-2-Peer program, the CVE Task Force will include a dedicated communications and digital strategy team. We hope to continue to work with the private sector to ensure our country's most transformative technologies and innovations can be harnessed to promote and enable civil society messages of tolerance, inclusion, and pluralism as a means of degrading the appeal of the ISIL brand.

Our efforts to develop locally driven, prevention-based CVE frameworks incorporate both online and in-person efforts. Thank you for the \$10 million of CVE grant funding that Congress has appropriated and the fiscal year (FY) 2016 Omnibus Appropriations Act. We can now take our CVE efforts across the country to the next level.

Just this morning, Secretary Johnson announced that just today the fiscal year 2016 CVE grant program has been officially launched and the Notice of Funding has been issued this morning. This is the first Federal assistance program devoted exclusively to

providing local communities with resources to counter violent extremism in our homeland. This grant program was developed by the DHS Office of Community Partnerships in conjunction with our partners at the Federal Emergency Management Agency (FEMA). This grant opportunity is an important part of our ongoing work to build a comprehensive CVE model that incorporates both cyberspace and community spaces.

Mr. Chairman, thank you for the opportunity to speak here today and for your continued support at DHS. I look forward to any questions you and the Committee may have.

Senator PORTMAN. Thank you, Mr. Selim. Ms. LaGrafte.

**TESTIMONY OF MEAGEN M. LAGRAFFE,¹ CHIEF OF STAFF TO
THE COORDINATOR AND SPECIAL ENVOY, GLOBAL ENGAGE-
MENT CENTER, U.S. DEPARTMENT OF STATE**

Ms. LAGRAFFE. Chairman Portman, Ranking Member McCaskill, Members of the Subcommittee, thank you for the opportunity to testify and answer your questions today.

I am here to discuss our government's international efforts to counter violent extremist propaganda, online, in social media, as well as in traditional media. This is a critical effort, especially when it comes to our whole-of-government efforts to degrade and destroy ISIL because it is clear that, to our enemy, the information battlespace is as important as the physical battlespace.

Prior to March of this year, I served as the Chief of Staff in the Office of Special Operations and Low-Intensity Conflict at the Pentagon. I feel confident that our U.S. military and coalition has significant capabilities to eliminate militants from the battlefield and is doing so each and every day. Daesh has already lost nearly half of its territory in Iraq and 20 percent in Syria.

At the same time, we must also confront the messages that these groups push out daily to recruit people and inspire them to violence. Addressing radicalization to violence and recruitment in the information battlespace is a key piece of any serious, meaningful, and enduring approach to countering violent extremism long-term.

To meet that challenge, President Obama signed an Executive Order in March which created the Global Engagement Center, re-vamping our countermessaging strategy.

Prioritizing countermessaging is nothing new in the national security arena, and, in fact, it is not even new in this administration. The Center's predecessor organization, the Center for Strategic Counterterrorism Communications (CSCC), focused on al-Qaeda propaganda. But while al-Qaeda was producing videos that took months to get out, our adversary today is using social media in ways not seen before.

The quality and volume of violent extremist messaging has advanced dramatically since our predecessor organization was established 5 years ago, or even from the time when Daesh began metastasizing into its current form 3 years ago.

The Global Engagement Center is charged with coordinating integrating, and synchronizing all government communications di-

¹ The prepared statement of Ms. Lagrafte appears in the Appendix on page 59.

rected at foreign audiences abroad used to diminish the influence of violent extremists.

The Center is designed to be as agile and as adaptive as our adversary. We are armed with new authorities, new personnel, and cutting-edge technology.

The Center is using state-of-the-art digital analytics tools from the intelligence community, from the Defense Advanced Research Projects Agency (DARPA), and from the private sector. These tools and technologies help us tailor our messages to our audience as well as measure those messages' effectiveness.

Importantly, the President's Executive Order grants the Center expanded hiring authorities as well, allowing us to hire leaders and experts from the private sector to join us in this effort.

When fully operational, the Center will comprise staff from the private sector as well as the Departments of Defense, Treasury, Justice, State, Homeland Security, and the intelligence community. Working across these agencies, the Center is already identifying efficiencies and opportunities in the messaging space.

Even more substantial than changes to personnel or to budgets, the Center is taking a fundamentally new approach in the information battlespace. We have pivoted toward partner-driven messaging and partner-driven content. While the U.S. Government has a good message to tell, we are not always the most credible voice to tell it.

Instead, there is an abundance of credible and diverse voices across the Middle East, Africa and Europe, their governments, non-governmental organization (NGO's), and civil society groups, all of whom we are now leveraging in this fight. We are not publicizing who many of our partners are, of course, so that we do not undermine their credibility, but I would like to give you one example.

In Kosovo, we recently completed a training program with local NGO's, designed to amplify credible voices there. We ran workshops to train local influencers about designing and executing their own messaging campaigns. Kosovo is a compelling location for this kind of work because it has not only the highest number of foreign terrorist fighters in Europe, it also has an active NGO community focused on this very issue.

Using a partners-first, data-driven approach, the Center is particularly focused on changing audience behavior rather than changing attitudes and beliefs. While we may have less success altering what an individual thinks, we can certainly be more effective at preventing individuals from turning those beliefs into violence.

I appreciate this Committee's oversight and continued support as we revamped our fight against violent extremism in the information battlespace. As you all know, any long-term success in this space cannot focus exclusively on killing terrorists. We also have to stem the recruitment of new ones.

Thank you very much for your time, and I am happy to answer any questions.

Senator PORTMAN. Thank you, Ms. LaGrafte, and good point. And I appreciate the testimony from all three witnesses and look forward to the opportunity to get into a more in-depth discussion in questions and answers.

We have one business item we need to dispose of here, so I apologize for this interruption. We are going to take a quick break and report a nomination to the floor. I want to thank the Chairman of the full Committee, Senator Johnson, who is with us here today, for his courtesy in providing us this hearing room today for our important hearing. This will just take a minute, so everybody please keep their seats.

With that, the Subcommittee will be in recess subject to the call of the Chair.

[Recess.]

This hearing is now back in session, and, again, I thank the witnesses very much for their testimony, and we look forward to having a good back-and-forth.

We have a number of Members here, so I am going to be very short, knowing that I am going to be around until the end of this hearing and have a chance to ask you questions. But let me just start, if I could, with you, Mr. Steinbach, just very briefly.

Your boss, the Director of the FBI, said last October that he believes the main threat facing the United States comes from lone-wolf terrorists who are radicalized online. Is that still the FBI's assessment?

Mr. STEINBACH. Yes, sir, it is.

Senator PORTMAN. Thank you. I think that is important to lay that as a predicate for our questions. Senator McCaskill.

Senator MCCASKILL. I just also have some questions for Ms. LaGraffe. Part of the problem we face from a messaging standpoint is the efforts of our government to message and realizing that our government is probably not the right messenger if we are going to combat an ideology that sees our country as part of the problem, not part of the solution. They see that wrongly, I might add, but nonetheless that is what they see.

There is a built-in bias against truthfulness about anything that comes from the U.S. Government. So to get around that, I understand that you and your predecessor are developing partnerships with voices perceived as more credible to disseminate the counter violent extremism message. What I am trying to understand is how this works from an oversight perspective. Are we pushing money out to groups? Are we sending them checks? Are we in a contractual relationship with them as contractors? How is this actually working in terms of how money is being passed along to messengers that we think would be more effective?

Ms. LAGRAFFE. Thank you, Senator, for your question. You are absolutely correct. The Global Engagement Center is focused on building a network of partners around the world, and as I mentioned, those partnerships take many forms. We partner with foreign governments; we partner with NGO's; we partner with local civil society groups as well.

With that in mind, the partnerships we currently have, we use a variety of different funding streams in order to make sure that these groups are empowered and armed with the right tools and resources to get these messages out. For example, if I may, we have a foreign government partnership called the "Sawab Center." It is a joint message—

Senator MCCASKILL. UAE.

Ms. LAGRAFFE. Exactly, and that is a partnership where we have provided technical assistance and staff so that the government can then provide their own content and their own messaging across nearly two dozen countries in the region. That is one example.

Senator MCCASKILL. That is a government. But aren't we also partnering with private groups and NGO's?

Ms. LAGRAFFE. We absolutely do.

Senator MCCASKILL. How do we get them money?

Ms. LAGRAFFE. I think one of the benefits of having the Global Engagement Center as an interagency group, we work very closely with not only our colleagues within the State Department but more broadly within the broader interagency to identify funding streams for potential projects and shared priorities. So the Global Engagement Center is not a grantmaking organization. We work very closely with the interagency to identify appropriate funding streams.

Senator MCCASKILL. So the money you are getting is not going to partners?

Ms. LAGRAFFE. Not exclusively. I would like to get you the numbers of how exactly our budget breaks down in terms of what money we give out via contracts. But, again, the Global Engagement Center itself does not offer grants.

Senator MCCASKILL. I understand, but I am trying to figure out how we are funding this, and we cannot get a straight answer.

Ms. LAGRAFFE. OK.

Senator MCCASKILL. Our staff has tried.

Ms. LAGRAFFE. OK.

Senator MCCASKILL. I have watched money go for good causes, and it disappeared. And I am trying to get a handle on how we are actually doing this. I mean, it all sounds great, and I want it to be great. But I also know that if we are not paying attention as to who we are paying and how, that is how money walks away.

Now, the second part of my question is performance metrics. You said you were data driven. Do you have data you can share with us? Have you set up performance metrics for these various groups that we are partnering with on messaging? How are we ever going to figure out if what they are doing is effective? Because it is very hard to quantify what you prevent.

Ms. LAGRAFFE. We are currently building our data analytics shop so that we cannot only do measuring on the front end of any messaging campaign to identify what particular messages might resonate with a particular audience, but also on the back end of any campaign measure our effectiveness. So thus far, what that looks like is making sure we know the potential reach for a particular message and how that message plays out over time.

For each campaign, we sort of build in, we bake in an expectation for analysis on the back end so we can continue to refine our messages each and every time we—

Senator MCCASKILL. Well, I would love to see the data. I would love to see how that data is actually being set up and how it is being collected.

Ms. LAGRAFFE. OK.

Senator MCCASKILL. So there are two assignments: one, how are we funding these efforts, where is the money coming from, who is

getting it, and what form is it taking; and, second, the data that will help us figure out if this money is doing any good.

Ms. LAGRAFFE. Absolutely.

Senator MCCASKILL. Thank you.

Senator PORTMAN. Senator Johnson.

Chairman JOHNSON. Thank you, Mr. Chairman.

Ms. LaGrafte, you talked about the progress we have been making on the ground in Iraq and Syria, 50 percent territory reclaimed in Iraq, 20 percent in Syria. And yet the Central Intelligence Agency (CIA) Director Brennan testified before the Senate Intelligence Committee a couple of weeks ago and said that ISIS remains a formidable, resilient, and largely cohesive enemy and that we have not reduce their terrorist capability and global reach. Do you agree with that assessment?

Ms. LAGRAFFE. Senator, I can only speak from the messaging perspective, and if we are using the number of foreign terrorist fighters as a measure of efficacy of policy, I would say that we see promising signs of having an effect in the messaging space against the enemy in Iraq and Syria.

Chairman JOHNSON. Mr. Steinbach, do you agree with CIA Director Brennan's assessment that we have not reduced their terrorism capability and global reach?

Mr. STEINBACH. I agree with that assessment completely. While we have reduced the space in Syria in Iraq, their reach globally with their affiliates is just as devastating, if not more so.

Chairman JOHNSON. We talk about lone wolves. Now we are starting to see wolf packs, correct? We have witnessed not only the inspiration, these attacks being inspired by ISIS, but now we have evidence of them actually directing, for example, the attack in Brussels and probably in Istanbul. Is that correct?

Mr. STEINBACH. I think ISIL has for some time now focused on an external piece, which includes directed attacks in Europe and in other places, so yes.

Chairman JOHNSON. Do you believe that increased activity in the 22 months since President Obama declared our goal toward ISIS was to degrade and defeat them? That was 22 months ago. Have they increased their ability using social media?

Mr. STEINBACH. So I think from my perspective—and I stated this before—that as we squeeze ISIL in space in Syria and Iraq, they will seek to reach out and lash out where they can. So my perspective is that as we have success on the ground in Syria and Iraq, we may see a more dangerous world in the short term because they will try to message that to their advantage by conducting attacks worldwide.

Chairman JOHNSON. The analogy I have been using is that of a beehive. Let us say you have a beehive of killer bees in your back yard. I think the solution is obvious. You take out the hive, you kill the bees. But what we have been doing is we have been poking it with a stick. We have maybe been damaging the hives, but the problem is we have stirred up the bees, and they are leaving the hive, and they are setting up new hives in Libya, Afghanistan, and other places. Correct? Is that a relatively accurate analogy and assessment?

Mr. STEINBACH. I would say that they are definitely pushing out a campaign to develop more affiliates, like you mentioned, all those places you mentioned—Afghanistan, Indonesia, and other places. They continue to expand globally.

Chairman JOHNSON. So we have not reduced their capability. There was an interesting article in the New York Times last week, a pretty good analysis that said since September 2014, again, the month that President Obama declared our goal to defeat ISIS, there have been 97 ISIS-inspired or—directed attacks outside of Syria and Libya—or Syria and Iraq, over 1,200 innocents killed in those attacks. That is a pretty frightening assessment, is it not?

Mr. STEINBACH. I would agree. Yes, sir.

Chairman JOHNSON. I really have no further questions.

Senator PORTMAN. Thank you, Chairman Johnson.

Senator Carper has left us. Senator Ayotte.

OPENING STATEMENT OF SENATOR AYOTTE

Senator AYOTTE. Thank you, Chairman.

Mr. Steinbach, to the point that Senator Johnson was making, as we look at the metastasizing essentially of ISIS, you see them in Libya, Philippines, Sinai, Somalia, and branching out in other areas. And then you see the pattern of attacks. You see Istanbul, Brussels, Paris, Saudi Arabia, obviously our own country, San Bernardino, Orlando. Aren't they just expanding the battlefield?

Mr. STEINBACH. I think they are expanding the battlefield, but I think they are doing it because of the lack of success they felt in Syria and Iraq. And I think they will continue—if we squeeze them in Syria and Iraq, they will continue to seek other places where ungoverned space or places where they can thrive and conduct attacks.

Senator AYOTTE. And what I wanted to ask you, in terms of the tools that the FBI needs, as we look at the use of social media—and you talked about this a little bit in your testimony—as we look at the use of the Internet, some of the basic tools, I would imagine that in every terrorism investigation now not only in the preventative context of knowing what is happening online, but also, unfortunately, when we have had an event, it is critical that the FBI also has those tools in advance to prevent terrorism attacks and if we have one, God forbid, that you can investigate them. And, recently, on the Senate floor, we had a vote on an amendment offered by Senator McCain which would have given the FBI National Security Letter authority with respect to electronic communications, transactional records, and terrorism investigations. And, unfortunately, that vote failed, as I understand, 58–38.

How important is it that you have that ability to do that? Because having been a prosecutor myself, and was surprised to learn of what I understand was an oversight in leaving this language out of the statute, that we could not even get that passed on the Senate floor, because in your basic online investigation of a child predator, I could get that information as a prosecutor in a criminal case. And right now regarding the FBI, we are making it difficult for you to get it in a terrorism investigation. So how important is it that we give you tools like that?

Mr. STEINBACH. So as you stated, ma'am, I think that the world that we live in today, the threat starts online in many cases. So we need a robust set of tools to focus on the online space. We need open-source tools as well as high-side data sets. We need to lay those over each other to fully identify what we have. Tools like the National Security Letter (NSLs) and the ECTR fix allow us to very agilely identify not only the bad guy but the bad guy's network. Twenty years ago, we had telephones, and you looked at the telephone, you looked at the to-from to see who the bad guy was communicating with. Now, in today's world, with the spread of social media, with the spread of the online threat, we need those tools in the online space to identify who the bad guys are contacting.

Senator AYOTTE. And right now essentially where you are is you can get the telephone records, you can get the financial records, but you cannot get the basic Internet records—which do not involve content, by the way, but that I could get if I were prosecuting a basic criminal case. So I hope we take this back up because I know that this is Director Comey's No. 1 priority, and, this is one where it is kind of hard to believe in the context that we live in that the Senate did not pass this. So I hope we do this again and take it back up and pass it in light of what we are hearing today.

I wanted to also follow-up, as you think about the tools that you need, and looking at what happened recently in Orlando, can you share with us at all in terms of how the Internet played in the terrorism attack that occurred in Orlando and what lessons we have learned in terms of investigative tools that would be helpful in the context of that? And also in San Bernardino? I think one of the challenges we are facing here is we obviously want to engage people online to prevent this, but also have good intelligence up front if an attack is coming to be able to stop it before it happens.

Mr. STEINBACH. So I think the challenge we face today is that we start in a place where people are passively consuming content, which, of course, is not against the law. So our challenges, as I mentioned in my opening comments, is to look through the volume of individuals who are online consuming, passively consuming this material, and look for those individuals who are doing more than just passively consuming that online content who have expressed an intent to do harm.

So when we go through this volume, we have to have tools that help us identify trends, patterns, so that we can then lay over our deeper-dive analytics to reach into those particular cases, to figure out what the noise is and what the signals are, to identify the subjects away from just people exercising their constitutional right to consume and repost material. That is the challenge we are in, and the tools we have are a set of tools that will need to be continually expanding as technology changes. We need to, on a regular basis, reassess exactly what tools we have, both in open source and on the high side, and make sure they are robust enough to address the threat.

Senator AYOTTE. My time is up, but just to be clear, the individual in Orlando was consuming this type of information, as I understand it.

Mr. STEINBACH. The individual in Orlando was consuming material, yes.

Senator PORTMAN. Senator Lankford.

OPENING STATEMENT OF SENATOR LANKFORD

Senator LANKFORD. Thank you, Mr. Chairman.

Ms. LaGrafte, can I pick up where Senator McCaskill left off on this? It is extremely important to us to get some kind of data analytics, the metrics for how the different outside sites are evaluated, and we are all for trying to get multiple hooks in the water to be able to help other people, help us with our messaging and to make it clear. Trying to determine where those dollars go and how they are being well spent by the taxpayer is extremely important.

With that, you had mentioned a lot about outside sources and mentioned a lot about—I am sorry, a little bit about some of the things the State Department is doing specifically. I want to ask you about how you are evaluating the “Think Again Turn Away” Twitter page and some of those internal sites that the State Department is running, compare that to some of the outside—because my understanding that “Think Again Turn Away” site is about a \$5 million investment to be able to do that Twitter page. So help me understand value in metrics and evaluation.

Ms. LAGRAFFE. “Think Again Turn Away” was a product that was produced by our predecessor organization. We no longer use “Think Again Turn Away.” As I mentioned in my opening statement—

Senator LANKFORD. Why? Because that had to be a metric-driven piece, too, that helps us understand how things were evaluated.

Ms. LAGRAFFE. As I mentioned in my opening statement, when the CSCC, our predecessor organization, was stood up, it was designed to fight a different enemy in a different time. We as the Global Engagement Center (GEC) are now fighting a more agile enemy, Daesh, in a social media space. So we have moved away from some of the direct online engagement of our predecessor organization.

I think that that is a reflection of the kind of analysis we are trying to build into our organization. Inevitably, there will be things that we do not do well and we want to adjust, be agile, move on, and get better.

Senator LANKFORD. So tell me the process of how you evaluated, for instance, that site, other sites, things that were internal, to make the decision we are going to turn this off and not do this, we are going to turn in a different direction? Tell me about the process of how that decision is made.

Ms. LAGRAFFE. For the Global Engagement Center, when we are preparing our proposed messaging, as I mentioned, we do analytics on the front end to assess the target audience susceptibility as well as doing analytics on the back end of every campaign to see the reach and resonance of what we are doing.

Senator LANKFORD. That will help us. We want to get a look at some of those analytics and see how things are evaluated so we can also participate just in that conversation, just as good stewards with it.

Mr. Steinbach, good to see you again. Thank you for all your work. Thank you for all of your work in this area, by the way.

Mr. Steinbach, I want to just run back through the past 5 days and some of the things that are happening internationally and here in the United States, because social media played a part in all of these, or at least had some connection with an ISIS threat.

In Indonesia, in the last 24 hours, in Saudi Arabia, 48 hours ago, three different, separate attacks there. In Iraq, 250 people dead in one attack in Baghdad. In Bangladesh, 20 people at least that we know of that are dead. And then, on Friday, something that I know you did not miss but a lot of Americans missed, the FBI picked up a gentleman names Mohamed Jalloh, and he was a person plotting an attack similar to a Fort Hood attack here in the United States that seems to be self-radicalized online by watching videos of Anwar al-Awlaki. That could have been a very different day for America, Friday, but the FBI was engaged.

What can we learn just about the engagement of that particular or things like what happened with Mohamed Jalloh and ways that social media or outside sources help influence him?

Mr. STEINBACH. Thank you, sir. So as I mentioned in my opening remarks, in general, we have three types of attacks—or three types of plots: directed, enabled, and inspired. And, of course, the largest threat to the United States is that HVE subset, the group that is inspired or enabled to conduct an attack and that are, quite frankly, the hardest because they are not communicating. So as Director Comey has spoken in the past, we have roughly 1,000 of these HVE cases across the country. They are difficult at times, and we need to use social media to the extent possible. As was mentioned, the majority of our cases last year, the arrest, all had significant aspects in social media. Many of the cases began with an anonymous online moniker, and so we need to understand that that is the dynamic of the world we live in.

So as we focus on the HVE threat, we need to focus on the online space so that we can properly identify and predicate investigations and then use all the tools that we are afforded, all the tools in our tool chest to quickly act on individuals who have the intent and stop them before they obtain that capability to conduct an attack.

Senator LANKFORD. So a way to be able to guess at this point for the FBI, cases like Mohamed Jalloh, that have happened in the past year where the FBI learns about this individual, self-radicalized online, preparing to actually carry out an attack, and then there is an engagement by the FBI.

Mr. STEINBACH. So I think the most concerning trend that we have seen in the past year when we identify these individuals online is the speed with which they mobilize. So that flash-to-bang effect you have heard us talk about is going now in days, even weeks, as opposed to months and years. That for us is a very concerning fact. We have to quickly identify and work to mitigate the threat faster than we had to do even 2 years ago.

Senator LANKFORD. Thank you.

Senator PORTMAN. Thank you, Senator Lankford.

We have a vote that has been called, and so we have a short amount of time. We are going to try to get three people in here quickly. We have Senator Carper and then Senator Heitkamp and then Senator Baldwin. And if any member wants to run over and

vote and come back, we will keep this going. Otherwise, we will recess briefly, have the votes, and come back. Senator Carper.

Senator CARPER. Let me yield to the other Senators. Thanks.

Senator PORTMAN. Senator Heitkamp.

OPENING STATEMENT OF SENATOR HEITKAMP

Senator HEITKAMP. Thank you. Thank you, Mr. Chairman, and thank you, Mr. Chairman.

Two issues, and I want to thank you for coming over to my office, Mr. Selim, and briefing us on the kinds of efforts that we can engage in locally, with local law enforcement, with local communities, the need to have—what I would call it—a “force multiplier.” There are not enough of you to actually be out there when we are talking about volume. Obviously, encryption is a unique issue, but certainly we can do more to multiply the force. And I think the other piece of this is best practices, what I would call a “best practice kind of model.” When we did training on school shootings when I was Attorney General (AG), we did trainings and did major initiatives on fighting methamphetamines. We are in the process now on opioids. We need to have the ability to, No. 1, say these are tactics and strategies that work, this is what we are going to request of and engage with local law enforcement and local communities, faith-based communities. We talked a little bit about the information that we know of in Canada and how Canada engages in anti-radicalization kinds of efforts.

And so, No. 1, what are we doing, George, in terms of multiplying the force by working with local law enforcement, working with local communities? And what message should we all take back to our hometowns, to our law enforcement communities, in terms of what role DHS is going to play?

Mr. SELIM. Senator, thank you for those questions, and I appreciate you and your staff making time to really get engaged on these issues and understand the message that we are trying to communicate and taking that back to your constituents as well.

Your first question in terms of multiplying the efforts, two immediate thoughts. The business model of the Office for Community Partnerships at DHS is to supply products and services to a range of stakeholders across the country. Our three major sets of stakeholders are: State and local law enforcement, first responders, homeland security professionals across the country. Our second major set of stakeholders is municipal officials—mayors, county council members, people in elected or appointed local positions, whether they be security or not security related. And the third real set of constituents we have is civic leaders, civil organizations, not-for-profit organizations and so on.

So in terms of getting out the message for the products and services DHS is offering and further taking advantage of the grant opportunity that we announced today to multiply and expand efforts across the country at this, our ultimate goal here is to create a much broader prevention framework in cities and municipalities—

Senator HEITKAMP. My concern is that you can give people tools, but if they do not see how they fit into a broader strategy of anti-radicalization, it may be difficult for them to utilize those tools. But

I think the more that we get out there with grants, the more we work with communities, the more we will establish a pattern of best practices, which I think is the kind of critical development that we need here, and it really is incumbent, I think, on a community policing model where you really look at the entire community. Obviously, tensions in communities can lead to stress and can lead to bad outcomes. And so how do we avoid polarization which could lead to isolation which could lead to radicalization? How do we avoid that? And what are you looking for—in 2 years, what do you hope you have learned from all of the grants and all of the resources that you have provided?

Mr. SELIM. Senator, fundamental to the work of countering or preventing violent extremism in the homeland is community inclusiveness and those types of interpersonal relationships that you are referring to. That is foundational in this business. The ability for individuals who sense someone's behavior may be changing, there might be something they are concerned about, having the ability to say something to someone if they do not trust law enforcement to do so, having the right mental health, social service, and education providers to do so.

