15

Communicate, Cooperate, and Collaborate (C^3) Through Public-Private Partnerships (P^3) to Counter the Convergence of Illicit Networks

Celina Realuyo

Today, we face a broad spectrum of security threats, such as global terrorism, transnational organized crime, economic crises, cyber-attacks, extreme natural disasters, and revisionist states that have made national security more challenging than ever before. The complexity of these security threats, particularly from illicit networks, like terrorists, criminals, and proliferators, requires a multidisciplinary approach to comprehend and counter. The convergence of these illicit networks, and the magnitude, velocity, and violence associated with their illicit activities are overwhelming governments and threatening state sovereignty and prosperity. Governments are no longer able to guarantee the security, prosperity, rule of law, and governance their people expect and deserve. Oftentimes, average citizens who "see something and say something" are the first to recognize anomalies and identify threats; they know their sector, workplace, or community best. Therefore, governments need to actively identify and engage partners in the private and civic sectors to better detect, dismantle, and deter the illicit networks that undermine our security and prosperity.

This chapter will emphasize the need to foster robust partnerships among the public, private, and civic sectors of society to counter the convergence of illicit networks at home and abroad. It will examine three specific areas where multi-sector collaborations are underway and have experienced some success: (1) protecting privacy, cyberspace, and critical infrastructure with the private sector through formal information sharing mechanisms; (2) combating threats to the international banking system, such as terrorist financing, money laundering, and cybercrime, in partnership with the financial services sector; and (3) countering violent extremism and foreign fighter recruitment by the Islamic State of Iraq and the Levant (ISIL) with local communities and civil society organizations in the United States. These examples illustrate the challenging nature of these security threats and the importance of harnessing resources across various sectors to counter them. Since the government no longer enjoys a monopoly on national security or the use of force as it did in the past, it must adopt a "whole of society" approach to understand and address the evolving threats to our security and prosperity in this globalized world. In the 21st century, all sectors need to communicate, cooperate, and collaborate (C^3) through public-

private partnerships (P^3) to counter the convergence of illicit networks and ensure national security.

Protecting Cyberspace

Cybersecurity is considered one of the most daunting security challenges of the 21st century. It has become a leading security concern at the individual, enterprise, national, and international levels. Not a day goes by without some headline news item featuring the latest cyber-hack or cyber espionage case around the world. Whether it be the Target data breach with 110 million records compromised in 2013 or the massive disclosure of up to 21.5 million U.S. government employees' personal and biometric data through the Office of Personnel Management (OPM) hack revealed in 2015, cyber vulnerability affects each of us personally and professionally.[1] Privacy and civil liberties are at the center of the debate over data breaches through cyberspace.

Perhaps the most publicized cyber-attack to date was the one against Sony Pictures Entertainment on November 24, 2014, which crippled its movie and television studio. The cyber intrusion compromised data including personal information, such as the social security numbers of Sony Pictures' employees and their families, sensitive emails between employees, executive compensation information, and copies of (previously) unreleased Sony films. Since the discovery of the attack, Sony has been working to repair the damage caused by a group calling itself "Guardians of Peace," in an assault that the U.S. government has blamed on North Korea, spending an estimated $15 million.[2]

Sony Pictures is not the only corporate victim of cyber insecurity. Pricewaterhouse Coopers' Global State of Information Security 2015 Survey reported that the number of detected data security incidents among companies queried soared to a total of 42.8 million in 2014, a 48 percent leap over the number in 2013. This increase comes at great cost, with total financial losses attributed to security compromises increasing 34 percent over 2013.[3] For the past decade, the United States and many other countries have been grappling with how to define cybersecurity and how to protect against the broad spectrum of security threats that emanate from the cyber domain. Cyber threats can emerge from a number of different sources: nation-states that might engage in cyber warfare, foreign intelligence services, corporate espionage, terrorists, criminals, hackers, hacktivists, and insider threats.[4]

U.S. Cybersecurity Efforts

The Obama Administration considers cybersecurity one of the most important challenges facing the nation today. President Obama has said:

> America's economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable internet. Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property. Although the threats are serious and they constantly evolve, I believe that if we address

them effectively, we can ensure that the internet remains an engine for economic growth and a platform for the free exchange of ideas.[5]

To secure cyberspace, the U.S. government has implemented a wide range of policies, both domestic and international, to improve our cyber defenses, enhance our response capabilities, and upgrade our incident management tools. Several of these initiatives entail close collaboration between the public and private sectors to protect our critical infrastructure and safeguard our privacy. The Obama Administration's Priorities on Cybersecurity are:

1. Protecting the country's critical infrastructure—our most important information systems—from cyber threats;
2. Improving our ability to identify and report cyber incidents so that we can respond in a timely manner;
3. Engaging with international partners to promote internet freedom and build support for an open, interoperable, secure, and reliable cyberspace;
4. Securing federal networks by setting clear security targets and holding agencies accountable for meeting those targets; and
5. Shaping a cyber-savvy workforce and moving beyond passwords in partnership with the private sector.

The Administration is employing the following principles in its effort to strengthen cybersecurity: a whole-of-government approach, network defense first, protection of privacy and civil liberties, public-private collaboration, and international cooperation and engagement.[6] On February 12, 2013, President Obama signed *Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity*, a new approach to critical infrastructure cybersecurity, and released Presidential Policy Directive (PPD) 21, which seeks to increase the overall resilience of our national critical infrastructure.[7] Together, these measures drive action toward a whole of community approach to risk management, security, and resilience.

The Cybersecurity Framework developed by the National Institute of Standards and Technology (NIST) working with industry, consists of standards, guidelines, and best practices, to promote the protection of critical infrastructure through cyber risk management.[8] To support these goals, the Department of Homeland Security (DHS) created the Critical Infrastructure Cyber Community C³ (pronounced "C-cubed") Voluntary Program in February 2014. This program is an innovative P³ designed to help align critical infrastructure owners and operators with existing resources that will assist their efforts to adopt the Cybersecurity Framework and manage their cyber risks.[9]

The C³ Voluntary Program emphasizes three C's:

1. *Converging* critical infrastructure community resources to support cybersecurity risk management and resilience through use of the Framework;

2. *Connecting* critical infrastructure stakeholders to the national resilience effort through cybersecurity resilience advocacy, engagement, and awareness; and
3. *Coordinating* critical infrastructure cross-sector efforts to maximize national cybersecurity resilience.[10]