At the end of the next 2 years, for example, the impact that we are trying to develop is creating a more integrated approach in cities and municipalities across the country where not just a community policing model exists but a more integrated approach of mental health, social service, and education providers are part of this prevention framework.

Senator HEITKAMP. Thank you so much. I look forward to hearing more about the grant applications and understanding more what the overall strategy is.

Senator PORTMAN. Senator Baldwin.

OPENING STATEMENT OF SENATOR BALDWIN

Senator BALDWIN. Thank you, Mr. Chairman.

We often do not hear about the good news or the encouraging news, but earlier this year, Mr. Steinbach, the FBI prevented a terrorist attack in my home State of Wisconsin. It reached the newspapers that a 23-year-old man had a vicious plan to kill at least 30 people at a Masonic temple in downtown Milwaukee.

In my conversations with the FBI, officials indicated that fusion centers and FBI databases, such as eGuardian, which allow law enforcement to share intelligence were particularly useful. I know that FBI Joint Terrorism Task Forces can be critical in sharing time-sensitive information, gathering evidence, and making arrests.

So I want to hear from you about how we can expand and support these sort of law enforcement-coordinated efforts while also ensuring privacy protections and how we can better utilize coordination tools such as fusion centers and FBI databases to continue to prevent attacks like the one that was thwarted in my home State?

Mr. STEINBACH. Yes, ma'am, thank you. So I think it begins with all of those tools. The threat is changing. It is dynamic, and it is much faster. So it is not just—as I mentioned in my opening remarks, it is not just sharing information. It is how quickly—the speed of information sharing. So having fusion centers and Joint

Terrorism Task Forces with multiple agency participation in them, active participation, as the information or the intelligence comes in, whether it is through eGuardian, through a tip, through foreign partners, when we get that information, we very quickly assess it using databases to identify the totality of what we know and then quickly act and use all of the tools that we are allowed to use, understanding that the individual's right to privacy is paramount to how we do things.

So we quickly assess the information with our partners, State and local. As you know, State and local are force multipliers for us, and we quickly act within the limits of our authority to mitigate that. And the case that you refer to was an example of that that we try to replicate over and over again.

Senator BALDWIN. And then, quickly—I know our time is running out—thank you, Mr. Selim, for being here. And if you covered this before I arrived, I apologize for the repetition, but, obviously, as a part of this effort that you lead, it is critical that no group is targeted or discriminated against on the basis of religion or national origin. And it is also important that CVE grants are not used to perpetuate the alienation of any group or population.

And so what I want to hear from you is, if you could speak to any specific training that your staff receives, civil liberty training that your office receives, and also oversight mechanisms that will be in place after the grants are awarded.

Mr. SELIM. Thank you, Senator, for that question. It is really important to underscore the civil rights, civil liberties, and privacy protections that are in place on all CVE initiatives across government domestically.

The first point I would add is of my 10 years at DHS, 6 of those years were spent worked in the Office for Civil Rights and Civil Liberties, so I appreciate the spirit of your question.

On the CVE grants question, we have built into the Notice of Funding which was released this morning a comprehensive scoring and evaluation that we have for any potential applicant who applies for those grants that has to demonstrate, the intent of what the money will go towards, partnerships that have been developed, and a whole range of options. If we see any applications submitted that are in any way, infringing on an individual's or group's civil rights, civil liberties, or privacy, we are not even going to score those applications.

Within the Department, part of the evaluation of those applications, the Office for Civil Rights and Civil Liberties provides outstanding oversight to my office on all our programs, and they are partners with us on the oversight of this grant initiative as well. So that is built in and baked into everything we do.

And the last point I would mention, Senator, is that the programs that we are administering, whether they are grants or initiatives we take in other places in the country, are completely voluntary. We are being responsive to community requests for CVE-related programming. And it may not be termed "CVE." It might be "building or enhancing community resilience" or "preventing extremism" or some other title. And so our job is to supply the product services or technical assistance irrespective of what a locality might call it, but be responsive to their needs, and we are not im-

posing a DHS model per se. We are responding and helping customize localized approaches.

Senator PORTMAN. Mr. Selim, thank you for that answer.

We are going to now recess subject to the call of the Chair. I apologize. Again, I ask the indulgence of the panel if you would not mind hanging around for a little while longer. I am going to be playing tag team with Senator McCaskill as we run back and forth and vote. But we do have some additional questions for you that I was not able to ask earlier in order to allow some of my colleagues to ask questions.

So we will now recess subject to the call of the Chair, and we will be right back.

[Recess.]

The hearing will come to order. Again, I appreciate the indulgence of our two—now three distinguished witnesses who have come back to the table. I do not know if I am going to be joined by any of my colleagues because we have another at least two votes coming up. I am going to run back and forth. I will let you all go after my questions, of course, and then we will take another recess and ask the second panel if they would be willing to stick around, because I know Senator McCaskill is coming back, and I assume some of my colleagues are as well. But I thought we got into a lot of good back-and-forth with the previous questions that were asked, and, again, going back to how we started, Mr. Steinbach talked about the fact that he agrees with the assessment from last year, which is that the lone-wolf terrorist radicalized online is the main threat facing the United States. And we talked a lot about the two programs that are represented here today: one is the new program at the Department of Homeland Security called the “Global Engagement Center”—I am sorry, the “Office of Community Partnership,” and then, of course, the State Department’s Global Engagement Center. So what I would like to focus on a little bit is whether you feel you have the authorities you need to be able to do your job right.

On the domestic side, Mr. Selim, you are not as aggressive as they are on the global side, in part because of some legal challenges that you face. They can do and say some things that you cannot. You also have not had the amount of time they have had to put together your digital effort. I think that is fair to say. By the same token, I think it is clear, including from some of the back-and-forth you had with some of my colleagues, that there is an enormous opportunity here domestically to be able to develop a message that is more compelling than the ones we currently have out there. We talked earlier about some of the messages coming from the jihadists, and, in fact, we had some photographs here earlier of sort of a romanticized version of jihad.

And so I guess my first question to you would be: Are you happy with the progress that the Department has made, particularly on the digital counterterrorism communications front? And, specifically, how many online campaigns has DHS, particularly your office, devised or funded or launched, even through third parties, over the past year? What is the scale and composition of the audiences you have reached? How do you measure your results? Do you feel as though on the domestic side we are beginning to catch up?

Mr. SELIM. Thank you, Mr. Chairman, for your question. In terms of the first point you made regarding the authorities that we have, we have looked at this issue. Our current posture in the programs that we are implementing, we do not see any immediate impediments in terms of regulations or authorities for promoting and really taking to scale the programs that we have just started. The program—

Senator PORTMAN. Let me interrupt you there just for a second. I was going to get into this further with regard to the Global Engagement Center, but one of the things that, of course, this Committee is interested in is to ensure that you have the authority to be able to be an effective interagency leader, and that requires you to be able to direct and task people. We talked earlier about the FBI's role in this, which is a law enforcement role, but obviously, there is some interaction between your role as the communications person in the law enforcement side.

Do you feel specifically that you have the tasking authority you need to be able to be an effective interagency leader?

Mr. SELIM. As of today, I can say that I do. I have been fully empowered by the Secretary and in my role as the Director of the CVE Task Force. Deputies across departments and agencies, including the FBI, the Department of Justice, the National Counterterrorism Center, and a range of other agencies came together to affirm this body come together and help coordinate and synchronize our domestic CVE efforts. So I feel like I do have those authorities, sir.

Senator PORTMAN. Good. Well, that is something that certainly was the intent of this Committee to support you in that, to be able to have that tasking authority, which, frankly, your predecessor organization I am not sure felt like they had in terms of that interagency cooperation. So if you do not mind, go ahead and I will let you answer the question about the digital communications efforts, the campaigns.

Mr. SELIM. Yes. In terms of the campaigns that we have initiated, the methodology that we are currently implementing is not for the Department or Department personnel to issue or to create campaigns and then implement them via social media or some other means. We are really utilizing the methodology behind prizes, challenges, competitions, and engaging young people and Millennials on these issues. So the effort that I mentioned in my beginning statement and in my written statement, the Peer-2-Peer Challenge Extremism competition, what we have done is essentially we have created a 15-week academic curriculum for college and university students both in the United States and across the globe to, in a 15-week academic semester, identify a target audience for challenging extremism, create a campaign, implement the campaign, and measure the effectiveness of that campaign on a 15-week academic semester.

Mr. Chairman, you asked for some statistics. Roughly, to date we have run this program for about three academic semesters with approximately 150 colleges and universities across the globe. This coming fall, we are interested in scaling that effort significantly with up to 200 colleges and universities across the globe. And our metrics for assessment are on an individual university-based pro-

gram and then on an aggregate, the level of impressions and influence that each of those campaigns are having.

To date, of the programs that we have implemented, we have anywhere between 30,000 and a million social media impressions and campaigns that have made micro impressions on various social media platforms that have attempted to counter or negate the message of ISIL in terms of recruitment and radicalization. I think this is one of the initiatives that we can take to scale significantly in the semesters to come, and the program has the flexibility to allow us to scale or tweak or adjust our measurements, our assessments, and the number of universities we are implementing on a semester-by-semester basis.

Senator PORTMAN. On the composition of the audience, what kind of metrics do you have and what kind of information do you have to share with us today? In other words, who are you reaching?

Mr. SELIM. So there are several different criteria of audiences, audience criteria that we are assessing. At-risk individuals on the fence are those that can be amplifiers of positive or alternative narratives. And each of the campaigns that is initiated is required to assess how to best target or communicate with that audience and then implement the campaign to effectively do so.

Senator PORTMAN. Do you have metrics?

Mr. SELIM. We do. Again, on a university-by-university assessment we do, and then as an aggregate we do overall.

Senator PORTMAN. But not in terms of the audiences that are being reached, the composition of the audiences who you are reaching?

Mr. SELIM. We do, and I will share with you one set of data and analytics as an anecdote. Just a few weeks ago, at the State Department we launched the completion of our third successful semester of this competition. One of the finalist universities from the United States was the Rochester Institute of Technology from New York. They had one specific statistic that was worth mentioning. Prior to the implementation of their campaign, roughly 87 percent of respondents of a 300-person survey they conducted associated Islam with terrorism and had a negative interpretation of the religion or of Muslims writ large.

After the implementation of their campaign, 97 percent or 98 percent of the respondents of that same survey understood the distinction between Islam, Muslims, and terrorism and had a positive or favorable view in terms of both the Middle East, American Muslims, and American Arabs and felt the need to be compelled to do proactive work with their communities in terms of reaching out to Arab, Muslim, and South Asian communities.

Senator PORTMAN. Well, again, I think we are catching up. The jihadists we talked about earlier have been at this really for 3 years, I would say it is fair to say. It has been an evolution but in a very sophisticated way online. You talked about three semesters. That is good that we have gotten started, but we have a lot to catch up on. And I think having this data on the composition is important. It is important that we are distinguishing between the Muslim community and the terrorist community, as you just said. It is also important, though, we are meeting some of these vulnerable people online where they live and communicating that mes-

sage. And I guess that would be what I and I think the Committee would be very interested in, is to know how can we come up with a better metric to judge that. Every marketing department in practically every company in the United States, certainly every online company, is focused on this. How do you reach your audience? And that is certainly something that—Peer-2-Peer is a good start in my view. I support it. But I think it needs to be even broader than that and we need to have better data coming back.

I would say, Mr. Steinbach, as a general matter, it seems to me there is both a public and an encrypted part of this communication strategy on the public part, as I understand, and you correct me. There is a wide net being cast by the jihadists who are online to create this sense of interest or excitement in the jihad or the mission, and that is very public. And we see it, you see it. Mr. Selim, your people see it. That is what you are countering, I hope, with these messages, is telling the truth, dealing with the disinformation.

Then there becomes, once those people make contact, I assume that is when what you talked about earlier occurs, which is the encrypted part of the communication, which is more challenging. Is that an accurate assessment of what is going on?

Mr. STEINBACH. I think that is a very simple but accurate model. We see the volume piece, the initial piece, public information pushed out through a variety of means of social media, the hundreds and hundreds of companies casting a wide net, trying to identify individuals who are like-minded, who are willing to act, who are willing to travel. And then once they identify somebody who raises their hand and says yes, then the conversation switches to mobile messaging apps that are encrypted so that there is complete secrecy.

Senator PORTMAN. And this is the challenge you talked about earlier and Director Comey has talked about in this Committee publicly, is how do we deal with that second stage. Is there anything you can tell us today about any attempts that you are making to be able to break through on that second tier? And what is the way in which we can intervene there as well?

Mr. STEINBACH. So I think it is important to understand that the FBI looks at this as an important issue for the American public to vigorously discuss, and that really is privacy versus national security, encryption versus national security. I think all of us as citizens, myself included, want strong encryption. But we need to continue to have conversations about where the limits of that are, and we would argue that strong encryption, although important, must be balanced with national security interests so that when a judge or a magistrate provides authority, we have the ability, law enforcement has the ability to see those unencrypted communications or have access to that. We feel that is an appropriate balance.

Ultimately, it is a decision for the American public through Congress, but that for us is fundamental. We see today more and more of our bad actors using encrypted communications in a variety of ways. Without the ability to see those encrypted communications, we are dark, we are blind as to their operational intent. So we try to identify workarounds, but those are few and far between.

Senator PORTMAN. Well, I appreciate that, and that is not really the topic so much of this conversation. And, in fact, a lot of that is better, I guess, undertaken in a classified setting. But the reality is that the funnel starts in a more broad and public way, and to keep people from going into that funnel, I would say the funnel of darkness, we have an opportunity on the public side. And I think that is where Mr. Selim and Ms. LaGrafte have an opportunity of working with you to try to avoid so many people going into that place where it is much more difficult for you to be able to understand what their communications are.

Are there any models, to you, Mr. Steinbach, or you, Mr. Selim, that you look at globally that you think are working better in terms of dealing with this challenge of online recruitment and online propaganda and disinformation?

Mr. SELIM. I would say as we think about countering violent extremism domestically, it needs to be a blend of both online and offline programs. While the radicalization and recruitment can start online, what we have seen and what the data has shown us are primarily from closed and processed FBI investigations is that individuals around someone who is being radicalized—friends, neighbors, peers, associates—see some type of behavior that may be out of place, but do not report it for one reason or another.

So to the extent that radicalization and recruitment starts online, it can end offline, like we have seen tragically happen in several American cities. And so we are really working diligently toward an integrated approach where there are countermessages online and there is a prevention framework offline as well. And it is really that combination that we are working toward.

Senator PORTMAN. And I assume a prevention framework online as well.

Mr. SELIM. Correct.

Senator PORTMAN. In other words, part of the audience we talked about earlier is the vulnerable potential jihadists, but it is also to the friend and the co-worker and the neighbor.

Mr. SELIM. Correct.

Senator PORTMAN. And the family member, and San Bernardino being perhaps the most recent tragic example of that, where there are people who after the fact said, "Something seemed strange, but I felt that I was constrained, I could not report it," for some reason. And that is part of your effort, I assume.

Mr. SELIM. It is to raise awareness. The three primary—

Senator PORTMAN. And you empower people to step forward.

Mr. SELIM. Exactly. The three primary objectives of our office are: No. 1, really raise awareness as to the nature and scope of threat of radicalization and recruitment, online and offline, and we have discovered, dozens of cases where community-based groups are not aware to the extent that radicalization is happening online. We need them to come in and provide tools and resources to those communities and help develop and sustain long-term partnerships for them, whether they be with Federal, State, and local law enforcement or other trusted community institutions—mental health, social service, and education providers.

Senator PORTMAN. When I was looking for a model, I was hoping you would talk about the British Research Information and Com-

munications Unit (RICU), which has gotten some good plaudits internationally for being very aggressive in pumping out messaging, being very aggressive online, using third parties, as you are now doing with Peer-2-Peer. They use traditional media as well as social media, as you know.

I think we have some legal constraints the British do not have in this regard, so we cannot do exactly what they are doing. But what do you know about what they are up to? And why have they been successful and what can we learn from them? For either one of you.

Mr. STEINBACH. I am not familiar with that, sir.

Senator PORTMAN. OK. George?

Mr. SELIM. I am pretty familiar with the British model on this. I was recently there would Deputy Secretary Mayorkas, General Taylor, and a senior leadership team from DHS. They provided a deep dive in terms of their program, their analytics and so on. Senator, as you pointed out, their legal structure affords them a number of different flexibilities that we do not have here in the homeland, and from my perspective as the Director of the CVE Task Force, it is important to have a comparative understanding of what is happening not just in the U.K. but in Germany, France, other Western European and, frankly, other coalition countries outside of Europe. The RICU model is an interesting model. They have some interesting data and analytics that has proven effective so far. And it is important that both the U.S., the U.K., and other partner countries keep in close contact with not just best practices but really promising practices that are showing effectiveness.

Senator PORTMAN. This brings us really to the global effort, and, again, if you do not mind providing more information to us as to what you think we can learn from them and with regard to the legal constraints, just to be sure we are all on the same page, we understand what constraints you feel you might have. I know you also likely are going to tell us today that you have some resource constraints. You would not be doing your job if you did not. And, that is another issue that I think maybe the British have put a greater emphasis on this in terms of their resource allocation, as I understand it, within their budget.

But on the global side—I do not want to leave Ms. LaGrafte out of this conversation—do you think that the Global Engagement Center, which is also aimed at changing attitudes over the long term, is adequately using the data analytics tools we talked about here to focus on those who are most vulnerable to radicalization? And to the extent you can, can you give us one or two examples of where the Center has done that kind of micro targeting?

Ms. LAGRAFFE. Thank you, Senator. To answer your first question, the data analytics shop within the Global Engagement Center, as you know, is in its sort of early stages, and we are working very closely with the State Department Office of the Legal Adviser to make sure the analytics tools we identify to be potentially most appropriate for our organization are in keeping with the regulations specifically related to the Privacy Act.

Thus far, what that has looked like in practice is that we have identified tools that give us access to aggregate data, so we are able to see in near-realtime trends on social media platforms to really

assess what messages and what themes are resonating most with potential target audiences.

Senator PORTMAN. Yes, I think it would be good, to the extent you are able, to explain what you are talking about to the Committee today. You are talking about the Privacy Act, I assume.

Ms. LAGRAFFE. Yes.

Senator PORTMAN. Which you mentioned the Office of Legal Adviser at the State Department giving you advice on this. My understanding is that the Privacy Act prevents the government from collecting certain information about Americans or lawful permanent residents but not about foreigners. Is that accurate?

Ms. LAGRAFFE. I am not an attorney. I think the way you characterized it is accurate. My understanding of the challenge we face at the Global Engagement Center is, as you have said, we are not a law enforcement agency, nor are we an intelligence agency and, therefore, have restrictions related to the Privacy Act. These restrictions mostly focus around what is called “user-level data,” so we have worked, as I mentioned, closely with the legal adviser’s office to determine what tools we need to get aggregate-level data, but the user-level analysis is something that we as the Global Engagement Center do not have authority to access.

Senator PORTMAN. I think we should have further discussion of this because I think it is in all of our interest that you do micro target. Again, as I mentioned, every company in the United States practically, as well as those online companies, are doing this—and wouldn’t it be ironic if our own State Department is not able to do that to fight terrorism?—to be able to understand who the people are who are most vulnerable to these potential disinformation campaigns and then provide them the countermessaging.

So I am concerned about the way in which the State Department has interpreted the act. I think what they would say—and, I am a recovering lawyer so I have to be careful here, and did work at one point during law school at the legal adviser’s office. But I think what they are saying is that it could inadvertently collect information about Americans. So it is not that you are unable to collect information about foreigners or, again, this vulnerable overseas group we are talking about. It is that apparently they think that there could be information collected about Americans inadvertently. Is that your understanding?

Ms. LAGRAFFE. It is.

Senator PORTMAN. OK. What are you losing by not being able to do that kind of micro targeting?

Ms. LAGRAFFE. I do not think we as an organization have yet fully fleshed out what missed opportunities there may be in either lack of analysis in this realm or any other. Frankly, it is so early days for the Global Engagement Center—we have been up and running for just a few months—that we are focused more on what opportunities we can identify to actually start having a result in the aggregate.

Senator PORTMAN. Well, again, I think we are in a crisis mode in the sense that, as Mr. Steinbach has talked about today, this online messaging is a huge part of the radicalization effort, and certainly this relates both to domestic and overseas. So I would want to be sure that, as hard as your task is, it is not made harder by

constraints that keep us from targeting the very population that is most vulnerable or more predisposed to accepting the disinformation and the message from the jihadists.

So I would just say, as one member of the Committee, I would like to follow-up on that further with you all and to get some information about how the State Department is interpreting the privacy rule as it relates to foreigners and what that keeps us from doing in terms of being able to target these groups.

Senator McCaskill has now returned, so I am going to turn to her for her questions. And, again, we are going to sort of tag team here. I may not have the opportunity to speak to the three of you again, so thank you very much for your service to our country. And I know each of you has a distinguished background of service in various law enforcement and State Department and now communications areas, and we need you very badly right now to be able to have an effective countermesssage out there. I think it is as important as anything else that is being done, and everything else, as I said at the outset of the hearing, can be done successfully, the military side, protecting the homeland in other ways, and still, if we do not deal with this threat of the disinformation online and the radicalization that is going on, we will not be successful. So we thank you for your hard work and for your willingness to continue to work harder to do even better to redouble our efforts to be more successful. Senator McCaskill.

[Pause.]

Senator MCCASKILL. Sorry. We are trying to figure out how we can vote and do this hearing at the same time.

Senator PORTMAN. Call the second panel whenever you want.

Senator MCCASKILL [Presiding.] OK. A couple of things.

Mr. Steinbach, I was the elected DA in Kansas City in the 1990s, and we had an awful lot of work that the Justice Department did through the Bureau of Justice Assistance (BJA) and other parts of Justice about gangs and how did we stop somebody from being radicalized into a group that was intent on violence. And there were millions and millions and millions of dollars spent on how we gain cooperation of the community, how we identify young men—and sometimes young women but primarily young men—from entering gangs.

I am reading a lot of things in preparation for this hearing, and so much of it began to take on a ring of familiarity. And I am wondering to what extent have we taken out the volumes of research and work that were done in terms of accessing communities, getting the help of communities, identifying someone who is being radicalized to a life of violence. The only clear difference I see here is that obviously this is being clothed in a false costume of religion, and it is convincing people that they should die for this, although the young gang members at the time would say, they were proud of going—I do not know if you remember. You probably do remember this. You were probably working as an agent at that point. I am guessing. Were you or are you too young to have worked as an agent in the 1990s?

Mr. STEINBACH. No. I was an agent.

Senator MCCASKILL. OK. So you know that one of the saddest things that law enforcement encountered were some of these young

men that were 12 and 13 years old going with their first pile of cash to buy caskets and to plan their funerals. So they were anticipating their death.

Has there been any work—I mean, Homeland Security was not around then, but has there been any work at Justice to try to pull off some of the strategies that proved to be effective in fighting the gang wars of the 1990s as it applies to radical extremism that we are working with now?

Mr. STEINBACH. Yes, ma'am. I think you are right on. I think at the core, the reasons for disaffected youth joining something they can belong to, whether it is a gang or radical Islam, there is something to that. So in partnership with all these agencies at the table, we look to the communities to answer our questions. So just as we used the communities and developed trust within the neighborhoods, we do the same thing with the communities of interest now. We work with the communities, focusing our efforts, empowering them to identify—because once an individual comes to the FBI's attention and we have predicated an investigation, it is too far down the road. It is gone. It is too late. We need to identify those individuals as they start down that path of radicalization, and the key to that, quite frankly, is in the communities. The only difference between the 1990s and today is the online space and working within the online arena, which is where I think George's efforts are focusing on.

Senator MCCASKILL. And have we looked at—I mean, I know that we are talking about calling in psychologists and psychiatrists and paying money to contractors. I mean, what I am really wanting to make sure is we are not reinventing a wheel that we have already spent a lot of taxpayer dollars researching since the problems are so similar. Is anybody pulling out any of the work that was done by professionals? Are any of you familiar with any of that work that was done by professionals back when we were dealing with extremism in the form of gangs?

Mr. SELIM. Senator, if I may, we are indeed very familiar with a great body of that work, which is the wealth of information that the Justice Department as our partners and the Executive Office of U.S. Attorneys, many of whom have been prosecutors at the State, local, and now at the Federal level for the past several decades, bring to bear in this regard. I think when we are thinking about prevention models, whether it be gang prevention, we have looked at the model of the National Center for Missing and Exploited Children (NCMEC), how does that public-private partnership with law enforcement and NGO work, how do you prevent whether it is human trafficking and smuggling, prevent recruitment and radicalization to transnational gangs and other models like that, we have definitely pulled heavily from that body, and that has helped inform the models that we apply today.

Senator MCCASKILL. Mr. Steinbach, I know that you all are engaging in the Muslim community in the United States. Can you give us anything in this setting as to what percentage of the leads that you all work actually are generated by Muslims who are concerned about someone at their mosque or someone in their community that they believe might be subjected to some kind of radicalization of their faith?

Mr. STEINBACH. Yes, ma'am, and the answer is no, I do not have those numbers with me. And part of the problem is when incoming tips come in, we are not cataloguing them by the type of person that provides it. But I will say that every field office commander through all 56 field offices of the FBI works closely in partnership with the communities of interest, with the mosques, the churches, the temples, and develops strong relationships for a number of reasons. They recognize, those field office commanders, that the leaders of those communities do not want that bad apple, those bad apples affecting their children or impacting in a negative way their areas of worship, their places of worship, their communities. And so there is quite a bit of communication back and forth at the foundational level in the communities. I could not give you a number on the number of tips. I will say that we get a lot of information and assistance from those communities, however.

Senator MCCASKILL. Is it your sense from talking to your SACs that are out there in the field and that are working with these communities, do you sense a frustration with them that these communities are failing to cooperate? What is your overall impression about the willingness of the Muslim community in the United States to try to be helpful as opposed to the way they are sometimes categorized in the media or by other politicians?