The primary goals of the C³ Voluntary Program are to support industry in increasing cyber resilience, to increase awareness and use of the Cybersecurity Framework, and encourage organizations to manage cybersecurity as part of an all-hazards approach to enterprise risk management. With over 85 percent of U.S. critical infrastructure in the hands of the private sector, government programs like C³ are fundamental to promote P³ in the cyber arena.[11] Homeland Security Secretary Jeh Johnson considers counterterrorism and cybersecurity the top priorities for his agency and emphasizes that his team cannot execute these missions without working hand in hand with the private and civic sectors.[12]

2015 White House Cybersecurity Summit

Highlighting the importance of collaborating with the private and civic sectors, the Obama Administration held a White House Summit on Cybersecurity and Consumer Protection on February 13, 2015 at Stanford University. The Summit convened leaders from businesses throughout the economy, consumer and privacy groups, educators, students, law enforcement, and other government agencies. Private sector participants included the CEOs of Apple Inc., American International Group Inc., American Express Corp., Bank of America Corp., Pacific Gas & Electric Co., Kaiser Permanente, and MasterCard.[13] At the event, over two dozen companies made commitments to share best practices, adhere to stronger security standards, use the Cybersecurity Framework of Standards and Best Practices to manage their cyber risk, share cyber threat information, and adopt more secure payment technologies.[14]

On the occasion of the Summit, President Obama issued an *Executive Order (EO) on Promoting Private Sector Cybersecurity Information Sharing* to encourage the development of Information Sharing and Analysis Organizations (ISAOs). These ISAOs would serve as the hubs for sharing critical cybersecurity information and promoting collaboration for analyzing this information both within and across industry sectors; the private sector has been organizing its communities of interest and forming ISAOs. However, some of the corporate executives at the Summit said the government needed to do more, including passing legislation that offers liability protection to companies participating in sharing programs.[15] The EO clarifies DHS' authority to enter into agreements with ISAOs, streamlines private sector companies' ability to access classified cybersecurity threat information, and provides strong privacy and civil liberties protections.[16]

To enhance collaboration, DHS has developed a system for the automated sharing of cyber threat indicators with the private sector and government that includes privacy and civil liberties protections. Interested companies can work with the National Cybersecurity and Communications Integration Center (NCCIC) to prepare their networks for the

automated sharing of cyber threat indicators. In addition, NIST has created the National Cybersecurity Center of Excellence to partner with the private sector, academia, and other government agencies in order to find solutions to security problems inherent in technology. The center will produce generally available standards-based reference designs, templates, and example "builds," in order to reduce costs and complexities and enable companies in all sectors to use more secure technology.[17]

International Cooperation

Since cyberspace knows no borders and cyber threats can have worldwide impact, the Obama Administration has taken several steps to strengthen U.S. global leadership on the cyber front through bilateral and multilateral engagements. In 2011, the White House issued the "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World" that seeks a future of cyberspace open to innovation, interoperable the world over, secure enough to earn people's trust, and reliable enough to support their work. The strategy focuses on the following policy priorities for securing cyberspace:

- Economy: Promoting International Standards and Innovative, Open Markets; Protecting Our Networks; Enhancing Security, Reliability, and Resiliency.
- Law Enforcement: Extending Collaboration and the Rule of Law.
- Military: Preparing for 21st-Century Security Challenges.
- Internet Governance: Promoting Effective and Inclusive Structures.
- International Development: Building Capacity, Security, and Prosperity.
- Internet Freedom: Supporting Fundamental Freedoms and Privacy.[18]

Cybersecurity is becoming a regular agenda item in diplomatic engagements and international security conferences. During Chinese President Xi Jinping's state visit to Washington in September 2015, cybersecurity was one of the most prominent and controversial issues that resulted in a groundbreaking bilateral agreement on corporate espionage. After intense discussions, President Obama said the United States and China had reached a "common understanding" that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors. President Obama said that he had told President Xi during two hours of meetings at the White House that the escalating cycle of cyber-attacks against American targets "has to stop," and warned his Chinese counterpart that the United States would go after and punish perpetrators of those offenses through traditional law enforcement tools and, potentially, with sanctions.[19]

While the agreement marks progress in addressing the sensitive subject of cyber espionage and intellectual property theft with China, many observers, including President Obama, are taking a "trust but verify" approach to see what actual impact this pact will have on cyber intrusions. Director of National Intelligence James Clapper and other top U.S.

military officials have said cyber threats are increasing in frequency, scale, sophistication, and severity, and the United States needs the same kind of deterrent capability in cyberspace that it maintains for nuclear weapons. He told the Senate Armed Services Committee that the U.S.-China agreement did not include specific penalties for violations, but that the U.S. government could use economic sanctions and other tools to respond if needed. He viewed the cyber agreement between China and the United States on curbing economic cyber espionage as a "good first step," but noted it was not clear how effective the pact would be.[20] It is not yet clear if P^3 can help bridge that gap, as private companies are often the targets of Chinese attacks.

Cyberspace is the new operating environment for consumers, producers, private enterprise, government agencies, and nongovernmental organizations (NGOs). While the internet has engendered many of the positive aspects of globalization, like better access to goods, services, capital, and information, cyberspace and the critical infrastructure it supports are vulnerable to a broad spectrum of threats. As all countries are grappling with the evolving challenges of cybersecurity, there are calls for the establishment of international norms to assist with common definitions regarding cyber threats and responses to attacks. More confidence-building measures and capacity building in cybersecurity are needed, especially in emerging markets, to promote information sharing across sectors and borders, according to Ambassador Makita Shimokawa, Japanese Foreign Ministry deputy director of UN Affairs and Cyber Policy.[21] Cyber actors, including nation-states, terrorists, criminals, and hackers, capitalize on vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. To keep up with technological advances and protect cyberspace, governments and the private sector need to deepen their collaborations on cybersecurity to complement the initiatives described above.

Safeguarding the International Financial System

After the September 11 attacks, there was intense focus on stemming the flow of funding to al-Qaeda. This financial front of the war on terror complemented the formidable military and intelligence campaign in Afghanistan, known as Operation *Enduring Freedom*. This multifaceted approach recognized that financing is perhaps the most critical enabler for any terrorist organization to proselytize, plot, and execute their agenda. Financial forensic analysis of the 9/11 attacks demonstrated how the al-Qaeda operatives used the international financial system, through prominent banks and money services businesses, to fund the planning and execution of the largest terrorist attack on American soil in our country's history.[22] The 9/11 Commission estimated that the September 11 attacks cost al-Qaeda about $500,000, killed 19 hijackers and nearly 3,000 innocent victims, and changed the national security landscape of the U.S. forever.

Since the 1970s, the U.S. government has been working with the private sector to pursue financial crimes like fraud, tax evasion, and money laundering. Under the Bank Secrecy Act (BSA) of 1970, U.S. financial institutions are required to assist U.S. government

agencies to detect and prevent money laundering. Specifically, the BSA requires banks to keep records of cash purchases, file reports of cash transactions exceeding $10,000, and report suspicious activity that might indicate money laundering, tax evasion, or other criminal activities.[23] Financial institutions are required to know their clients (and their clients' clients), monitor their transactions for anomalies, and report them to the authorities. In the United States, the Financial Crimes Enforcement Network (FinCEN) serves as the country's financial intelligence unit (FIU), collecting and analyzing suspicious transaction reports. FinCEN has global counterparts, providing the opportunity for global cooperation. Once it came to light that al-Qaeda used the formal banking system to finance the 9/11 attacks, banks and other financial institutions, concerned with reputational risk, realized they had a new and vital task—to detect and report possible cases of terrorist financing. Now bankers needed to understand and identify how terrorist groups raise, move, store, and use money, and what vulnerabilities exist in the banking system to prevent future cases of terrorist financing.

U.S. Counterterrorism Financing and Anti-Money Laundering Efforts

The U.S. law enforcement and intelligence communities work closely with officials at various financial institutions, who have been vetted and hold an active security clearance, to investigate and prosecute specific cases of terrorist financing and money laundering. In many instances, bank officials are former law enforcement agents or bank regulators. The financial sector has invested billions in human, technological, and financial resources to enhance their anti-money laundering/counterterrorist financing (AML/CTF) compliance capabilities. While these relationships between the public and private sectors have been quite productive, particularly in detecting Iranian sanctions violations, some financial institutions have expressed frustration regarding the lack of information flow from the government on the impact this cooperation has had on actual cases. The private sector has called for better two-way communications and more information to justify the immense investment in AML/CTF programs to their shareholders; they want to see how "following the money trail" has fought terrorism and crime.

In 2010, the Financial Intelligence and Information Sharing Working Group (FIIS WG) was established, following the completion of a P³ pilot project under the auspices of the Office of the Director of National Intelligence's Office of Private Sector Partnerships. The project's content aside, both the analysts and the business people involved found that the shared communication about threat-finance typologies was productive. To keep the dialogue going, they started a freestanding group, which organically blossomed due to the information sharing gaps in this area. While the group has no affiliation with the government, the FIIS WG is intended to provide experts in the financial services industry and the U.S. government with a forum to informally discuss relevant topics, including protection of critical financial infrastructure, prevention of fraud, terrorist financing, and money laundering.

FIIS WG meetings and the relationships formed at those events facilitate information flow and bridge cultural gaps between government and industry. The FIIS WG eventually

found a home with the American Security Project, and its members include hundreds of representatives of both public and private sector entities, including regulatory, intelligence, defense, and law enforcement agencies, financial institutions, think tanks, consultancies, and academia.[24] The FIIS WG is considered a peer-to-peer community of practice and useful forum to discuss red flags, trends, emerging financial technologies, new payment systems, virtual currencies, alternative value systems, and the threats and vulnerabilities that accompany them.

Besides the banks themselves, several trade associations and NGOs have become actively involved in raising awareness, training, and educating the financial industry on the threats to the international financial system from financial crimes. One such example is the Association of Certified Anti-Money Laundering Specialists (ACAMS). It is the largest international membership organization dedicated to enhancing the knowledge, skills, and expertise in AML/CTF, as well as financial crime detection and prevention. Members represent various financial institutions, regulatory bodies, law enforcement agencies, and industry sectors. ACAMS circulates and discusses the latest trends and case studies in money laundering and terrorist financing through seminars, forums, international conferences, and local chapters.[25] The participation of senior U.S. government officials from the Departments of Treasury, Justice, and Homeland Security, the bank regulators, and law enforcement agencies responsible for combating terrorist financing and money laundering, at ACAMS events, demonstrates the active outreach conducted by the U.S. government to promote P^3.

Countering Emerging Threats to Financial Sector

Another example of cross-sector collaboration to protect the international financial system is the Financial Services Information Sharing and Analysis Center (FS-ISAC). It serves as the global financial industry's "go-to" resource for cyber and physical threat intelligence analysis and sharing. FS-ISAC is unique in that it was created by and for members in 1999 to prepare for Y2K and operates as a member-owned nonprofit entity. It was established by the financial services sector in response to the 1998 Presidential Decision Directive 63 (later updated by the 2003 Homeland Security Presidential Directive 7) that mandated that the public and private sectors share information about physical and cybersecurity threats and vulnerabilities to help protect U.S. critical infrastructure, of which the financial sector is a vital component.[26]

In response to emerging global threats in cyberspace to the financial sector, FS-ISAC's board extended its charter in 2013, to share information between financial services firms around the world. Constantly gathering reliable and timely information from financial services providers, commercial security firms, federal/national, state and local government agencies, law enforcement, and other trusted resources, the FS-ISAC can quickly disseminate physical and cyber threat alerts and other critical information to other organizations. This information includes analysis and recommended solutions from leading industry experts.

The Center's Critical Infrastructure Notification System (CINS) allows the FS-ISAC to send security alerts to multiple recipients around the globe almost simultaneously, while providing for user authentication and delivery confirmation. The system also provides an anonymous information sharing capability across the entire financial services industry. This protects members' proprietary information and client confidentiality. When they receive a submission, industry experts verify and analyze the threat and identify any recommended solutions before alerting FS-ISAC members. This procedure assures that member firms receive the latest tried-and-true procedures and best practices for guarding against known and emerging security threats.[27] Peer-to-peer collaboration brokered by organizations like FS-ISAC, combined with notifications to the appropriate government officials in the United States and elsewhere, is an example of timely and effective mechanisms to detect, address, and prevent threats to the financial system in the traditional and cyber domains.