Mr. STEINBACH. I would say overwhelmingly the religious communities across the United States are very helpful to us in identifying sources of radicalization, whether that is Islam, Christianity, Judaism. We could not do our job without them. So I would not characterize it as an adversarial relationship or a negative relationship at all. It is a very positive relationship.

Senator MCCASKILL. I am usually here preaching about interagency cooperation, and now I am going to ask a question that I did not really anticipate that I would ever be asking. But we now have the National Counterterrorism Center, the DHS-led Interagency Task Force, and the Global Engagement Center, and there are probably a few others. Now we are in danger of the interagency groups not coordinating with other interagency groups because we have a plethora of interagency groups.

Can any of you speak to any sense you have of how well we are cooperating with these various interagency groups that are all ostensibly driving towards the same purpose?

Mr. SELIM. I will start, and I will ask my co-panelists to join in. From where I sit at the Director of this Task Force, what we have done by creating the Global Engagement Center, the CVE Task Force, and other models across the Federal Government, including the National Counterterrorism Center, we have really honed in and specialized in what the key tasks and objectives are. So the National Counterterrorism Center is a part of the intelligence community, and they cannot play the same role that a DHS or a Justice Department official has due to their authorities and regulations and so on.

In terms of cooperation with my colleagues at the State Department on the Global Engagement Center, the Department of Homeland Security has a full-time detailee at the Global Engagement Center, again, a very discrete mission set different from ours, and we meet regularly. If not several times a month, every few weeks

we get together, our leadership gets together to figure out how we can better coordinate or integrate our efforts abroad and domestically.

And so I think what you have identified, Senator, is a number of interagency bodies that have been really honed in on a specific set of tasks rather than aggregated overall to a department or agency's mission.

Senator McCASKILL. It would be really helpful, to the extent that you can in a nonclassified setting, not for testimony today but if somebody would put on paper how you would diagram this in terms of responsibilities. The thing I am most concerned about is being sure who is accountable for a situation. That is the other thing that happens sometimes when you have more than one group in charge. I have seen it. I will not give specific examples, but I could, bunches of them. If you just look at contracting in Iraq, it was a big old quagmire of a mess between United States Agency for International Development (USAID) and the Comprehensive Everglades Restoration Plan (CERP) funds and, there were just a lot of things that there was not really—it was not clear who was watching all the money.

And so I would love a diagram as to what are the different responsibilities between these different interagency task forces and who is reporting to whom and who is ultimately accountable—besides the President, who obviously is ultimately accountable.

I am sure I will have other questions for the record.

I really appreciate all of your work, your dedication. I like to remind people that are so cynical about their government, I have not met any of you types that came into this line of work for money. And, frankly, for the vast majority of you and your colleagues, it is not for glory either. So it is a sense of purpose and a sense of serving the public and a sense of accomplishment. So please convey to all of your colleagues how appreciative we are. Even though you do not get probably enough love day in and day out other than from your families, what you do is really important, and I respect it very much. And we will call the next panel.

[Pause.]

Thank you all for being here.

Peter Bergen is vice president of New America where he directs the international security program which conducts research and analysis on extremist groups, homeland security, and other things. He is a contributing editor at Foreign Policy Magazine, a professor at Arizona State University, and writes a weekly column for CNN. Mr. Bergen is also a member of the Aspen Security Group and a documentary producer and author.

Alberto Fernandez is the vice president of the Middle East Media Research Institute and a member of the board at the Center for Cyber and Homeland Security at George Washington University. From 2012 to 2015, he served as the State Department's Coordinator for Strategic Counterterrorism Communications and prior to that was a Foreign Service Officer for over 30 years.

Thank you both for being here today. It is the custom of this Subcommittee to swear in all witnesses, so at this time I would ask both of you to please stand and raise your right hand. Do you swear that the testimony you are about to give before the Sub-

committee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. BERGEN. I do.

Mr. FERNANDEZ. I do.

Senator McCASKILL. Let the record reflect the witnesses have answered in the affirmative.

All of your written testimony will be printed in the record, and we would ask that you try to limit your oral testimony to 5 minutes.

Mr. Bergen, we will hear from you first.

TESTIMONY OF PETER BERGEN,¹ VICE PRESIDENT, NEW AMERICA FOUNDATION

Mr. BERGEN. Senator McCaskill and other Members of the Committee, thanks for this opportunity.

You asked a question of Michael Steinbach, and I think I have an answer. He did not have an answer for the reasons he laid out, but we looked at more than 330 jihadi terrorist cases since 9/11. We found based on the public record that a third of them, a third of those cases were generated either by community tips or family member tips. So there is a high degree of cooperation amongst the community.

Turning to just my overall comments, on Friday we saw something that I think is indicative of something we need to be concerned about, which is terrorists are now the media. Maggie Thatcher, when she was Prime Minister, famously said that terrorists were—the “oxygen of publicity” is terrorism. She said that in 1985. Well, what if terrorists themselves control the media, they completely bypass the traditional media? We saw on Friday, for instance, that the attackers in Bangladesh murdered the people in the cafe. They immediately posted it all to Amaq, which is effectively ISIS’ news agency, which then in turn published it.

So now we have an interesting situation where the terrorists are the perpetrators, the producers of the media around this, and the propagators. And this is something new.

We saw in Paris the ISIS-inspired militant last month who killed the French police official and his partner. He immediately posted pictures and videotape a whole disquisition about his allegiance to ISIS on Facebook.

In the Orlando case and in the San Bernardino case, as you know, the perpetrators immediately pledged their allegiance to Facebook in the middle of the attack.

So one big idea is terrorists are now the media, and that is something that is new. They have always tried to influence the media.

The second, I think, big idea is that ISIS is effectively crowdsourcing jihad, and we have had a lot of testimony today about that fact. But there are obviously results. In the United States, in the last 2 years we have had six ISIS-inspired attacks, two of them lethal in San Bernardino and Orlando, four of them luckily not lethal in places like Garland, Texas, in New York City, in Philadelphia, and in California. But even in the nonlethal cases, people were severely wounded in a couple of these cases.

¹ The prepared statement of Mr. Bergen appears in the Appendix on page 64.

So who is ISIS appealing to in the West? At New America, where I work, we looked at—and also in the United States, we looked at 715 cases, again, based on public records and trials, and we found that one in eight were women, which is unprecedented. In previous jihads we had never seen that. The average age is 25. The average age for the females is 22. Many of them had family ties to jihad. A third of them had family ties to jihad, a brother or father who went, they got married over there. And we found that the profile of the Americans who joined the jihad or tried—either succeeded or attempted to join ISIS was very similar. So one in seven were women, the average age was just under 25, a fifth of them had family ties to jihadism; and, crucially, more than three-quarters were very active online, meaning not that they were just sending emails but they were posting jihadi material on Facebook or Twitter. So I think none of that is necessarily surprising, but I think that has implications for how you try and contest this.

What are ISIS' messages? Again, if we understand what the message is, we can contest them. One is they are victorious, and, at one point they controlled territory the size of the United Kingdom and a population the size of Switzerland. That is now going down. They created a utopian society, it is the caliphate. There is a cool factor, there is a romanticist factor. The message shifted in early 2015 from joining the caliphate to attacking the West if you look at their kind of messaging.

What to do? In the 1 minute I have left, I have a few ideas.

One is I think with CVE there has been kind of a rather crucial conceptual confusion between countering radicalization and countering recruitment. And these things are related. But at the end of the day, what we are trying to do is stop people joining the gangs in the 1990s or joining ISIS, and trying to stop radicalization. It is not illegal in this country to have bad ideas, and it is a very hard task. Tens of millions of people probably have militant ideas. Very few of them join ISIS. Maybe 60,000 over the last 2 years have actually—30,000 from around the world have joined ISIS.

So employing defectors is useful. Employing clerics like Imam Magid, who works not far from here, who has personally intervened with a number of cases in Northern Virginia. Twitter obviously enforcing its terms of use. The military campaign has had some success.

Finally, just to round it up, what we should not do is ban immigration from Muslim countries, as is being proposed. That would have absolutely no effect on this issue. Every lethal terrorist attack in the United States since 9/11 has been carried out by an American citizen or American legal permanent resident. And so I will leave it at that.

Senator McCASKILL. I will certainly give you time for any other ideas in a minute as soon as Mr. Fernandez finishes his testimony. Mr. Fernandez.

**TESTIMONY OF ALBERTO M. FERNANDEZ,¹ VICE PRESIDENT,
MIDDLE EAST MEDIA RESEARCH INSTITUTE**

Mr. FERNANDEZ. Thank you, Senator. I am happy to be here.

If we look at the space that the Islamic State and its rivals and colleagues occupy, we do see over the past couple of years some small measures of incipient progress. Certainly, the military campaign has begun a little bit to dent the victory narrative that the Islamic State has propagated.

Social media companies, government, and the private sector, civil society groups have begun to at the very least dismantle the diffuse online networks that the Islamic State had for many years.

In 2014, none of this stuff was being taken down. In 2016, the stuff is being taken down more rapidly. When people return, they return with less followers. So the space of the fan boys, the space of the online networks is being shrunk and being contested, has been contested, there is more material, there is more messages of defectors. There is a really good NGO, the International Center for the Study of Violent Extremism which is producing defector videos, which I highly recommend. So there is more stuff happening.

However, the ISIS brand has to a large extent been internalized and metastasized to a large extent of the population. Now, of course, we are talking about minorities. We are not talking about 1.5 billion Muslims. We are talking about a small percentage of the population where the ISIS message has been internalized. It does not even need new material. It is old material that functions. It is old things that work. It is not the latest thing.

By the way, in the time that this session has taken place, the Islamic State Al-Furqan released a 15-minute high-quality video talking about itself, talking about how great it is, which they announced on social media ahead of time this morning that they were going to do. I think it underscores Peter Bergen's point, that they are able to get—despite the pressure that we put on them, despite the fact that we are taking stuff down quickly, they are able to surge and get their message out at will when and where they want.

Now, what has not been touched? I think there are several points that we need to think about when we think about what we have done and what has not been done. We still have not gotten the full benefit we have out of the slow but real military progress we are making on the ground.

We should be talking in the last few days about ISIS' defeat at Fallujah and ISIS' near defeat at Mambij. And instead what are we talking about? Orlando, Istanbul, Medina, Bangladesh, et cetera, et cetera, et cetera. They have succeeded in changing the narrative. Instead of talking about how they are physically under great pressure in the field, we are seeing how the digital caliphate and the work that they do overseas is kind of serving as a substitute for military victory. So that is an area where they are still undented.

The other area where they are still undented and something that almost no one either in the United States or overseas touches is the ideology, the building blocks of the ISIS message. The Salafi jihadist world view which empowers it and generates it is largely untouched. I can understand the government not wanting to do

¹ The prepared statement of Mr. Fernandez appears in the Appendix on page 82.

this. This is something that the U.S. Government is probably not very good about talking about, the intersection of politics and religion. But this is not something that is happening anywhere.

As a thought process, when I was writing my testimony, I went on YouTube, and I put in some of the key terms that Salafi jihadists like ISIS use to radicalize people. I put them in English on YouTube. I thought, "What if I was a 17-year-old boy, I am confused, I do not know what is what," and I put in these terms. And every single time the immediate return you got on YouTube was that of extremists, not of humanistic, tolerant, good people that we have in the Muslim community in the United States or overseas.

One of the key terms, "Al-Wala wal-Bara," which is about loyalty to radical Islam and hating the West and hating the country you are in, the No. 1 person that returned to it was Anwar al-Awlaki. So Anwar al-Awlaki 5 years after his death is still helping to radicalize people.

So the ideological challenge of the Islamic State has not been challenged yet, and the sectarian dimension, even our victories in the region, are tainted by the sectarian dimension. So while we are making real progress on the ground against the Islamic State and even in cyberspace, some of the key building blocks for the Islamic State of today and of tomorrow are actually untouched or even enhanced by events on the ground.

Thank you.

Senator McCASKILL. Thank you, and I have 2 minutes left to go, and Senator Portman has not returned. So I am going to ask you to sit tight. I am going to run to vote. He will be back I am sure before I will, but we will be back in—and I apologize for this, but it cannot be helped.

Senator PORTMAN [Presiding.] Thank you, and I assume we did not recess. OK. Thank you all very much for your patience. I apologize. I have gotten my exercise for the day literally running back and forth. We think we are done voting. We may have one more, but we will not ask you to stay if we leave again. I promise you.

First of all, I apologize not to be here to hear your testimony, but I got a chance to review your testimony, and as I said at the outset, I really appreciate both of you being here and your distinguished backgrounds in this area trying to figure out, what the best things are to do. The government panel we heard from a little while ago told us that—and the FBI Director had said this late last year—the lone-wolf radicalization online he believes is the biggest threat to our national security here at home. And we now know the nature of that threat, but we need to get a deeper understanding of some of the trends that we are seeing. That is where you guys can be really helpful.

In these attacks here, in all but one, I think there was no what you would consider, I suppose, direct contact between the terrorists and an ISIS cell overseas. Is that accurate, Mr. Bergen?

Mr. BERGEN. Yes. The only case is the Garland, Texas, case, where there was an actual attack in motion where they had communicated with ISIS.

Senator PORTMAN. Why do you think there has not been an overseas element in most of these U.S. attacks? Either one of you.

Mr. BERGEN. Let me try to answer that. On 9/11 there were 16 people on the no-fly list. Now there are 47,000. There are like a million and a half people on the Terrorist Identities Datamart Environment (TIDE) list. On 9/11, the FBI and the CIA barely talked to each other. On 9/11, there was no NCTC, TSA, DHS. We have tripled our intelligence budget, and we are a much harder target. In fact, the last time a foreign terrorist organization tried to attack us unsuccessfully was May 1, 2010, with the Faisal Shahzad Pakistani Taliban attack. So the point is the reason we are talking about lone wolves is because we have erected these very large defenses against foreign terrorist organizations directing somebody, training somebody, sending them to us.

Senator PORTMAN. You note in your testimony that about 20 percent of American ISIS members had a familial connection to jihad. That was your quote.

Mr. BERGEN. Yes.

Senator PORTMAN. Can you elaborate on that point? I ask because I think it implies that even here in the U.S. there might be a strong in-person element to radicalization, which is an interesting wrinkle to the story, in addition to what happens online.

Mr. BERGEN. Well, an example of that is the Khan family from Chicago, three teenagers, 19, 17, and 16, they have kind of radicalized together, two boys and one girl. They were all planning to join ISIS. They were arrested at O'Hare airport. That is one kind of example.

Another kind of example is people go to join ISIS, of which there have not been that many Americans who have succeeded, but sometimes they marry somebody in ISIS or associated with ISIS when they get there.

Senator PORTMAN. And the content of the ISIS propaganda and how it is uniquely suited to the Internet is something you both have addressed. Ambassador Fernandez, you have noticed that this brand can be all things to all extremists. Mr. Bergen, you have also commented on this, and you have noted that the thrust of the ISIS message is that it offers a sense of purpose and community—we talked about this earlier—to the vulnerable, the disillusioned, the alienated.

To both of you guys, what kind of countermessaging challenges and opportunities does that present for us?

Mr. FERNANDEZ. Well, a couple of things. No. 1, of course, is the most effective countermessaging are people that know the Islamic State best, and those are defectors, those are families of victims. The Islamic State is essentially a Sunni Arab Muslim organization. Yes, it has thousands of non-Arabs in it, but in terms of its world view, it is a Sunni Arab Muslim organization. That is where the issue comes from. That is the heart of its core. Those are the voices that are most useful. We often focus on many of the victims who are not Sunni Arab Muslims. Obviously, we care about all the victims, including Americans. But it is that core audience that it appeals to that we need to work on.

The other thing, of course, is that the ideological dimension of the ISIS appeal is rarely touched. What are these elements that mobilize people, concepts of jihad, of kufr, of shirk, of Al-Wala wal-Bara, of taghut? These terms which are complicated, nuanced

terms in Islamic history which ISIS uses as bumper stickers to kill. It is not Islam for Dummies. It is Salafi jihadism for Dummies. And so those are two of the challenges that we face in that space.

Senator PORTMAN. In some of your testimony, you talk about the fact that our messaging can be more effective, and we talked a little bit about that yesterday at the staff level about, what works and what does not work. You mentioned defectors, for instance. That seems to be more effective, for instance, than, as you say, someone who is not connected.

You also talk about the victory narrative and that that is something that we need to respond to because that victory narrative encourages more people to feel as though they are part of something that is working.

In your written testimony, you contrast our message that you thought was relatively ineffective after retaking Fallujah with that of a more productive messaging after taking a different Iraqi city. From a message perspective, can you talk about the difference between those two and just elaborate on your comments on what is most effective in terms of messaging?

Mr. FERNANDEZ. Sure. Both the taking of Fallujah and the taking of Mambij in Syria are good. They are good because you are taking something from ISIS. You are defeating them. So there is benefit even in a flawed retelling of military victory. So even Fallujah, which has been controversial in the pan Arab media and the Sunni Arab media—these are, Iranian militias and Shia death squads. That is some of the rhetoric out there. But even the way it has turned out, taking it from the Islamic State is a good thing.

The point I make is that it could have been a better thing. It could have been a victory of a united Iraq, a united multiethnic, multireligious Iraq against the Islamic State. And that is not exactly how it was portrayed.

In contrast, the Syrian Democratic Forces, the Kurdish Allied Forces in northern Syria that we support took a different tack. What they did is they put up front Sunni Arab Muslims who were allied with the Kurds in the taking of Mambij, and this is what is called the “Mambij Military Council.” So they took a back seat. They had the Arab Muslims take a front seat. That presented a less sectarian, less provocative way of doing things. They were both good. Victory in Fallujah is good, and victory in Mambij is good. Any defeat of the Islamic State is good. But you want to wring all the benefit that you can out of military victory, and we are not doing that. We are talking too much about what they are doing and not what we are doing to them.

Senator PORTMAN. Well, thank you. I have some additional questions for you both about the narrative and specifically what we ought to be doing better. But I would like to give my colleague an opportunity to ask questions. Senator Ayotte was here earlier. She has a background as a prosecutor and is on the Armed Services Committee and has spent a lot of time on these issues, and I would like her to have a chance to ask some questions.

Senator AYOTTE. Thank you so much, Chairman.

Mr. Bergen, when you testified before the Committee before and I see it again in your written testimony, the discussion about—unlike prior terrorist groups that we have dealt with, that they have

been—that there are many women involved, and you and I had an exchange on that.

As I read your testimony today from where we were before, that continues, I think, to be the case, no diminishment in that, and obviously we saw with the San Bernardino situation, while that was more of a radicalization here, still, obviously, she was a big driver in this.

So have you seen any diminishment in that and what we should be doing in terms of, as we are thinking about individuals that were involved in ISIS—and in your steps of recommendations, you say—and I think that Mr. Fernandez just talked about that as well. If you have been a member of ISIS, get people who have been part of it, and then also get them to go out online and obviously talk about the real experience. What about with women? Are we having any success with how we are going to engage women who join ISIS and why it is so attractive to women as well?

Mr. BERGEN. I mean, Senator, yes, I think they are still recruiting women. Part of it is sort of a romantic message, that you can marry the man of your dreams in part, which has been reinforced by people who get married there. What the countermessaging is to that I am not really sure, except I think I completely agree with Ambassador Fernandez that defectors are the most effective approach. And, the New York Times ran a very interesting massive piece with two women who defected. They gave them pseudonyms. They painted a very bleak picture.

I think the United States faces an interesting question, which is we have a guy in Alexandria, Virginia, Mohamad Khweis, who is 26, who has defected. He could face 20 years in prison. He has obviously defected because he thinks ISIS is against Islam. So, the kind of bigger question is: What do we do with people who are defectors, American defectors? Do we throw them in prison for 20 years, or do we come up with something more creative?

Senator AYOTTE. Ambassador, did you want to comment on that?

Mr. FERNANDEZ. Yes. One of the problems we have, even when we have defectors, I am sure you have seen the images. The ISIS spokesman is looking at you, unmasked, telling you about his life, telling you about his personal testimony. He is unashamed, unembarrassed. And then we have all too often the defector, and what does the defector look like? The defector is masked or covered, obviously—

Senator AYOTTE. Because they are afraid.

Mr. FERNANDEZ [continuing]. For security reasons. So this is the disadvantage that we have with them.

Senator AYOTTE. Right.

Mr. FERNANDEZ. Their personal testimony is more powerful than ours, and it is more numerous than ours. So this is the challenge that we face, kind of a technical basic problem that we face.

Senator AYOTTE. I was interested also, Mr. Bergen, as I looked at your action items, this idea that you had about a database of foreign fighters, because we do know obviously that there are a number of individuals who have flown back and forth, especially fewer Americans, significant, a couple hundred Americans, but also with the Europeans, thousands. And as you raise the issue, it seemed clear to me that we still have significant information-shar-

ing issues across our allies in Europe, and even with countries like Turkey, and that we probably do not know all are collecting in one place, people that we do know, in fact, have joined. And I think that is a significant issue that you point out that we should address.

Mr. BERGEN. Yes, I mean, Interpol has 5,000 names. We have 30,000 people who have joined from around the world.

Senator AYOTTE. Right.

Mr. BERGEN. So we are 25,000 short. And my intuition is we had no idea about any of these people who blew themselves up over the past month in Bangladesh and Turkey. I think with the British and other European partners there is pretty good information sharing, but clearly a lot more has to be done.

Senator AYOTTE. And even if you look at countries like what happened in Belgium, with the deficiencies there, with some of the law enforcement deficiencies there in terms of compiling that, that seems something in terms of an intelligence tool that would be helpful to all of us.

What other things, if you think about the intelligence front, that you think, the two of you think that we should be focusing on?

Mr. BERGEN. Well, one thing I would look at is if Amaq is ISIS' new service—and there are a couple of other entities that put out ISIS' message—why aren't we taking them down? I mean, I am not saying—

Senator AYOTTE. Right.

Mr. BERGEN. I mean literally taking out their production facilities. They must exist.

Senator AYOTTE. Exactly. It makes logical sense that we would do that, and that is something we should be asking our officials. Why aren't we just taking them down? I know it is a Whack-A-Mole situation.

Mr. BERGEN. Well, you whack enough moles—

Senator AYOTTE. Exactly, and you make it harder enough to do something, then they are—it is not that it will not come back, but why would you let it continue if you know it is there.

Mr. FERNANDEZ. And one thing we have seen, we have seen with the—initially people were skeptical about, well, taking stuff down on the Internet, right? They are just going to come back. And, yes, there are individuals who have been taken down 500 times and are back for the 501st time. But what we have seen is that many, many of the maybe less motivated people drop off. So the Whack-A-Mole work on social media does pay dividends over time.

Recently at MEMRI, we saw that, they have been driven mostly off of Twitter, and they are on Telegram, which is this German-Russian site, and we recently saw—just 2 days ago, we saw an ISIS message calling for people to return to Twitter, because even though Telegram is very useful and is a safe haven for them, nothing is as good as mobilizing, getting your message out very broadly as Twitter. So we need to continue to be mowing the lawn on Twitter because they will come back if they are given the space to do so.

Senator AYOTTE. And the other issue is, as you heard Director Steinbach testify—and it is replete in your testimony as well—that they are consuming this extremist material. Now, there is line of,

obviously, what can you consume without taking action in terms of where you can take legal action. But it is a strong indicator, if somebody is consuming this extremist material, that this is something that we have to be focused on, obviously not just eliminating the ability to push this out on the Internet, but we have seen it over a series of attacks, that that is one of the components of an individual who ends up being radicalized, or self-radicalized.

Mr. FERNANDEZ. At the very least, you want to give the potential consumer in the United States the same ability to access material that is not going to radicalize them, that is going to counter that as the radicalization material. To me, it is unconscionable that you go on YouTube, which is an American company, and you put in a term, an Islamic term, which is not necessarily an ISIS term, and the No. 1 thing you get is the algorithm gives you basically a well-known American terrorist that we killed.

There has to be ways that, you do the algorithms or whatever you do to make sure that the voices of tolerance, the voices of reason, the voices of humanity are there, at least to compete with the extremists if you cannot take them down.

Senator AYOTTE. It seems to me that, of course, we can do that, and we know that not only what the government activity and responsibilities but the private sector responsibility in terms of how these sites are being used. And we know that they are taking some steps that are important, but I think further engaging on that is critical.

Well, I appreciate both of you being here today, and thank you, Chairman. I know you have more questions.

Senator PORTMAN. I just have a couple more questions.

One, building on what you just said, Ambassador Fernandez—and, Mr. Bergen, I would like to hear your view on this—you mentioned the Twitter work. I said in my opening statement they have closed down more than 100,000 ISIS-linked accounts, and you have to assume a lot of that comes back. But you were saying also, “mowing the grass” I think is the analogy you used, it is important to keep that up. I hope Twitter, Facebook, and others are continuing that effort. Do you think what Facebook has done, which is apparently worked to remove offending users but also to help promote counter-jihadist propaganda, has also been effective?

Mr. FERNANDEZ. I believe that there has been progress across the board by the Big Three—by Twitter, YouTube, and Facebook. So there has been tremendous progress if we are looking at 2 years ago or even 1 year ago. That is a good thing.

Facebook has been particularly effective or particularly aggressive in taking material down and shutting things down. So we want to encourage that. We want to encourage all of them to do that.

And then we want to focus on these other safe havens where they are jumping to, so Telegram, JustPaste.it, Archives.org, what can be done with these companies, these entities that are in the West, to at least make life a little more difficult for the extremists? Realizing that in the end the message is going to get out, and the message has to be countered, it has to be answered. But we certainly do not want to give them a free ride in our own space.