International Cooperation

However, unilateral, single-country efforts will not be sufficient to address this threat. Our international financial system is far more interconnected and interdependent than ever before. International cooperation between the public and private sectors is, therefore, paramount. The Financial Action Task Force (FATF) is an intergovernmental body established in 1989, by the ministers of its 34 member jurisdictions. The FATF sets standards and promotes effective implementation of legal, regulatory, and operational measures for combating money laundering, terrorist financing, and other related threats to the integrity of the international financial system. It serves as a "policy-making [sic] body" working to generate the necessary political will to bring about national legislative and regulatory reforms to protect the global financial system. The FATF has developed a series of recommendations that are recognized as the international standard for combating money laundering, the financing of terrorism, and the proliferation of weapons of mass destruction.[28]

The FATF values private sector expertise and operational knowledge, as essential resources to evaluate the application of the AML/CFT requirements to business practices, and to encourage the practical adoption of the standards. The private sector can serve as a helpful sounding board to test or assess the potential impact of measures under consideration, or brainstorm on possible technical solutions in a specific field affecting the financial industry. It is also an important way to learn about market developments and access new information regarding emerging threats and vulnerabilities to the global financial system.[29] The FATF Private Sector Consultative Forum is the formal means to reach out to and cooperate with private sector stakeholders. It holds open consultations with interested stakeholders and sets up working groups to examine specific issues including financial innovations like mobile payments, virtual currencies, and store of value cards that could be vulnerable to money laundering or terrorist financing.[30] These examples of domestic and international P³ have strengthened the international financial system's ability to detect and deter terrorist financing, money laundering, and other financial crimes. According to

declassified intelligence reports, groups like al-Qaeda and Mexican drug cartels decided to refrain from using the formal banking sector due to the enhanced compliance and monitoring measures adopted by the private sector.

Countering Violent Extremism

Terrorism and political violence have existed since the dawn of civilization. Unfortunately, the tragic attacks of September 11 perpetrated by the Islamic terrorist group al-Qaeda turned the threat of violent extremism into stark reality with 19 terrorists using airplanes as weapons of mass destruction to kill 2,977 innocent victims in New York, the Pentagon, and Shanksville, Pennsylvania. Since then, the United States and other governments have been trying to devise effective strategies to counter terrorism. The calls to counter violent extremism (CVE) have grown louder lately, since the April 2013 Boston Marathon bombing and the rapid rise of the Islamic State of Iraq and the Levant (ISIL) and its ability to recruit tens of thousands of sympathizers and foreign fighters from around the world. Fears that an ISIL foreign fighter could return to his or her country of origin and commit acts of terror have heightened homeland security concerns and redoubled CVE efforts in Western countries.

The Threat of Violent Extremism in the United States and Foreign Fighter Flow

With the rise of ISIL, law enforcement and intelligence officials at the federal, state, and local levels around the country have been on high alert for possible terrorist attacks at levels not seen since the immediate post-9/11 period. Counterterrorism analysts are hard at work monitoring all three phases of radicalization: online radicalization, recruitment, and violent action. Federal Bureau of Investigation (FBI) Director James Comey told the Senate in July 2015 that more than 200 Americans have tried to join Islamic extremists in Iraq and Syria. "Whether or not the individuals are affiliated with a foreign terrorist organization and are willing to travel abroad to fight or are inspired by the call to arms to act in their communities," he said, "they potentially pose a significant threat to the safety of the United States and its citizens."[31] As of September 1, 2015, U.S. authorities have charged 64 men and women in 20 states with alleged ISIL activities; men outnumber women in those cases by about 5 to 1, with an average age of 25. The FBI reports that, in a handful of cases, it has disrupted plots targeting U.S. military or law enforcement personnel.[32]

More recently, on October 8, 2015, Comey testified before Congress that while counterterrorism remains the FBI's top priority, the threat itself has changed in two significant ways. First, the "progeny of al-Qaeda"—including ISIL, al-Qaeda in the Arabian Peninsula (AQAP), and al-Qaeda in the Islamic Maghreb (AQIM)—have become our focus, rather than al-Qaeda itself. Second, we are faced with an explosion of terrorist propaganda and training on the internet, in particular social media, that has made recruitment possible even without operatives within the United States.[33] Dozens of people in the United States are engaged in conversations with overseas supporters of ISIL that the FBI cannot monitor.

Director Comey has been warning for months that when ISIL supporters find someone in the United States through messages on social media, they then employ software that encrypts their communications, making it impossible for the FBI to follow them, even with a court order. This is known as the challenge of "going dark."[34] ISIL has demonstrated a surprising level of social media sophistication in its ability to attract sympathizers and recruit foreign fighters. The evolution of terrorist recruitment through the use of the internet has underscored the urgent need for better CVE strategies; ultimately, this will require robust partnerships between governments and civil societies.

According to a September 2015 Homeland Security Committee's Bipartisan Foreign Fighter Task Force Report, ISIL has recruited some 25,000 foreign fighters since 2011. The report found that despite concerted efforts to stem the flow, the United States has largely failed to stop Americans from traveling overseas to join jihadists. Of the hundreds of Americans who have sought to travel to the conflict zones in Syria and Iraq, authorities have only interdicted a fraction of them. The report concluded that:

- The U.S. government lacks a national strategy for combating terrorist travel and has not produced one in nearly a decade;
- To catch foreign fighters, intelligence needs to be exchanged quickly, but at home and abroad, we still face barriers to information sharing;
- Despite improvements since 9/11, some foreign partners are still sharing information with us about terrorist suspects in a manner that is ad hoc, intermittent, and often incomplete;
- Since 9/11, America has gotten better at keeping terrorists out of the country, but we are doing far too little to keep Americans from leaving to train in terrorist safe havens;
- Few initiatives exist nationwide to raise awareness about foreign fighter recruitment; and
- Gaping security weaknesses overseas—especially in Europe—are putting the U.S. homeland in danger by making it easier for aspiring foreign fighters to migrate to terrorist hot spots and for jihadists to return to the West.[35]

"The alarming threat of extremist ideology possibly influencing foreign fighters is very apparent in today's world," said Ranking Member Bennie Thompson (D-MS). "The Task Force has found that although there are serious government efforts to address the radicalization of foreign fighters, there is much more we can do in terms of sharing information with our international partners, assisting law enforcement, and bolstering community awareness."[36] These conclusions underscore the continued importance of pursuing vigorous CVE strategies that engage all sectors of society and our foreign counterparts.

The Threat of Homegrown Terrorism and ISIL-Inspired Attacks in the United States

FBI Director Comey flagged the threat of homegrown terrorism when he stated in October 2015 that over 900 FBI investigations of ISIL suspects were underway in 50 states; these are active, open investigations and do not include the 66 Muslim men and women around the country who have already been charged with alleged ISIL activities over the past 2 years.[37] While ISIL initially focused on consolidating its power base in Syria and Iraq, the Paris attacks on November 13, 2015, directed by ISIL and perpetrated by radicalized French and Belgian citizens, and the ISIL-inspired attack in San Bernardino, California, demonstrate the global aspirations and reach of ISIL and turned terrorism into the leading national security concern in the 2016 U.S. presidential election debates.

The San Bernardino attack killed 14 people and seriously injured 22 at a San Bernardino County Department of Public Health training event and holiday party on December 2, 2015. Syed Rizwan Farook, an American-born U.S. citizen of Pakistani descent, who worked as a health department employee and his Pakistani-born wife, Malik, who came to the United States on a fiancée visa, carried out the attack against his coworkers. The FBI considered the couple "homegrown violent extremists" (HVEs) inspired by foreign terrorist groups, who had become radicalized over several years prior to the attack. Farook and Malik had traveled to Saudi Arabia in the years before the attack and had amassed a large stockpile of weapons, ammunition, and bomb-making equipment in their home. They jointly pledged allegiance to ISIL on social media shortly before they were killed in a shootout with police, according to the FBI.[38] In light of this attack in the homeland, the U.S. strategy to degrade and destroy ISIL and programs to counter violent extremism have come under close scrutiny and criticism for their lack of effectiveness as ISIL expanded its influence in 2015.

U.S. Efforts to Counter Violent Extremism

CVE includes the preventative aspects of counterterrorism, as well as interventions to undermine the attraction of extremist movements and ideologies that seek to promote violence. CVE efforts by the U.S. government seek to address the root causes of extremism through community engagement, including the following programs:

- *Building Awareness* - including briefings on the drivers and indicators of radicalization and recruitment to violence;
- *Countering Extremist Narratives* - directly addressing and countering violent extremist recruitment narratives, such as encouraging civil society-led counter-narratives online; and
- *Emphasizing Community-Led Intervention* - empowering community efforts to disrupt the radicalization process before an individual engages in criminal activity.[39]

In August 2011, the White House released "Empowering Local Partners to Prevent Violent Extremism in the United States," the first national strategy to prevent violent extremism domestically. The U.S. strategy is based on two premises: that communities provide the solution to violent extremism; and CVE efforts are best pursued at the local level, tailored to local dynamics, where local officials continue to build relationships within their communities through community policing and outreach mechanisms. It considers the federal government's most effective role in strengthening community partnerships and preventing violent extremism is as a facilitator, convener, and source of research and findings.[40]

Since the release of the 2011 Strategy, local governments and communities around the country have developed prevention frameworks that address the unique issues facing their respective communities. Three cities—Boston, Los Angeles, and the Twin Cities—with help from the federal government, have created pilot programs to foster partnerships between local government, law enforcement, mayors' offices, the private sector, local service providers, academia, and many others who can help prevent violent extremism. Each city has created an action plan addressing the root causes and community needs they identified. The pilot framework developed by these three cities emphasizes the strength of local communities with the premise that well-informed and well-equipped families, communities, and local institutions represent the best defense against violent extremist ideologies.

The Role of the Department of Homeland Security in CVE

With its counterterrorism mission and a full-time CVE coordinator, DHS serves as the de facto lead agency in CVE in the United States. According to DHS, violent extremists are defined as "individuals who support or commit ideologically motivated violence to further political goals." DHS recognizes that the threat posed by violent extremism is neither constrained by international borders nor limited to a single ideology. Violent extremist threats within the United States can come from a range of violent extremist groups and individuals, including domestic terrorists and HVEs. A domestic terrorist differs from an HVE in that the former is not inspired by, and does not take direction from, a foreign terrorist group or other foreign power.[41]

The increasingly innovative use of the internet, social media, and information technology by violent extremists is making CVE efforts more difficult and complex. Accordingly, DHS has designed a CVE approach that addresses all forms of violent extremism, regardless of ideology, and that focuses not on radical thought or speech, but instead on preventing violent attacks. This approach provides numerous physical and virtual environments to promote information sharing and collaboration between federal, state, local, territorial, tribal, private, civilian, and international entities working to counter the threat of violent extremism.[42]

The DHS' CVE efforts are focused on three broad objectives:

1. *Understand Violent Extremism* - Support and coordinate efforts to better understand the phenomenon of violent extremism, including assessing the threat it poses to the nation as a whole and within specific communities;
2. *Support Local Communities* - Bolster efforts to catalyze and support community-based programs, and strengthen relationships with communities that may be targeted for recruitment by violent extremists; and
3. *Support Local Law Enforcement* - Deter and disrupt recruitment or individual mobilization through support for local law enforcement programs, including information-driven, community-oriented policing efforts, which for decades have proven effective in preventing violent crime.[43]

The DHS Building Communities of Trust (BCOT) initiative focuses on developing relationships of trust between law enforcement, fusion centers, and the communities they serve, particularly immigrant and minority communities, so that the challenges of crime control and prevention of terrorism can be addressed. In coordination with federal partners, DHS hosts conferences, workshops, and online forums for federal, state, local, territorial, tribal, private sector, civilian community, and international partners in order to share information about CVE in the form of outreach.

In collaboration with the Department of Justice and state and local law enforcement partners, DHS has trained thousands of frontline officers, first responders, and community leaders, and continues to provide CVE training to interested communities. These efforts work to improve communication, build trust, and encourage collaboration between officers and the communities they serve and protect. Training topics include effective policing without the use of ethnic or racial profiling, and best practices in community outreach.

DHS prioritizes CVE activities through grants that directly support state and local partners and community outreach efforts to understand, recognize, report, and respond to potential indicators of terrorist activity. In addition, DHS produces substantial analysis and research on trends in HVE, domestic terrorism, and terrorist propaganda to support federal, state, local, territorial, and tribal officials in identifying and mitigating violent extremist threats to the homeland.[44] These projects are too new to provide robust evidence of their successes; however, even in their nascent stage they have shown promise.

International CVE Efforts

The disturbing beheadings of Western hostages, remarkable military offensives in Iraq and Syria, the persecution of religious minorities, and compelling foreign fighter recruitment campaign by ISIL in the summer of 2014 directed the world's attention to countering terrorism once again. The United Nations designated ISIL as a terrorist group on June 2, 2014 under the UN al-Qaeda Sanctions List. President Obama, addressing the UN General Assembly in September 2014, called on member nations to do more to address

violent extremism within their regions. He chaired a UN Security Council summit that unanimously adopted UNSC Resolution 2178, condemning violent extremism and underscoring the need to prevent travel and curb support for foreign terrorist fighters (FTFs) destined for ISIL.