Senator PORTMAN. I think that is very sensible, and, this Subcommittee has worked hard on this issue in some other contexts with human trafficking where there is a challenge, the “dark side of the Internet,” as I call it, and that same dark side unfortunately is being utilized by some of these radicalized elements.

Something that struck me in your testimony, Mr. Bergen, was about women and the fact that ISIS has had luck in attracting more women to its ranks, and this is remarkable to me because of how poorly they treat women. As one example, ISIS has women marry fighters, and if a woman’s husband dies, she is quickly married off again, I am told, sometimes in violation of Islamic law. You talked a little about that earlier. But what accounts for this phenomenon? Why are women feeling compelled to sign up given the reality?

Mr. BERGEN. I do not have a good answer to that, but I think in the 1970s they might have joined the Weather Underground or the Black Panthers or some other utopian group that promised utopia through revolutionary violence, and this is one of the last revolutionary ideologies left standing. And so, I mean, that is an attempt at answering the question, but, given their ultra misogyny, it is really a mystery.

Senator PORTMAN. And, again, the counternarrative needs to be out there, defectors included, and there are women who have defected who have come forward, and that seems to me to be, one of our opportunities given the phenomenon.

On the Global Engagement Center and the work that we talked about earlier with the previous panel, Ambassador Fernandez, of course, you have lots of experience with the predecessor, the head of the Center for Strategic Counterterrorism Communications. I know it is early—the Global Engagement Center is really only a few months old—but what are you encouraged by so far? What are you discouraged by? In your written statement, you talk about the Global Engagement Center not having a dedicated line item budget appropriation, the funding issue that I mentioned earlier; emphasis on building out a professional staff, they need to still do that; too much emphasis on transitory events rather than building out something that is focused on combating the threat long-term. Can you elaborate on your concerns and any suggestions you have for improvement?

Mr. FERNANDEZ. Well, I am encouraged in the work that they are doing with recanters, with defectors. That is good. I am encouraged with the idea of building proxies, building a network of proxies across the world that do stuff. So that is the good stuff.

The areas where I am concerned is a lot of what the work of proxies are doing is not very impressive. It is just churning stuff out. It is not well aligned. It is material that—“Do not do drugs,” right? That kind of stuff. Of course, yes, do not become a terrorist. But it does not go deep. It is not as personal. It is not as powerful as one would want it to be.

Now, it is early days, but there is a lot of movement and not necessarily progress yet. So I think they need to—they need some more time. I see some good things, and I see some things which are a little concerning.

Senator PORTMAN. Part of what I am hearing you say is that we need to target the message more precisely. This is the analytics point that we were making earlier, and I talked about this particular issue of the legal constraint of the Privacy Act. You had to deal with that as well, I assume.

Do you have thoughts on that? To me it just does not make sense that we would not be able to target those most vulnerable, susceptible who are foreigners, not American citizens, not permanent residents. Do you have thoughts on that?

Mr. FERNANDEZ. Well, we assumed, sir, when I headed CSCC, that if we are messaging in Arabic, Urdu, and Somali in platforms that we know are outside the United States, we are going to assume that the overwhelming majority of the people that we are messaging against or with or to are not Americans. Yes, some guy in Minneapolis could see what we are doing, but we are assuming that if we are messaging or looking at a Yemeni tribal forum, which is one of the places that we looked at, most of the people there are not Americans.

So that was actually not a concern of ours at all. I was actually kind of very surprised by that testimony myself.

Senator PORTMAN. Well, we are going to be digging into that further, as you know from my questions there. We have an opportunity here online, in addition to the other things we talked about earlier that need to be done on the military side or, protecting the homeland through law enforcement and so on. But we have an opportunity here to step up our game, don't we? And not that there is any one silver bullet, but to me this is the most difficult and perhaps, therefore, the most important part of the entire effort to better protect our homeland and better protect the free world from this terrorist threat.

So we thank you for your expertise on it. You want us to keep writing about it. What is the book that you have next to your microphone there?

Mr. FERNANDEZ. I mentioned the International Center for the Study of Violent Extremism, Dr. Anne Speckhard of Georgetown University, and this is actually the book that just came out as part of their work, and it actually collates the testimony of defectors.

Senator PORTMAN. OK.

Mr. FERNANDEZ. And it has a recommendation by Peter Bergen and Alberto Fernandez on the back.

Senator PORTMAN. Wow. You are on the book cover. So Bergen has a book, too. He has a 1-800 number for his book. [Laughter.]

What is your new book, Peter?

Mr. BERGEN. "United States of Jihad: Investigating America's Homegrown Terrorists," and it is an attempt to look at many of the issues we just discussed.

Senator PORTMAN. Well, you get to talk about your book because you were kind enough to come here and testify before us, spend your day with us. Sorry about the interruptions, and thank you for your expertise and your willingness to help us to be more effective in our fight against terrorism, specifically this countermessaging online.

The hearing record will remain open for 15 days for additional comments or questions by any of the Subcommittee members.

This hearing will now be adjourned.
[Whereupon, at 4:36 p.m., the Subcommittee was adjourned.]

A P P E N D I X

HEARING OF THE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
“ISIS ONLINE: COUNTERING TERRORIST RADICALIZATION &
RECRUITMENT ON THE INTERNET & SOCIAL MEDIA”
JULY 6, 2016

OPENING STATEMENT OF CHAIRMAN ROB PORTMAN

This hearing will come to order.

When the Subcommittee began planning this hearing, we did not know it would fall just three weeks after the most deadly terrorist attack on American soil since September 11, 2001. The evil terrorist attack in Orlando last month that targeted the LGBT community was yet another reminder of the urgent need to reexamine and redouble our government’s efforts to combat violent Islamic jihadism both at home and abroad — and particularly to disrupt and ultimately destroy the so-called Islamic State of Iraq and Syria or ISIS. There is no room for complacency on this issue. It warrants continuous scrutiny and oversight from Congress as our government’s understanding of the enemy evolves.

ISIS specializes in savagery—violence inspired by delusions of sectarian conquest from another age. Yet it has effectively deployed modern technology of the information age to spread its propaganda and recruit killers to its cause. ISIS has developed a sophisticated information warfare capability. It has pioneered a distinctive strategy of targeted online recruitment, while disseminating sleek viral videos and messages, primarily from two media centers, al-Hayat and al-Furqan through a constantly evolving set of online platforms. As FBI Director James Comey has noted, even if we are able to keep foreign terrorists *physically* out of the United States, online communication and social media allow ISIS to “enter as a photon and radicalize somebody in Wichita, Kansas.” ISIS has weaponized online propaganda in a new and lethal way.

The damage wrought by that weapon is considerable. Orlando—49 dead. San Bernardino—14 dead. Fort Hood—13 dead. The Boston Marathon—3 dead and hundreds wounded. Each of these killers was

reportedly radicalized to some degree by online jihadist content. And so many other attacks inspired by means of social media have been thwarted. Indeed, experts tell us that throughout last year, social media played some part in radicalization of all 60 people arrested in the United States for criminal acts in support of ISIS. Most recently, of course, the FBI has publicly stated that it is “highly confident” that the Orlando killer Omar Mateen was “radicalized at least in part through the Internet.”

One longstanding aim of the ISIS propaganda machine is to attract foreign fighters to ISIS-controlled territory. Often ISIS tells its recruits tales of high adventure, joined with false narratives of an Islamic extremist utopia. The bizarre images behind me, for example, appear in a ISIS film exhorting Muslims around the world to join the Islamic State; rather than show ISIS fighters for what they are — murderers of innocent victims who are themselves *overwhelmingly* Muslim — they are shown playing with laughing children and shopping in local marketplaces. Appeals like these have helped draw an estimated 30,000 foreign fighters, including at least 6,000 Westerners, to take up arms with ISIS. The good news is that the Defense Department reports a significant decrease in the flow of foreign fighters to ISIS territory. At the same time, however, ISIS has increasingly *shifted* its propaganda efforts to inciting sympathizers to commit acts of terror in the West—including in the United States.

Online propaganda, amplified by social media and peer-to-peer communication, is now a key weapon in ISIS's arsenal. We should, of course, resist over-simplifying the problem. Not all radicalization in the United States occurs online, and in-person interaction often reinforces the process. But unlike the more common European pattern of jihadist radicalization in clusters or in prison, the U.S. threat so far is predominantly that of the lone wolf terrorist—an individual radicalized on his own, often in front of his computer screen with access to online jihadist content and videos that create a kind of virtual training camp.

In addition to a clear military strategy and vigilant law enforcement efforts here at home, the United States and our allies need a more robust, coordinated strategy to expose the enemy's lies, counter its false narratives, and encourage credible voices to tell the truth to

those most susceptible or receptive to ISIS's lies. And that is true both of foreign and U.S. audiences. Although the ISIS online radicalization threat is well-recognized, there is a range of opinion on how best to *combat* it, and U.S. government efforts are still in early stages. Today we will examine the counter-messaging initiatives that show promise—and where the U.S. government has fallen short and could accelerate its efforts.

In January, the State Department began a revamp of its counterterrorism messaging and coordination efforts with the launch of the Global Engagement Center—a better funded and (at least on paper) more empowered version of its predecessor, the Center for Strategic Counterterrorism Communications. Previous efforts to address this threat have struggled to overcome bureaucratic hurdles, unclear authorities, and a lack of interagency communication and unity of effort. These structural deficiencies will continue to hinder future administrations—both Republican and Democrat—unless they are addressed. That is why I recently introduced legislation with Senator Murphy to help resolve some of these issues and the impact they have on our ability not only to counter propaganda and disinformation from extremist groups like ISIS but also the equally pressing challenges posed by state-sponsored propaganda from countries like Russia and China.

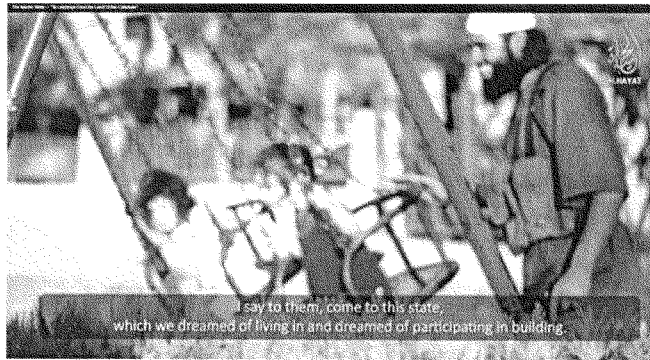
The Department of Homeland Security also recently consolidated its countering-violent-extremism or CVE efforts in a new Office of Community Partnerships. We'll be hearing more about those efforts in our first panel today, and I will be interested in exploring whether these initiatives are backed by sufficient authorities and resources.

In addition, social media firms including Facebook and Twitter have stepped up their voluntary efforts to police their own terms of service, which prohibit incitements to terrorism. Twitter has closed more than 100,000 ISIS-linked accounts, and Facebook has actively worked to remove offending users while working in various ways to promote content to counter jihadist propaganda. Those actions have helped to degrade ISIS's social media megaphone, according to the Middle East Media Research Institute, but its online presence remains strong.

Let's be very clear: To defeat ISIS, it is necessary to destroy the enemy where they live and prosper — in Iraq and Syria, and in their major cells around the world. Online counter-messaging is no substitute for a clearly defined and vigorously executed military strategy. But a military strategy must be reinforced by a coordinated effort to undermine and disrupt the powerful disinformation spread by Islamic jihadists. Today, we will be hearing from three federal agencies involved in that effort, as well as a distinguished panel of experts who have been engaged on these issues for many years.

With that, I will turn to Senator McCaskill for her opening statement.





**STATEMENT OF
MICHAEL STEINBACH
EXECUTIVE ASSISTANT DIRECTOR
FEDERAL BUREAU OF INVESTIGATION**

**BEFORE THE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
UNITED STATES SENATE**

**AT A HEARING CONCERNING
THE FEDERAL GOVERNMENT'S EFFORTS TO MONITOR, DISRUPT, AND COUNTER
TERRORIST PROPAGANDA, WITH PARTICULAR FOCUS ON
THE ISLAMIC STATE OF IRAQ AND THE LEVANT'S ("ISIL") ONLINE COMMUNICATIONS**

**PRESENTED
JULY 6, 2016**

Good afternoon Chairman Portman, Ranking Member McCaskill, and Members of the Subcommittee. Thank you for the opportunity to appear before you today to discuss the widespread reach of terrorists' influence, which transcends geographic boundaries like never before. As technology advances so, too, does terrorists' use of technology to communicate — both to inspire and recruit. Their widespread use of technology propagates the persistent terrorist message to attack U.S. interests whether in the Homeland or abroad. As these threats to Western interests evolves, we must adapt and confront the challenges, relying heavily on the strength of our Federal, State, local, and international partnerships.

Preventing terrorist attacks remains the FBI's top priority. The terrorist threat against the United States remains persistent and acute. The threats posed by foreign fighters, including those recruited from the U.S., traveling to join the Islamic State of Iraq and the Levant ("ISIL") and from homegrown violent extremists are extremely dynamic.

ISIL has proven relentless in its violent campaign to rule and has aggressively promoted its hateful message, attracting like-minded extremists, including among Westerners. To an even greater degree than al Qaeda or other foreign terrorist organizations, ISIL has persistently used the Internet to communicate and spread its message. From a Homeland perspective, it is ISIL's widespread reach through the Internet and particularly social media which is most concerning as ISIL has aggressively employed this technology for its nefarious strategy. ISIL blends traditional media platforms, glossy photos, in-depth articles, and social media campaigns that can go viral in a matter of seconds. No matter the format, the message of radicalization spreads faster than we imagined just a few years ago.

Unlike other groups, ISIL has constructed a narrative that touches on all facets of life — from career opportunities to family life to a sense of community. The message is not tailored

solely to those who are overtly expressing symptoms of radicalization. It is seen by many who click through the Internet every day, receive social media push notifications, and participate in social networks.

As a communication medium, social media is a critical tool that terror groups can exploit. One recent example occurred last week. An individual was arrested for providing material support to ISIL by facilitating an associate's travel to Syria to join ISIL. The arrested individual had multiple connections, via a social media networking site, with other like-minded individuals.

As I have testified previously, there is no set profile for the susceptible consumer of this propaganda. However, one trend continues to rise — the inspired youth. We have seen certain children and young adults drawing deeper into the ISIL narrative. These individuals are often comfortable with virtual communication platforms, specifically social media networks. Ultimately, many of these individuals are seeking a sense of belonging.

ISIL continues to disseminate its terrorist message to all social media users — regardless of age. Following other groups, ISIL has advocated for attacks by lone individuals. Several incidents have occurred in the United States and Europe over the last year that indicate this “call to arms” has resonated among ISIL supporters and sympathizers.

The targeting of U.S. military personnel is also evident with the release of hundreds of names of individuals serving in the U.S. military by ISIL supporters. The names were posted to the Internet and quickly spread through social media, demonstrating ISIL's capability to produce viral messaging. Threats to U.S. military and coalition forces continue today.

Lastly, social media has allowed groups, such as ISIL, to use the Internet to spot and assess potential recruits. With the widespread distribution of social media, terrorists can identify vulnerable individuals of all ages in the United States — spot, assess, recruit, and radicalize — either to travel abroad to join ISIL or to conduct a homeland attack. The foreign terrorist now has direct access into the United States like never before.

Some of these conversations occur in publicly accessed social networking sites, but others take place via private messaging platforms. It is imperative the FBI and all law enforcement organizations understand the latest communication tools and are positioned to identify and prevent terror attacks in the homeland. We live in a technologically driven society and just as private industry has adapted to modern forms of communication so too have the terrorists. Unfortunately, changing forms of Internet communication are quickly outpacing laws and technology designed to allow for lawful access to communication content. This growing gap the FBI refers to as Going Dark is the source of continuing focus for the FBI; it must be urgently addressed as there are grave risks for both traditional criminal matters as well as in national security matters. We are striving to ensure appropriate, lawful collection remains available. Whereas traditional voice telephone companies are required by CALEA to develop and maintain capabilities to intercept communications when law enforcement has lawful authority, that

requirement does not extend to most Internet communications services. Although law enforcement may access stored communications with lawful process, some services are being developed that do not store communications, and, therefore, do not give law enforcement the ability to collect information critical to criminal and national security investigations and prosecutions.

The FBI, in partnership with the Department of Homeland Security, is utilizing all lawful investigative techniques and methods to combat the threat these individuals may pose to the United States. In conjunction with our domestic and foreign partners, we are rigorously collecting and analyzing intelligence information as it pertains to the ongoing threat posed by foreign terrorist organizations and homegrown violent extremists. In partnership with our many Federal, State, and local agencies assigned to Joint Terrorism Task Forces around the country, we remain vigilant to ensure the safety of the American public. Be assured, the FBI continues to pursue increased efficiencies and information sharing processes as well as pursue technological and other methods to help stay ahead of threats to the Homeland.

Chairman Portman, Ranking Member McCaskill, and subcommittee members, I thank you for the opportunity to testify concerning terrorists' use of the Internet and social media as a platform for spreading ISIL propaganda and inspiring individuals to target the Homeland. I am happy to answer any questions you might have.

**Written Statement of George Selim, Director
Office for Community Partnerships
U.S. Department of Homeland Security**

**U.S. Senate Committee on Homeland Security and Governmental Affairs
Permanent Subcommittee on Investigations**

**Hearing: ISIS Online: Countering Terrorist Radicalization and Recruitment on the
Internet and Social Media**

July 6, 2016

Chairman Portman, Ranking Member McCaskill, and distinguished Members of the Subcommittee, thank you for the opportunity to be here. I welcome the opportunity to appear before you to discuss priorities and key actions of the Department of Homeland Security (DHS) to address ISIL and other terrorist's attempts at online recruitment and radicalization to violence.

Overview of Threat

In recent years, the threat from violent extremism has evolved. Terrorists at home and abroad are attempting to radicalize and recruit individuals to violence within the United States. As Secretary Johnson has said, we are in a new phase in the global terrorist threat. We have moved from a world of terrorist-directed attacks to a world that increasingly includes the threat of terrorist-inspired attacks, one in which the attacker may never have come face-to-face with a member of a terrorist organization and instead lives among us and radicalizes to violence, inspired perhaps by messages and propaganda ISIL and other groups disseminate through social media. By their nature, such inspired attacks are harder for intelligence and law enforcement to detect and could occur with little or no notice, presenting a more complex security challenge.

We are concerned about attempts by ISIL and other groups to inspire lone offenders. For example, ISIL consistently releases high-quality English-language videos and magazines promoting its alleged caliphate and calling for supporters in the West to pursue attacks in their homelands.

We were forcefully reminded of this on the morning of June 12, when over 300 individuals were terrorized in an Orlando night club by a man who shot and killed 49 individuals and injured 53 more. We believe he may have been inspired in part by terrorist organizations overseas, resulting in the worst act of terrorism in the U.S. since 9/11 and the worst mass shooting in U.S. history.

Development of CVE

Over the past several years, the U.S. government has acknowledged the need to go beyond traditional counterterrorism and law enforcement approaches to address the evolving threat from homegrown violent extremists and develop more comprehensive efforts aimed at addressing root causes to prevent the next generation of recruits.

This recognition has led to the prioritization of a prevention framework, known to many as Countering Violent Extremism (CVE). Whereas “counterterrorism” implies attempting to stop an individual who, in the eyes of the law, has already taken steps toward committing a terrorist act or joining a terrorist group using law enforcement, screening and protection activities, CVE counters the violent extremist recruitment, focusing on the root causes of many underlying motivations, and working to prevent those drivers, or provide “off-ramps” for individuals who may have taken steps toward embracing violent extremism. CVE encompasses a number of efforts, including prevention and intervention programming, as well as alternative dispositions which involves the possible development of disengagement programs in the post-crime context, both prior to trial and following conviction.

Our federal approach to CVE is described in the 2011 White House *National Strategy for Empowering Local Partners to Prevent Violent Extremism in the United States*, and is outlined in the subsequent *Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States*.

Since 2012, the federal government has collectively held thousands of community engagements in cities around the country. These include, but are not limited to, Community Engagement Roundtables which have been hosted by the DHS Office for Civil Rights and Civil Liberties since 2005, Town Hall Meetings, Community Awareness Briefings and Community Resilience Exercises. I personally led our engagement efforts in Detroit and Dearborn, Michigan, and several other cities from 2006 to 2012. In addition, Office for Community Partnerships (OCP) field staff provide on-the-ground strategic engagement, outreach, logistical, training, and CVE subject matter expert support to the southern CA and Denver regions.

In February 2015, the White House convened a three-day summit on CVE to bring local leaders together and discuss concrete steps to enhance support for community-led efforts. The White House CVE Summit showcased prevention frameworks that Boston, Los Angeles and Minneapolis developed, through programs and initiatives tailored to their local communities. These cities continue to advance local efforts, such as through engagement with mental health professionals, community outreach programs, and countering the message of violent extremist groups.

Taking our CVE Efforts to the Next Level

Recognizing the need to respond to the emerging threats, in 2015 Secretary Johnson announced an Office for Community Partnerships. This Office is dedicated to focusing the Department’s efforts in countering violent extremism and works to build relationships and promote trust with local communities across the United States.

We are focused on partnering with and empowering communities by providing them a wide range of resources to use in countering violent extremism. In addition, we are partnering with the private sector to find innovative, community-based approaches to countering violent extremism in social media.

Advancing that effort also means working in a unified and coordinated way across the U.S. government, which is the purpose of the interagency CVE Task Force, announced in January 2016 and which is responsible for organizing all CVE efforts across the federal government.

The Task Force is hosted and currently led by DHS, and the leadership will rotate every two years between a DHS and a Department of Justice (DOJ) executive. The Task Force includes participation from over 10 departments and agencies across the federal government. Its major objectives include developing intervention programs; synchronizing federal CVE outreach and engagement; managing CVE communications and leveraging digital technologies to engage, empower, and connect CVE stakeholders; and coordinating and prioritizing federal CVE research and establishing feedback mechanisms to increase the relevance of CVE findings. Ensuring that the nation's CVE efforts are sufficiently resourced has been an integral part of our overall efforts.

Countering Online Recruitment and Radicalization to Violence

As terrorist groups such as ISIL continue to undertake a deliberate strategy of using social media to reach into our country and recruit, radicalize, and mobilize some of those among us to violence, engagement with the private sector on this issue has become critically important.

Various departments and agencies have long engaged with a range of key technology companies to encourage efforts to counter ISIL and other groups online, and we have recently stepped up government efforts. For example, Secretary Johnson, Attorney General Lynch, and other senior Administration officials met with social media executives in San Francisco in January 2016, and with tech leaders in New York in November 2015. DHS OCP and DOJ staff engaged with the technology industry representatives during a meeting in February 2016; the goal of the meeting was to build on a dialogue with the social media industry to determine how best to build partnerships to address use of the Internet for terrorist purposes.

As part of supporting efforts to counter extremism online, the Department supports the Peer-2-Peer (P2P) Challenging Extremism contests. P2P is a government-sponsored competition, launched in 2015, to empower universities to develop innovative and powerful social media campaigns that include positive, alternative, or counter narratives to counter violent extremism. Student teams work with a faculty advisor, while earning academic credit, to research, design, and launch a real social media campaign that has measurable impact on their campus, community and country. Since its inception in spring 2015, over 3,000 students representing 125 university teams from over 30 countries have participated in this unique program.

Facebook became the first technology partner to join the P2P project in the summer of 2015. As part of the partnership, Facebook sponsors a competition of the top three teams who demonstrate the best integration of the Facebook platform into their broader digital and social media campaigns at the Facebook Global Digital Challenge event. Facebook also provides advertisement credits on the Facebook platform to each of the teams during the competition. Facebook's participation has also allowed the initiative to expand into more international schools.

On June 27, the State Department, one of our partners in this initiative, hosted its third P2P competition with teams competing as finalists from Azerbaijan, Belgium, as well as the Rochester Institute of Technology in New York. And on June 28, Facebook hosted their P2P Global Digital Challenge, with teams from Belgium, Afghanistan, Spain and the Netherlands.

Through the P2P Program, we have seen that young people are essential to our work in creating credible and positive messages that counter violent extremism and hate. That is why, for example, DHS is currently working with partners across the government to scale up domestic student-designed campaigns and projects. This will require additional funding, as well as support from government, non-government organizations, and private sector partners to transition viable student projects to market.

At the Department, we are aware that there is a limit to the effectiveness of government efforts with regard to countering terrorist recruitment and radicalization to violence, particularly in the online realm, and those local communities online and offline must address these issues since they are best positioned to intervene. Consequently, we at DHS can act as a facilitator, connector, and convener, but ultimately, communities and individuals are best positioned to take action to counter violent extremism.

That is why the Department focuses on cultivating and empowering partners – particularly those in civil society and the private sector – to develop and amplify content that resonates against ISIL, al-Qaida, and other violent extremist groups.

In addition to supporting the P2P Program, the CVE Task Force includes a team dedicated to communications and digital strategy. The Task Force will build partnerships with the private sector to identify and amplify credible voices to counter narratives promoted by ISIL, domestic terrorists, and other violent extremists. This will include a multi-platform communications strategy that leverages the use of digital technologies to engage, empower, and connect CVE stakeholders.

Ultimately, the Department and the Administration believe that the innovative private sector that created so many technologies our society enjoys today can also help create tools to limit terrorists from using these technologies for terrorist recruitment and radicalization to violence; ways their creators never intended. We applaud and are encouraged by companies' increasing efforts to address the tiny fraction of their users exploiting their technologies for nefarious ends. In addition, we recognize the critical role that private sector and NGO groups can play in continuing their efforts to develop creative and effective solutions to counter how terrorists use media platforms for these purposes. Going forward, we will continue to convene a wide range of disciplines, including civil society, technology companies, and content producers. We are encouraged by a number of initiatives underway and applaud those who see the common challenge terrorism poses and are continuing to take proactive steps to make it harder for terrorists operate.