The United States established and leads a coalition of more than 60 partners committed to degrading and ultimately destroying ISIL. Besides the military, intelligence, and financial lines of effort of the campaign to counter ISIL, the Coalition is working to erode ISIL's appeal by strengthening capabilities to counter the group's messages of hate. The State Department's Center for Strategic Counterterrorism Communications (CSCC) was created to coordinate, orient, and inform government-wide foreign communications activities targeted against terrorism and violent extremism, particularly al-Qaeda and its affiliates and adherents.[45] It operationalized an Interagency Counterterrorism Communications (ICC) cell to improve cross-government collaboration on countering ISIL's online messaging.[46] The ICC plans to enlist U.S. Embassies, military leaders, and regional allies in a global messaging campaign to discredit groups such as ISIL. The plan is to be "more factual and testimonial," said Rashad Hussain, 36, a former White House adviser brought in to lead this effort. It will seek to highlight ISIL hypocrisy, emphasize accounts of its defectors, and document its losses on the battlefield—without recirculating its gruesome images or matching its snide tone.[47] With an annual budget of less than $6 million though, the CSCC is still struggling to effectively stem the spread of al-Qaeda and ISIL ideology.

White House 2015 CVE Summit

From February 17 to 19, 2015, the White House hosted the Summit on CVE to highlight domestic and international efforts to prevent violent extremists from radicalizing, recruiting, or inspiring individuals or groups in the United States and abroad to commit acts of violence. Foreign leaders from over 65 countries, senior officials from the UN and regional organizations, and private and civil society representatives convened at the Department of State to discuss a broad range of challenges facing nations working to prevent and counter violent extremism.[48]

At the Summit, President Obama asked participants to focus on how to empower communities to protect their families, friends, and neighbors from violent ideologies and recruitment. He suggested the following specific areas for international cooperation on CVE:

- First, we must remain unwavering in our fight against terrorist organizations and continue our mission to degrade and ultimately destroy ISIL.
- Second, we have to confront the warped ideologies espoused by terrorists like al-Qaeda and ISIL, especially their attempt to use Islam to justify their violence.
- Third, we must address the grievances that terrorists exploit, including economic grievances.
- Fourth, we have to address the political grievances that terrorists exploit and protect human rights.[49]

Continuing the work of the February 2015 CVE Summit, President Obama convened another summit on September 29, 2015 at the UN General Assembly, highlighting the international community's efforts to counter ISIL, address FTFs, and CVE. The president made it clear that ISIL poses a threat to the United States and the international community, and that we will use all instruments of power to defeat it. He has also emphasized that this fight will not be won quickly, or solely through military means. This is a long-term struggle that will be won with a comprehensive approach in concert with state and nongovernmental actors across the globe—which is exactly what we are doing.

The Summit showcased some new CVE initiatives like the Strong Cities Network to support the development of effective rights-based community focused programs and training to build resilience against violent extremism; the Global Youth Summit to Counter Violent Extremism that brought together more than 80 global youth leaders and organizations from more than 45 countries to build support for innovative youth-led initiatives; and the Peer-to-Peer Global University Challenge.[50]

The Peer-to-Peer Global University Challenge is a program within the State Department geared towards millennials to counter extremism among their peers and in their communities around the world. The objective is to design and implement a social or digital initiative, product, or tool to motivate and empower their peers to join the movement in CVE. Teams of students at 23 universities in the United States, Canada, North Africa, the Middle East, Europe, Australia, and Asia started the competition in January 2015. Participants were encouraged to use creative messaging and tactics to best reach their peers such as websites, campus and community events, social campaigns, viral videos, social movements, mobile apps, blogs, and education tool kits.[51]

The top three teams were invited to the U.S. Department of State to present their campaigns in June 2015. "Millennials can speak better to millennials, there's no question about that," State Department Principal Deputy Assistant Secretary Kelly Keiderling said, who was a judge in the competition. Missouri State University (Springfield, Missouri, U.S.) won the competition with their campaign, One95, a virtual collaboration platform targeting middle school students with a social media component, curriculum for teachers, and created the hashtag #EndViolentExtremism. Curtin University (Perth, Australia) took second place with their mobile application, 52Jumaa, that sends daily positive affirmations about Islam to users' smartphones, allows them to connect with other Muslims and asks them to complete a selfless act of kindness every Friday, the day of prayer. Mount Royal University (Calgary, Alberta, Canada) launched a prevention campaign called the WANT Movement ("We Are Not Them"). The team hosted a series of workshops and seminars that taught the differences between the Islamic faith and the belief systems embraced by terrorist organizations, and won third place.[52]

Reorganization of U.S. CVE Efforts

On January 8, 2016, the Obama Administration announced it was revamping its CVE efforts. It would establish a new counterterrorism task force, based at the DHS, to

coordinate the government's domestic counter-radicalization efforts and serve as a conduit for ideas, grants, and other resources to community groups across the country. The task force will be led by George Selim, a Homeland Security official, who previously served at the White House as director for Community Partnerships, where he was in regular contact with local law enforcement agencies and Muslim communities. U.S. officials said that the new unit will be made up of representatives from at least 11 departments or agencies and that its mission will involve using data to find better ways to combat radicalization, as well as funding and supporting intervention efforts.[53]

In addition, the State Department is refocusing its CVE communications efforts through a new Global Engagement Center. This center will more effectively coordinate, integrate, and synchronize messaging to foreign audiences that undermines the disinformation espoused by violent extremist groups, including ISIL and al-Qaeda, and that offers positive alternatives. The Center will focus more on empowering and enabling partners, governmental and nongovernmental, who are able to speak out against these groups and provide an alternative to ISIL's nihilistic vision. To that end, the Center will offer services ranging from planning thematic social media campaigns to providing factual information that counters disinformation, to building capacity for third-parties to effectively utilize social media, to research and evaluation.

According to the State Department, the Global Engagement Center will employ a strategy defined by:

- Drawing upon data and metrics to develop, test, and evaluate themes, messages, and messengers;
- Building narratives around thematic campaigns on the misdeeds of our enemy (e.g., poor governance, abuse of women, narratives of defectors), not the daily news cycle;
- Focusing on driving third-party content, in addition to our own; and
- Nurturing and empowering a global network of positive messengers.

The Center will implement its strategy by:

- Seeking out and engaging the best talent, within the technology sector, government and beyond;
- Engaging across our government to coordinate, integrate, and synchronize counterterrorism communications directed toward foreign audiences;
- Identifying and enabling international partners with credibility and expertise;
- Establishing and implementing a campaign-focused culture;
- Scaling up data science and analytics and using both throughout the design, implementation and evaluation phases of these campaigns;
- Providing seed funding and other support to NGOs and media startups focused on CVE messaging;

- Identifying gaps in U.S. government messaging and counter-messaging capabilities directed toward foreign audiences, and recommending steps to resolve them;
- Sharing information and best practices with U.S. government agencies focused on the challenge of HVE; and
- Amplifying the successes of the Counter-ISIL Coalition in defeating ISIL on both the military and information battlefield.

The Center will continue to be housed within the Department of State and staffed by experts from the private sector and U.S. government agencies charged with protecting our national interests and security—as well as the security of our allies—against the threat of international terrorism.[54]

These new initiatives based at the Departments of Homeland Security and State are aimed at disrupting recruitment and radicalization efforts by terrorist groups that increasingly exploit social media platforms and encrypted communications technologies, often developed in the United States but beyond the reach of law enforcement. The Administration hopes this streamlining of CVE efforts at the DHS, complemented by the strategic communications efforts at the State Department will have more impact than other CVE programs to date.

CVE initiatives require close collaboration between the public, private, and civic sectors and cross-border cooperation as well to have real impact. Messaging to CVE must come from civil society rather than the government. Government needs to serve as a more engaged facilitator and enabler to get that messaging out into the respective communities.

Conclusion

The complexity of 21st-century security threats reflects the dark side of globalization that has empowered the convergence of illicit networks like terrorists, criminals, and cyber actors. Governments have been hard-pressed to counter these emerging threats with traditional security strategies and policies. They can no longer go at it alone to ensure our prosperity and security. A whole-of-society approach that employs the vast knowledge and resources of the public, private, and civic sectors is essential to devise innovative responses to address these formidable threats. The examples described above from the cybersecurity, financial services, and CVE arenas illustrate some productive initiatives of communication, cooperation, and collaboration through cross-sector partnerships at the national and international levels.

Governments need to institutionalize more mechanisms for P^3 to address emerging security issues. In addition, they should dedicate funding to support these initiatives and measure their effectiveness. Governments should document and publicize success stories of whole-of-society solutions to national security issues the way the "see something, say something" campaign helped two street vendors alert the police to avert a car bomb attack at New York's Times Square in 2010. Senior leaders across the governments, private

enterprise, and civil society organizations must also advocate and support efforts towards collaborative problem-solving.

Governments should actually go one step further and deputize their citizens as proactive contributors to their national security environment. As those closest to their community or industry know their environment best, they are best suited to contribute as first alerts, if not actual first responders, in the face of an emerging threat, whether it be criminal, terrorist, cyber, or critical infrastructure in nature. Governments need to make it easy for citizens to report security anomalies and share information effectively without compromising their privacy. Educating and sensitizing our citizenry to emerging security threats in the 21st century should be a basic element of government outreach programs. Communicating, cooperating, and collaborating (C^3) by promoting public-private partnerships (P^3) is just good public policy to enhance our national security at home and abroad.

Notes

[1] Elizabeth Palermo, "The 10 Worst Data Breeches of All Time," *Tom's Guide*, February 6, 2015, available at <http://www.tomsguide.com/us/biggest-data-breaches,news-19083.html>.

[2] Ryan Faughnder, "Sony says studio hack cost it $15 million in fiscal third quarter," *Los Angeles Times*, February 4, 2015, available at <http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-hack-cost-20150204-story.html>.

[3] "Global State of Information Security® 2015 Survey," *PwC*, available at <http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/key-findings.html>.

[4] For more details, see Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), "Cyber Threat Source Descriptions," *Department of Homeland Security*, available at <https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions>.

[5] "Cybersecurity," *White House*, available at <https://www.whitehouse.gov/issues/foreign-policy/cybersecurity>.

[6] Ibid.

[7] Office of the Press Secretary, "FACT SHEET: Administration Cybersecurity Efforts 2015," press release, July 9, 2015, available at <https://www.whitehouse.gov/the-press-office/2015/07/09/fact-sheet-administration-cybersecurity-efforts-2015>.

[8] "Executive Order 13636: Cybersecurity Framework," *NIST Cybersecurity Framework*, available at <http://www.nist.gov/cyberframework/>.

[9] Suzanne Spaulding, "DHS Launches the C³ Voluntary Program, A Public-Private Partnership to Strengthen Critical Infrastructure Cybersecurity," *Department of Homeland Security*, February 12, 2014, available at <http://www.dhs.gov/blog/2014/02/12/dhs-launches-c%C2%B3-voluntary-program>.

[10] Ibid.

[11] U.S. Government Accountability Office, *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics*, GAO-07-39 (Washington, DC: U.S. Government Accountability Office, October 16, 2006), available at <http://www.gao.gov/products/GAO-07-39>.

[12] Secretary of Homeland Security Jeh Johnson, "Jeh Johnson on U.S. Cybersecurity Readiness" (remarks at the Council on Foreign Relations, Washington, DC, November 4, 2015), available at <http://www.cfr.org/homeland-security/jeh-johnson-us-cybersecurity-readiness/p37196>.

[13] Rachel King, "Obama Signs Info Sharing Executive Order, But Concerns Remain," *Wall Street Journal* CIO Report, February 13, 2015, available at <http://blogs.wsj.com/cio/2015/02/13/obama-signs-info-sharing-executive-order-but-concerns-remain/>.

[14] Office of the Press Secretary, "FACT SHEET: Administration Cybersecurity Efforts 2015."

[15] King, "Obama Signs Info Sharing Executive Order."

[16] Office of the Press Secretary, "FACT SHEET: Executive Order Promoting Private Sector Cybersecurity Information Sharing," press release, February 12, 2015, available at <https://www.whitehouse.gov/the-press-office/2015/02/12/fact-sheet-executive-order-promoting-private-sector-cybersecurity-inform>.

[17] Office of the Press Secretary, "FACT SHEET: Administration Cybersecurity Efforts 2015."

[18] The White House, "International Strategy for Cyberspace," *White House*, available at <https://www.whitehouse.gov/sites/default/files/rss_viewer/International_Strategy_Cyberspace_Factsheet.pdf>.

[19] Julie Hirschfeld Davis and David E. Sanger, "Obama and Xi Jinping of China Agree to Steps on Cybertheft," *New York Times*, September 25, 2015, available at <http://www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html?_r=0>.

[20] Andrea Shalal, "Top U.S. Spy Says Skeptical sbout U.S.-China Cyber Agreement," *Reuters*, September 30, 2015, available at <http://www.reuters.com/article/2015/09/30/us-usa-cybersecurity-idUSKCN0RT1Q820150930>.

[21] Ambassador Makita Shimokawa, Japanese Foreign Ministry Deputy Director of UN Affairs and Cyber Policy, "Global Approaches to Cybersecurity" (remarks at the Council on Foreign Relations, Washington, DC, November 4, 2015).