Moving Forward

Our efforts to develop a locally-driven, comprehensive prevention-based CVE framework remain ongoing. We have taken great strides over recent months to professionalize and institutionalize the CVE infrastructure of the Department and the U.S. Government as a whole. However, more work remains.

Recently, Congress appropriated CVE funds in the FY 2016 Omnibus Appropriations Act, which allocated \$10 million in CVE grant funding to be administered jointly by OCP and FEMA. This is the first time federal funding at this level will be provided, on a competitive basis, specifically to support local CVE efforts. The funding will be competitively awarded to state, tribal, and local governments, nonprofit organizations, and institutions of higher education to support new and existing community-based efforts to counter violent extremist recruitment and radicalization to violence. We look forward to receiving applications for this funding opportunity and will continue to update Congress as the program moves forward.

Conclusion

As recent events have tragically demonstrated, the radicalization and recruitment to violence of American citizens perpetrated by ISIL and other terrorist organizations remains a real and persistent threat. As such, the CVE efforts undertaken by both the Department and the CVE Task Force are paramount to address one of the most significant homeland security challenges facing the nation.

Chairman Portman, Ranking Member McCaskill, and Members of the Subcommittee, this is the vision we are working to implement today, not only digital engagement but also through the important work of building a comprehensive CVE model that ensures safe and resilient communities in the homeland. Thank you again for allowing me the opportunity to appear before you today on this critical issue. I look forward to answering your questions.

STATEMENT OF MEAGEN M. LAGRAFFE

CHIEF OF STAFF

GLOBAL ENGAGEMENT CENTER

BEFORE THE 114th CONGRESS

U.S. SENATE COMMITTEE ON HOMELAND SECURITY & GOVERNMENTAL
AFFAIRS

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

JULY 6, 2016

2:00 PM

DIRKSEN SENATE OFFICE BUILDING

Chairman Portman, Ranking Member McCaskill, members of the Committee, thank you for the opportunity to testify and answer your questions today.

I am here to discuss our government's international efforts to counter violent extremist propaganda, online, and in both social media and traditional media. This is a critical effort, especially when it comes to our whole-of government efforts to degrade and destroy ISIL, because it is clear that to our enemy, the information battlespace is as important as the physical battlespace.

Prior to March of this year, I served as the Chief of Staff in the office of Special Operations and Low-Intensity Conflict at the Pentagon. Based on that experience, I can tell you with confidence that the U.S. military and coalition has significant capabilities to eliminate militants from the battlefield and is doing so every day. Da'esh has already lost nearly half of its territory in Iraq, and 20 percent in Syria.

We must also continue to confront the messages that these groups push out daily to recruit people and inspire them to violence. Addressing radicalization to violence and recruitment in the information space is a key piece of any serious, meaningful, and enduring approach to countering violent extremism long-term.

To meet that challenge, President Obama signed an Executive Order in March which created the Global Engagement Center, revamping our counter-messaging strategy.

The quality and volume of violent extremist messaging has advanced dramatically since our predecessor organization was established five years ago, or even from the time when Da'esh began metastasizing into its current form, some three years ago.

The Global Engagement Center is designed to be as agile and adaptive as our adversary. We are armed with new authorities, personnel, and cutting-edge technology. The Center is charged with coordinating, integrating, and synchronizing all government communications directed at foreign audiences abroad used to diminish the influence of violent extremists.

When fully operational, the Center will comprise staff from the Departments of Defense, Treasury, Justice, State, Homeland Security, and the Intelligence Community. Working across these agencies, the Center is identifying efficiencies and opportunities in the messaging space, particularly with the Department of Defense and the Intelligence Community.

The Center is also receiving vitally needed funding and we appreciate the support of Congress. For too long, these efforts have been under resourced. In Fiscal Year 2015, the CSCC's budget was just over \$11 million, and this year, our budget has increased to a little more than \$15 million.

However, more substantial than changes to personnel or budgets, the Center is taking a fundamentally new approach in the information space. We have pivoted from direct online engagement to partner-driven messaging and content. While the U.S. government has a good message to tell, we are not always the most credible voice to tell it.

Instead, there is an abundance of credible and diverse voices across the Middle East, Europe, and Africa—governments, NGOs, and civil society groups—that we are now leveraging in this fight. We are not publicizing who many of our partners are, so that we don't undermine their credibility, but I'll give you a couple of brief examples.

In Kosovo, we recently completed a training program with local NGOs, designed to amplify credible voices there. We ran workshops to train local influencers about designing and executing a messaging campaign. For example, one participant hosts one of the most popular radio shows in his country, and has more than 200,000 individuals visiting his Facebook page. Kosovo is a compelling location because it has both the highest number of foreign terrorist fighters per capita in Europe, and an active NGO community focused on countering violent extremism.

In East Africa we worked with a civil society partner to establish an online, mobile-enabled radio station in Swahili. It airs youth-produced programming that counters the rising volume of violent propaganda in the region. The content is aimed at youth living in neighborhoods where violent extremists recruit. Separately, in the same region, we run an interactive SMS program to reach populations in inaccessible areas.

Another major difference from previous efforts is that the GEC uses state of the art digital analytics tools from the Intelligence Community, the Defense Advanced Research Projects Agency (DARPA), and the technology sector. These tools and technologies help us tailor messages to our audience and measure impact.

Based on that approach, there is a particular focus on changing audience behavior instead of attitudes and beliefs. While we may have less success in altering what an individual thinks, we can be more effective at preventing individuals from turning their beliefs into violence.

I appreciate this committee's oversight and continued support as we have revamped our fight against violent extremism in the information space.

As you all know, any long-term strategy to counter violent extremism cannot focus only on killing terrorists; it also means preventing the

recruitment of new ones. That is why successful execution of our mission is so important.

Thank you. I would be happy to answer your questions.

**ISIS Online: Countering Terrorist Radicalization &
Recruitment On the Internet & Social Media**

**U.S. Senate Committee on Homeland Security,
Permanent Subcommittee on Investigations**

Testimony by Peter Bergen

July 6, 2016

Peter Bergen, ~~Vice President~~ Vice President of International Security and Fellows Programs, New America, Professor of Practice, Arizona State University and CNN National Security Analyst. Thanks to David Sterman of New America for his help in preparing this testimony.

This testimony will consider, first, the reach of ISIS online propaganda; second, the profile of ISIS' Western and American recruits, third, the content of ISIS propaganda and fourth, how might that propaganda be countered.

1. The reach of ISIS propaganda in the U.S.

Early in the morning of June 12, 2016 a strange call came into the 911 operators in Orlando. The caller said, "I wanna let you know, I'm in Orlando and I did the shootings... My name is, I pledge of allegiance to Abu Bakr al-Baghdadi of the Islamic State." The caller then abruptly hung up. Shooting his victims with a legally purchased military-style assault rifle inside the Pulse nightclub in Orlando, the mystery 911 caller, Omar Mateen, paused to speak on the phone to a police negotiator, describing himself as an "Islamic soldier" and demanding that the United States "stop bombing Syria and Iraq." He also claimed that he was wearing an explosive-laden vest, similar to those worn by the ISIS terrorists in Paris who had killed 130 people eight months earlier. Just so there would be absolutely no ambiguity about his affiliation, Mateen also called a local TV station and told a producer that answered the phone that he was carrying out his attack for ISIS.

In an audiotape posted online, one of the leaders of ISIS had three weeks earlier urged that sympathizers of the group should carry out attacks in the West during the holy month of Ramadan, which was by now in full swing. Omar Mateen was a regular consumer of ISIS propaganda.

Before police shot Mateen dead around 5 a.m., three hours into his murderous spree, he had killed 49 and wounded 53. It was not only the worst terrorist attack on American soil since 9/11, it was also the deadliest mass shooting in the United States. The attack was emblematic of the problem that the United States faces from "homegrown" militants today, more than three quarters of whom are active on jihadist websites; almost all of whom identify with ISIS, and a number of whom have attempted or succeeded in carrying out lethal attacks in the States following ISIS' commands. None of these "homegrown" terrorists have had any formal connections, training or financing from ISIS. In other words, *ISIS is crowdsourcing jihadist terrorism in the States.*

So what's the level of threat in the States?

Unfortunately, ISIS' English-language propaganda is finding a number of takers in the United States. The FBI says that there are ISIS terrorist investigations in all 50 states, and that there are about 900 terrorism investigations in progress, the majority of which are ISIS-related. During 2015 there was also an unprecedented spike in terrorism cases in the States with more than 70 – mostly ISIS related – during the year, the most cases in any year since 9/11.

Over the past year and half, there have also been six ISIS-inspired attacks in the United States. The most lethal was in Orlando in June. Another lethal attack occurred in San Bernardino, California, in December, when a married couple attacked office workers attending a holiday party killing 14.

In the fall of 2014, Zale Thompson allegedly attacked police officers with a hatchet in New York. He is believed to have been inspired by ISIS. Last May, gunmen inspired by ISIS and also in direct contact with members of the terrorist group, opened fire at a cartoon contest of the Prophet Mohammed held in Garland, Texas. The gunmen, Elton Simpson and Nadir Soofi, were killed by police. And in November, a student at the University of California, Merced stabbed four people on campus, after visiting ISIS websites. In January, Edward Archer allegedly shot Philadelphia police officer Jesse Hartnett. Archer told police, "I pledge my allegiance to the Islamic State, and that's why I did what I did."

The good news, though, is that we are not so far seeing Americans trained by ISIS in Syria in paramilitary tactics then returning to the United States as we have seen with the multiple French and Belgian recruits to ISIS, including those who carried out the Paris attacks that killed 130 in November.

James Clapper, the U.S. director of National Intelligence has said that at least 6,900 militants from Western countries have traveled to Syria since 2012. But relatively few of these are Americans, and only seven have been publicly identified as having returned to the United States. Of these, one returned to Syria to carry out a suicide attack in 2014, and one has been charged with attempting an attack on the United States. Abdirahman Sheik Mohamud of Columbus, Ohio is believed to have

left for Syria in April 2014 and fought there before returning to the United States around two months later. The government alleges that before he was arrested he discussed some kind of plan (with an informant) to kill American soldiers at a military base in Texas. Mohamud has pleaded not guilty.

All this suggests that while continued ISIS-inspired attacks are certainly a very strong possibility in the United States, they would likely be "lone wolf" attacks in which the perpetrator has no formal links to ISIS and has had no training from the terrorist group. The lack of ISIS training generally makes these lone wolves less lethal than the trained killers we saw in Paris.

What U.S. counterterrorism officials are particularly concerned about is what they term a "blended" attack in the States, which is both inspired by ISIS but also directed by the terrorist organization. Under this scenario, an American recruit inspired by ISIS might reach out directly to members of ISIS in Syria over an encrypted social media platform, seeking some kind of specific directions for an attack.

We already saw a harbinger of this last May, when the FBI says one of the two ISIS-inspired militants who attacked the Prophet Mohammed cartoon contest in Texas sent more than 100 encrypted messages to an ISIS terrorist in Syria.

How does ISIS crowd source jihad in the States?

As FBI director James Comey noted when referring to the 2013 arrest of Terry Loewen, who was accused of plotting an attack on Wichita airport in Kansas, "We have made it so hard for people to get into this country, bad guys, but they can enter as a photon and radicalize somebody in Wichita, Kansas." The "photon" Comey was talking about was, of course, the Internet. The only profile that tied together American militants drawn to the Syrian conflict is that they were active in online jihadist circles. More than three quarters were posters of jihadist material on Twitter or Facebook, or were in direct contact with ISIS recruiters over social media.

This raises the question of how we should conceptualize lone wolves in the age of social media. A militant radicalizing in front of his or her computer by himself at home is now not really alone. He/she is swimming in a virtual sea of jihadist

recruiters, cheerleaders, and fellow travelers who are available for interaction with him or her 24/7. Contrast this with a classic lone-wolf American terrorist of the past such as the Unabomber, Ted Kaczynski, who mailed his targets more than a dozen bombs between the late 1970s and the mid-1990s that killed three people and injured some two dozen others, all in service of his obscure, Luddite beliefs. Kaczynski did this entirely by himself while living like a hermit in a remote cabin in Montana with—forget the Internet—no electricity.

Today's lone wolf is instead plugged into a vast self-referential and interactive ecosystem where he or she can virtually, instantly find thousands of other people around the world who share his or her beliefs. Take the case of Alex, a twenty-three-year-old sometime Sunday school teacher living in a remote part of Washington State who converted to Islam. In 2015 multiple members and fans of ISIS spent thousands of hours online with her, promising that they would find her a suitable husband and even sending her gifts of chocolate and books about Islam. Three teenage Khan siblings from Chicago were in regular touch with virtual recruiters in Turkey and Syria and militants in the United Kingdom before attempting their emigration to the caliphate in 2014. In the useful formulation of the Israeli counterterrorism expert Gabriel Weimann, the lone wolf is now part of a virtual pack.

2. Who are ISIS' Western and American recruits?

Who exactly are the estimated 6,900 Westerners who have been drawn to join ISIS and other militant groups in Syria? To provide some answers to that question, New America collected information about 715 individuals from 26 Western countries who have been reported by credible news sources as having left their home countries to join ISIS or other Sunni jihadist groups in Syria or Iraq. The Western fighters drawn to Syria and Iraq represent a new demographic profile, quite different than that of other Western militants who fought in Afghanistan in the 1980s or Bosnia in the 1990s.

First, women are represented in unprecedented numbers. One in eight of the militants in New America's data set are women. Women were rarely, if at all, represented in previous jihadist conflicts. While Western women are not going to fight in the war in Syria, they are playing supporting roles, often marrying front-

line fighters and sometimes working as a kind of police officer enforcing ISIS's draconian laws. They are women like Sally Jones, 44, from the United Kingdom, who took her 10-year-old son to Syria in 2013, and Emilie Konig, 31, one of the first women to leave for Syria, who left France and her two children behind in 2012 to join her husband there. The U.S. State Department says both women have encouraged terrorist attacks in their native countries, and it has officially designated both of them terrorists.

Second, the recruits are young. The average age of Western volunteers drawn to the Syrian jihad is 25. For female recruits, the average age is 22. Almost one in 6 are teenagers, almost than a third of whom are female.

Third, many have familial ties to jihadism. More than a third of Western fighters have a familial connection to jihad, whether through relatives who are also fighting in Syria and Iraq, through marriage or through some link to other jihads or terrorist attacks. For instance the father of British ISIS recruit Abd el-Majed Abdel Bary is Adel Abdel Bary, who was convicted in New York for his role in the 1998 U.S. embassy bombings in Kenya and Tanzania. Of those with a familial link, about one third are through marriage, many of them marriages between female recruits and male fighters conducted after they arrive in Syria. Almost half of Western fighters with familial ties to jihad have a relative who has also left for Syria. For example, the Deghayes family in the United Kingdom had three sons, ages 16 to 20, fighting in Syria together.

Fourth, the Americans drawn to the Syrian jihad -- 250 who have tried or have succeeded in getting to Syria -- share the same profile as the Western fighters overall: Women are well-represented, and the volunteers are young, and many have family ties to jihad. One in seven of the Americans drawn to the Syrian conflict are women. The average age of the American militants is just under 25, with a fifth still in their teens. Almost a fifth of the American militants have a familial connection to jihad. The American recruits are, perhaps unsurprisingly, particularly active online: More than three quarters of the American militants were active in online jihadist circles, posting jihadist material on Twitter or Facebook, or were in direct contact with ISIS recruiters over social media.

Fifth, for Western militants, the wars engulfing Syria and Iraq have often proved deadly. Almost half of the male fighters and 8% of the female recruits have been killed in Syria or Iraq.

Sixth, few of the Western fighters who have traveled to Syria and Iraq are in government custody. Only one-fifth of Western fighters in New America's data set are in custody, and almost two-fifths of individuals are still at large. The remaining two fifths are dead.

Seventh, overwhelmingly the most popular route to Syria is through Turkey. Almost forty percent of the Western foreign fighters made their way to Syria or Iraq via Turkey. Only one of the militants is documented as attempting to use an alternative route via Lebanon. For the rest of the Western militants, it's not clear from the public record how they arrived in Syria.

Eighth, where an affiliation can be determined, the majority of the Western fighters have joined ISIS: More than three-fifths have joined ISIS, fewer than one in ten joined al-Qaeda's Syrian affiliate Jabhat al Nusra, and the others joined smaller groups or their affiliation is unknown.

3. The content of ISIS propaganda

A review of ISIS propaganda shows a diverse mix of motivations and themes that ISIS uses for its recruiting strategy. These include:

- Opposition to the Assad regime;
- The spiritual benefit of participating in jihad;
- The religious duty to live in the caliphate;
- Anger at Western society;
- Objections to U.S. foreign policy;
- Glorifying attacks carried out in the West to inspire others to action;
- A comfortable life with ISIS that includes being paid; free groceries and free medical care;
- We are victorious:
- The "coolness," and even romance, of holy war.

In July 2014 ISIS began publishing its online, English-language magazine, *Dabiq*, which is now in its 14th iteration, (the most recent edition was released in April). Articles in *Dabiq* report on the group's military activities as well as aim to reassure readers that ISIS is an actual state that provides social services and maintains infrastructure. One issue of *Dabiq* included photos with captions showing "services for Muslims," including street cleaning, electricity repairs, care homes for the elderly, and cancer treatment centers for children. The first issue of *Dabiq* even had a sort of classified ad for "all Muslim doctors, engineers, scholars, and specialists" to come and join ISIS. (ISIS has also launched similar magazines in Russian, French, and Turkish.)

ISIS initially downplayed the merits of "homegrown" extremism, concentrating on wooing its "foreign fighter" recruits to travel to join the "caliphate" in Syria. Whereas al-Qaeda in Yemen's *Inspire* webzine focused largely on inspiring attacks in the West, ISIS' *Dabiq*, which models itself on *Inspire* in many ways, was initially geared more toward perpetuating ISIS's successful insurgencies in Iraq and Syria. *Dabiq* encouraged followers to join the jihad; a writer in the third issue of *Dabiq* in 2014 declared, "This life of jihad is not possible until you pack and move to the #Khilafah."

ISIS has disseminated online guidebooks to encourage its Western recruits. ISIS posted online in early 2015 a handy fifty-page booklet, *Hijrah to the Islamic State*. *Hijrah* is an Arabic word that means emigrating for religious reasons. The booklet's jaunty subtitle explained, *What to Packup. Who to Contact. Where to Go. Stories & More!* Inside, ISIS aspirants in the United States and other English-speaking countries could read how to make the journey to Syria. Some of the advice was obvious: ISIS told its would-be recruits not to tell "anyone, even family" of their plans. Other tips were subtler. ISIS suggested that anyone trying to reach its de facto capital in Syria, Raqqa, near the Turkish border, should not buy a ticket to Turkey, as enough "foreign fighters" had already passed through Turkey that this might attract attention from law enforcement. It instead advised volunteers to buy a ticket for a less "suspicious" vacation spot, such as Spain or Greece, buying a ticket to Turkey once they arrived there.

ISIS recommended bringing a sleeping bag and a good backpack with plenty of pockets “as you will definitely have to move around in *Sham* [Syria] once you get here.” A solar charger for electronics was also advised “since electricity is a big problem here,” as well as a headlamp suitable for use in dark conditions. Because of the cold of the Syrian winter, recruits were urged to pack a good, warm jacket and a “beanie hat.”

Once in Turkey, recruits were told, they would wait in a hotel and make contact with an ISIS facilitator, often a “Twitter contact.” ISIS even helpfully provided the Twitter handles of seventeen ISIS recruiters to whom potential recruits could send private Direct Messages in order to set up their travel from Turkey into Syria. The booklet urged operational security for such messaging, telling recruits to use the Tor browser to disguise their IP addresses, and recommending Androids as “securer” than iPhones.

If asked in Turkey about the purpose of their trip, ISIS recruits were advised to say “tourism.” To give credibility to this cover story, they were urged to bone up on well-known tourist spots. They were also advised not to pack knives that could be used as weapons, or combat boots that might give away their ultimate purpose in Syria. There was also special advice to ISIS “sisters” (female recruits) not to travel as a “pack” on a plane and to “be chill to the airport officers” because “you’re just tourists.”

The group painted an idealized yet accessible picture of life under ISIS’s rule: recruits would receive free housing, electricity and water (but not free gas); they would receive free groceries such as pasta, canned foods, rice, and eggs; they would be given monthly allowances and free medical care; and they would pay no taxes. Presenting itself as a real state with plentiful social services and constructed infrastructure was a smart innovation on ISIS’s part—it made al-Qaeda’s high-flown rhetoric about the restoration of the caliphate seem like concrete reality.

ISIS also promised a place where pious young Muslim men and women could come to find their perfect marriage partner. One of the most active of ISIS’s recruits on social media was a Malaysian doctor in her mid-twenties who had married a foreign fighter she met only once briefly before the marriage ceremony.

The doctor explained in one of her frequent posts in English that no one would force women recruits to marry, and that marriages consummated under ISIS's black banners were truly "blessed." She helpfully noted that the banks of the Euphrates River were "almost every newly married couples' favorite spot."

An ISIS video showed smiling kids taking amusement park rides at a city fairground in Mosul. According to ISIS propaganda, life in the Islamist utopia was, almost above all, *normal*.

Another 2015 ISIS publication, a one-hundred-page booklet titled simply *The Islamic State*, outlined the training regime new male recruits would go through. This included learning how to use "basic firearms" such AK-47s and also "medium heavy" weapons such as machine guns, mortars, and rocket-propelled grenades, as well as "chemical" and "electronic" warfare. ISIS advised that those who wanted to perform a suicidal "martyrdom" operation "are put on a waiting list," implying that there were more volunteers for suicide operations than ISIS could handle. Page after page showed dead militants "smiling," having seen their home in Paradise just before their souls left their bodies. The bodies of these martyrs, the booklet assured, did not decay.

Collectively, ISIS's English-language propaganda machine offered an answer to the big question: Why would anyone in the United States or the West want to give up his comfortable life to join ISIS? Making it look easy might help one overcome practical objections, but inspiration was another matter. The answer for ISIS's recruits was, as for so many militants, the desire to belong to something greater than themselves. In the minds of ISIS's recruits the group was doing something of cosmic importance by defending Sunni Muslim civilians from the onslaughts of the Assad regime. The final, inevitable battle between the West and Muslims would presage the arrival of the *Mahdi*, the Islamic savior, and the victory of Islam; the battle against Assad was its opening salvo.

All this bloviation was made easier to swallow because ISIS was, at least initially, *victorious*. In the summer of 2014 the group released a video showing a bulldozer breaking down the great sand berm that demarcated the Iraq-Syrian border, first established by Britain and France in a secret agreement to carve up the Ottoman

Empire following the end of World War I. This was ISIS's symbolic first step toward expunging all vestiges of Western influence in the Arab world. Al-Qaeda had never controlled such large swaths of the Middle East (a territory by some estimates around the size of the United Kingdom) or ruled over millions of people.

The group has also secured pledges of allegiance from two-dozen militant organizations from around the Muslim world, including in Egypt's Sinai region and Egypt's neighbor Libya, while around 10 other groups have declared some form of solidarity with ISIS. The key to ISIS's success is not the group's military strength — ISIS in Syria and Iraq may number only about 20,000 to 30,000 fighters — but the weaknesses of the regimes where the group is doing well.

Think of ISIS as a pathogen that preys on weak hosts in the Muslim world. In fact, there something of a law: The weaker a Muslim state the stronger will be the presence of ISIS or like-minded groups.

As with all totalitarian regimes, mythmaking became essential to ISIS's rhetorical authority. It celebrated its creation of the purportedly perfect state as a way of enchanting new believers. In a propaganda video released in August 2014, shortly after the group had seized control of key Iraqi cities and declared its official name to be simply the Islamic State, a global brigade of fighters (British, Finnish, Moroccan, South African, Trinidadian) all extolled the wonders of living in the caliphate. Filmed during "golden hour," near sunset, the video showed groups of boys with guns and happy ISIS fighters. An ISIS fighter from South Africa said, "I don't have the words. I don't have the words to express myself about the happiness to be here." The video closes with two boys armed with guns in a park waving to the camera. Text on the screen read, "I wish you were here." In other words, "Yes, we have created an Islamist utopia here on earth! And you should be part of it." Another ISIS fighter helpfully noted, "You can still survive even if you don't speak Arabic. You can find almost every race and nationality here."

ISIS leader Abu Bakr al-Baghdadi has also lent his voice to the effort to recruit foreign fighters. In May 2015, ISIS released an online audio recording of Baghdadi in which he called for all Muslims to make hijrah to ISIS's territory, saying there is no excuse for any able Muslim not doing so.

The establishment of ISIS “caliphate” was a powerful draw for some of ISIS recruits. Hoda Muthana, a 20-year-old woman from Alabama, told her father in a phone call from Syria that she traveled there for missionary work because the caliphate had been declared and every Muslim was required to travel there in order to get to heaven. Before attempting to travel to Syria in 2014, Chicago teen Mohammed Hamzah Khan left a letter for his parents in which he explained “there is an obligation to ‘migrate’ to the ‘Islamic State’ now that it has ‘been established.’” Virginia teen Reza Niknejad called his mother on February 5, 2015, after having reached Syria to join ISIS, telling her about how well he was being treated in the “Khalifah.”

Others have cited feelings of alienation or oppression in Western society. Mohammed Hamzah Khan’s 17-year-old sister wrote a letter to her parents before attempting to travel to Syria, saying: “I could not bear to live in ... the land who’s people mock my Allah, my beloved Prophet...” Muthenna Abu Taubah, a 24-year-old fighter from central London who later died in an accident at a bomb-making factory in Raqqa, the de facto ISIS capital, commented to a BBC reporter: “Look at China—men aren’t allowed to grow beards and Muslims aren’t allowed to fast. Look at France—women can’t wear niqab. Look at the USA and U.K.—you can’t even talk about jihad.”