[22] National Commission on Terrorist Attacks Upon the United States, *9/11 Commission Report*, 2005, available at <http://www.9-11commission.gov/report/>.

[23] "Bank Secrecy Act," *FinCEN*, available at <http://www.fincen.gov/statutes_regs/bsa/>.

[24] "Threat Finance and Financial Intelligence," American Security Project, available at <http://www.americansecurityproject.org/asymmetric-operations/threat-finance-and-financial-intelligence/>.

[25] "What is ACAMS?" ACAMS, available at <http://www.acams.org/join-acams/#tabbed-nav=what-is-acams>.

[26] "About FS-ISAC," *Financial Services Information Sharing and Analysis Center*, available at <https://www.fsisac.com/about>.

[27] Ibid.

[28] "Who we are," *FATF*, available at <http://www.fatf-gafi.org/about/>.

[29] FATF, *Public and private sector partnership in fighting financial crime: The FATF Recommendation* (Paris: FATF, February 2012), available at <http://www.fatf-gafi.org/documents/documents/publicandprivatesectorpartnershipinfightingfinancialcrime.html>.

[30] FATF President, "G8 Public-Private Sector Dialogue on anti-money laundering and countering the financing of terrorism (AML/CFT)," *FATF*, available at <http://www.fatf-gafi.org/publications/fatfgeneral/documents/ppsdsept13.html>.

[31] Julian Hattem, "FBI: More than 200 Americans have tried to fight for ISIS," *The Hill*, July 8, 2015, available at <http://thehill.com/policy/national-security/247256-more-than-200-americans-tried-to-fight-for-isis-fbi-says>.

[32] Adam Goldman, Jia Lynn Yang, and John Muyskens, "The Islamic State's suspected inroads into America," *Washington Post*, September 8, 2015, available at <http://www.washingtonpost.com/graphics/national/isis-suspects/>.

[33] FBI News Blog, "Director Briefs Senate Committee on Current Threats to the Homeland," *FBI*, October 8, 2015, available at <https://www.fbi.gov/news/news_blog>.

[34] Pete Williams, "FBI: Dozens in U.S. in Secret Conversations With ISIS," *NBC News*, October 8, 2015, available at <http://www.nbcnews.com/storyline/isis-terror/fbi-dozens-u-s-secret-conversations-isis-n440946>.

[35] House Committee on Homeland Security, "Final Report of the Task Force on Combating Terrorist and Foreign Fighter Travel," September 29, 2015, available at <https://homeland.house.gov/wp-content/uploads/2015/09/FINAL_2pager1.pdf>.

[36] Homeland Security Committee Press Release, "Committee Unveils Foreign Fighter Task Force's Final Report," press release, *Homeland Security Committee*, September 29, 2015, available at <https://homeland.house.gov/press/committee-unveils-foreign-fighter-task-forces-final-report/>.

[37] Kevin Johnson, "Comey: Feds Have Roughly 900 Domestic Probes About Islamic State Operatives, Other Extremists," *USA Today*, October 23, 2015, available at <http://www.usatoday.com/story/news/politics/2015/10/23/fbi-comey-isil-domestic-probes/74455460/>.

[38] "Everything we know about the San Bernardino terror attack investigation so far," *LA Times*, December 14, 2015, available at <http://www.latimes.com/local/california/la-me-san-bernardino-shooting-terror-investigation-htmlstory.html>.

[39] Office of the Press Secretary, "FACT SHEET: The White House Summit on Countering Violent Extremism," press release, February 18, 2015, available at <https://www.whitehouse.gov/the-press-office/2015/02/18/fact-sheet-white-house-summit-countering-violent-extremism>.

[40] The White House, *Empowering Local Partners to Prevent Violent Extremism in the United States* (Washington, DC: White House, August 2011), available at <https://www.whitehouse.gov/sites/default/files/empowering_local_partners.pdf>.

[41] "Countering Violent Extremism," *Department of Homeland Security*, available at <http://www.dhs.gov/topic/countering-violent-extremism>.

[42] Ibid.

[43] "DHS' Approach to Countering Violent Extremism," *Department of Homeland Security*, available at <http://www.dhs.gov/dhss-approach-countering-violent-extremism>.

[44] Ibid.

[45] "Global Engagement Center," *U.S. Department of State*, available at <http://www.state.gov/r/cscc/>.

[46] Office of the Press Secretary, "FACT SHEET: Leaders' Summit to Counter ISIL and Violent Extremism," press release, September 29, 2015, available at <https://www.whitehouse.gov/the-press-office/2015/09/29/fact-sheet-leaders-summit-counter-isil-and-violent-extremism>.

[47] Greg Miller and Scott Hingham, "In a propaganda war against ISIS, the U.S. tried to play by the enemy's rules," *Washington Post*, May 8, 2015, available at <https://www.washingtonpost.com/world/national-security/in-a-propaganda-war-us-tried-to-play-by-the-enemys-rules/2015/05/08/6eb6b732-e52f-11e4-81ea-0649268f729e_story.html>.

[48] "Countering Violent Extremism," *U.S. Department of State*, available at <http://www.state.gov/j/cve/>.

[49] Office of the Press Secretary, "Remarks by the President at the Summit on Countering Violent Extremism," *White House*, February 19, 2015, available at <https://www.whitehouse.gov/the-press-office/2015/02/19/remarks-president-summit-countering-violent-extremism-february-19-2015>.

[50] Office of the Press Secretary, "FACT SHEET: Leaders' Summit to Counter ISIL and Violent Extremism."

[51] EdVenture Partners, "Peer 2 Peer: Challenging Extremism," *evp*, available at <http://edventurepartners.com/peer-to-peer/>.

[52] Alyssa Bereznek, "Marketing the anti-extremism message to millennials," *Yahoo News*, June 24, 2015, available at <https://www.yahoo.com/politics/marketing-the-anti-extremism-message-to-122267261971.html>.

[53] Greg Miller and Karen de Young, "Obama administration plans shake-up in propaganda war against ISIS," *Washington Post*, January 8, 2016, available at <https://www.washingtonpost.com/world/national-security/obama-administration-plans-shake-up-in-propaganda-war-against-the-islamic-state/2016/01/08/d482255c-b585-11e5-a842-0feb51d1d124_story.html>.

[54] Office of the Spokesperson, "A New Center for Global Engagement," press release, *U.S. Department of State*, January 8, 2016, available at <http://www.state.gov/r/pa/prs/ps/2016/01/251066.htm>.