Based on court records and press reports, New America identified several Western militants acting as online recruiters. Among them are a number of Americans. For instance, Abdi Nur, a 20-year-old from Minnesota, allegedly took on the role of online recruiter after leaving for Syria in the summer of 2014. A complaint filed in November 2015 that charged six Minnesota men with trying to go to join ISIS accuses Nur of acting as an online recruiter and providing encouragement and advice to the men via Kik and other social media platforms from Syria. Another is Hoda Muthana, the 20-year-old American woman from Alabama, who was identified by BuzzFeed as the individual behind the Twitter account Umm Jihad, which encouraged militants to leave for Syria._____

By early 2015, however, ISIS’s message had shifted from “come join the caliphate” to encouraging attacks in the West. Issue seven of *Dabiq* carried a four-page article extolling the virtues of Amedy Coulibaly, who had conspired

with the attackers at the satirical French magazine *Charlie Hebdo* and had recently killed four Jews at a kosher supermarket in Paris. Though he self-radicalized in France, Coulibaly had released a video in which he declared his ISIS allegiance,

"How to Survive in the West" is an ISIS online guidebook about how to "be a secret agent" in a Western country, giving readers tips on the making of Molotov cocktails, cell phone detonators; hiding weapons in secret compartments of vehicles, in the same fashion as gangs; and how to identify and evade police surveillance, even suggesting that readers watch the Jason Bourne film series for tips on employing evasion tactics. Tips also included making sure to have a Western-sounding nickname so as to attract less suspicion and wearing colored contact lenses after an attack to confuse the police. There were also instructions on how to build a bomb using a microwave oven.

Abu Muhammad al-Adnani, the spokesman for ISIS, released an audiotape in late May in which he called for attacks in the Muslim world and also in the West, saying, "Ramadan, the month of conquest and jihad... make it a month of calamity everywhere for the non-believers." ISIS-inspired attackers subsequently struck in the West, first in Orlando where 49 people were killed in the nightclub and, the day after the Orlando attack, an ISIS-inspired terrorist killed a police official and his partner in a town outside Paris.

In 1985 British Prime Minister Margaret Thatcher spoke about terrorism at the annual convention of the American Bar Association. Following a recent high profile hijacking of a TWA passenger jet in Beirut that had received lavish media coverage, Thatcher urged that news organizations, "must try to find ways to starve the terrorist and the hijacker of the oxygen of publicity on which they depend." It's a dilemma that news organizations have grappled with for many decades since. Terrorist attacks are, of course, news, but terrorists also depend on "the oxygen of publicity" provided by the media to spread accounts of their violence.

But what if: *Today's terrorists are the media?* On Friday ISIS militants took hostages at a upscale café in Dhaka Bangladesh and killed twenty, mostly non-Muslim foreigners. During the massacre, the militants sent images of their victims lying in pools of blood on the floor of the café to the ISIS media outlet Amaq,

which posted them for the world to see.

In the past terrorists had to rely on the media to get their messages out, but now they can completely control their own message, from making their own content to ensuring its widespread distribution. Terrorists are now broadcasting their crimes through their own “news agencies” in real time.

Consider also that ISIS produces its own lavish TV productions shot in High Definition and filmed professionally of everything from its murder of civilians, to profiles of its heroic fighters, to the supposedly idyllic life that can be lived under its purportedly utopian rule. The terrorist organization also publishes multiple ISIS webzines in English, French, Russian and Turkish, while ISIS and its supporters maintain many tens of thousands of social media accounts to further propagate the ISIS message. The group also has its own de facto news agency, Amaq, that credibly reports on ISIS own atrocities.

In a new twist of the past three years, ISIS and other jihadist militants are now reporting on their own bloody work in real time. During the Westgate mall attack in Kenya in 2013 in which at least 67 were killed, someone close to the Shabaab terror group was live tweeting details of the attack, which were often far more accurate than any other source. As the assault at the Westgate mall was underway, a Twitter account used by the Somali terrorist group Al-Shabaab tweeted: "The Mujahideen ('holy warriors') entered Westgate mall today at around noon and they are still inside the mall, fighting the Kenyan kuffar ('infidels') inside their own turf."

It was the first confirmation that the attack was the work of Al-Shabaab, and journalists around the world quickly reported this. Crucially, Al-Shabaab then explained in a tweet that the mall attack was going to be a fight to the death in which there would be no negotiations for the lives of the hostages the gunmen had taken: "We'll not negotiate with the Kenyan govt as long as its forces are invading our country, so reap the bitter fruits of your harvest #Westgate." This key aspect of the assault on the mall was also reported globally.

The Westgate mall attack was the first major terrorist attack that was live tweeted by someone close to the perpetrators. In recent weeks we have seen an appalling

new iteration of this trend with the terrorists posting pictures of their victims in real time, as we saw in the attack in Bangladesh on Friday.

Similarly, last month, Larossi Abballa, the ISIS-inspired militant who killed the police official and his partner in a town outside of Paris, immediately after the murders, videotaped himself live on Facebook declaring his allegiance to ISIS. While Abballa was taping this statement, near him was the couple's terrified three-year-old son.

Pledging allegiance to ISIS on Facebook after a murderous attack is now almost routine for terrorists in the West. Omar Mateen, the terrorist in Orlando who killed 49 at the nightclub, pledged his allegiance to ISIS on Facebook as he carried out his attack. So too did the terrorists in San Bernadino in December who killed 14 attending an office holiday party.

One of the big ideas of modern terrorism, from the Munich Olympics of 1972 during which Palestinian terrorists kidnapped Israeli athletes, to 9/11 itself, is to use widespread TV coverage of violent acts to propagate and advance the political ideas of the militants.

Today, terrorists bypass traditional media entirely and they now act simultaneously as the protagonists, producers and propagators of their acts of nihilistic violence.

4. How to Defeat ISIS' Online Propaganda: Eleven Action Items:

There seems to be some conceptual confusion in the U. S. government about what "Countering Violent Extremism" programs are attempting to do: Is it counter-radicalization? Or is it counter-recruitment? Counter-radicalization--turning many millions of Muslims away from radical ideas---seems both a nebulous mission, but also one that may not be achievable. A far more specific task is trying to stop the relatively small number of Muslims who are trying to join ISIS or sign up for its ideology from doing so. From an American national security perspective that is, after all, what we all want to prevent. Thinking "bad" ideas isn't illegal nor has anyone satisfactorily answered how to replace these bad ideas with better ideas.

What follows are some specific action items about how to counter ISIS recruitment efforts that can be undertaken by civil society and the government.____

1. Enlist defectors from ISIS to tell their stories publicly. Nothing is more powerful than hearing from former members of the group that ISIS is not creating an Islamist utopia in the areas it controls, but a hell on earth. The flow of “foreign fighters” to ISIS from around the Muslim world is estimated to be about 1,000 a month. Reducing that flow is a key to reducing ISIS manpower. Muhammad Jamal Khweis, 26, of Alexandria, Virginia, was held by Kurdish fighters after allegedly deserting from ISIS in early 2015. Khweis gave an interview to a Kurdish TV station in which he said: "My message to the American people is: the life in Mosul [the Iraqi capital of ISIS] it's really, really bad. The people [that] were controlling Mosul don't represent the religion. Daesh, ISIS, ISIL, they don't represent the religion, I don't see them as good Muslims."

U.S. prosecutors could throw the book at Khweis for joining ISIS, and he could get 20 years or more, but they also could try something more creative -- a deal in which he tells prosecutors what he knows about ISIS in return for a reduced prison sentence. And one more thing: He would also have to appear before the American public explaining that ISIS is creating hell in the areas it controls.

2. Amplify voices such as that of the ISIS opposition group Raqqa is Being Slaughtered Silently, which routinely posts photos online of bread lines in Raqqa, the de facto capital of ISIS in northern Syria, and writes about electricity shortages in the city. This will help to undercut ISIS propaganda that it is a truly functioning state.

3. Amplify the work of former jihadists like the Canadian Mubin Shaikh, who intervenes directly with young people online, who he sees are being recruited virtually by ISIS.

4. Support the work of clerics such as Imam Mohamed Magid of Northern Virginia, who has personally convinced a number of American Muslims seduced by ISIS that what the group is doing is against Islam.

5. Keep up pressure on social media companies such as Twitter to enforce their

own Terms of Use to take down any ISIS material that encourages violence. Earlier this year, Twitter took down 125,000 accounts used by ISIS supporters, but the group continues to use Twitter and other social media platforms to propagate its message.

6. Keep up the military campaign against ISIS. The less the ISIS “caliphate” exists as a physical entity, the less the group can claim it is the “Islamic State” that it purports to be. That should involve more U.S. Special Forces on the ground embedded with Iraqi and other coalition forces and more U.S. forward air controllers calling in close air support strikes for those forces.

7. Applaud the work that the Turks have already done to tamp down the foreign fighter flow through their country to ISIS in neighboring Syria, and get them to do more. Turkey, which had long been criticized by Western countries for allowing foreign fighters to move through its territory on their way to Syria, has started to clamp down on that traffic into Syria. Those efforts by the Turks are paying off, according to ISIS itself. In early 2015, ISIS posted advice in one of its English-language online publications to would-be foreign fighters, saying, “It is important to know that the Turkish intelligence agencies are in no way friends of the Islamic State [ISIS].”

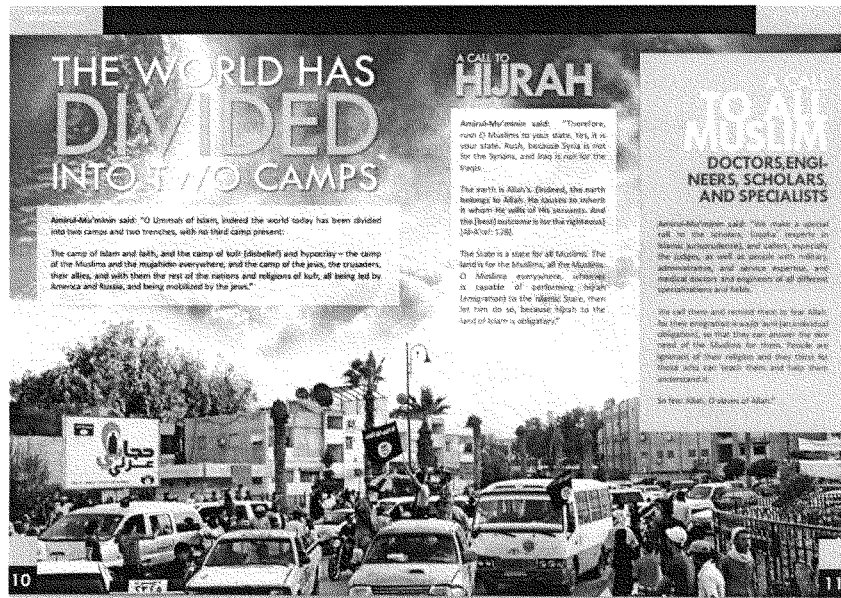
8. Provide “off ramps” to young ISIS recruits with no history of violence, so that instead of serving long prison terms for attempting to join ISIS — as they presently do in the United States — they would instead serve long periods of supervised probation. This will help families that presently face a hard choice: If they suspect a young family member is radicalizing and they go to the FBI, that person can end up in prison for up to 15 years on charges of attempting to support ISIS; but if they don’t go to the authorities and their child ends up traveling to Syria, he or she may well end up being killed there. Providing off-ramps would offer families a way out of this almost impossible choice.

9. Educate Muslim-American parents about the seductive messages that ISIS is propagating online.

10. Relentlessly hammer home the message that ISIS positions itself as the defender of Muslims, but its victims are overwhelmingly fellow Muslims.

11. Build a database of all the foreign fighters who have gone to Syria to fight for ISIS and the al-Qaeda affiliate there, the Nusra Front. This is one of the recommendations of the House Homeland Security Committee's September 2015 report on foreign fighters in Syria and it is a very good one. How can you prevent an attack by returning foreign fighters if you are not cognizant of their names and links to ISIS? Right now INTERPOL has a list of some 5,000 foreign fighters, but that is simply dwarfed by the estimated 30,000 foreign fighters who have gone to fight in Syria.
12. Either through electronic warfare or other means find and destroy ISIS' media production arms.

ISIS Online: Countering Terrorist Radicalization & Recruitment on the Internet & Social Media



Written testimony submitted to the Senate Committee on Homeland Security and Governmental Affairs, July 6, 2016

The Honorable Alberto M. Fernandez, Vice-President, Middle East Media Research Institute (MEMRI), Washington, D.C.

It is particularly fitting to be holding this hearing almost exactly two years from when the Islamic State burst into the global psyche in a spectacular way. An organization that changed its name and altered its focus in 2006 and that has immediate roots going back into Jordan in the 1990s, it is in June 2014, with the double blow of the fall of Mosul and the declaration of the Caliphate that the “State of the Islamic Caliphate” either galvanized or horrified much of the world.

And while June 2014 serves as an appropriate political marker, it also is a key milestone in the evolution of ISIS propaganda. The media output of the Islamic State began to change in 2013, as ISIS moved into Syria and it began to produce better, more multifaceted, multi-language and sophisticated material than it had when it confined its efforts to the struggle in Iraq. But it is in the summer of 2014 that ISIS launches the Al-Hayat Media Center (HMC), focusing on non-Arabic speaking audiences and that the first issue of their online magazine *Dabiq* appears. Indeed, ISIS spokesman Abu Muhammad al-Adnani’s statement announcing the return of the Caliphate was released in June 2014 in Arabic and in English, Russian, French and German by the HMC.

In addition to evocative material on Mosul and on the Caliphate, June 2014 saw the release of emblematic, high quality productions with original material including two effective videos on erasing the borders between Syria and Iraq, and two music videos (German-English and English-Arabic) combining male acapella singing and the sounds of the battlefield. Also released in June was the recruitment video “There is No Life Without Jihad” featuring British and Australian ISIS members, with the memorable line that the “cure for (Western lifestyle induced) depression is Jihad.” This English language production was, not surprisingly, heavily covered in the Western media.

All this material was aggressively pushed out across all social media platforms but especially on Twitter with hashtags such as #AllEyesonISIS. Amazingly, none of this material nor the diffuse online networks amplifying and embroidering on the material were taken down at the time with social media companies, government and law enforcement deciding – for different reasons – not to do so. At the time, individual supporters of the Islamic State, including in the West, openly proclaimed their allegiance, churned out tens of thousands of tweets and aggressively promoted ISIS materials without negative consequences.

I remember, as then Coordinator of the Center for Strategic Counterterrorism Communications (CSCC), surveying this landscape in June 2014 and asking colleagues, “how do you counter the fall of Mosul and declaration of a Caliphate with a video or a tweet?” Creativity and our rough and ready guerilla attitude so at variance with the way government usually worked could only go so far. The sense

of being heavily outgunned and outnumbered was palpable, both in terms of our own resources and in what everyone else was doing against this adversary worldwide. This was especially true given that the sense in much of Washington – both official Washington and the punditocracy – since the death of Bin Ladin in 2011 and until the fall of Mosul was that the global Salafi Jihadist threat was ebbing, that al-Qa’ida and its franchises (which at the time would have included the Islamic State of Iraq) were contained and on a downward trend, with the threat becoming more localized, inward looking and fractured.

Two years later what has changed? As pioneers in the field, we at the Middle East Media Research Institute (MEMRI) have closely monitored and minutely analyzed Jihadist propaganda for years, long before ISIS became fashionable and so we have been well positioned to track subtle changes over time in the jihadosphere and in the content, style and delivery of ISIS material.

First, a quick survey of ISIS propaganda in June 2016 shows the dimensions of the ongoing challenge. As a graphic example of their continued potency, the Islamic State released 29 separate videos during the month. Interestingly enough, the rival, al-Qa’ida-aligned Nusrah Front (JN) alone in Syria was almost as prolific as ISIS in its video production during this particular month with all of its material being very Syria-centric and localized. So the overall, Jihadist media “pie” has grown and ISIS and al-Qa’ida struggle for dominion. Both Nusrah’s production and that of ISIS were overwhelmingly in Arabic. ISIS releases that month included videos produced by ISIS *wilayat* in Aleppo, Raqqa, Ninawa, Dijla, Al-Furat, Al-Khayr, Salah al-Din, Al-Jazira, Fallujah, Anbar, Homs and Khurasan.

Videos included the bloody execution of “spies” and journalists, praise for the Orlando terrorist attack, repeated calls to attack the West, the announcing of a new ISIS *wilaya* in the Philippines, the second anniversary of the declaration of the “Caliphate,” and, of course, footage on daily life in ISIS territory, on Ramadan, and of combat operations. While the production was prodigious and of a high quality, a considerable amount of the footage was recycled stock image previously used in other products. There were no real videos of military victory because the Islamic State had none to claim.

Given the intimate connection between the political-military reality in the region and its projection onto the virtual world, the biggest change from two years ago is the continuation of a series of increasingly important military reverses on the ground which began with the retaking of the Mosul Dam in August 2014 and are ongoing with recent key milestones such as the taking of Fallujah and Manbij by local forces working with the international coalition. Slowly, all too slowly perhaps, the Islamic State “victory narrative” is being deflated although ISIS

propagandists have ably sought to obscure this to date by highlighting other events, such as the work of international franchises, spectacular overseas terrorist operations, and topics related to the implementation of Islamic governance in the territory it still controls. Despite Al-Adnani's important May 23, 2016 remarks preparing the ground for the possibility of future reverses, the overall impression Islamic State propaganda still projects is, not surprisingly, one of assured confidence in victory and in their steadfastness. An important fact for us to deal with is that they are still doing a better job at projecting strength while slowly retreating than ISIS's enemies have done while slowly advancing.

The recent military successes in Manbij and Fallujah underscore the challenge that our allies have in even reporting good news. The technical quality of material released by both the Syrian Defense Forces and the Iraqi military still does not match that of the basic ISIS video but more concerning is the overall context. Both events, but especially the Fallujah operation, occurred within the context of heightened sectarian and ethnic discourse in both social and broadcast Arabic-language media.

This is an example of where the broader sectarian (Sunni-Shia) conflict raging in the Middle East reinforces the overall ISIS narrative. It wasn't so much the Islamic State pushing that narrative on Fallujah (ISIS supporters certainly did do that) but media outlets and voices ostensibly opposed to and independent of ISIS that did so.

Rather than being portrayed as a success for a united Iraq and an Iraqi Security Force liberating everyone against ISIS brutality, the narrative on pan-Arab media, especially, and incessantly on Al-Jazeera, was about the sectarian nature of the siege, and the suffering of Fallujah's Sunni Arab Muslim civilians even after the fall of the town. By one account, if you followed only Al-Jazeera for your news, you would have thought that Iraqi Security Forces had suffered more than 1400 dead in the battle for Fallujah while ISIS was reported as suffering less than 40 dead.

And while Al-Jazeera tends to be particularly sectarian – and has a long, controversial track record on Fallujah – it must be said in their defense that many in the Western media made very similar points, at least about civilians. The graphic language and sectarian imagery used by some PMU militias before and during the taking of the city provided ample ammunition for the critics.

Shiites in outskirts of **Fallujah** Cursing Aesha R.A by showing a **shoe** towards her name



Even what should have been an unalloyed propaganda bounty can be muted by confusion. The destruction of an ISIS convoy fleeing Fallujah in the last few days did just that with US spokesmen speaking of the destruction by American and Iraqi aircraft of over 175 vehicles in two convoys while the head of the Iraqi Air Force spoke of over 700 vehicles. Some of the coverage suggested that there may have been at least a few civilians mixed in with fighters, a fact acknowledged by Americans and denied by Iraqi military spokesmen.

This is not to deny the overall success of taking Fallujah from ISIS, nor its real propaganda value. An ISIS defeat is a defeat even if not handled perfectly. And even with the overblown rhetoric, the very real concerns about human rights abuses of Fallujah's civilian population and the skewed regional coverage, showing ISIS losing is a key element in the propaganda battle. But at the very least, this is a victory which could have been more complete and convincing in influencing the basic ISIS demographic of Sunni Arab Muslims inside and out of Iraq. A more successful example of quality media coverage that was both convincing and riveting was Vice News embedding with the Iraqi Golden Division's Special Forces on the "Road to Fallujah"

(<https://news.vice.com/video/fighting-the-islamic-state-with-iraqs-golden-division-the-road-to-fallujah>) in June 2016. This news product captured some of the

edginess and immediacy of ISIS videos and also portrayed a picture of Iraqi government forces that was nuanced but mostly positive.



Cahida Dersim @andersin3 Jun 4
Notes from #Manbij. Two Arab women smoke the first cloarette after their villages was liberated from ISIS by #SDF

The equally important but more modest operation in the taking of Manbij was better handled as far as overall spin is concerned. Manbij was a far less sectarian issue than Fallujah, of course, (with less overheated regional media rhetoric) and the Syrian Democratic Forces/YPG use of the “Manbij Military Council” was a smart move to at least give a stronger impression of Sunni Arab and other non-Kurdish involvement and highlighting the positive voices of liberated local people (https://www.youtube.com/watch?v=k5ChxobTh8o&index=2&list=PLNxxX7r4A554rJNXnTIO5_7rAPGqVNol0). Again, one would have liked to have seen greater technical quality, more volume and more compelling stories and packaging but Manbij was an ISIS safe haven much used by foreign fighters, including a strong contingent from Western Europe, so a strong message has been sent by the inability of the Islamic State to hold on to it.

So two years later, ISIS propaganda is still being extensively produced. The continued pummeling of the Islamic State territory in Syria, Iraq and Libya should eventually puncture the ISIS victory narrative and weaken some of its appeal. Still another positive factor has been the shrinking of the ISIS online presence in social media. An unprecedented terrorist media success like the Islamic State still has a considerable footprint, still gets its message out and still influences but today ISIS publicists online are more contested, more frequently shut down than ever before.

They stay on for shorter periods and their ability to build large stable online networks has been interdicted.

J.M. Berger has estimated recently that the median follower count of a typical ISIS support twitter account is down about 90% from 2014. The Twitter hashtags for the delivery of Adnani's May 2016 speech were rapidly interrupted and the material removed or feed corrupted. It is a far cry from the halcyon days of 2014 when ISIS supporters felt themselves invincible and numerous. MEMRI has tracked this over the past year as the decline of the ISIS presence on Twitter has been coupled with rapid rise of Telegram as an alternate platform. Since October of 2015, 35% of our material comes from Telegram, 34% from Twitter. 10% from Internet Archive, 7% from YouTube and 10% from Jihadi forums. Facebook as a source declined from 25% to 2%.

Telegram today is probably the single most important online safe haven for ISIS. In a recent discussion by ISIS supporters that we at MEMRI monitored, one infamous ISIS fanboy described Telegram as his "hideout" and lamented that he wasn't able to keep up with the many suspensions on Twitter. "Remember Twitter back in 2014 when we hijacked hashtags and spread the news for the entire world," he noted wistfully. So the efforts of social media companies, of government agencies and of people of good will everywhere to take down ISIS material, to challenge it, and to mock it is having some effect in terms of the viability of their stable presence online.

But this success is not permanent. Only two days ago, on July 4th, the Al-Wafa Foundation, a pro-ISIS media outlet, produced an article calling on ISIS supporters to return to Twitter and Facebook and not limit themselves to Telegram. The author praised the advantages of Telegram, especially its policy of avoiding the mass suspension of Jihadist accounts but lamented that it is not as conducive as other platforms for rapidly and broadly spreading ISIS content.

We are also seeing a growing ISIS member/supporter presence on Instagram even after some are suspended. This community seems to include militants and friends from places as diverse as Malaysia, Indonesia, Chechnya and Turkey. Instagram is a valuable secondary tool for these extremists because of the power of its visuals and accessibility. There is also a real extremist presence on Snapchat and we recently documented an English language blog on Tumblr run by ISIS medical personnel with the purpose of encouraging doctors to flee to the Islamic State and providing them with practical information on how to prepare to do so.

But while jamming ISIS hashtags with rainbow flags and porn or generating disinformation about the fate of Al-Baghdadi through bogus Amaq News Agency

accounts are perfectly legitimate, even better is disseminating content that actually adds something to the anti-extremist discussion. Content that does not just distract or confuse but inform is also key. In this field, the establishment of initiatives such as the International Center for the Study of Violent Extremism (<http://www.icsve.org/>) in July 2015 which documents the voices and stories of ISIS defectors and recanters is worthy of continued support by both public and private partners. It is particularly effective to have such material tracked and disseminated by the private sector and by independent media rather than directly by governments.

Despite the progress made in this area over the past year, there are still more unheard stories of the ISIS disaffected that need to be captured, as well as those of the many Sunni Arab Muslim victims of ISIS brutality. Obviously all victims of terrorism are worthy of respect and solidarity but we are talking here about the use of victim narratives in a way that could influence the key demographic from which ISIS draws support and which are of greatest concern to us: Sunni Arab Muslims and members of Muslim diaspora communities in the West.

How many Western Muslims, for example, are familiar with the dramatic/horrific stories of Syrian and Iraqi Sunni Muslim tribal resistance to the Islamic State? How many know of the hundreds of Iraqi Sunni clerics killed at its hands over the past decade? How many know of the lives and deaths of young men from the Shaitaat or Albunimr tribes told in their own voices and made available in English or French or German?

There is no one silver bullet or kryptonite in the fight against ISIS propaganda. There is no substitute for the continued steady working away on a variety of political, military, social, economic and ideological fronts. The situation we are in is the result of actions taken, and not taken, over decades by both Western governments and Middle Eastern ones. If progress has been made on the battlefield and in the realm of cyberspace and in the stories of defectors, what then are the great lacunae, the things we are still missing?

We must recognize that while the physical Islamic State in Syria and Iraq may be on a slow slope towards eventual decline it has also, in a very important way, already succeeded. It has succeeded in creating – for a small, but not inconsiderable, zealous and deadly clique – a sturdy and mature revolutionary brand that still endures and inspires. Of particular concern to our own homeland security ISIS and its fans, as a lively and defiant English-language sub-culture, is still here and still largely impervious to obvious subverting. These are not going to be deterred by rainbow flag spamming.

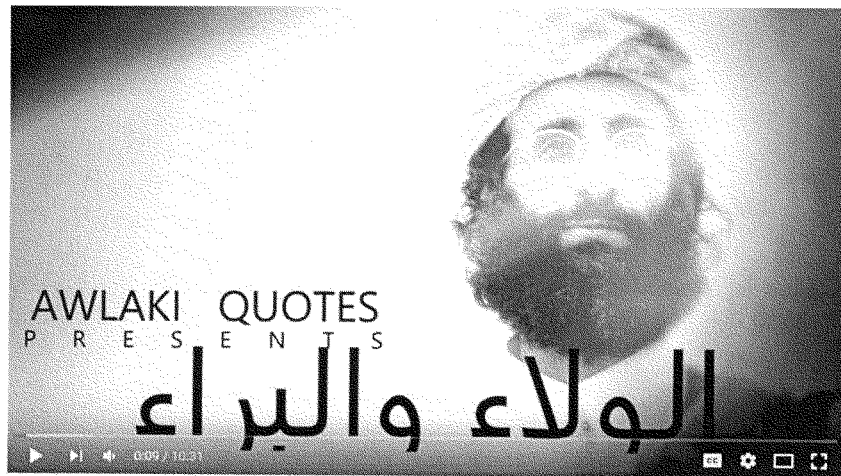
MEMRI recently documented the creation of an ISIS supporters' matrimony group on Telegram in June 2016. Initially the group was called "Baqiya Matrimony" but was soon changed to the less conspicuous "Love Fillah." While some commentators initially reacted angrily that this must be some sort of Western plot, the organizers reassured that this was not the case and posted a sarcastic meme related to security with a young Muslim man saying "Salaams, beautiful sister. I'm planning to join ISIS soon. Do you love me?" To which the answer comes, "Yes, I do love you coz I'm an FBI agent and you are going to jail."

"Baqiya Matrimony" is just one small brick in a larger Baqiya Family edifice that is a lasting result of all those intensive ISIS mobilization efforts of the past years. Some of it may seem ridiculous and some may be deadly, but this is now a brand which has to a large extent already been internalized. The commitment, identity, distinctiveness and autonomy of this ISIS subculture (whether online or not) is intimately tied to an innate understanding of the ISIS brand and the broader ideology that undergirds it. It is often fully understood and does not necessarily require a new video or new conversation with extremists to be maintained. French ISIS killer Larossi Abballa, who livestreamed the killing of a Paris police officer and his wife in June 2016 put it this way, "Allah said that if you follow the majority of people on earth, they will lead you away from the path of Allah. Through this verse, Allah tells us that there will be only a minority on the right path, thank him and bow to his greatness. Yes, Allah has chosen you and not all the other billions of people."

Whether in the form of mere identity groups and propagandists or as actual DIY terrorists in places like San Bernardino and Orlando, the ISIS brand can be all things to all extremists, a rallying cry to rebellion clothed in the language of righteous violence. It makes everything "better" and more purposeful, making what might have just been the seamy and sad violence of a lost soul into something transcendent, translating what would purely be the local and the personal into part of a larger whole that is global and ideological. This shouldn't come as much of a surprise: the ranks of the Islamic State today are full of former petty criminals and troubled people who have finally found purpose in life. And no one epitomized this more than Abu Musab al-Zarqawi himself, the godfather of what became the Islamic State shortly after his death in 2006.

The neutralization of this pro-ISIS sub-culture is still extremely difficult, except when individuals clearly overstep legal bounds and come to the notice of law enforcement. But aside from that type of preventive action, the ideological building blocks of the ISIS of tomorrow, of the Salafi Jihadist threat 2.0 to come, are still there, fully intact and ready to be redeployed.

As an experiment, I went to YouTube a few days ago and entered in English the name of key themes that are an essential part of the worldview of the Islamic State and other Salafi Jihadist groups. These are Islamic Arabic terms with a rich, nuanced and complicated history over centuries but which extremists have simplified and weaponized and wield with great effectiveness to brainwash the young, zealous and untutored recruit. They are *Kufr* (unbelief), *Shirk* (polytheism or ascribing partners to God), *Al-Wala wal-Bara* (loyalty and disavowal), *Taghut* (tyranny), *Rafidah* (rejectionists, a pejorative term for Shia Muslims) and *Tawhid* (oneness or strict monotheism of God). Except for *Tawhid*, which is the key Islamic doctrine not limited to Salafis, all searches returned results of English-language voices reinforcing the underlying bases of the Islamic State narrative even though none of the voices were of actual ISIS members or supporters. The top entry for *al-wala wal-bara* – the key concept of actively hating non-Muslims and giving loyalty to the (right) Muslims – was by none other than the late Anwar al-Awlaki.



Al Wala wal Bara - Imam Anwar Al Awlaki

Shiraz Maher in his magisterial new book (*Salafi-Jihadism: The History of an Idea*, 2016) notes about this key element in the ISIS/Al-Qa'ida discourse that

“all of this was ultimately shaped to create alternative structures of legitimacy and authority for Salafi-Jihadi actors who typically operate

beyond the framework of the state. It allowed them to delegitimize their opponents for not having displayed adequate levels of *al-wala wal-bara*, while presenting themselves as the custodians of a pure, unadulterated form of Islam.”

So while we fight on the battlefield, and in cyberspace, while we seek to find personal stories that can be useful to the anti-ISIS fight, there is still a larger ideological challenge that needs to be fought more effectively. This is something that most fragile and conflicted regimes in the Middle East are loathe to take on themselves even though the ideological challenge is a direct threat to their survival.

Wouldn't it be amazing if a YouTube search on these incendiary topics brought back returns which did NOT fit in so well with the ISIS narrative? So that the young, searching American youth, struggling with identity issues and conflicting emotions and driven to look for knowledge in this most modern and personal of ways might have a better chance?

A potential project worth funding would be to find some smart, tech-savvy American Muslim civil society group that can come up with better, more tolerant and convincing, answers for those searching for these terms and make sure that the algorithm is in place for them to be easily accessed.

One can, and should be, cautiously heartened by much of the work the Federal Government, our allies, the private sector and community organizations have done over the past couple of years, once reality hit them on the forehead in 2014, in the fight against ISIS, including in the key field of online communications used to radicalize and recruit individuals. Progress has been made in removing content, in contesting or crowding the space, and in kinetic operations. But that is not enough.

Much of the information surrounding the new inter-agency Global Engagement Center (GEC), the newest iteration of the old CSCC I headed, seems to be White House spin directed at a gullible public by repackaging old duties and mandates in new verbiage. There is also perhaps entirely too much emphasis on transitory GEC events, such as hackathons and coordination meetings, which add too little to the fight and not enough on building a permanent and professional organization dedicated to what is clearly going to be a generational fight.

One question evidently not clarified by the new March 2016 Executive Order creating GEC is whether this is actually an organization with a dedicated, line item budget appropriation or whether it is – as was the case until 2015 – an organization funded entirely out of the discretionary budget of the State Department's Under-Secretary for Public Affairs and Public Diplomacy (“R” in State Department parlance) and emergency funds of other organizations.

I am encouraged, however, by some of GEC's work, especially in promoting voices of defectors and discrete funding of proxies but wonder if its long-term mission would be better served as part of the more integrated Counter-Terrorism Bureau (CT) at State rather than under R, traditionally a weak performer in the Department's leadership. Such a move could also shield GEC somewhat from the temptation of micro-managing from aspiring White House communications czars.

While ISIS may have peaked as a formal organization in its Syrian-Iraqi heartland, the ISIS style, especially its style of violence, has not yet done so and still shows great potency and staying power. It is incumbent on us, at the very least, to keep the pressure on social media and to try to shrink and hem in its presence there as much as possible while trying to change facts on the ground in the region - particularly the very public destruction of the ISIS "Caliphate" - and come up with better answers to its powerful toxic narrative of empowerment, grievance and faith. This is, after all, a narrative largely shared by its bitter rivals in al-Qa'ida.

While I have dwelt at length on the ideological challenge of the Islamic State, a cocktail strong enough to inspire well educated, upper class boys in Dhaka to stab total strangers to death a few days ago, this challenge is, of course, expressed powerfully through narratives. And what is a narrative but a story? As Hassan Hassan relates in his recent seminal work on ISIS's hybrid ideology:

"The Islamic State relies heavily on stories and events from Islamic history because they can be more powerful than the citation of Islamic principles, especially if the stories and events support Quranic verses or hadiths. The group makes the most of any example it can find, and borrows from what Muslim clerics consider isolated incidents that should not be followed as rules. It uses stories not always to argue a religious idea: they may be offered to help Islamic State members who struggle with committing acts of extreme violence."

In 2014, ISIS used the slaughter of the supposedly rebellious Jewish Beni Qurayza tribe in Medina, exterminated at the time of the Prophet Muhammad, to justify the slaughter of the rebellious Syrian Sunni Muslim Shaitaat tribe. As George Orwell wrote, "he who controls the past controls the future. He who controls the present controls the past."

We are doing much to fight the Islamic State, but little is being done to reclaim Islamic history and it's telling from them. While this is a task best left to Arab Muslim regimes and individuals (despite its affiliates and worldwide supporter, ISIS is overwhelming an Arab Muslim organization influenced by that society), the great and deadly unwinding of existing Arab regimes, the ongoing crisis of

authority happening in the region means that these governments may not be capable enough to pull this reclaiming of the narrative off.

One last word about narratives. The ISIS narrative is indeed a powerful, revolutionary one but we must never forget that one of the blessings of the United States of America is that we have our own powerful narrative. In this we are fortunate indeed compared to some Western countries in the world struggling for meaning in a seemingly untethered, post-modern world.

As an immigrant and a refugee myself, I tell you that the American identity, pride in our country, in its past and in its future, identification with its propositions and in its symbols, its inclusiveness and its power for good in the world, is something to be nurtured, to be supported and promoted as an important ideological safeguard for both native born and immigrant Americans. Such a patrimony is something of value in the world today. And that unity of purpose, patriotism, and social harmony is of great importance to us and to the world in this ongoing bitter struggle that has some years yet to run.



The American-Arab Anti-Discrimination Committee

**Written Testimony to the
United States Senate
Homeland Security and Government Affairs Committee
Subcommittee on Investigations**

on

ISIS Online: Countering Terrorist Radicalization & Recruitment on the Internet & Social Media

Yolanda Rondon, Esq., ADC Staff Attorney
American-Arab Anti-Discrimination Committee
1990 M Street NW Suite 610
Washington, DC 20036
Phone: (202) 244-2990
Fax: (202) 333-3980
E-mail: legal@adc.org
Web: www.adc.org

Dear Chairman Rob Portman and Ranking Member Claire McCaskill:

I am writing to you on behalf of the *American-Arab Anti-Discrimination Committee (ADC)*, the nation's premier Arab-American civil rights organization. ADC is a secular, non-partisan grassroots civil rights organization founded in 1980 by former U.S. Senator James Abourezk. ADC has protected the Arab-American community for over thirty five years: (1) defending and promoting human rights, civil rights, and civil liberties of Arab Americans and other persons of Arab heritage, (2) combatting stereotypes and discrimination against and affecting the Arab-American community in the United States, (3) serving as a public voice for the Arab American community in the United States on domestic issues, (4) educating the American public in order to promote greater understanding of Arab history and culture, and (5) organizing and mobilizing the Arab American community in furtherance of the organization's objectives.

ADC routinely works with a broad coalition of national organizations to protect the rights of communities of color in the United States. ADC has standing commitment to open government, and government transparency and accountability. ADC opposes surveillance, racial and religious profiling, and interference with Constitutional rights, particularly the First Amendment, Fourth Amendment, and Fourteenth Amendment. The constitutional, civil and human rights of Arab Americans are more than ever at stake. ADC respectfully takes this opportunity to provide a statement for the record with comments regarding the Subcommittee's recent hearing titled *ISIS Online: Countering Terrorist Radicalization & Recruitment on the Internet & Social Media*.

ADC understands the government's position of thwarting terrorist attacks. However, the sentiment that occurred during the congressional hearing was over-simplistic. It was stated that individuals follow a fixed trajectory towards violent extremism that starts with and is further promoted through online propaganda. A hypothetical stated in the hearing that Alberto Fernandez cites is that of a confused and vulnerable 17-year-old teenager who merely searches terms relating to the Arab world on YouTube, only to be met with violent video results. The hypothetical continues to suggest that these video results will serve as the catalyst that will radicalize this teenager.

Academics have long discredited the above proffered radicalization theory. There is absolutely no statistically significant evidence to prove that there is a link between extreme ideas as indicative of conduct, behavior or commission of a violent act. To put it simply—consuming violence or extreme speech does not make you a criminal. To categorize on any person who views extreme speech or violence under a blanket label of potential “terrorist” influenced by propaganda serves to avoid and undermine the real issues that may cause someone to commit a violent act. Focusing our resources on countering propaganda is ineffective and counterproductive. For example, the United Kingdom implemented a mass initiative to remove terrorist content from the Internet—but still remains a major ISIS recruiting hub.

Resources need to be dedicated to enforcing hate crime statutes, policies and practices that respect human and civil rights, accountability to law enforcement abuse and misconduct, and opportunity to marginalized and underserved communities. Resources and funding, whether for education and afterschool programs, mental health services, employment and job training opportunities, should not be provided under a law enforcement lenses – Countering Violent Extremism (CVE). Federal and local law enforcement community engagement should also not be securitized under CVE.

The congressional hearing focused on the rising threat of 'lone wolf' terror in the Arab and Muslim communities. The exaggeration on the 'lone wolf' threats paves the way to unconstitutional surveillance programs. These programs promote the infiltration of minority and activist communities. Lone-wolf terror represents a risk, but a risk that is similar if not less than risk of any other crime.

Under the CVE programs, government agencies intend to employ defectors of terrorists groups or alleged former violent extremists to provide testimony and use this testimony for outreach efforts. While the existence of a former violent extremist is questionable, measures must be put in place to ensure participants are not incentivized through the CVE economy. Defectors and alleged former violent extremist's testimonials must be vetted for veracity, accuracy, and appropriateness, with adequate restraints on testimonial identification and use. Defectors and alleged former violent extremists should not be compensated or provided any monetary benefits and/or gifts for use of testimonials and/or participation. This is essentially monetarily incentivizing individuals for engaging in criminal activity and begs into question the credibility of such testimony.

The panelists at the congressional hearing failed to provide a concrete explanation of what civil rights and privacy safeguards are in place for the rollout and implementation of CVE programs and initiatives. As the government aims to recruit private and civil society for its CVE programs, we cannot compromise our Constitutional rights and right to freedom of speech. Currently, the government has made request for private companies and technology entities to censor and remove content off the internet. The government has failed to be transparent and forthcoming with its content removal requests and standards for such requests.

UN Resolution 30/15 recognized that "[V]iolent extremism, in all its forms and manifestations, cannot and should not be associated with any religion, nationality, civilization or ethnic group." UN Special Rapporteur Ben Emmerson's February 22, 2016 Report on the Promotion & Protection of Human Rights & Fundamental Freedoms in Countering Terrorism Efforts also articulated serious concerns with implementation of Countering Violent Extremism (CVE) efforts in the educational setting impact on the right to education and academic freedom.

Educators should not be required to act as watchdogs or intelligence officers, nor should they be obliged to act in ways that might impinge the right to education, academic freedom or freedom of expression, thought, religion or belief. Such measures may lead pupils and students to self-censor to avoid being branded 'extremist', cause teachers and other staff to view pupils and students as potential threats or avoid discussing certain issues or inviting guest speakers whose views may be controversial. The lack of certainty about what elements to take into consideration may also lead educators to be overly cautious and needlessly report through fear of sanctions.

Special Rapporteur Ben Emmerson's Report also found that it is essential to address the respect and enforcement of human rights in the context of countering violent extremism.

Key points from the 2016 Special Rapporteur Report:

- Attempts to address violent extremism through security-based counter-terrorism measures have been insufficient to prevent the emergence of violent extremist groups;
- There is no accepted definition of violent extremism;
- Serious concerns arise with use of violent extremism & terrorism interchangeably, & without a clear definition of each & the difference between the terms;

- Too much focus on religious ideology as the driver of terrorism & violent extremism rather than conduct;
- No authoritative statistical data on the pathways towards individual radicalization exist.

Impact on Human Rights of Measures to Counter/Prevent Violent Extremism:

- Limitations on Freedom of Expression & Censorship Online
 - Measures taken to prevent or remove messages communicated through the Internet or other forms of technology constitute an interference with the right to freedom of expression;
 - Bans on the operation of certain sites should not be generic but content-specific. No site or information dissemination system should be prohibited from publishing material solely on the basis that it may be critical of the government or the social system espoused by the government.
 - "[F]reedom of expression applies to all forms of ideas, information and opinions, including those that offend, shock or disturb the State or any part of the population."
 - "Educators should not be required to act as watchdogs or intelligence officers, nor should they be obliged to act in ways that might impinge the right to education, academic freedom or freedom of expression, thought, religion or belief. Such measures may lead pupils and students to self-censor to avoid being branded 'extremist', cause teachers and other staff to view pupils and students as potential threats or avoid discussing certain issues or inviting guest speakers whose views may be controversial. The lack of certainty about what elements to take into consideration may also lead educators to be overly cautious and needlessly report through fear of sanctions."
- Limitations on the Freedom of Movement:
 - Countries must ensure that all persons enjoy the substantive right to nationality without discrimination & violation must have effective remedy & due process protections.
- Targets Persons or Groups Based on Identity or Beliefs
 - Countries counter violent extremism strategies are broad to encompass anyone but in practice are disproportionately applied to target specific groups classified as 'at risk' to violent extremism;
 - Countries strategies to identify individuals, indicators, and who is qualified to refer raise concerns.

The CVE programs and initiatives are actually counterproductive our national security and do not address the root causes of mass violence. Rather CVE securitizes our communities; the security lenses focus on our community for "civic engagement" improperly paints the Arab and Muslim American community as a population that must be controlled, criminals, predisposed to violence and terrorism, or vulnerable to ISIS. Meanwhile the fact is that there have been only approximately 250 American citizens who have been inspired to, and/or travelled to support ISIS overseas. 250 Americans out of nearly 320 million Americans equates to less than 1% of the population (0.00000078%). Thus broad surveillance of Arab and Muslim communities based on identity and not individual particularized facts of an individuals that meet the probable cause legal standard, prevents our law enforcement from actually focusing on the real threats.

The Combating Terrorism Center at West Point found that since 2007 there has been a dramatic rise in the number of violent plots from persons who identify with far-right of American politics. However, the major ideological movements linked to violence varied from "a racist/white supremacy movement, an anti-federalist movement and a fundamentalist movement," but did not include Arabs or Muslims. In fact, the only documented link between Arab and/or Muslim community centers and violent extremism is that mosques were often the targets of violent attacks. The report noted that "the great majority of attacks perpetrated by the racist groups are aimed against individuals or groups affiliated with a specific minority ethnic groups, or identifiable facilities (churches, mosques, synagogues, or schools affiliated with minority communities)." Additionally, the 2014 European Union Terrorism Situation and Trend Report found that the majority of terrorist attacks are committed by separatist groups, rather than particular religious or ethnic groups. The recent acts of terrorism in

Charleston, South Carolina also demonstrate that the model of profiling minority religious and ethnic groups is fundamentally flawed.

The conflation of ideology and religion with violence is a false narrative. Religious, ethnic or behavioral traits cannot be substantively linked to violent extremism. Religion is not an indicator of violence. Targeting Muslims and those perceived to be Muslim including Arab Americans, based on their identity for CVE and other initiative to combat terrorism are not objective measures that actually address mass violence. There should be more focus on resources to address misuse of authority and systematic abuse by law enforcement, and enforcement of hate crime reporting by local and state law enforcement.

CVE and congressional members assert that violent acts can be eliminated by combating radical ideology. The error in this reasoning is that there is no solid connection between radical ideology and violence. There are many people in this country that hold views that can be considered extreme, but belief in such ideas and the perpetration of violence are two separate things entirely. Government agencies cannot be allowed to police ideas, thoughts and beliefs, and restraint should be exercised even as applied to questioning persons about extremist views on immigration applications. Any efforts to curb mass violence must focus on conduct, not identity or belief.

ADC requests this subcommittee to report on the detailed explanations of the initiatives discussed in the hearing by the panelists including but not limited to what training and oversight measures are in place, what are the performance and effectiveness metrics, and evaluation methods for grant applications on civil rights and civil liberties. The speakers stated that there is a need to counter the threat of online propaganda through private and public partnerships, as well as with teachers and schools. The community should know exactly where CVE funding will go and in what form for these online initiatives. The exact terms of partnership and online strategies should be explicitly outlined, and publicly available and accessible including but not limited to the "scorecard" for grant applications.

There are too many unanswered questions about CVE and too many concerns raised by the limited information we do know. We must know everything about what these programs entail, and what safeguards are in place to guarantee the civil rights and civil liberties of all. ADC strongly urges the subcommittee to require government agencies to produce any and all information related to implementation and procedures, groups and organizations funded and how funding used, and require procedures and policies to be set up in place prior to any consideration and grant of additional funding. As the program has largely been operated in secrecy, but been proffered as a community program, Congress and the community must know what is going on before any more money is put into CVE.

**“ISIS ONLINE: COUNTERING TERRORIST RADICALIZATION & RECRUITMENT
ON THE INTERNET & SOCIAL MEDIA”**

July 6, 2016

**QUESTIONS FOR THE RECORD FOR GEORGE SELIM
FROM SENATOR CLAIRE MCCASKILL**

- 1) I understand the Department of Homeland Security’s Office for Community Partnerships (OCP) has a \$50 million budget for Fiscal Year 2016, \$10 million of which will be used for a countering violent extremism (CVE) grant program. Please summarize OCP’s plans for spending the remaining \$40 million of its budget in FY2016.

Response: OCP was not directly appropriated \$50 million in the omnibus; rather, OCP was appropriated \$3.1 million for its operations.

DHS was appropriated \$50 million for emergent threats under three programs:

- \$10 million is for a CVE Grant program that OCP is administering jointly with FEMA Grant Programs Directorate. OCP is in the process of reviewing the grant proposals to make recommendations for awards.
- \$39 million is for an initiative for FEMA to help state and local governments prepare for, prevent, and respond to complex, coordinated terrorist attacks.
- \$1 million is for FEMA’s Joint Counterterrorism Awareness Workshops to help regions improve their counterterrorism preparedness posture, including the ability to address the threat of complex terrorist attacks.

- 2) I recognize that measuring CVE outcomes is difficult. We often can’t prove a negative – that someone wasn’t recruited or didn’t commit an act of terror because of a particular prevention strategy. That said, please describe how DHS officials, the OCP and members of the interagency CVE Task Force plan to measure the success of grant-funded programs.

Response: In general, prevention of and intervention in violent extremist recruitment and radicalization can be measured in a manner similar to preparedness and readiness in emergency management and defense contexts; that is, by measuring and exercising proven capabilities. Currently, only a handful of areas in the country have developed “whole-of-society” prevention planning and intervention capabilities relevant to CVE. The mission of OCP and the Task Force is to enhance those efforts.

Academic research indicates that, among other things, multidisciplinary approaches, buy-in from various elements of society, and developing an infrastructure to intervene with vulnerable individuals contribute to a community's resiliency to violent extremism. OCP and the Task Force will measure how much of the country is covered by such plans and capabilities. They will also measure the reach and impact of messages online and in traditional media that challenge violent extremist recruiters' narratives.

The DHS FY2016 CVE Grant Program is aimed at enhancing resiliency to violent extremist recruitment and radicalization to violence. OCP developed three goals in the grant program that are identified in Appendix A of the Notice of Funding Opportunity. Each goal also contains the grant program's specific intended outcomes. Each grant recipient's project performance measures will feed into measuring these outcomes and goals. Grant recipients will report quarterly over the two year period of performance, will make other ad hoc reports, and will participate in OCP site visits and other oversight as necessary to ensure optimal performance toward meeting the established project objectives.

Additionally, each recipient, by accepting an award, will agree to participate in an evaluation, either conducted by the recipient, an independent outside entity, or DHS's Science and Technology Directorate (S&T), will select some recipients for evaluation as part of its own ongoing CVE research efforts. OCP will work with the CVE Task Force as necessary and appropriate to find efficiencies between the grant funded activities and Task Force members' activities. Task Force Members may also be tasked to provide relevant technical assistance to enhance the project performance of high performing grantees or correct poor performance.

Recipients will also make quarterly financial reports to FEMA and may be subject to additional FEMA or DHS Inspector General oversight. Furthermore, there will be rigorous oversight and monitoring of grant recipients to ensure compliance with the terms of the awards. In addition to general grant oversight mechanisms, DHS has planned significant staff time for oversight and performance measurement, and has specifically required review prior to implementation of training materials and narrative campaigns produced with the awards.

- 3) DHS recently facilitated a CVE pilot program in three cities: Los Angeles; Minneapolis; and Boston.

What were some of the lessons learned from the three-city pilot program?

Response: From approximately April 2014 to February 2015, culminating at the White House Countering Violent Extremism Summit, the U.S. Government supported CVE Pilot efforts in Los Angeles, Minneapolis/St. Paul, and greater Boston. Through these pilots the federal government learned several valuable lessons,

- Federal, State and Local Governments should engage a wide range of community members before crafting strategies in partnership with those communities and ensure the process is open and transparent.

- Local officials should work collaboratively with communities to prioritize and address concerns.
- CVE strategies should proactively address the protections of civil rights, civil liberties, and privacy.
- Local officials should be given flexibility to label and scope their initiatives in a way that addresses local needs and concerns.

Through S&T, DHS is supporting an independent, external assessment of the CVE initiatives in Los Angeles and Boston. The research teams have assessed resources, activities, as well as current and planned CVE programs. The research teams are currently completing a formative evaluation of each city's programs, expected to be completed in early 2017. After the formative evaluations, the research teams will evaluate the impact of programs in LA and Boston. This project is expected to complete in Q4 2017.

4) What products, if any, were produced?

Response: All three of the pilot regions developed local frameworks for building resilience against violent extremism. The fact sheets and the full local frameworks are available at: www.dhs.gov/cve.

5) Which programs, if any, were continued after the pilot period and how were they funded?

Response: Each pilot region received \$216,000 in federal funding to begin implementation of local frameworks. The pilot effort in the Twin Cities has also secured state and private funding.

6) I am also somewhat familiar with curriculum that has been developed to get college and university students involved in the CVE effort as well as DHS's Peer-2-Peer (P2P) Challenging Extremism contests.

What metrics are being used to measure the success of these programs?

Response: Individual P2P projects are assessed based on the following metrics, which are adapted from standard social media marketing metrics:

- **Analysis of the campaign's target audience:** "the silent majority," "uncommitted populations," or "civic minded individuals."
- **Social media marketing metrics:** number of people who see the content (**reach**); the number of times the content is displayed (**impressions**); and the number of interactions that people have with content (**engagement**).

- **Demographic analysis of social media users:** Including age, gender and other factors.
- **Pre and post-test surveys** of activities and events.

Additional measures of the scope, effect, and impact of the P2P program will also be developed during an independent, objective evaluation of P2P in the United States that has been recently funded by the National Institute of Justice.

- 7) What data can you share regarding the reach and resonance of student CVE campaigns developed via the P2P program?

Response: Overall, P2P campaigns have reached tens of millions of people (estimating online and in person metrics across projects and semesters), and some campaigns have continued after the competition ended. Notable examples include:

- Missouri State University's One95 campaign has been adopted as part of the youth Countering Violent Extremism Platform by the Counter Extremism Project, a non-governmental organization located in New York.
- Curtin University's (Australia) 52JUMAA mobile app has received funded support to bring it online. The app sends reminders with positive encouragement to young Muslims.
- The College of Europe's (Belgium) "Don't Flirt with Extremism" campaign received commendation from the Minister for Security and Home Affairs.
- Middle Tennessee State University's honorable mention campaign "Double Take" was adopted by the Student Government Association for a university-wide campaign against stereotypes.
- In June 2016, the U.S. Attorney's Office in Denver provided seed grant funding to three Colorado teams, including Community College of Aurora, the U.S. Air Force Academy, and the University of Colorado, Boulder, to continue their projects in the future.

- 8) As I told you at the July 6 hearing, I am concerned about the extent to which multiple interagency groups can effectively integrate and coordinate their respective CVE strategies.

Please describe the ways in which the OCP and interagency CVE Task Force are communicating and cooperating with other interagency groups, such as the State Department's Global Engagement Center (GEC), the Global Engagement Center Coordination Office (GECCO) and the National Counterterrorism Center (NCTC).

Response: The Office of Community Partnerships (OCP) and the CVE Task Force work closely with the National Counterterrorism Center (NCTC) and the Global Engagement Center (GEC). The CVE Task Force is domestically focused, while the GEC is internationally focused, so their respective efforts are not duplicative of one another. OCP and Task Force leadership regularly meet with senior leadership at NCTC. Additionally, NCTC currently provides two detailees to

the CVE Task Force in both the Digital Strategies and Research lines of effort to support efforts at the Task Force and ensure coordination back to their home agencies.

With regard to the Global Engagement Center (including the Global Engagement Center Coordination Office), the OCP, Task Force, and GEC leadership regularly meet to discuss a range of CVE issues. In addition, key personnel at the GEC and Task Force connect regularly to ensure situational awareness and coordination. The Task Force receives GEC guidance on messaging opportunities as well as ongoing strategic guidance on themes used by the Global Coalition to Counter ISIL, which the Task Force then disseminates to key CVE stakeholders as appropriate. Finally, OCP also has a full-time detailee to the GEC who regularly reports to and meets with OCP and Task Force personnel.

- 9) How do you believe that your roles and responsibilities at OCP and the CVE Task Force differ from the roles and responsibilities of other departments and agencies that are focused on CVE initiatives?

Response: The CVE mission space in the U.S. Government cuts across multiple departments and agencies, each of which have their own unique roles and authorities both domestically and internationally. The CVE Task Force was created to coordinate domestic CVE initiatives across Departments and Agencies. This broad coordination and synchronization role allows the CVE Task Force to ensure that domestic CVE initiatives are as efficient and effective as possible.

The Office for Community Partnerships (OCP) coordinates CVE initiatives within the Department of Homeland Security and leverages OCP's own resources within the Department to support successful implementation of domestic CVE initiatives. With the Department's existing capabilities, OCP is working to support efforts by key stakeholders to prevent radicalization and recruitment to violence.

Neither of these roles displaces the critical work of partner Departments and Agencies like the Department of Justice, Federal Bureau of Investigation, National Counterterrorism Center, Department of State, or USAID.

- 10) Besides President Obama, which government official and office is ultimately responsible for CVE efforts across the federal government?

Response: The CVE Task Force coordinates a "whole of government" approach to empowering local partners to prevent violent extremism in the United States. The principal of each participating Department or Agency retains ultimate responsibility for the programs of his or her department or agency.

Post-Hearing Questions for the Record
Submitted to George Selim, Director, Office of Community Partnerships, U.S. Department
of Homeland Security
From Senator Jon Tester

Permanent Subcommittee on Investigations Hearing: “ISIS Online: Countering Terrorist
Radicalization & Recruitment on the Internet & Social Media”
July 6th, 2016

Mr. Selim, you served at the Department of Justice at the Community Relations Service. The Office for Community Partnerships seems to have a similar function of engaging State and local government, law enforcement, and community groups in order to build relationships and promote trust.

1. Could you highlight some of the major differences in the Community Relations Service at the Department of Justice and the Office of Community Partnerships at the Department of Homeland Security?

Response: The Department of Justice Community Relations Service (CRS) is a **conflict resolution** agency. CRS works with communities to uncover the underlying interests of all of those involved in the conflict and facilitates the development of viable, mutual understandings, and solutions to the community’s challenges. CRS assists communities in developing local mechanisms and community capacity to prevent and resolve racial and ethnic tensions. In addition, CRS works with communities to prevent and respond more effectively to hate crimes based on actual or perceived race, color, national origin, gender, gender identity, sexual orientation, religion, or disability.

In contrast, Department of Homeland Security (DHS) Office of Community Partnerships (OCP) is dedicated solely to the mission of countering violent extremism, and its objective as the DHS leader in CVE is to support, improve, expand and coordinate the Department’s existing community based CVE efforts by working with key stakeholders and partners at local, state, tribal, territorial, and federal levels.

OCP’s mission is to develop and implement a full-range of partnerships to support and enhance efforts by key stakeholders to prevent radicalization and recruitment to violence by violent extremists.

2. What else does the Office of Community Partnerships bring to the table that the DHS Office for Civil Rights and Civil Liberties does not?

Response: The Office for Community Partnerships was established to streamline and head the Department’s efforts to counter violent extremism domestically. OCP is the primary source of leadership, innovation, and support for the improved effectiveness of partners at federal, state, local, tribal and territorial levels. The Office also leverages the resources and relationships of the Department of Homeland Security and applies the personal leadership of the Secretary to

empower leaders in both the public and private sectors to spur societal change to counter violent extremism.

OCP implements a full-range of partnerships to support and enhance efforts by faith leaders, local government officials, and communities to prevent radicalization and recruitment by terrorist organizations. OCP also provides these stakeholders with training and technical assistance to develop CVE prevention programs in support of resilient communities.

The DHS Office for Civil Rights and Civil Liberties (CRCL) was created to support the Department's mission to secure the nation while preserving individual liberty, fairness, and equality under the law. CRCL integrates civil rights and civil liberties into all of the Department activities by promoting respect for civil rights and civil liberties in policy creation and implementation by advising Department leadership and personnel, and state and local partners; communicating with individuals and communities whose civil rights and civil liberties may be affected by Department activities, informing them about policies and avenues of redress, and promoting appropriate attention within the Department to their experiences and concerns; investigating and resolving civil rights and civil liberties complaints filed by the public regarding Department policies or activities, or actions taken by Department personnel; and leading the Department's equal employment opportunity programs and promoting workforce diversity and merit system principles.

Thus, CVE is not and has never been the primary focus of CRCL, though CRCL's extensive community engagement across the country has occasionally included some CVE programming.

Concerning the Department's community engagements efforts, CRCL has been integral in our efforts at engaging communities, and will continue to be. Civil rights and civil liberties are invariably part of the discussion when this Department engages communities. CRCL will therefore participate, as needed, with the Office for Community Partnerships when we engage communities. More specifically, as we enter this new phase of our efforts, CRCL will, in consultation with the Office for Community Partnerships, continue to lead, improve and expand this Department's community engagements, including Community Engagement Roundtables, Town Hall Meetings, and Youth Forums across the country.

However, in addition to its community engagement efforts, OCP also leads the Department's CVE mission with a number of additional objectives, including:

- Field Support Expansion and Training
- Grant Support
- Philanthropic Engagement and
- Tech Sector Engagement.

3. Please provide to my office the Office of Community Partnerships Strategic Plan for the upcoming year.

Response: The Office for Community Partnerships will ensure that its strategic plan is shared.

U.S. law enforcement has – for years – been reaching out to local communities throughout the U.S., including faith-based groups. But the creation of the Office of Community Partnerships was announced late last year.

1. If previous outreach efforts to certain groups have been a problem, why do you believe it has taken so long for the Office of Community Partnerships to be created?

Response: In 2015, Secretary Johnson acknowledged that in order for DHS's CVE efforts to be improved, the Department's CVE efforts would have to be consolidated into one component and taken "to the next level." OCP was established for that purpose, given the evolution and diversity of threats to the homeland.

OCP's objective as the Department's leader in CVE, is to support, improve, expand and coordinate the Department's existing community based CVE efforts by working with key stakeholders and partners at local, state, tribal, territorial, and federal levels.

While outreach and community engagement are key elements of OCP's mission, as stated above, OCP was established to fulfill the Department's CVE mission which also includes a number of additional objectives (field support expansion and training, grant support, philanthropic engagement and tech sector engagement).

In its recruitment efforts online, ISIS has project a compelling, but twisted, narrative: that it alone is a source of victory and certainty in this world and that all others will submit to it. So, when ISIS is online recruiting these men and women, they are speaking to the alienated, the angry, and the confused. But the U.S. has its own far more compelling, far more universal narrative of freedom, inclusiveness, and opportunity.

1. What sorts of narratives and counter-messaging have you found to be most effective in your efforts thus far?

Response: While DHS does not conduct specific counter-messaging campaigns against ISIL, we have learned some promising practices about creating online narratives and counter-messaging campaigns to push back on violent extremist messaging. We recognize first and foremost the need to provide alternative messages to the volumes of terrorist messages online. DHS has supported the development of these alternative messages through the Peer to Peer: Challenging Extremism Program. The program works with university student teams to create and disseminate counter-messages against violent extremism by using social media. Research has also pointed to the potential for the messages of former violent extremists as being powerful for dissuading others from becoming violent extremists, and this is an area that DHS's Office for Community Partnerships is currently exploring along with the CVE Task Force and other federal

agencies. Finally, as we have learned from the Peer to Peer program and the work from our colleagues at the Department of State's Global Engagement Center, campaigns are successful when they incorporate both online and offline components, such as providing individuals an opportunity to share messages of tolerance and understanding online while meeting in person to develop collaborative projects to take action.

2. Do you believe that the narratives we use here in the U.S. are capable of being universally applicable? If not, how do you think we could modify counter-narratives to be more successful overseas?

Response: There may be some elements of counter-narrative campaigns that may be universally applicable, such as those that expose myths or falsehoods or that appeal to an individual's self-worth or sense of identity. We are working with our colleagues at the CVE Task Force, the Department of State, and the Department of Defense to discuss these ideas and to build better models to support successful counter-narrative campaigns.

**Questions for the Record Submitted to
Chief of Staff Meagan M. LaGrafte by
Senator Jon Tester (#1)
Homeland Security and Government Affairs Committee
July 06, 2016**

Question:

What sorts of narratives and counter-messaging have you found to be most effective in your efforts thus far?

Answer:

We have found that the most effective narratives come from those individuals who are deeply familiar with Da'esh and who oppose their ideology. We characterize these narratives as defectors stories – the stories of people who left their homes and traveled to fight in Syria and Iraq and then became so disillusioned by the reality of Da'esh that they escaped, choosing to return home even in the face of near certain arrest. Effective messaging also comes from highlighting the plight of the families of Da'esh's recruits. These first-hand accounts—describing the horrible second and third-order effects on a family when an individual leaves his or her home to fight with Da'esh—are both emotional and potent.

**Questions for the Record Submitted to
Chief of Staff Meagan M. LaGrafte by
Senator Jon Tester (#2)
Homeland Security and Government Affairs Committee
July 06, 2016**

Question:

Do you believe that the narratives we use here in the U.S. are capable of being universally applicable? If not, how do you think we could modify counter-narratives to be more successful overseas?

Answer:

We have seen time and again that local, familiar voices are the most effective in this context. The U.S. government has a good message to tell but we are generally not the most effective messenger. Instead, there is a wealth of credible voices across the Middle East, Europe, and Africa—governments, non-governmental organizations and civil society groups—who can be instrumental in this fight. These include people from vulnerable communities who have first-hand knowledge and experience of Da'esh's violence, including defectors, family members, clerics, and youth.

**Questions for the Record Submitted to
Chief of Staff Meagan M. LaGrafte by
Senator Jon Tester (#3)
Homeland Security and Government Affairs Committee
July 06, 2016**

It is clear that most people understand how pervasive and all-consuming the Internet has become, particularly among younger generations. People are spending more time plugged into this online universe that offers an incredible amount of advertising, information, and propaganda.

Question:

What do you believe is the most effective way to cut through this noise and mount a successful online counter-campaign to combat the online efforts of terrorist recruiters?

Answer:

At the end of the day, it takes a networked approach to defeat a network. The GEC's strategy is to cultivate a global network of credible voices to counter-message Da'esh. This GEC-facilitated network continues to grow and represents an enduring web of partners that responds quickly to and overwhelms violent extremist propaganda, online, in social media, and in traditional media. The Center also disseminates broad thematic CVE campaigns that are coordinated and executed with our Coalition partners and third party voices. Working together, these campaigns will help us degrade and ultimately defeat Da'esh, Al Qaeda, and other terrorist organizations.

**Questions for the Record Submitted to
Meagen LaGrafte
by Senator Claire McCaskill (#1)
Senate Committee on Homeland Security and Governmental Affairs
July 6, 2016**

Question:

Please provide me with a breakdown of the GEC's budget that clearly delineates how much money is going to these different types of partnerships.

Answer:

In line with the revamped counter-messaging strategy, developing and maintaining partnerships are fundamental principles of our work, and these activities involve all aspects and offices within the Global Engagement Center.

Fiscal Year 2016 expenditures were, by office: \$6.4 million for our Content Office, \$5.2 million for our Partnerships Office, \$2.6 million for our Resources Office, \$1.1 million for our Data Analytics Office and \$120,000 for our Operations Office.

Funding for the Content Office is used for social media campaigns, in-house content production, and to purchase content created by third party partners. Funding for the Partnerships Office is used to build capacity within and generate content from our foreign government and non-governmental partners. Projects conducted in partnership with the social media industry (such as Facebook, YouTube, and Twitter) are funded out of the Analytics Office's budget.

**Questions for the Record Submitted to
Meagen LaGrafte
by Senator Claire McCaskill (#2)
Senate Committee on Homeland Security and Governmental Affairs
July 6, 2016**

Question:

Please also categorize each type of partnership by its funding source (e.g. direct funding, contracts, memoranda of understanding, in-kind assistance, grants, etc.).

Answer:

The Global Engagement Center (GEC) funds its various partnerships and programs through direct transfers of funds for grants, contract vehicles, and interagency agreements. To date, the GEC has not had in-house grant-making authority. However, the GEC expects to have that capacity in FY2017, allowing us to expand the breadth and depth of existing and potential partnerships.

In FY 2016, direct funds transfers by GEC for partnerships and other programming accounted for approximately \$2.2 million and contracts accounted for \$11.9 million.

We also use interagency agreements to transfer funds to other agencies and offices. One example of these is an agreement with the Combating Terrorism Technical Support Office (CTTSO) at the Department of Defense. With this agreement and funding, CTTSO is working with a partner in academia to develop and employ a social media engagement and Twitter analytics tool.

**Questions for the Record Submitted to
Meagen LaGrafte
by Senator Claire McCaskill (#3)
Senate Committee on Homeland Security and Governmental Affairs
July 6, 2016**

Question:

If GEC is not directly funding these partnerships, which agencies and accounts fund these efforts? Do you expect these accounts to be available for these efforts indefinitely?

Answer:

As outlined in Executive Order 13721, which directed the Secretary of State to establish the Global Engagement Center, the GEC is tasked to coordinate, integrate, and synchronize all U.S. government counterterrorism messaging efforts directed at foreign audiences abroad. As such, the GEC works in collaboration with a variety of interagency partners in its mission, and that includes leveraging resources of the interagency for shared aims. The GEC works on campaigns and programs with interagency partners, and jointly funds those efforts in certain instances. The interagency list of partners includes: the Bureau of Counterterrorism (CT) in the Department of State, USAID, the Broadcasting Board of Governors, the interagency Counter Violent Extremism (CVE) Task Force, the Department of Homeland Security's Office for Community Partnerships, the Department of Defense and its subordinate commands, the Intelligence

Community (IC), the Department of Justice (including FBI), and the Department of the Treasury.

**Questions for the Record Submitted to
Meagen LaGrafte
by Senator Claire McCaskill (#4)
Senate Committee on Homeland Security and Governmental Affairs
July 6, 2016**

Question:

Lastly, please list all recipients of GEC funding by name, type and the amount of money each recipient is set to receive in Fiscal Year 2016.

Answer:

The Global Engagement Center (GEC) does not publicly identify our partners so that we can protect their safety. However, I would be happy to discuss our various partnerships with you and your staff in a non-public setting. I can tell you that the GEC expended almost \$20 million on our various partnerships, in the form of social media campaigns, tools, training workshops, and other programs during FY 2016.

**Questions for the Record Submitted to
Meagen LaGrafte by
Senator Claire McCaskill (#5)
Senate Committee on Homeland Security and Governmental Affairs
July 6, 2016**

Question:

Please give me a plain English description of the metrics that are being used to evaluate the effectiveness of the GEC's CVE messaging strategy.

Answer:

The Global Engagement Center (GEC) tracks several measures of performance across social media accounts in support of our counter violent extremism (CVE) messaging strategy. These metrics enable the GEC to make data-driven decisions quickly, which is of paramount importance to an agile organization confronting an adaptive enemy.

None of these metrics are perfect, and all should be taken together, alongside qualitative analysis and approximations. Some of these metrics include mentions, impressions, reach, and engagement rate.

- **Mentions:** Mentions are the number of times that a brand, campaign, or hashtag is used across social media. This is an estimate of the overall size of a conversation.
- **Reach:** Reach is the actual number of unique people that see a message. One common way of estimating this is to add the number of friends or followers of a given account plus the number of friends or followers of anyone that reposts their messages, since this is an upper bound on the number of people that could have read them.

- Impressions: The number of times that a message is actually displayed to a user is referred to as the number of impressions it receives.
- Engagement Rate: Engagements is another metric that counts the number of interactions that an audience has with a message, such as clicks, comments, favorites, shares, replies, or platform-specific actions such as “retweets” on Twitter or “likes” on Facebook. The engagement rate is typically expressed as the total number of engagements divided by the number of users or messages that could have elicited a response. This is one way to gauge the resonance of a particular message, campaign, or brand.

In addition to the above metrics, the GEC is currently investigating new approaches to gather further insights into the effectiveness of our messaging efforts. For example, the GEC is actively exploring observational studies to directly assess shifts in sentiment, behavior, and opinions that may be affected by our messaging efforts. One example would be to conduct anonymous polling online, where direct questions could be asked of our target audience, before and after a campaign. The GEC is currently exploring these types of approaches to gather further insights into the effectiveness of our messaging efforts.

**Questions for the Record Submitted to
Meagen LaGrafte by
Senator Claire McCaskill (#6)
Senate Committee on Homeland Security and Governmental Affairs
July 6, 2016**

Question:

To the greatest extent possible, please also provide me with a summary of any data your office has collected to date regarding the reach and resonance of online messages from the GEC and its partners.

Answer:

One common method of estimating the reach of the Global Engagement Center's (GEC) online messages is through impressions, which are defined as the number of times that a message is actually displayed to a human via an online platform. Since April 2016, the GEC's potential impression rate on Twitter has been approximately 665,000 per day according to a historical analysis conducted with Crimson Hexagon. Crimson Hexagon calculates the potential impressions on Twitter by summing the followers of each GEC tweet author along with anyone who re-tweets those messages for the specified time period.

The resonance of the GEC as measured through its engagements on Facebook has increased by 74 percent over the Center for Strategic Counterterrorism Communications (CSCC). That is according to a historical

analysis conducted with CrowdTangle from September 2011 through March 2016.

**Questions for the Record Submitted to
Meagen LaGrafte by
Senator Claire McCaskill (#7)
Senate Committee on Homeland Security and Governmental Affairs
July 6, 2016**

Question:

How do those numbers compare with data previously collected by the CSCC?

Answer:

We estimate that the Global Engagement Center's (GEC) 665,000 potential impressions per day represents a 16 fold improvement in reach over the Center for Strategic Counterterrorism Communications (CSCC) on Twitter. From the CSCC's inception on September 9, 2011, through March 14, 2016, the CSCC's potential impression rate on Twitter was approximately 41,000 per day according to a historical analysis conducted with Crimson Hexagon. The resonance of the GEC as measured through its engagements on Facebook has increased by 74 percent over the CSCC.

While it is natural to compare the GEC with the CSCC, especially using quantifiable metrics showing rising or falling trends, it is critical to highlight that we are diminishing the use of government accounts, in favor of partner-driven messaging.

**Questions for the Record Submitted to
Meagen LaGrafte by
Senator Claire McCaskill (#8)
Senate Committee on Homeland Security and Governmental Affairs
July 6, 2016**

Question:

Please describe the ways in which the GEC and Global Engagement Center Coordination Office (GECCO) are communicating and cooperating with other interagency groups, such as the Office for Community Partnerships at the Department of Homeland Security (DHS), the interagency CVE Task Force and the National Counterterrorism Center (NCTC).

Answer:

The GEC and the GECCO coordinate with various CVE-focused entities, including the Department of State's Bureau of Counterterrorism's (CT) office of Countering Violent Extremism (CVE), USAID, the Broadcasting Board of Governors, the interagency CVE Task Force, Department of Homeland Security's Office for Community Partnerships, the Department of Defense and its subordinate commands, the Intelligence Community, the Department of Justice (including the FBI), and the Department of Treasury.

As an interagency body, the GEC is able to leverage the resources and capabilities unique to these departments and agencies, in support CVE messaging activities. In order to coordinate and synchronize those activities, the GEC chairs

multiple meetings, conference calls, and secure video conferences. These include a weekly U.S. government video conference with all the departments and agencies that represent the nine counter-ISIL lines of effort, and daily phone calls with U.S. public affairs and public diplomacy officers globally.

**Questions for the Record Submitted to
Meagen LaGrafte by
Senator Claire McCaskill (#9)
Senate Committee on Homeland Security and Governmental Affairs
July 6, 2016**

Question:

How do you believe that your roles and responsibilities at GEC differ from the roles and responsibilities of other departments and agencies that are focused on CVE initiatives?

Answer:

The Global Engagement Center (GEC) differs from other departments and agencies primarily through our mandate to synchronize, integrate, and coordinate all government-wide messaging directed at foreign audiences abroad for the purpose of countering violent extremism and terrorism. This differs from the interagency Countering Violent Extremism (CVE) Task Force, which is primarily focused domestically on CVE, or the Department of Defense, which does not have the authority to coordinate the messaging efforts directed at foreign audiences abroad with other departments and agencies in this manner.

**Questions for the Record Submitted to
Meagen LaGrafte by
Senator Claire McCaskill (#10)
Senate Committee on Homeland Security and Governmental Affairs
July 6, 2016**

Question:

Besides President Obama, which government official and office is ultimately responsible for CVE efforts across the federal government?

Answer:

Executive Order 13721 assigns the Global Engagement Center (GEC) as the responsible office for the coordination, integration, and synchronization of all government communications directed at foreign audiences abroad for the purpose of countering violent extremism (CVE) and terrorist organizations abroad. The Coordinator of the Center reports to the Secretary of State through the Under Secretary of State for Public Diplomacy.

The Secretary of State has designated the Bureau of Counterterrorism (CT), led by the CT Coordinator, as the lead for coordinating and expanding the State Department's CVE diplomatic engagement and assistance efforts. In May, State and USAID released a joint CVE strategy that will guide State and USAID's CVE efforts. The CT Bureau also serves as the State Department's liaison with the interagency CVE Task Force, led by the Department of Homeland Security and the Department of Justice, in order to coordinate domestic and international CVE

efforts. The CVE Task Force is responsible for coordinating all interagency CVE efforts across the federal government; the Director of the Task Force is George Selim.

Additionally, the President's Homeland Security and Counterterrorism Advisor, Lisa Monaco, is responsible for advising the President on all aspects of counterterrorism policy and strategy and coordinating homeland security-related activities throughout the Executive Branch.